UNIT – 1

INTRODUCTION OF NETWORKS

Unit-01/Lecture-01

Introduction & Definition[RGPV/Dec 2010/ Jun 2014]

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

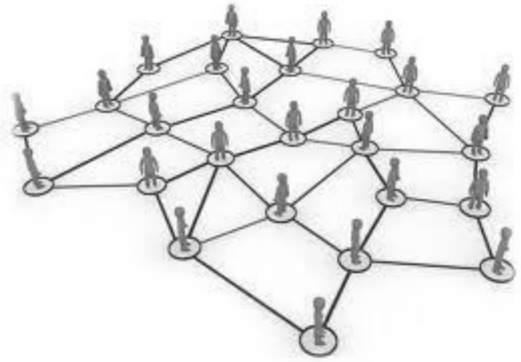


FIGURE 1.1: NETWORK

Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Performance

Performance can be measured in many ways, including transit time and response time.

Transit time is the amount of time required for a message to travel from one device to another.

Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Performance is often evaluated by two networking metrics: **throughput** and **delay.**

We often need more throughput and less delay. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Reliability

In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security

Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Need and advantages of computer network [RGPV/Dec 2010]

You have undoubtedly heard the “the whole is greater than the sum of its parts”. This phrase describes networking very well, and explains why it has become so popular. A network isn't just a bunch of computers with wires running between them. Properly implemented, a network is a system that provides its users with unique capabilities, above and beyond what the individual machines and their software applications can provide.

Most of the benefits of networking can be divided into two generic categories: **connectivity** and **sharing**.
Networks allow computers, and hence their users, to be connected together. They also allow for the easy sharing of information and resources, and cooperation between the devices in other ways. Since modern business depends so much on the intelligent flow and management of information, this tells you a lot about why networking is so valuable.

Here are some of the specific advantages generally associated with networking:

- **Connectivity and Communication** Networks connect computers and the users of those computers. Individuals within a building or work group can be connected into local area networks (LANs); LANs in distant locations can be interconnected into larger wide area networks (WANs). Once connected, it is possible for network users to communicate with each other using technologies such as electronic mail. This makes the transmission of business (or non-business) information easier, more efficient and less expensive than it would be without the network.

- **Data Sharing** One of the most important uses of networking is to allow the sharing of data. Before networking was common, an accounting employee who wanted to prepare a report for her manager would have to produce it on his PC, put it on a floppy disk, and then walk it over to the manager, who would transfer the data to her PC's hard disk. True networking allows thousands of employees to share data much more easily and quickly than this. More so, it makes possible applications that rely on the ability of many people to access and share the same data, such as databases, group software development, and much more. Intranets and extranets can be used to distribute corporate information between sites and to business partners.

- **Hardware Sharing** Networks facilitate the sharing of hardware devices. For example, instead of giving each of 10 employees in a department an expensive color printer one printer can be placed on the network for everyone to share.

- **Internet Access** The Internet is itself an enormous network, so whenever you access the Internet, you are using a network. The significance of the Internet on modern society is hard to exaggerate, especially for those of us in technical fields.

- **Internet Access Sharing** Small computer networks allow multiple users to share a single Internet connection. Special hardware devices allow the bandwidth of the connection to be easily allocated to various individuals as they need it, and permit an organization to purchase one high-speed connection instead of many slower ones.

- **Data Security and Management** In a business environment, a network allows the administrators too much better manage the company's critical data. Instead of having this data spread over dozens or even hundreds of small computers in a haphazard fashion as their users create it; data can be centralized on shared servers. This makes it easy for everyone to find the data, makes it possible for the administrators to ensure that the data is regularly backed up, and also allows for the implementation of security measures to control who can read or change various pieces of critical information.

- **Performance Enhancement and Balancing** Under some circumstances, a network can be used to enhance the overall performance of some applications by distributing the computation tasks to various computers on the network.

- **Entertainment** Networks facilitate many types of games and entertainment. The

Internet itself offers many sources of entertainment, of course. In addition, many multi-player games exist that operate over a local area network. Many home networks are set up for this reason, and gaming across wide area networks (including the Internet) has also become quite popular.

Physical Structures

Type of Connection[RGPV/ Dec 2013/ Jun 2014]

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time.

There are two possible types of connections: **point-to-point** and **multipoint**.

- **Point-to-Point** A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

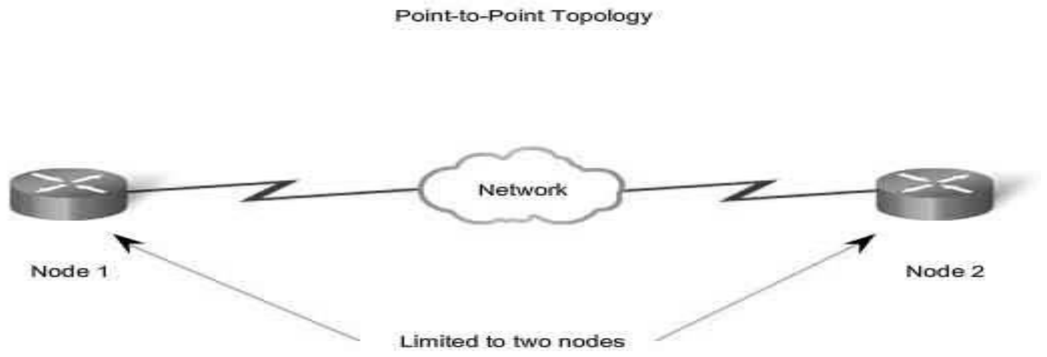


FIGURE 1.2: POINT TO POINT CONNECTION

- **Multipoint** A multipoint connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

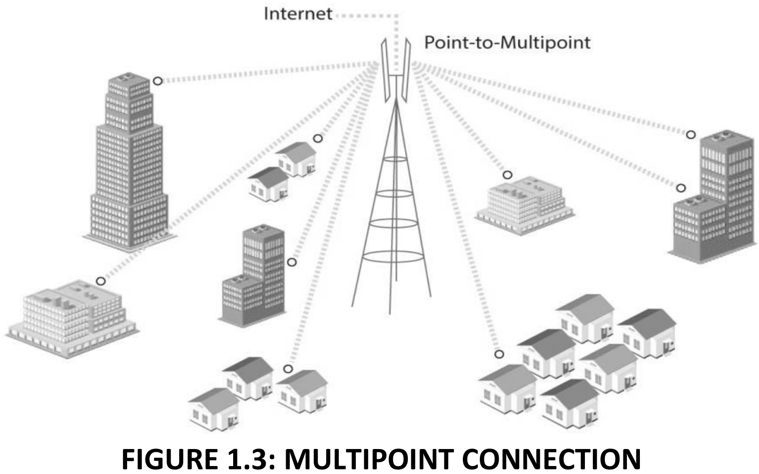


FIGURE 1.3: MULTIPOINT CONNECTION

Physical Topology[RGPV/Jun 2009, Jun 2013]

The term physical topology refers to the way in which a network is laid out physically: 1 or more devices connect to a link; two or more links form a topology.

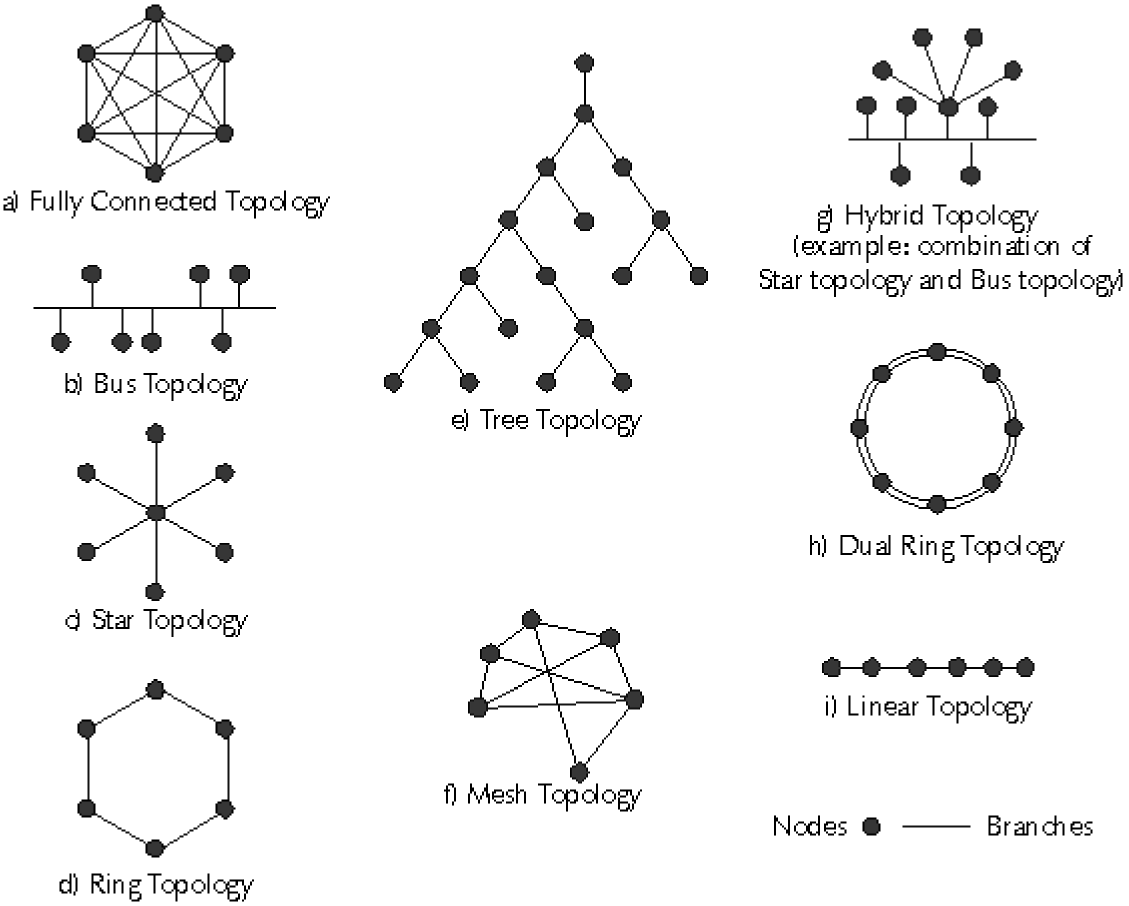


FIGURE 1.4: TOPOLOGY

- **Mesh** In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n - I nodes, node 2 must be connected to n – 1 nodes, and finally node n must be connected to n - 1 nodes. We need n (n - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need **N (n -1) /2** duplex-mode links.

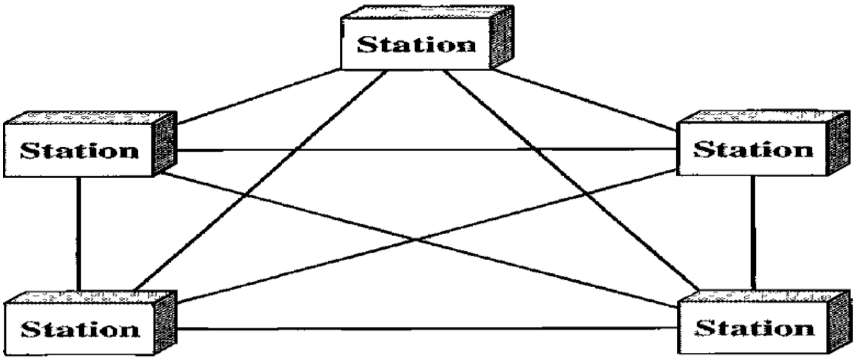


FIGURE 1.5: MESH TOPOLOGY

To accommodate that many links, every device on the network must have n – 1 input/output (VO) ports to be connected to the other n - 1 station. A mesh offers several advantages over other network topologies. First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices. Second, a mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system. Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages. Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution. The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required. First, because every device must be connected to every other device, installation and reconnection are difficult. Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

- **Star** A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
  Other advantages include robustness. If one link fails, only that link is affected. All other links remain active.

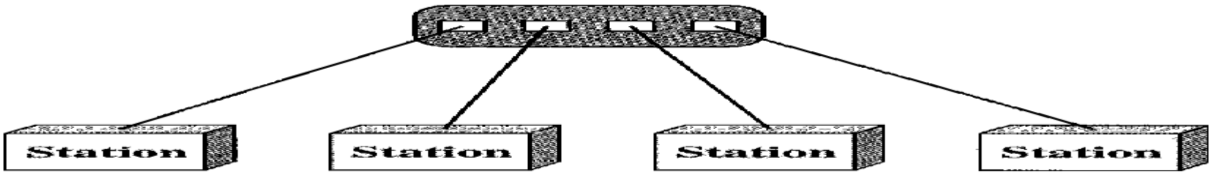


FIGURE 1.6: STAR TOPOLOGY

- **Hub** the hub is working, it can be used to monitor link problems and bypass defective links. One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
  Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).
  The star topology is used in local-area networks (LANs), High-speed LANs often use a star topology with a central hub.

- **Bus** The preceding examples all describe point-to-point connections. A **bus topology,** on the other hand, is multipoint. One long cable acts as a **backbone** to link all the devices in a network
  Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.
  Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, and then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.
  Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new

devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.

In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

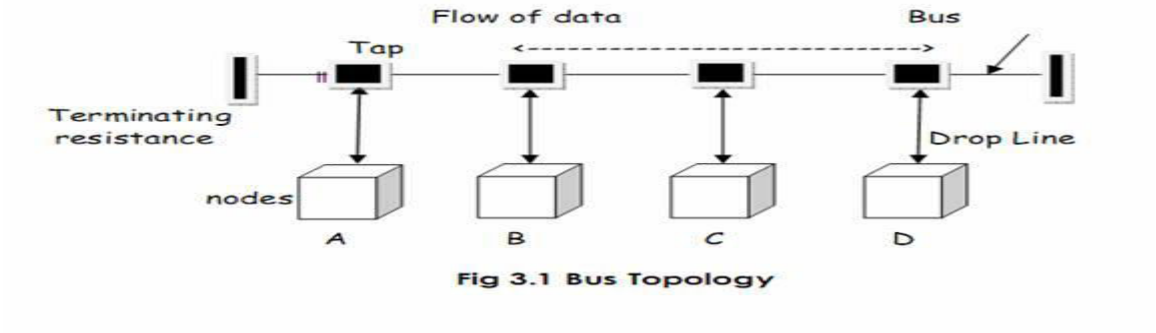


FIGURE 1.7: BUS TOPOLOGY

- **Ring** In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along

  A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbours (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location. However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

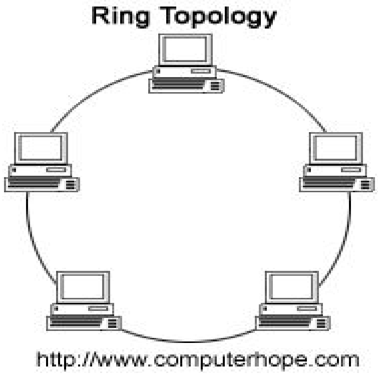


FIGURE 1.8: STAR TOPOLOGY

- **Hybrid** A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology.

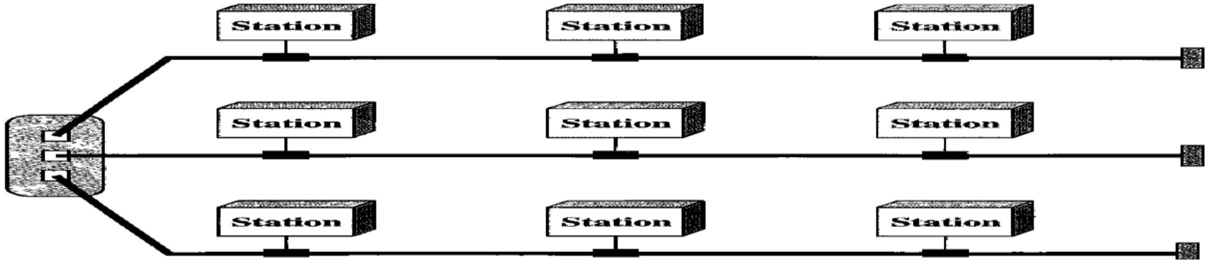


FIGURE 1.9: HYBRID TOPOLOGY

Categories of Networks [RGPV/Dec 2009, Jun 2013]

There are three primary categories:

- **Local area network(LAN)**
- **Metropolitan area network (MAN)**
- **Wide area network(WAN)**

The category into which a network falls is determined by its size. A LAN normally covers an area less than 200 m; a WAN can be worldwide. Networks of a size in between are normally referred to as metropolitan area.

- **Local Area Network** A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometres.

  LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data.

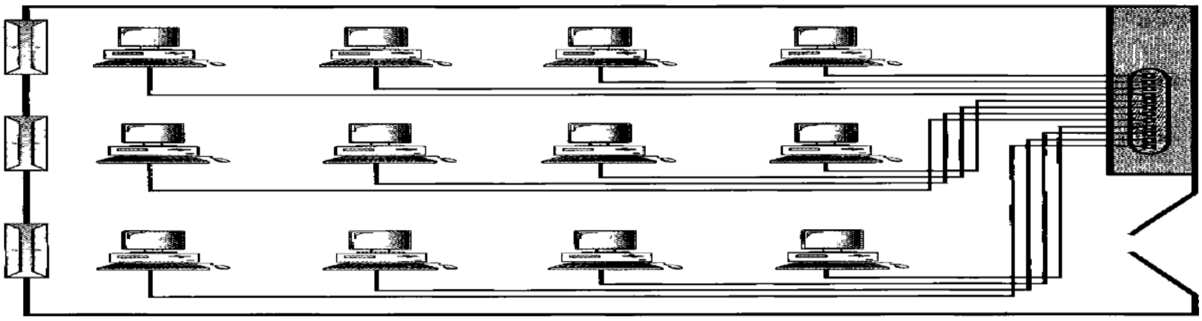


FIGURE 1.10: LOCAL AREA NETWORK (LAN)

A common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engineering workstations or accounting PCs. One of the computers may be given a large capacity disk drive and may become a server to clients. Software can be stored on this central server and used as needed by the whole group. In this example, the size of the LAN may be determined by licensing restrictions on the number of users per copy of software, or by restrictions on the number of users licensed to access the operating system.

In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps

- **Wide Area Network** A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet.

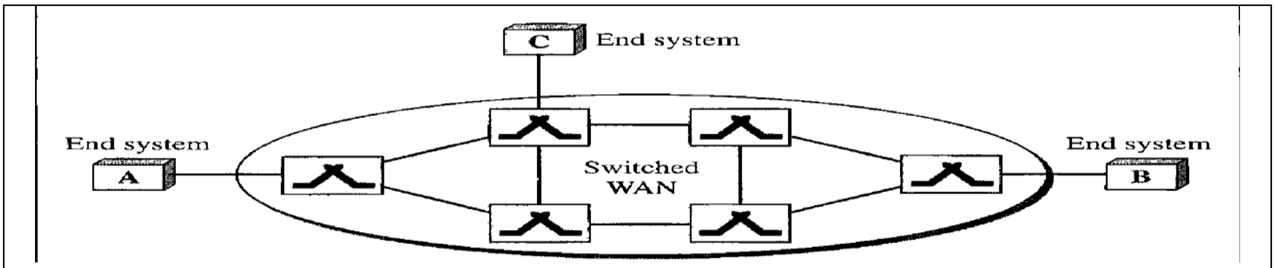


FIGURE 1.11: WIDE AREA NETWORK (WAN)

The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP).

- **Metropolitan Area Networks** A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer. Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet.

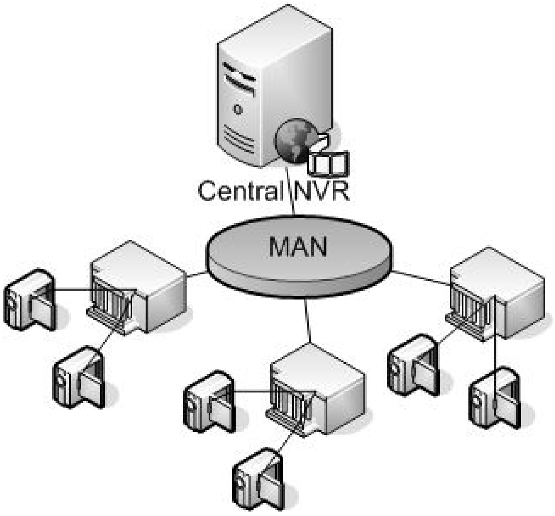


FIGURE 1.12: MAN AREA NETWORK (MAN)

Interconnection of Networks: Internetwork

When two or more networks are connected, they become an internetwork, or internet.

As an example, assume that an organization has two offices, one on the east coast and the other on the west coast. The established office on the west coast has a bus topology LAN; the newly opened office on the east coast has a star topology LAN. The president of the company lives somewhere in the middle and needs to have control over the company from her home. To create a backbone WAN for connecting these three entities (two LANs and the president's computer), a switched WAN (operated by a service provider such as a telecom company) has been leased. To connect the LANs to this switched WAN, however, three point-to-point WANs are required. These point-to-point WANs can be a high-speed DSL line offered by a telephone company or a cable modern line offered by a cable TV provider.

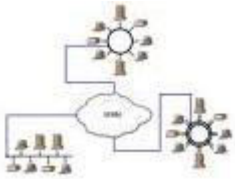


FIGURE 1.13: INTERNETWORK

Applications

In a short period of time computer networks have become an indispensable part of business, industry, entertainment as well as a common-man's life. These applications have changed tremendously from time and the motivation for building these networks are all essentially economic and technological.

Initially, computer network was developed for defense purpose, to have a secure communication network that can even withstand a nuclear attack. After a decade or so, companies, in various fields, started using computer networks for keeping track of inventories, monitor productivity, communication between their different branch offices located at different locations. For example, Railways started using computer networks by connecting their nationwide reservation counters to provide the facility of reservation and enquiry from anywhere across the country.

And now after almost two decades, computer networks have entered a new dimension; they are now an integral part of the society and people. In 1990s, computer network started delivering services to private individuals at home. These services and motivation for using them are quite different. Some of the services are access to remote information, person-person communication, and interactive entertainment. So, some of the applications of computer networks that we can see around us today are as follows:

- **Marketing and sales** Computer networks are used extensively in both marketing and sales organizations. Marketing professionals use them to collect, exchange, and analyze data related to customer needs and product development cycles. Sales application includes teleshopping, which uses order-entry computers or telephones connected to order processing network, and online-reservation services for hotels, airlines and so on.

- **Financial services** Today's financial services are totally depended on computer networks. Application includes credit history searches, foreign exchange and investment services, and electronic fund transfer, which allow user to transfer money without going into a bank (an automated teller machine is an example of electronic fund transfer, automatic pay-check is another).

- **Manufacturing**: Computer networks are used in many aspects of manufacturing including manufacturing process itself. Two of them that use network to provide essential services are computer-aided design (CAD) and computer-assisted manufacturing (CAM), both of which allow multiple users to work on a project simultaneously.

- **Directory services**: Directory services allow list of files to be stored in central location to speed worldwide search operations.

- **Information services**: A Network information service includes bulletin boards and data banks. A World Wide Web site offering technical specification for a new product is an information service.

- **Electronic data interchange (EDI)**: EDI allows business information, including documents such as purchase orders and invoices, to be transferred without using paper.

- **Electronic mail**: probably it's the most widely used computer network application.

- **Teleconferencing**: Teleconferencing allows conference to occur without the participants being in the same place. Applications include simple text conferencing (where participants communicate through their normal keyboards and monitor) and video conferencing where participants can even see as well as talk to other fellow participants. Different types of equipments are used for video conferencing depending on what quality of the motion you want to capture (whether you want just to see the face of other fellow participants or do you want to see the exact facial expression).

- **Voice over IP**: Computer networks are also used to provide voice communication. This kind of voice communication is pretty cheap as compared to the normal telephonic conversation.

- **Video on demand**: Future services provided by the cable television networks may include video on request where a person can request for a particular movie or any clip at anytime he wish to see.

Summary: The main area of applications can be broadly classified into following categories:

- **Scientific and Technical Computing :** Client Server Model, Distributed Processing , Parallel Processing, Communication Media

- **Commercial:** Advertisement, Telemarketing, Teleconferencing, Worldwide Financial Services

- **Network for the People** (this is the most widely used application nowadays) , Telemedicine, Distance Education, Access to Remote Information, Person-to-Person Communication, Interactive Entertainment

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	What are various network topologies? Explain with example.	Jun 2009	7
Q.2	Give the proper definition of “computer network”? What are the various network topologies? List the factors that affect the choice of a topology and transmission medium in a LAN.	Dec 2010	7
Q.3	What are some of the factors that determine whether a communication system is a LAN, WAN or MAN? Explain each of them in detail.	Dec 2009	7
Q.4	The original three network types were LAN, WAN, MAN. Describe how they differ from one another.	Jun 2013	5
Q.5	What are the advantages of multipoint connection over a point to point connection?	Dec 2013	7
Q.6	Explain different topologies used in designing networks.	Jun 2013	7
Q.7	Explain the use of computer networks and give their general classifications.	Jun 2014	7
Q.8	Give comparison between the following: (i) Broadcast and point to point networks. (ii) Client –server and peer-peer networks	Jun 2014	3 4

THE OSI MODEL

THE OSI MODEL[RGPV/Jun 2008, Jun 2009, Dec 2010, Jun 2013, Dec 2013, Jun 2014]

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

ISO is the organization. OSI is the model.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network. An understanding of the fundamentals of the OSI model provides a solid basis for exploring data communications.

The OSI model is composed of seven ordered layers:

1 physical (layer 1)
2 data link (layer 2)
3 network (layer 3)
4 transport (layer 4)
5 session (layer 5)
6 presentation (layer 6)
7 application (layer 7)

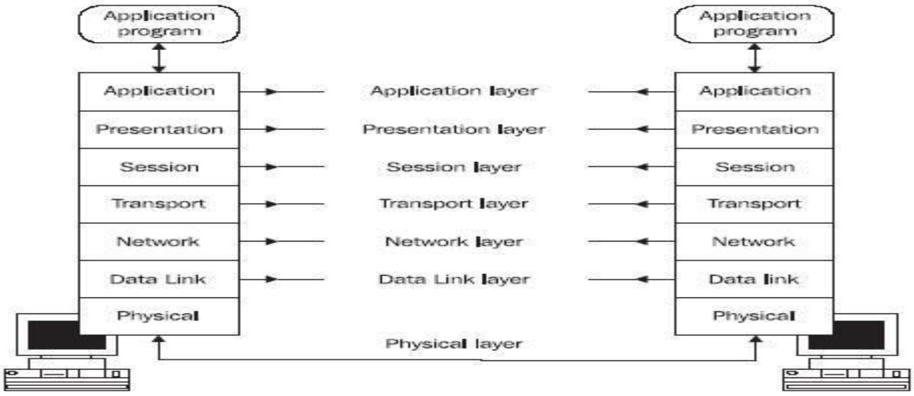


FIGURE 1.14: ISO- OSI MODEL

The layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.

In developing the model, the designers distilled the process of transmitting data to its most fundamental elements. They identified which networking functions had related uses and collected those functions into discrete groups that became the layers. Each layer defines a family of functions distinct from those of the other layers. By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible. Most importantly, the OSI model allows complete interoperability between otherwise incompatible systems.

Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer x on one machine communicates with layer x on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols. The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

Peer-to-Peer Processes

At the physical layer, communication is direct: device A sends a stream of bits to device B (through intermediate nodes). At the higher layers, however, communication must move down through the layers on device A, over to device B.

Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.

At layer I the entire package is converted to a form that can be transmitted to the receiving device. At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it. For example, layer 2 removes the data meant for it, and then passes the rest to layer 3. Layer 3 then removes the data meant for it and passes the rest to layer 4, and so on.

The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers. Each interface defines the information and services a layer must provide for the layer above it. Well-defined interfaces and layer functions provide modularity to a network. As long as a layer provides the expected services to the layer above it, the specific implementation of its functions can be modified or replaced without requiring changes to the surrounding layers.

The seven layers can be thought of as belonging to three subgroups. Layers I, 2, and 3-physical, data link, and network-are the network support layers.

The physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability). Layers 5, 6, and 7-session, presentation, and application-can be thought of as the user support layers; they allow interoperability among unrelated software systems. Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use. The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

Encapsulation

A packet (header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on. In other words, the data portion of a packet at level N - 1 carries the whole packet (data and header and maybe trailer) from level N. The concept is called encapsulation; level N - 1 is not aware of which part of the encapsulated packet is data and which part is the header or trailer. For level N - 1, the whole packet coming from level N is treated as one integral unit.

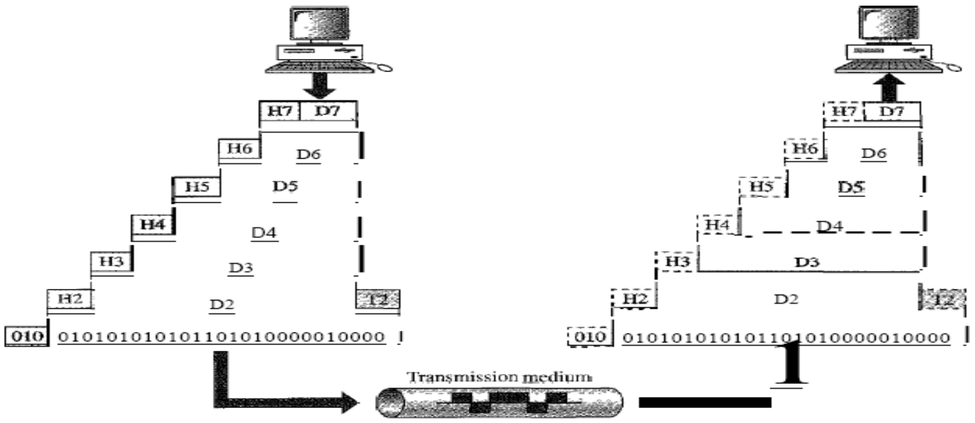


FIGURE 1.15: ISO- OSI MODEL HEADERS & TRAILERS

LAYERS IN THE OSI MODEL

In this section we briefly describe the functions of each layer in the OSI model.

Physical Layer The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur.

Transmission medium The physical layer is responsible for movements of individual bits from one hop (node) to the next.

The physical layer is also concerned with the following:

- **Physical characteristics of interfaces and medium** The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
- **Representation of bits** The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and I s are changed to signals).
- **Data rate** The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
- **Synchronization of bits** The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.
- **Line configuration** The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.
- **Physical topology** The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).
- **Transmission mode** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

Data Link Layer The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). The data link layer is responsible for moving frames from one hop (node) to the next.

Other responsibilities of the data link layer include the following:

- **Framing** The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- **Physical addressing** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
- **Flow control** If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- **Error control** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
- **Access control** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Other responsibilities of the network layer include the following:

- **Logical addressing** The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
- **Routing** When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

The transport layer is responsible for the delivery of a message from one process to another.

Other responsibilities of the transport layer include the following:

- **Service-point addressing** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly** A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
- **Connection control** The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
- **Flow control** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- **Error control** Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.
The session layer is responsible for dialog control and synchronization.

Specific responsibilities of the session layer include the following:

- **Dialog control** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Synchronization** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. The presentation layer is responsible for translation, compression, and encryption.

Specific responsibilities of the presentation layer include the following:

- **Translation** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

- **Encryption** To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- **Compression** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services. The application layer is responsible for providing services to the user.

Specific services provided by the application layer include the following:

- **Network virtual terminal** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
- **File transfer, access, and management(FTAM)** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **Mail services** This application provides the basis for e-mail forwarding and storage.
- **Directory services** This application provides distributed database sources and access for global information about various objects and services.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	OSI stack is now just a historical footnote. Justify.	Jun 2006	7
Q.2	Explain the ISO OSI model by writing two functions of each layer.	Dec 2010	7
Q.3	What do you mean by broadcast network? Discuss the need or lack of need for a network layer (OSI layer 3) in a broadcast network.	Dec.2009	7
Q.4	During the communication, how various layers of OSI model exchange information to establish a connection? Describe with the help of a suitable diagram.	Jun 2013	9
Q.5	Describe the design issues for different layers.	Dec 2013	7
Q.6	Draw ISO-OSI reference model and describe functions associated with each layer.		

TCP/IP PROTOCOL SUITE[RGPV/ Dec 2003, Dec 2012]

The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer.

The TCP/IP protocol suite is made of four layers:

- Physical Layer
- Network Layer
- Transport Layer
- Application Layer

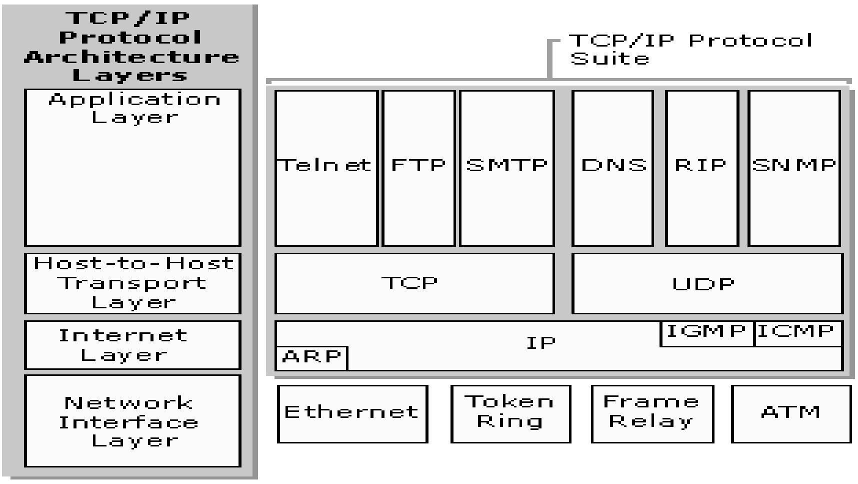


FIGURE 1.16: TCP/IP PROTOCOL SUITE

The first three layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first three layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer

TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent. Whereas the OSI model specifies which functions belong to each of its layers, the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system. The term hierarchical means that each upper-level protocol is supported by one or more lower-level protocols.

At the transport layer, TCP/IP defines three protocols:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Stream Control Transmission Protocol (SCTP)

At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols that support data movement in this layer.

Physical and Data Link Layers

At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

Network Layer

At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol. IP uses five supporting protocols:

- ARP
- RARP
- IP
- ICMP
- IGMP

- **Internetworking Protocol (IP)** The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol-a best-effort delivery service. The term best effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees. IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

- **Address Resolution Protocol** The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known

- **Reverse Address Resolution Protocol** The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

- **Internet Control Message Protocol** The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

- **Internet Group Message Protocol** The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport Layer

Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. Transport Layer uses three supporting protocols:

- UDP
- TCP
- SCTP

- **User Datagram Protocol** The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

- **Transmission Control Protocol** The Transmission Control Protocol (TCP) provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data. At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

- **Stream Control Transmission Protocol** The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

Application Layer

The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model .Many protocols are defined at this layer.

- HTTP
- HTTPS
- FTP
- STFT
- TFTP
- TELNET
- SSH
- NNTP
- LDAP
- NTP
- POP3
- IMAP4
- SMTP
- DNS
- SNMP

- **HTTP** (Hypertext Transfer Protocol) is the protocol that facilitates transfer of data via the “world wide web.” Typically, data is transferred in the form of pages, or HTML markup. HTTP operates on **TCP 80**.
- **HTTPS** (Secure HTTP) uses **TCP 443** to securely transfer HTTP data via SSL, or Secure Socket Layer. Sites that require increased security, such as an online merchant, use HTTPS to protect user information.
- **FTP** (File Transfer Protocol) operates on **TCP ports 20**(data) / **21**(transmission control). It is used in simple file transfers from one node to another without any security (transferred in cleartext).
- **SFTP** (Secure FTP) is a version of FTP that uses SSH to transfer data securely, thus using whichever port SSH uses. **Port 22** for those who can't figure it out.
- **TFTP** (Trivial FTP) is a UDP version of FTP that utilizes **UDP port 69**. It is called **“trivial” because it is relatively unreliable** and inefficient and so is more often used for inter-network communication (along routers) than in real node-to-node file transfers.
- **Telnet** (Telecommunications Network) is used to remotely connect to a node. All communications with telnet are in clear text (even the password for authentication) and should not be used in sensitive situations. It is called terminal emulation software because

the remote terminal is available upon connection. Telnet operates on **TCP 23**.

- **SSH (Secure Shell) is a secure replacement of Telnet**. Telnet transfers information in plain or clear text, but SSH allows terminal emulation in cipher text, which equates to enhanced and increased security. SSH operates on **TCP 22**.
- **NNTP** (Network News Transfer Protocol) is a protocol used by client and server software to carry USENET (newsgroup) postings back and forth over a TCP/IP network. NNTP operates on **TCP port 119**.
- **LDAP** (Lightweight Directory Access Protocol) is a **“Directory Services” protocol** that basically allows a server to act as a central directory for client nodes. A famous implementation of LDAP is **Microsoft’s Active Directory** (Domain). LDAP operates on **TCP and UDP 389**.
- **NTP** (Network Time Protocol) allows for synchronizing network time with a server. NTP operates on **UDP 123**.
- **POP3** (Post Office Protocol) is the mailbox protocol of the Internet and allows users to download mail from a mail server. The server will hold onto your mail until you access it. Once you try to access it, your client software will download all of your incoming mail and wipe it from the server. POP3 operates on **TCP 110**.
- **IMAP4** (The Internet Message Access Protocol) IMAP4 allows for server-based repositories of sent mail and other specialized folders. Basically, when using IMAP4 instead of POP3 as your incoming mail protocol, you download very minimal information to your local machine and when you want to access actual incoming mail, you are pulling this directly from the mail server. This allows you to access your mail from virtually anywhere. IMAP4 operates on **TCP 143**.
- **SMTP** (Simple Mail Transfer Protocol) is the **“postman” of the Internet**. It allows for mail to be sent. You would use this in conjunction with POP3 or IMAP4 to be able to send/receive mail. If you do not define SMTP (usually is, though), you will only be able to receive mail. SMTP operates on **TCP 25**.
- **DNS**(Domain Name System) Resolves easy to read domain names such as google.com into computer readable IP addresses such as 72.14.204.147 DNS operates on **UDP 53**
- **SNMP** (Simple Network Management Protocol) A protocol for managing devices on IP networks, such as modems, switches, routers, or printers. Works on **UDP 161**

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Write short note on TCP/IP.	Dec 2003	7
Q.2	Describe the various communication task performed by different layers of TCP/IP model. How it is different from the OSI reference model?	Dec 2012	7

s

Unit-01/Lecture-04

Difference between OSI and TCP/IP reference model

Difference between OSI and TCP/IP reference model[RGPV/Jun 2011, Dec 2012, Dec 2013, Jun 2014]

OSI Reference Model

- It has 7 layers
- Transport layer guarantees delivery of packets
- Horizontal approach
- Separate presentation layer
- Separate session layer
- Network layer provides both connectionless and connection oriented services
- It defines the services, interfaces and protocols very clearly and makes a clear distinction between them
- The protocol is better hidden and can be easily replaced as the technology changes
- OSI truly is a general model
- It has a problem of protocol filtering into a model

TCP/IP Reference Model

- Has 4 layers
- Transport layer does not guarantees delivery of packets
- Vertical approach
- No session layer, characteristics are provided by transport layer
- No presentation layer, characteristics are provided by application layer
- Network layer provides only connection less services
- It does not clearly distinguishes between service interface and protocols
- It is not easy to replace the protocols
- TCP/IP cannot be used for any other application
- The model does not fit any protocol stack.

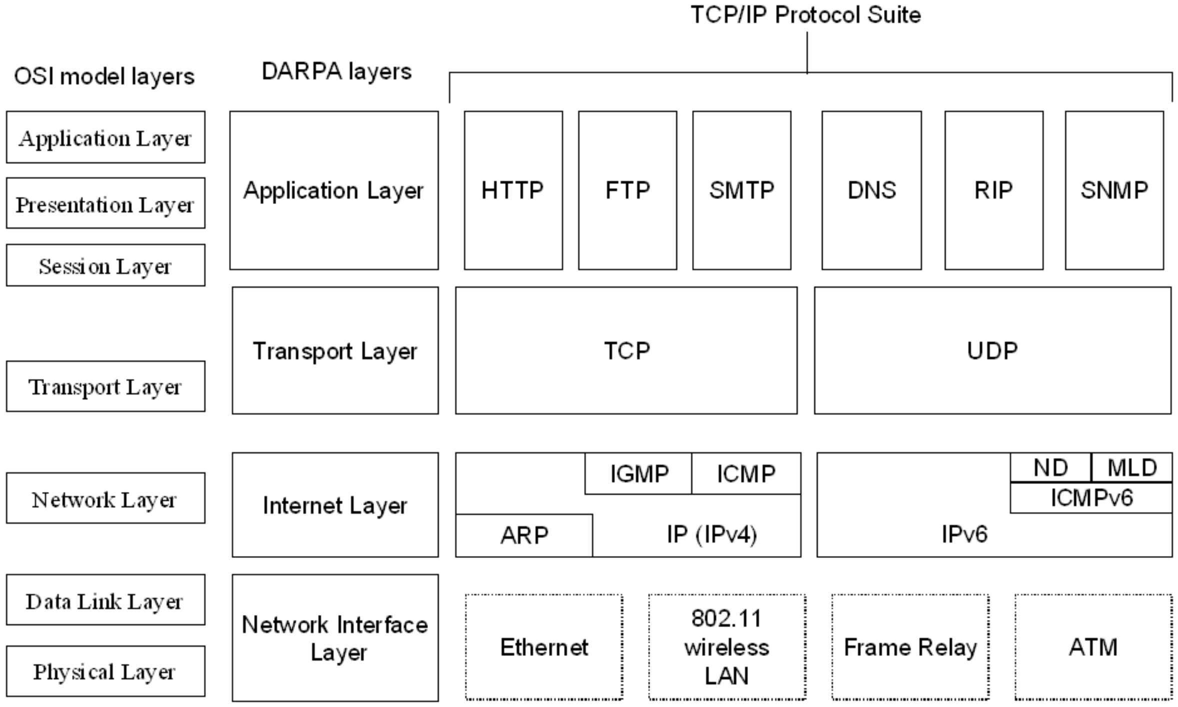


FIGURE 1.17: ISO- OSI MODEL VS. TCP/IP MODEL

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Write comparison between ISO-OSI and TCP/IP reference model.	Jun 2011 Dec 2013	7
Q.2	How TCP/IP model is different from the OSI reference model?	Dec 2012	7
Q.3	Compare ISO-OSI layered model with TCP/IP layered stack in detail naming the relevant protocols of each layers in both.	Jun 2014	7

Unit-01/Lecture-05

Connection-Oriented vs. Connectionless scheme

Connection-Oriented vs. Connectionless scheme[RGPV / Dec 2010,Dec 2011]

From one computer to another, transmitting/receiving data, and then releasing the call, just like a voice phone call. However, the network connecting the computers is a packet switched network, unlike the phone system's circuit switched network. Connection-oriented communication is done in one of two ways over a packet switched network: with and without virtual circuits.

- **Without virtual circuits** This is what TCP does in the Internet. The only two machines in the Internet that are aware a connection is established are the two computers at the endpoints. The Internet itself--its routers and links--have no information about the presence of a connection between the two computers. This means that all of the packets flowing between the two computers can follow different routes. One benefit of establishing the connection is that the flow of packets from the source to the destination can be slowed down if the Internet is congested and speeded up when congestion disappears. Another benefit is that the endpoints can anticipate traffic between them, and agree to cooperate to ensure the integrity and continuity of the data transfers. This allows the network to be treated as a "stream" of data.

- **Virtual circuit** This is not used in the Internet, but is used in other types of networks (eg. the "X.25" protocol). The routers within the network route all packets in one connection over the same route. The advantage is that video and voice traffic are easier to carry, because routers can reserve memory space to buffer the transmission.

Connectionless

Connectionless communication is just packet switching where no call establishment and release occur. A message is broken into packets, and each packet is transferred separately. Moreover, the packets can travel different route to the destination since there is no connection. Connectionless service is typically provided by the **UDP (User Datagram Protocol)**. The packets transferred using UDP are also called datagrams.

Comparison between Connection-oriented and Connectionless Communication

Feature	**Connectionless**	**Connection-oriented**
How is data sent?	one packet at a time	as continuous stream of packets
Do packets follow same route?	no	virtual circuit: yes without virtual circuit: no
Are resources reserved in network?	no	virtual circuit: yes without virtual circuit: no
Are resources reserved in communicating hosts?	no	yes
Can data sent can experience variable latency?	yes	yes
Is connection establishment done?	no	yes

Is state information stored at network nodes?	no	virtual circuit: yes without virtual circuit: no
What is impact of node/switch crash?	only packets at node are lost	all virtual circuits through node fail
What addressing information is needed on each packet?	full source and destination address	virtual circuit: a virtual circuit number without virtual circuit: full source and destination address
Is it possible to adapt sending rate to network congestion?	hard to do	virtual circuit: easy if sufficient buffers allocated without virtual circuit: harder to do

Differentiate between connection oriented and connectionless services

S.No.	Characteristic	Connectionless Service	Connection Oriented Service
1.	Example of Protocol	UDP (User Datagram Protocol)	TCP (Transmission control protocol).
2.	General Description	Simple, high-speed, low functionality "wrapper" that interfaces applications to the network layer.	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
3.	Connection setup	Data is sent without setup i.e. connectionless.	Connection must be established prior transmission.
4.	Data interface to application	Message-based; data is sent in discrete packages by the applications.	Stream-based; data is sent by the application with no particular structure.
5.	Reliability and acknowledgments	Unreliable, best efforts delivery without acknowledgments	Reliable delivery of messages; all data is acknowledged.
6.	Retransmission	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed and lost data is retransmitted automatically.
7.	Feature provide to	None	Flow control using sliding windows; window size

	manage flow of data.		adjustment heuristics congestion avoidance algorithm.
8.	Transmission speed	Very high	Low
9.	Data quantity Suitability	Small to moderate amounts of data.	Small to very large amounts of data

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	What is the difference between connection oriented communication and connectionless communication?	Dec 2011	7

UNIT 1/LECTURE 6

Novell Netware

NetWare is a computer network operating system developed by Novell, Inc. It initially used cooperative multitasking to run various services on a personal computer, with network protocols based on the archetypal Xerox Network Systems stack. Novell was acquired by The Attachmate Group in 2011, and now is a wholly owned subsidiary.

The original NetWare product in 1983 supported clients running both CP/M and MS-DOS, ran over a proprietary star network topology and was based on a Novell-built file server using the Motorola 68000 processor. The company soon moved away from building its own hardware, and NetWare became hardware-independent, running on any suitable Intel-based compatible system, and a wide range of network cards. From the beginning NetWare implemented a number of features inspired by mainframe and minicomputer systems that were not available in its competitors.

In the early 1990s, Novell introduced separate cheaper networking products, unrelated to classic NetWare. These were NetWare Lite 1.0 (NWL) and later Personal NetWare 1.0 (PNW) in 1993.

In 1993 the main product line took a dramatic turn when Version 4 introduced NetWare Directory Services (NDS), a global directory service to which Microsoft's Active Directory, released seven years later, was similar. This, along with a new e-mail system, GroupWise, application configuration suite ZEN works, and security product Border Manager were all targeted at the needs of large enterprises.

By 2000 however, Microsoft was making increasing inroads into Novell's customer base and Novell increasingly looked to a future based on a Linux kernel.

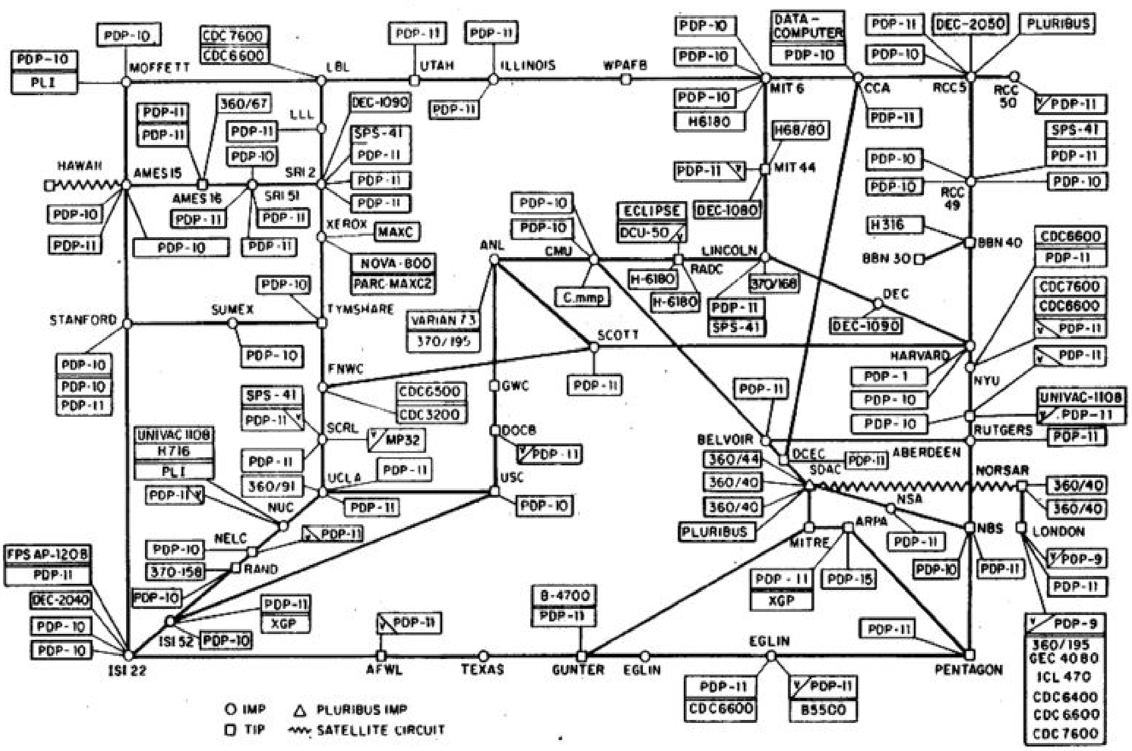
UNIT 1/LECTURE 7

ARPANET

ARPANET[RGPV/Jun 2010,Jun 2011]

The **Advanced Research Projects Agency Network** (**ARPANET**) was one of the world's first operational packet switching networks, the first network to implement TCP/IP, and the progenitor of what was to become the global Internet. The network was initially funded by the Advanced Research Projects Agency (ARPA, later DARPA) within the U.S. Department of Defence for use by its projects at universities and research laboratories in the US. The packet switching of the ARPANET, together with TCP/IP, would form the backbone of how the Internet works. The packet switching was based on concepts and designs by American engineer Paul Baron, Welsh scientist Donald Davies and Lawrence Roberts of the Lincoln Laboratory. The TCP/IP communication protocols were developed for ARPANET by computer scientists Robert Kahn and Vinton Cerf, and also incorporated some designs from Louis Pouzin.

ARPANET LOGICAL MAP, MARCH 1977



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

FIGURE 1.19: ARPANET

UNIT 1/LECTURE 8

X.25

X.25[RGPV/Jun 2011, Jun 2013]

X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication. An X.25 WAN consists of packet-switching exchange (PSE) nodes as the networking hardware, and leased lines, plain old telephone service connections or ISDN connections as physical links. X.25 is a family of protocols that was popular during the 1980s with telecommunications companies and in financial transaction systems such as automated teller machines. X.25 was originally defined by the International Telegraph and Telephone Consultative Committee (CCITT, now ITU-T)

While X.25 has, to a large extent, been replaced by less complex protocols, especially the Internet protocol (IP), the service is still used and available in niche and legacy applications.

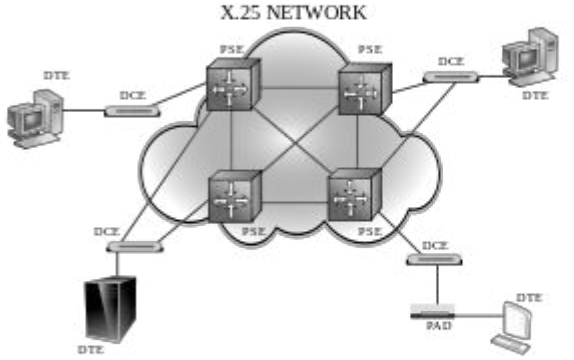


FIGURE 1.19: X.25 NETWORK

Architecture

The general concept of X.25 was to create a universal and global packet-switched network. Much of the X.25 system is a description of the rigorous error correction needed to achieve this, as well as more efficient sharing of capital-intensive physical resources.

The X.25 specification defines only the interface between a subscriber (DTE) and an X.25 network (DCE). X.75, a very similar protocol to X.25, defines the interface between two X.25 networks to allow connections to traverse two or more networks. X.25 does not specify how the network operates internally—many X.25 network implementations used something very similar to X.25 or X.75 internally, but others used quite different protocols internally. The ISO equivalent protocol to X.25, ISO 8208, is compatible with X.25, but additionally includes provision for two X.25 DTEs to be directly connected to each other with no network in between. By separating the Packet-Layer Protocol, ISO 8208 permits operation over additional networks such as ISO 8802 LLC2 (ISO LAN) and the OSI data link layer.[15]

X.25 originally defined three basic protocol levels or architectural layers. In the original specifications these were referred to as levels and also had a level number, whereas all ITU-T X.25 recommendations and ISO 8208 standards released after 1984 refer to them as layers. The layer numbers were dropped to avoid confusion with the OSI Model layers.

- **Physical layer** This layer specifies the physical, electrical, functional and procedural characteristics to control the physical link between a DTE and a DCE. Common implementations use X.21, EIA-232, EIA-449 or other serial protocols.

- **Data link layer** The data link layer consists of the link access procedure for data interchange on the link between a DTE and a DCE. In its implementation, the Link Access Procedure, Balanced (LAPB) is a data link protocol that manages a communication session and controls the packet framing. It is a bit-oriented protocol that provides error correction and orderly delivery.

- **Packet layer** This layer defined a packet-layer protocol for exchanging control and user data packets to form a packet-switching network based on virtual calls, according to the Packet Layer Protocol.

The X.25 model was based on the traditional telephony concept of establishing reliable circuits through a shared network, but using software to create "virtual calls" through the network. These calls interconnect "data terminal equipment" (DTE) providing endpoints to users, which looked like point-to-point connections. Each endpoint can establish many separate virtual calls to different endpoints.

For a brief period, the specification also included a connectionless datagram service, but this was dropped in the next revision. The "fast select with restricted response facility" is intermediate between full call establishment and connectionless communication. It is widely used in query-response transaction applications involving a single request and response limited to 128 bytes of data carried each way. The data is carried in an extended call request packet and the response is carried in an extended field of the call reject packet, with a connection never being fully established.

S.NO	RGPV QUESTION	YEAR	MARKS
Q.1	Explain briefly the X.25.	Jun 2011	7
Q.2	How is X.25 able to eliminate most of the control circuit of the EIA standard?	Jun 2013	7

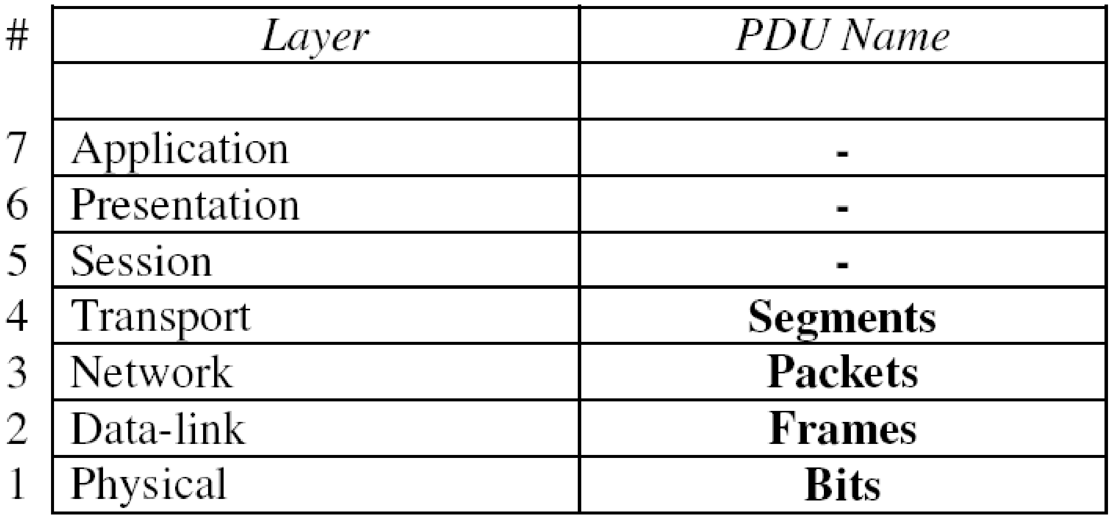
UNIT 1/LECTURE 09

Protocol data unit

Protocol data unit

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:



#	*Layer*	*PDU Name*
7	Application	-
6	Presentation	-
5	Session	-
4	Transport	**Segments**
3	Network	**Packets**
2	Data-link	**Frames**
1	Physical	**Bits**

FIGURE 1.20: PROTOCOL DATA UNIT

Commonly, network devices are identified by the OSI layer they operate at (or, more specifically, what header or PDU the device processes).

Service Primitives [RGPV/Dec 2011]

The OSI Network Layer Service Primitives

The network layer service is defined by a Set of Primitives. These primitives tell the service to perform some action. - These primitives seem very like programming language procedures. Because the network layer must provide 2 types of service, namely connection-oriented and connectionless, there are two sets of primitives.

Primitives for the Connection-Oriented service

With this service the primitives can be divided into 4 groups, depending on their function:

Making the connection - CONNECT

Sending information (i.e. using the connection) - DATA, DATA-ACKNOWLEDGE, EXPEDITED-DATA.

Closing the connection - DISCONNECT

Resetting the connection - RESET.

You make a connection and close a connection by using the CONNECT and DISCONNECT calls. Data is sent using DATA, DATA-ACKNOWLEDGE, and EXPEDITED-DATA (for those special expedited data transmissions). If something goes wrong, then the connection can be reset, using the RESET call.

Primitives for the Connectionless service

These primitives are divided into two groups:
Send a packet of data - UNITDATA
Enquire into the performance of the network - FACILITY, REPORT
Packets are to sent using UNITDATA. FACILITY can let you inquire to the network about things like average delivery statistics and the like. REPORT is used by the network to tell the host if there is a problem with the network, for example, if a machine has gone down.

Internet vs. www

What's the difference between the Internet and the World Wide Web?

The rapid growth of the Internet was greatly aided by the invention of the World Wide Web.
The Internet has become so ubiquitous it's hard to imagine life without it. It's equally hard to imagine a world where "www" isn't the prefix of many of our online activities. But just because the Internet and the World Wide Web are firmly intertwined with each other, it doesn't mean they're synonymous.

Let's go back to when it all began. President Dwight D. Eisenhower started the Advanced Research Projects Agency (ARPA) in 1958 to increase U.S. technological advancements in the shadow of Sputnik's launch. By October 29, 1969, the first ARPANET network connection between two computers was launched -- and promptly crashed. But happily, the second time around was much more successful and the Internet was born. More and more computers were added to this ever-increasing network and the megalith we know today as the Internet began to form. Further information about ARPA can be discovered by reading How ARPANET Works.

But the creation of the World Wide Web didn't come until decades later, with the help of a man named Tim Berners-Lee. In 1990, he developed the backbone of the World Wide Web -- the hypertext transfer protocol (HTTP). People quickly developed browsers which supported the use of HTTP and with that the popularity of computers skyrocketed. In the 20 years during which ARPANET ruled the Internet, the worldwide network grew from four computers to more than 300,000. By 1992, more than a million computers were connected -- only two years after HTTP was developed.

You might be wondering at this point what exactly HTTP is -- it's simply the widely used set of rules for how files and other information are transferred between computers. So what Berners-Lee did, in essence, was determine how computers would communicate with one another. For instance, HTTP would've come into play if you clicked the source link in the last paragraph or if you typed the http://www.howstuffworks.comURL (uniform resource locator) into your browser to get to our home page. But don't get this confused with Web page programming languages like HTML and XHTML. We use those to describe what's on a page, not to communicate between sites or identify a Web page's location.

S.NO	RGPV QUESTION	YEAR	MARKS
Q.1	Explain service primitives in detail	Dec 2011	7

UNIT – 2

DATA LINK LAYER DESIGN ISSUE

Unit-02/Lecture-01

FRAMING[RGPV/Dec 2008,Dec 2011,Dec 2013, Jun 2014]

Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination. The physical layer provides bit synchronization to ensure that the sender and receiver use the same bit durations and timing.

The data link layer needs to pack bits into frames, so that each frame is distinguishable from another. Our postal system practices a type of framing.

The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the delimiter. In addition, each envelope defines the sender and receiver addresses since the postal system is a many-to-many carrier facility.

Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Although the whole message could be packed in one frame that is not normally done. One reason is that a frame can be very large, making flow and error control very inefficient. When a message is carried in one very large frame, even a single-bit error would require the retransmission of the whole message. When a message is divided into smaller frames, a single-bit error affects only that small frame.

Fixed-Size Framing

Frames can be of fixed or variable size. In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter. An example of this type of framing is the ATM wide-area network, which uses frames of fixed size called cells.

Variable-Size Framing

In variable-size framing, we need a way to define the end of the frame and the beginning of the next. Historically, two approaches were used for this purpose:

A character-oriented approach and a bit-oriented approach.

Character-Oriented Protocols

In a character-oriented protocol, data to be carried are 8-bit characters from a coding system. The header, which normally carries the source and destination addresses and other control information, and the trailer, which carries error detection or error correction redundant bits, are also multiples of 8 bits. To separate one frame from the next, an 8-bit (I-byte) flag is added at the beginning and the end of a frame. The flag, composed of protocol-dependent special characters, signals the start or end of a frame.

The flag could be selected to be any character not used for text communication. Now, however, we send other types of information such as graphs, audio, and video. Any pattern used for the flag could also be part of the information. If this happens, the receiver, when it encounters this pattern in the middle of the data, thinks it has reached the end of the frame. To fix this problem, a byte-stuffing strategy was added to character-oriented framing. In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

Byte stuffing by the escape character allows the presence of the flag in the data section of the frame, but it creates another problem. What happens if the text contains one or more escape characters followed by a flag? The receiver removes the escape character, but keeps the flag, which is incorrectly interpreted as the end of the frame. To solve this problem, the escape characters that are part of the text must also be marked by another escape character. In other words, if the escape character is part of the text, an extra one is added to show that the second one is part of the text.

Byte stuffing is the process of adding 1 extra byte whenever there is a flag or escape character in the text.

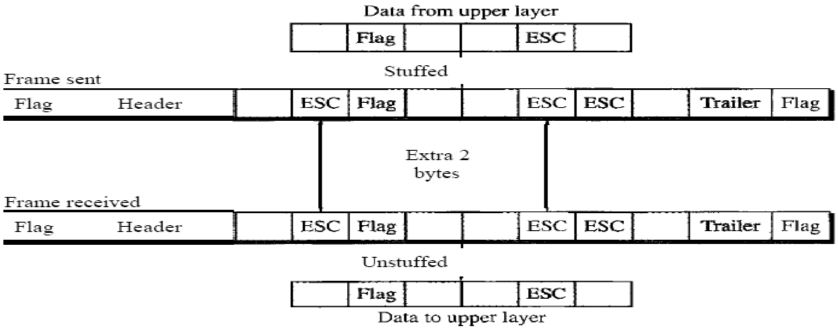


FIGURE 2.1: BYTE STUFFING

Bit-Oriented Protocols[RGPV/Dec 2007]

In a bit-oriented protocol, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on. However, in addition to headers (and possible trailers), we still need a delimiter to separate one frame from the other. Most protocols use a special 8-bit pattern flag 01111110 as the delimiter to define the beginning and the end of the frame,

This flag can create the same type of problem we saw in the byte-oriented protocols. That is, if the flag pattern appears in the data, we need to somehow inform the receiver that this is not the end of the frame. We do this by stuffing 1 single bit (instead of I byte) to prevent the pattern from looking like a flag. The strategy is called bit stuffing. In bit stuffing, if a 0 and five consecutive I bits are encountered, an extra 0 is added. This extra stuffed bit is eventually removed from the data by the receiver. Note that the extra bit is added after one 0 followed by five 1s regardless of the value of the next bit. This guarantees that the flag field sequence does not inadvertently appear in the frame.

Bit stuffing is the process of adding one extra 0 whenever five consecutive 18 follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.

Bit stuffing at the sender and bit removal at the receiver. Note that even if we have a 0 after five 1s, we still stuff a 0. The 0 will be removed by the receiver.

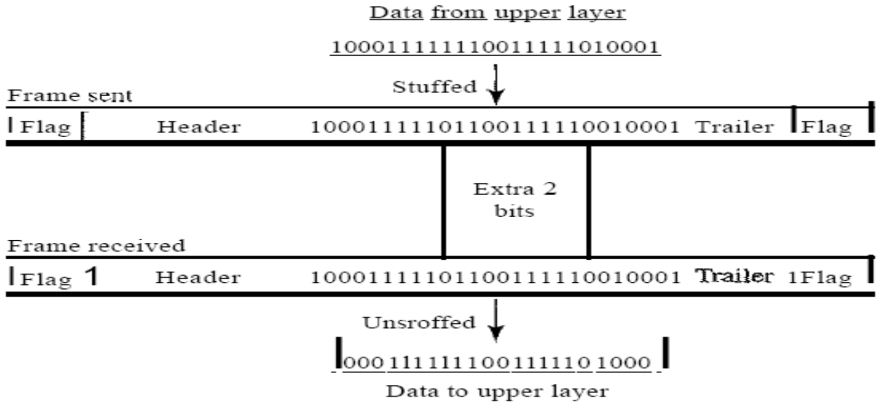


FIGURE 2.2: BIT STUFFING

FLOW AND ERROR CONTROL [RGPV/Jun 2014]

Data communication requires at least two devices working together, one to send and the other to receive. Even such a basic arrangement requires a great deal of coordination for an intelligible exchange to occur. The most important responsibilities of the data link layer are flow control and error control. Collectively, these functions are known as data link control.

Flow Control

Flow control coordinates the amount of data that can be sent before receiving an acknowledgment and is one of the most important duties of the data link layer. In most protocols, flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. The flow of data must not be allowed to overwhelm the receiver. Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data. The receiving device must be able to inform the sending device before those limits are reached and to request that the transmitting device send fewer frames or stop temporarily. Incoming data must be checked and processed before they can be used. The rate of such processing is often slower than the rate of transmission. For this reason, each receiving device has a block of memory, called a buffer, reserved for storing incoming data until they are processed. If the buffer begins to fill up, the receiver must be able to tell the sender to halt transmission until it is once again able to receive.

Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.

Error Control

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term error control refers primarily to methods of error detection and retransmission. Error control in the data link layer is often implemented simply: Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).
Error control in the data link layer is based on automatic repeat request, which is the retransmission of data.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Discuss the data link layer design issue.	Dec 2010 Dec 2013	7
Q.2	Name important functions of data link layer.	Dec 2006 Jun 2010	7
Q.3	Write a detail note on framing.	Dec 2011	7
Q.4	If start and end header is 100001 and the following data stream is to be bit	Dec 2007	7

	stuffed 100110001100001110000011 What will be the frame after bit stuffing?		
Q.5	Data link layer in computer networks address framing, flow control and error control issues. Explain why these functions are important and how they are implemented.	Jun 2014	7

DATA LINK LAYER PROTOCOLS

Unit-02/Lecture-03

Protocols

- Simplest
- Stop-and-Wait
- Stop-and-Wait ARQ
- Go-Hack-N ARQ
- Selective Repeat ARQ

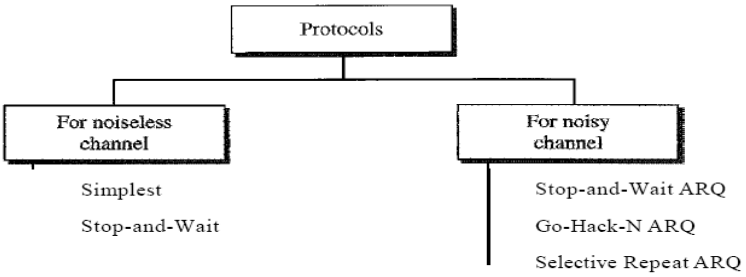


FIGURE 2.3: DATA LINK LAYER PROTOCOL

All the protocols unidirectional in the sense that the data frames travel from one node, called the sender, to another node, called the receiver. Although special frames, called acknowledgment (ACK) and negative acknowledgment (NAK) can flow in the opposite direction for flow and error control purposes, data flow in only one direction.
In a real-life network, the data link protocols are implemented as bidirectional; data flow in both directions. In these protocols the flow and error control information such as ACKs and NAKs is included in the data frames in a technique called piggybacking. Because bidirectional protocols are more complex than unidirectional ones.

NOISELESS CHANNELS[RGPV/ Jun 2014]
We have an ideal channel in which no frames are lost, duplicated, or corrupted. We introduce two protocols for this type of channel. The first is a protocol that does not use flow control; the second is the one that does. Neither has error control because we have assumed that the channel is a perfect noiseless channel.

- **Simplest Protocol** It has no flow or error control. It is a unidirectional protocol in which data frames are travelling in only one direction-from the sender to receiver. We assume that the receiver can immediately handle any frame it receives with a processing time that is small enough to be negligible. The data link layer of the receiver immediately removes the header from the frame and hands the data packet to its network layer, which can also accept the packet immediately. In other words, the receiver can never be overwhelmed with incoming frames.

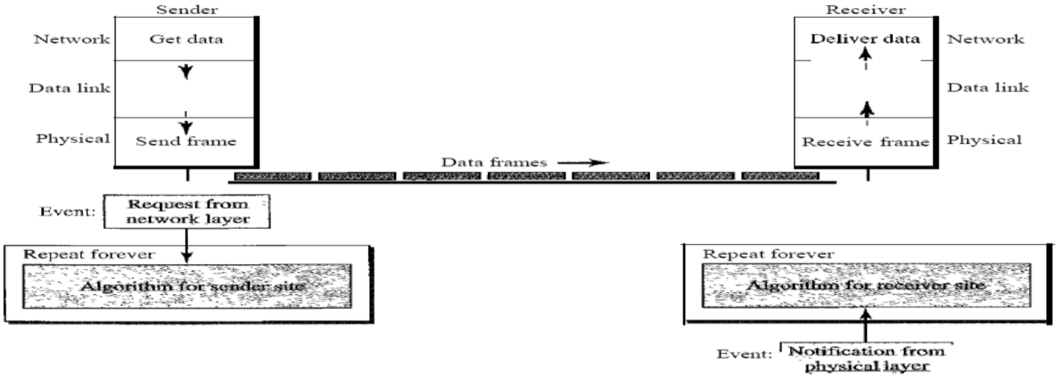


FIGURE 2.4: SIMPLEST PROTOCOL

Design

There is no need for flow control in this scheme. The data link layer at the sender site gets data from its network layer, makes a frame out of the data, and sends it. The data link layer at the receiver site receives a frame from its physical layer, extracts data from the frame, and delivers the data to its network layer. The data link layers of the sender and receiver provide transmission services for their network layers. The data link layers use the services provided by their physical layers (such as signalling, multiplexing, and so on) for the physical transmission of bits.

The sender site cannot send a frame until its network layer has a data packet to send. The receiver site cannot deliver a data packet to its network layer until a frame arrives. If the protocol is implemented as a procedure, we need to introduce the idea of events in the protocol. The procedure at the sender site is constantly running; there is no action until there is a request from the network layer. The procedure at the receiver site is also constantly running, but there is no action until notification from the physical layer arrives. Both procedures are Constantly running because they do not know when the corresponding events will occur.

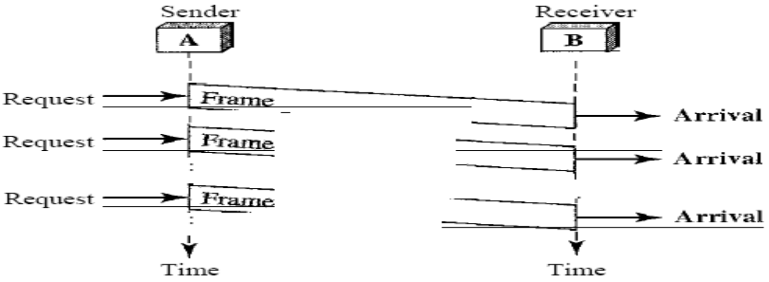


FIGURE 2.5: SIMPEST PROTOCOL

- **Stop-and-Wait Protocol[RGPV/Jun 2010, Jun 2011]**

  If data frames arrive at the receiver site faster than they can be processed, the frames must be stored until their use. Normally, the receiver does not have enough storage space, especially if it is receiving data from many sources. This may result in either the discarding of frames or denial of service. To prevent the receiver from becoming overwhelmed with frames, we somehow need to tell the sender to slow down. There must be feedback from the receiver to the sender.

  The protocol is called the Stop-and-Wait Protocol because the sender sends one frame, stops until it receives confirmation from the receiver (okay to go ahead), and then sends the next frame. We still have unidirectional communication for data frames, but auxiliary ACK frames (simple tokens of acknowledgment) travel from the other direction.

Design

We can see the traffic on the forward channel (from sender to receiver) and the reverse channel. At any time, there is either one data frame on the forward channel or one ACK frame on the reverse channel. We therefore need a half-duplex link.

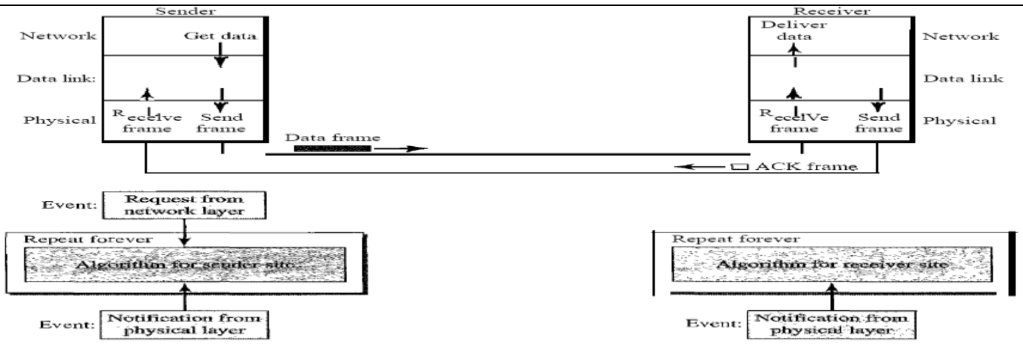


FIGURE 2.6: STOP & WAIT PROTOCOL

Analysis Here two events can occur: a request from the network layer or an arrival notification from the physical layer. The responses to these events must alternate. In other words, after a frame is sent, the algorithm must ignore another network layer request until that frame is acknowledged. We know that two arrival events cannot happen one after another because the channel is error-free and does not duplicate the frames. The requests from the network layer, however, may happen one after another without an arrival event in between. We need somehow to prevent the immediate sending of the data frame. Although there are several methods, we have used a simple canSend variable that can either be true or false. When a frame is sent, the variable is set to false to indicate that a new network request cannot be sent until canSend is true. When an ACK is received, canSend is set to true to allow the sending of the next frame.

After the data frame arrives, the receiver sends an ACK frame (line 9) to acknowledge the receipt and allow the sender to send the next frame.

The sender sends one frame and waits for feedback from the receiver. When the ACK arrives, the sender sends the next frame. Note that sending two frames in the protocol involves the sender in four events and the receiver in two events.

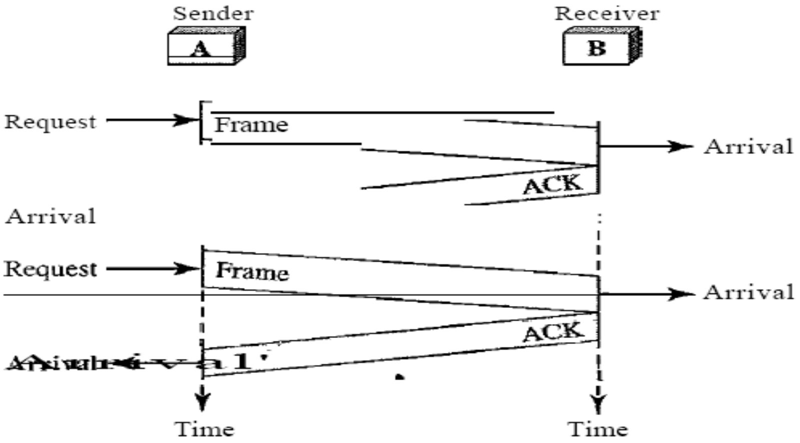


FIGURE 2.7: STOP & WAIT PROTOCOL FLOW DIAGRAM

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain stop & wait protocol.	June 2010 June 2011	7
Q.2	Write and explain window based flow control strategies.	Jun 2014	7

DATA LINK LAYER PROTOCOLS

Unit-02/Lecture-04/ Lecture-05/ Lecture-06

NOISY CHANNELS

Although the Stop-and-Wait Protocol gives us an idea of how to add flow control to its predecessor, noiseless channels are nonexistent. We can ignore the error (as we sometimes do), or we need to add error control to our protocols. We discuss three protocols in this section that use error control.

- **Stop-and-Wait Automatic Repeat Request[RGPV/Dec 2009, Jun 2013]**
  Our first protocol, called the Stop-and-Wait Automatic Repeat Request (Stop-and Wait ARQ), adds a simple error control mechanism to the Stop-and-Wait Protocol. Let us see how this protocol detects and corrects errors.

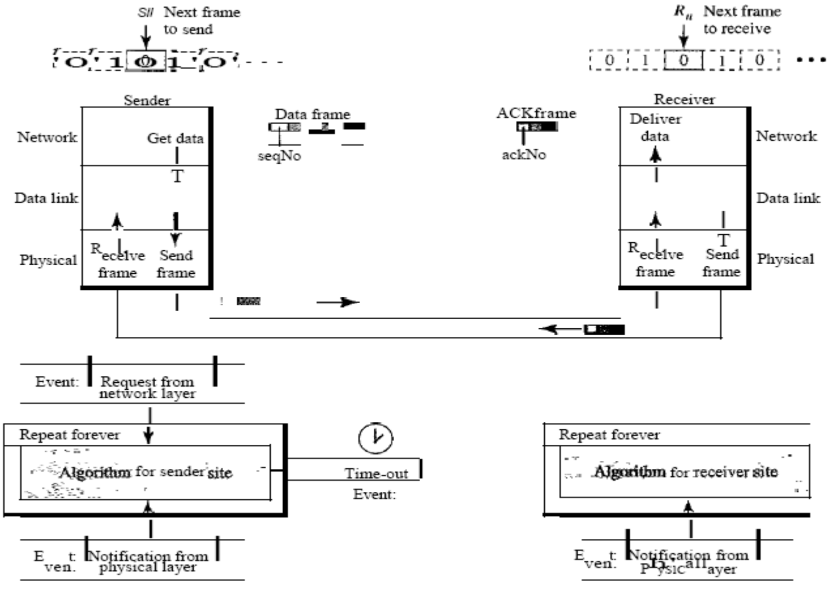


FIGURE 2.8: STOP & WAIT ARQ PROTOCOL

To detect and correct corrupted frames, we need to add redundancy bits to our data frame. When the frame arrives at the receiver site, it is checked and if it is corrupted, it is silently discarded. The detection of errors in this protocol is manifested by the silence of the receiver.

Lost frames are more difficult to handle than corrupted ones. In our previous protocols, there was no way to identify a frame. The received frame could be the correct one, or a duplicate, or a frame out of order. The solution is to number the frames. When the receiver receives a data frame that is out of order, this means that frames were either lost or duplicated.

The completed and lost frames need to be resent in this protocol. If the receiver does not respond when there is an error, how can the sender know which frame to resend? To remedy this problem, the sender keeps a copy of the sent frame. At the same time, it starts a timer. If the timer expires and there is no ACK for the sent frame, the frame is resent, the copy is held, and the timer is restarted. Since the protocol uses the stop-and-wait mechanism, there is only one specific frame that needs an ACK even though several copies of the same frame can be in the network.

Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires.

Since an ACK frame can also be corrupted and lost, it too needs redundancy bits and a sequence number. The ACK frame for this protocol has a sequence number field. In this protocol, the sender simply discards a corrupted ACK frame or ignores an out-of-order one.

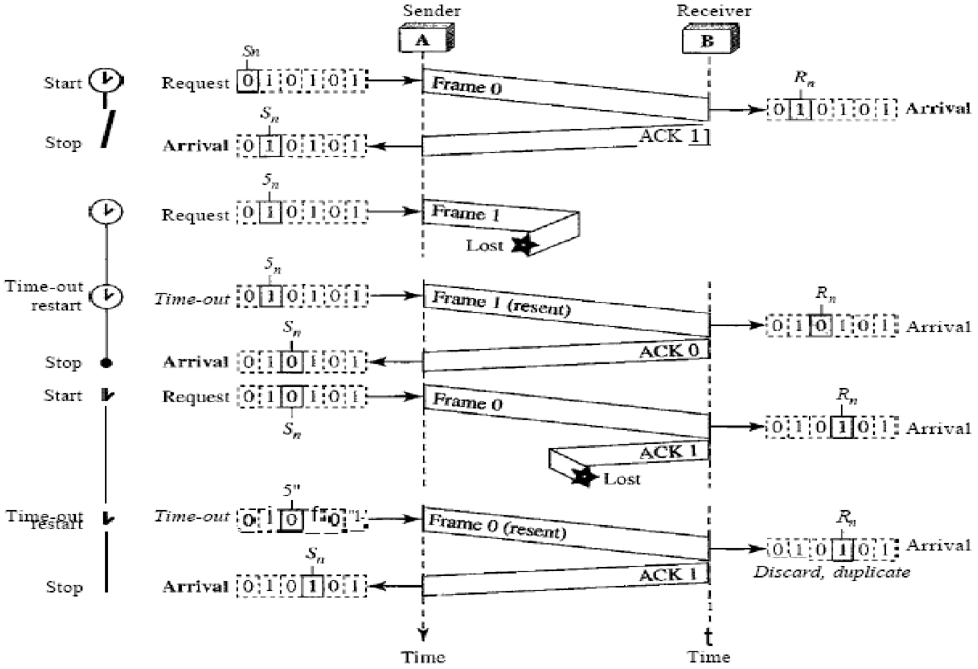


FIGURE 2.9: STOP & WAIT ARQ PROTOCOL FLOW DIAGRAM

Sequence Numbers

The protocol specifies that frames need to be numbered. This is done by using sequence numbers. A field is added to the data frame to hold the sequence number of that frame.

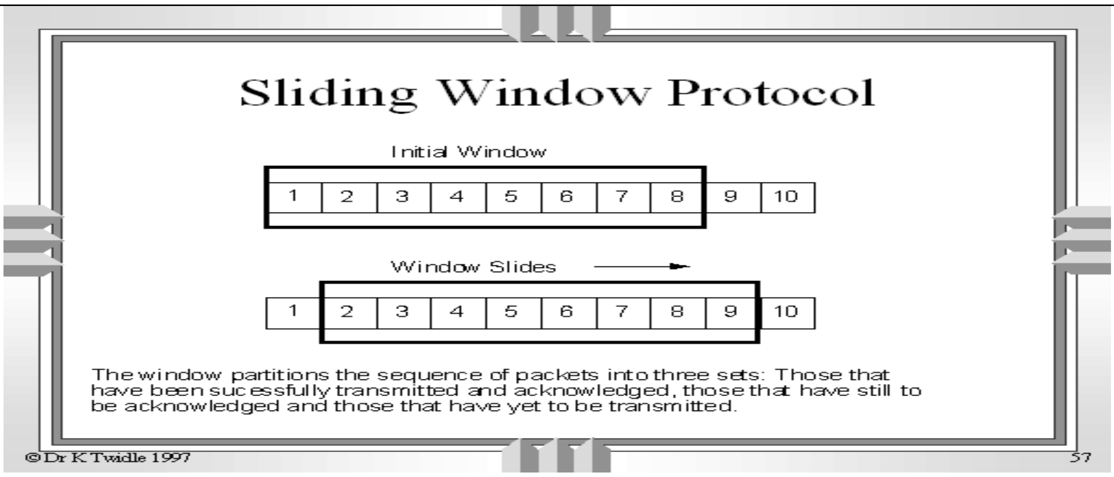
One important consideration is the range of the sequence numbers. Since we want to minimize the frame size, we look for the smallest range that provides unambiguous communication. The sequence numbers of course can wrap around. For example, if we decide that the field is m bits long, the sequence numbers start from 0, go to 2m - 1, and then are repeated.

Acknowledgment Numbers

Since the sequence numbers must be suitable for both data frames and ACK frames, we use this convention: The acknowledgment numbers always announce the sequence number of the next frame expected by the receiver. For example, if frame 0 has arrived safe and sound, the receiver sends an ACK frame with acknowledgment 1 (meaning frame 1 is expected next). If frame 1 has arrived safe and sound, the receiver sends an ACK frame with acknowledgment 0 (meaning frame 0 is expected).

Pipelining[RGPV/Jun 2010]

Improves the efficiency of the transmission if the number of bits in transition is large with respect to the bandwidth-delay product.



Sliding Window Protocol

Initial Window

1	2	3	4	5	6	7	8	9	10

Window Slides →

1	2	3	4	5	6	7	8	9	10

The window partitions the sequence of packets into three sets: Those that have been sucessfully transmitted and acknowledged, those that have still to be acknowledged and those that have yet to be transmitted.

©Dr K Twidle 1997 57

FIGURE 2.10: SLIDING WINDOW PROTOCOL

- **Go-Back-N Automatic Repeat Request[RGPV/Dec 2010, Jun 2013]**
  To improve the efficiency of transmission (filling the pipe), multiple frames must be in transition while waiting for acknowledgment. In other words, we need to let more than one frame be outstanding to keep the channel busy while the sender is waiting for acknowledgment.

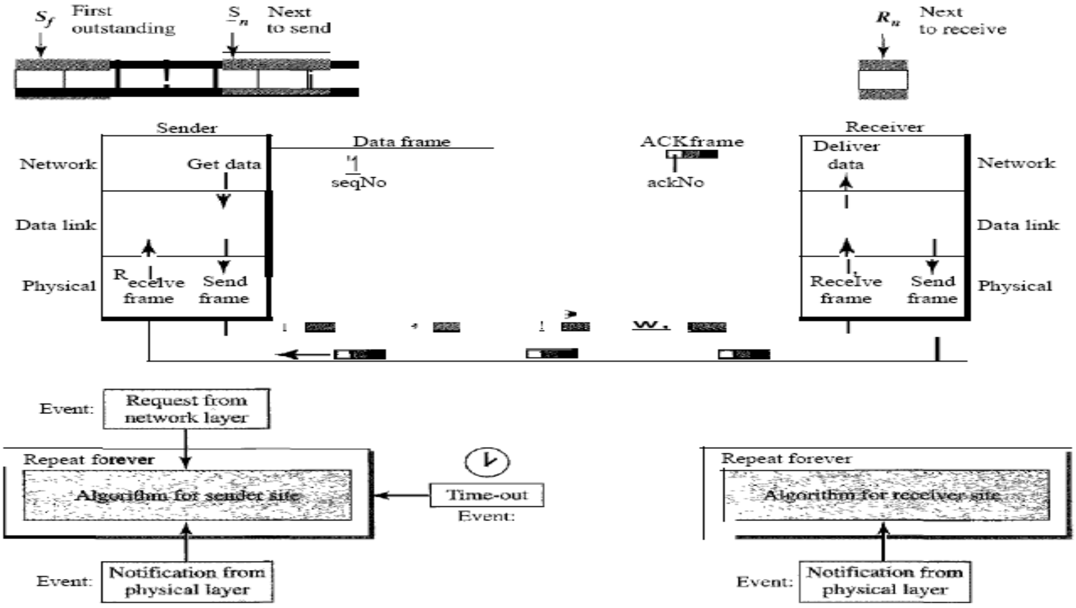


FIGURE 2.11: GO-BACK-N ARQPROTOCOL

The first is called Go-Back-N Automatic Repeat Request. In this protocol we can send several frames before receiving acknowledgments; we keep a copy of these frames until the acknowledgments arrive.

Sequence Numbers

Frames from a sending station are numbered sequentially. However, because we need to include the sequence number of each frame in the header, we need to set a limit. If the header of the frame allows m bits for the sequence number, the sequence numbers range from 0 to 2m - 1. For example, if m is 4, the only sequence numbers are 0 through 15 inclusive.

The send window can slide one or more slots when a valid acknowledgment arrives.

The receive window makes sure that the correct data frames are received and that the correct acknowledgments are sent. The size of the receive window is always I. The receiver is always looking for the arrival of a specific frame. Any frame arriving out of order is discarded and needs to be resent.

The receive window also slides, but only one slot at a time. When a correct frame is received (and a frame is received only one at a time), the window slides.

Timers

Although there can be a timer for each frame that is sent, in our protocol we use only one. The reason is that the timer for the first outstanding frame always expires first; we send all outstanding frames when this timer expires.

Acknowledgment

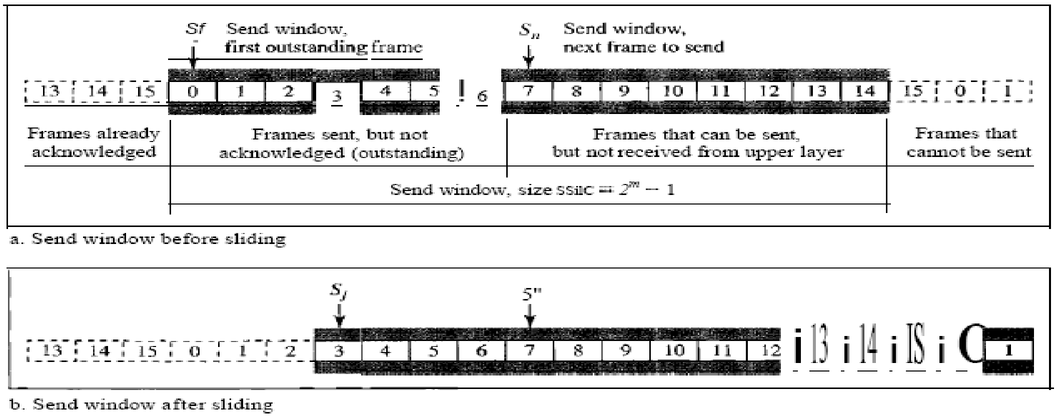
The receiver sends a positive acknowledgment if a frame has arrived safe and sound and in order. If a frame is damaged or is received out of order, the receiver is silent and will discard all subsequent frames until it receives the one it is expecting. The silence of the receiver causes the timer of the unacknowledged frame at the sender site to expire.

This, in turn, causes the sender to go back and resend all frames, beginning with the one with the expired timer. The receiver does not have to acknowledge each frame received.

It can send one cumulative acknowledgment for several frames. Resending a

Frame

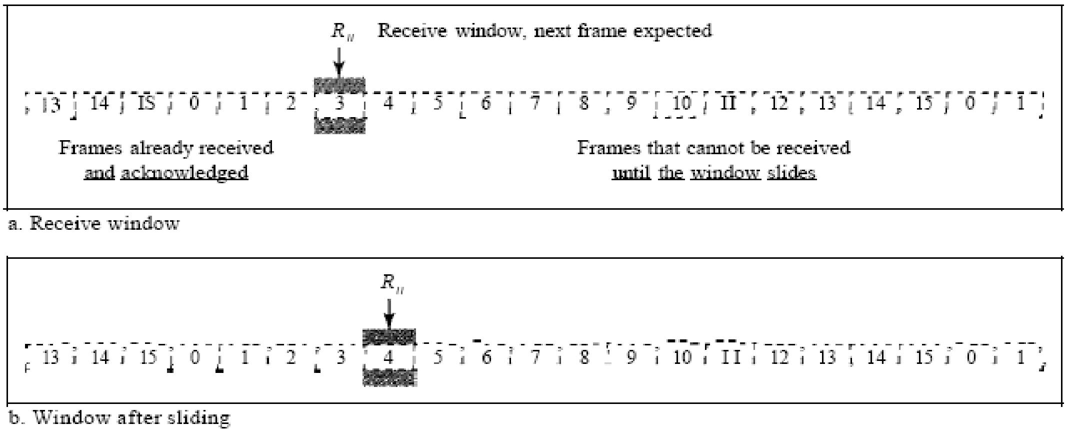
When the timer expires, the sender resends all outstanding frames. For example, suppose the sender has already sent frame 6, but the timer for frame 3 expires. This means that frame 3 has not been acknowledged; the sender goes back and sends frames 3, 4, 5, and 6 again. That is why the protocol is called Go-Back-N ARQ.


Sf Send window, first outstanding frame
Sn Send window, next frame to send
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already acknowledged
Frames sent, but not acknowledged (outstanding)
Frames that can be sent, but not received from upper layer
Frames that cannot be sent
Send window, size ssilc = 2^m − 1
Sf
Sn
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1

a. Send window before sliding

b. Send window after sliding

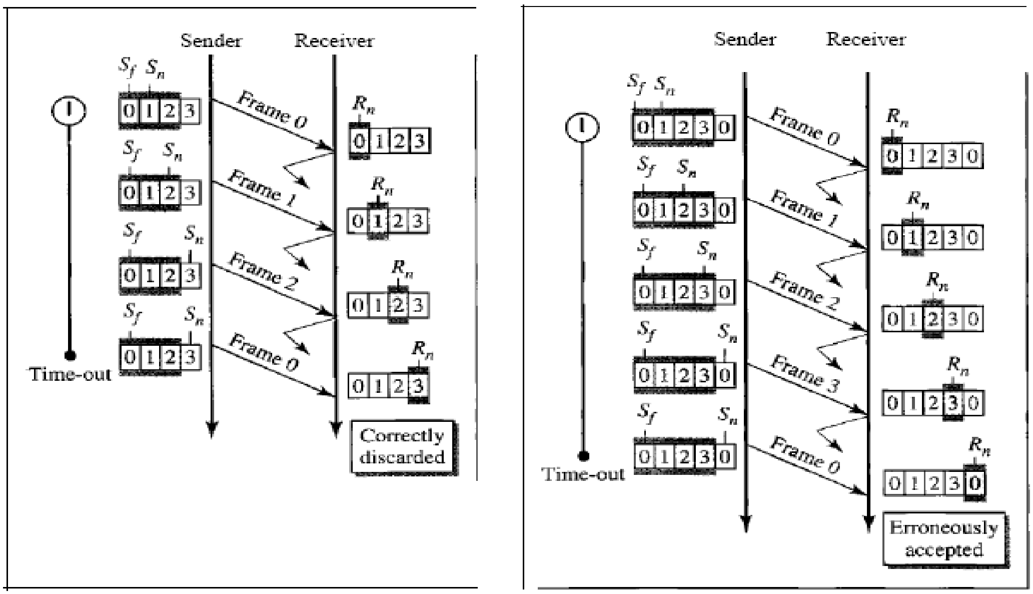
FIGURE 2.12: SENT WINDOW


Rn Receive window, next frame expected
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already received and acknowledged
Frames that cannot be received until the window slides
Rn
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1

a. Receive window

b. Window after sliding

FIGURE 2.13: RECIEVER WINDOW



a. Window size $< 2^m$ b. Window size $= 2^m$

FIGURE 2.14: GO-BACK-N ARQ PROTOCOL FLOW DIAGRAM

- **Selective Repeat Request Protocol[RGPV/Dec 2008/ Dec 2012]**

Design

Multiple frames can be in transit in the forward direction, and multiple acknowledgments in the reverse direction. The idea is similar to Stop-and-Wait ARQ; the difference is that the send window allows us to have as many frames in transition as there are slots in the send window.

Send Window Size

We can now show why the size of the send window must be less than 2m. As an example, we choose m =2, which means the size of the window can be 2m- 1, or 3.

It compares a window size of 3 against a window size of 4. If the size of the window is 3 (less than 22) and all three acknowledgments are lost, the frame timer expires and all three frames are resent. The receiver is now expecting frame 3, not frame 0, so the duplicate frame is correctly discarded. On the other hand, if the size of the window is 4 (equal to 22) and all acknowledgments are lost, the sender will send a duplicate of frame 0. However, this time the window of the receiver expects to receive frame 0, so it accepts frame 0, not as a duplicate, but as the first frame in the next cycle. This is an error.

Windows

The Selective Repeat Protocol also uses two windows: a send window and a receive window.

However, there are differences between the windows in this protocol and the ones in Go-Back-N. First, the size of the send window is much smaller; it is 2m- 1. Second, the receive window is the same size as the send window.

The send window maximum size can be 2m- 1. For example, if m = 4, the sequence numbers go from 0 to 15, but the size of the window is just 8 (it is 15 in the Go-Back-N Protocol). The smaller window size means less efficiency in filling the pipe, but the fact that there are fewer duplicate frames can compensate for this. The protocol uses the same variables as we discussed for Go-Back-N.

The timer for frame starts at the first request, but stops when the ACK for this frame arrives. The timer for frame I start at the second request restarts when a NAK arrives, and finally stops when the last ACK arrives.

The other two timers start when the corresponding frames are sent and stop at the last arrival event.

At the receiver site we need to distinguish between the acceptance of a frame and its delivery to the network layer. At the second arrival, frame 2 arrives and is stored and marked (colored slot), but it cannot be delivered because frame 1 is missing. At the next arrival, frame 3 arrives and is marked and stored, but still none of the frames can be delivered. Only at the last arrival, when finally a copy of frame 1 arrives, can frames 1, 2, and 3 be delivered to the network layer. There are two conditions for the delivery of frames to the network layer: First, a set of consecutive frames must have arrived. Second, the set starts from the beginning of the window.

After the first arrival, there was only one frame and it started from the beginning of the window. After the last arrival, there are three frames and the first one starts from the beginning of the window.

Another important point is that a NAK is sent after the second arrival, but not after the third, although both situations look the same. The reason is that the protocol does not want to crowd the network with unnecessary NAKs and unnecessary resent frames. The second NAK would still be NAKI to inform the sender to resend frame 1 again; this has already been done. The first NAK sent is remembered (using the nakSent variable) and is not sent again until the frame slides. A NAK is sent once for each window position and defines the first slot in the window.

The next point is about the ACKs. Notice that only two ACKs are sent here. The first one acknowledges only the first frame; the second one acknowledges three frames. In Selective Repeat, ACKs are sent when data are delivered to the network layer. If the data belonging to n frames are delivered in one shot, only one ACK is sent for all of them.

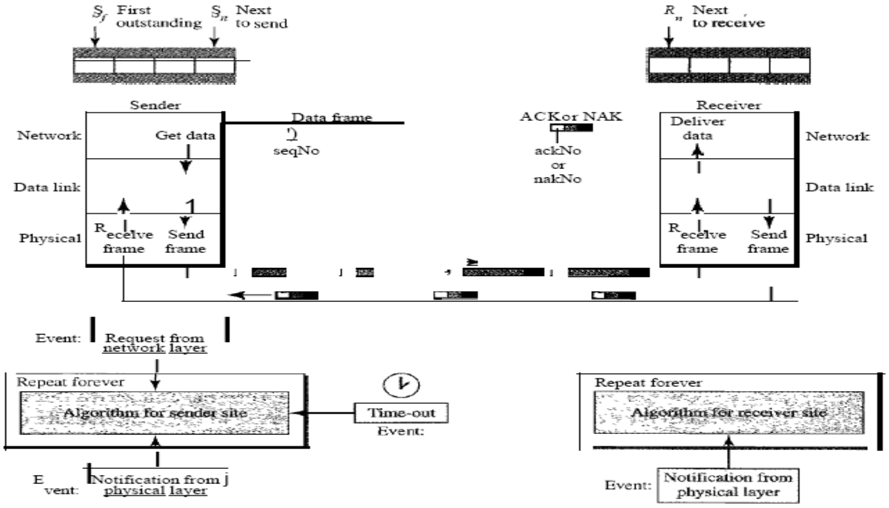


FIGURE 2.15: SELECTIVE REPEAT PROTOCOL

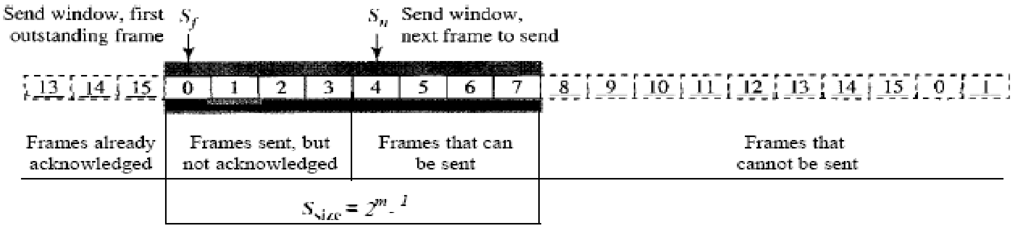

Send window, first outstanding frame
S_f
S_n
Send window, next frame to send
13
14
15
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
0
1
Frames already acknowledged
Frames sent, but not acknowledged
Frames that can be sent
Frames that cannot be sent
$S_{size} = 2^m - 1$

FIGURE 2.16: SENT WINDOW

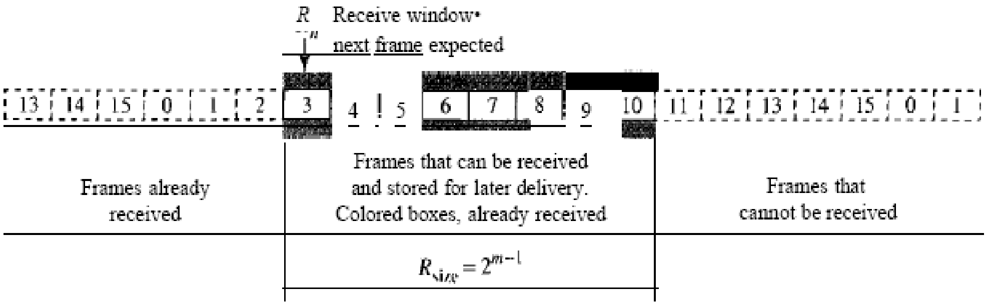
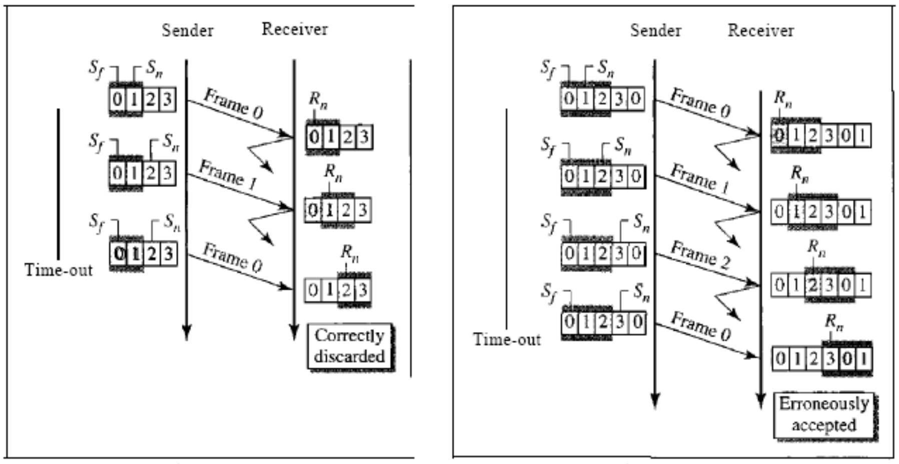

R_n Receive window• next frame expected
13
14
15
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
0
1
Frames already received
Frames that can be received and stored for later delivery. Colored boxes, already received
Frames that cannot be received
$R_{size} = 2^{m-1}$

FIGURE 2.17: RECIEVER WINDOW



a. Window size $=2^{m-1}$

b. Window size> 2^{m-1}

FIGURE 2.18: SELECTIVE REPEAT PROTOCOL FLOW DIAGRAM

Piggybacking[RGPV/Jun 2010, Dec 2012,Jun 2013]

The three protocols are all unidirectional: data frames flow in only one direction although control information such as ACK and NAK frames can travel in the other direction. In real life, data frames are normally flowing in both directions:

From node A to node B and from node B to node A. This means that the control information also needs to flow in both directions. A technique called **piggybacking** is used to improve the efficiency of the bidirectional protocols. When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain stop & wait for noisy channel and analyse its performance for channel utilization and optimal frame size.	Dec 2003	7
Q.2	How data link layer- (i) Achieves flow control (ii) Handles duplicates frame at receiver Using stop & wait protocol for noisy channel.	June 2006 June 2007	7
Q.3	Discuss and compare DLL "Go back n" and "Selective repeat" protocols.	June 2004 Dec 2004 Dec 2008	7
Q.4	With the aid of frame sequence diagrams and assuming a selective repeat error control scheme, describe how the following are overcome using both implicit and explicit retransmission- (i) A corrupted information frame (ii) A corrupted ANCK/NAK frame	June 2005	7
Q.5	What is the purpose of timer at the sender site in systems using ARQ? Discuss the size of the Go back n ARQ and selective repeat ARQ sliding window at both the sender sites.	Dec 2010	7
Q.6	In selective repeat protocol, what does the number on a NAK and ACK frame mean?	Dec 2011	7
Q.7	Assuming a send window of X deduce the minimum range of sequence numbers(frame identifiers) required	Jun 2005	7

	with each of the following error control schemes- (i) A selective repeat (ii) Go back n		
Q.8	Explain the working of stop & wait ARQ and Go back N ARQ protocol.	Jun 2013	7
Q.9	Explain the noisy channel protocol: go back N ARQ	Jun 2013	7
Q.10	Explain following: piggybacking	Dec 2012 Jun 2013	7
Q.11	Express why sliding window protocol is superior to stop n wait protocol. Justify your answer with an suitable answer.	Dec 2012	7
Q.12	What is the maximum window size in selective reject ARQ? Justify your answer with an example.	Dec 2012	3.5

Unit-02/Lecture-07

HDLC LAN Protocol

HDLC[RGPV/Jun 2006, Dec 2009,Jun 2010, Dec 2012,Dec 2013, Jun 2014]

High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links. It implements the ARQ mechanisms

Configurations and Transfer Modes

HDLC provides two common transfer modes that can be used in different configurations:
Normal response mode (NRM) and asynchronous balanced mode (ABM)

Normal Response Mode

In normal response mode (NRM), the station configuration is unbalanced. We have one primary station and multiple secondary stations. A primary station can send commands; a secondary station can only respond. The NRM is used for both point-to-point and multiple-point links.

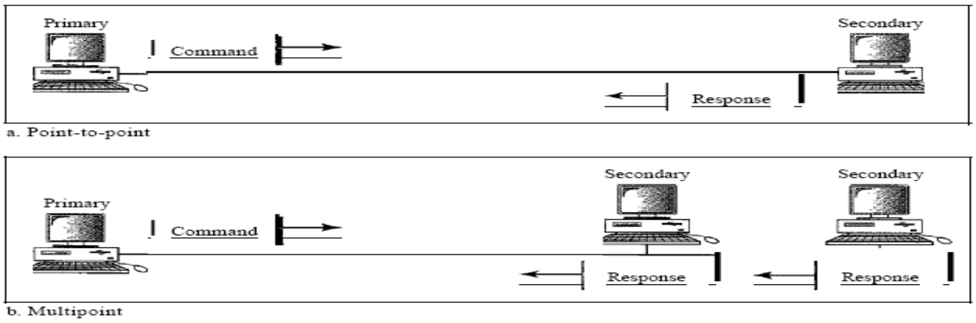


FIGURE 2.19: NRM

Asynchronous Balanced Mode

In asynchronous balanced mode (ABM), the configuration is balanced. The link is point-to-point, and each station can function as a primary and a secondary (acting as peers).

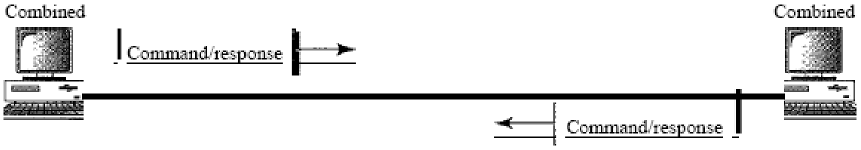


FIGURE 2.20: ABM

To provide the flexibility necessary to support all the options possible in the modes and configurations, HDLC defines three types of frames:

- Information frames (I-frames)
- Supervisory frames (S-frames)
- Unnumbered frames (U-frames)

Each type of frame serves as an envelope for the transmission of a different type of message.

I-frames are used to transport user data and control information relating to user data (piggybacking).

S-frames are used only to transport control information.

U-frames are reserved for system management. Information carried by U-frames is intended for managing the link itself.

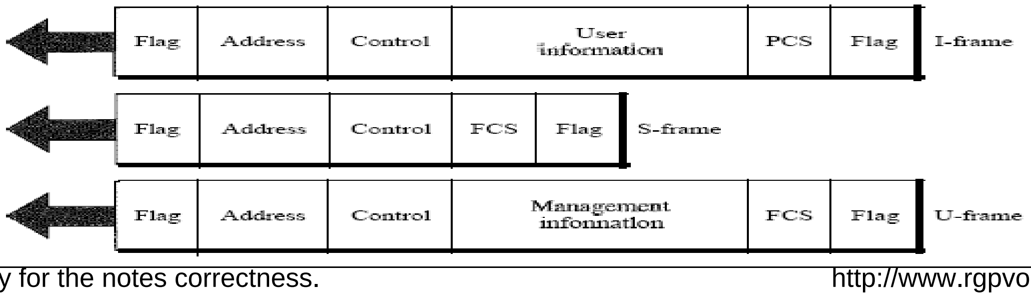


FIGURE 2.21: HDLC FRAMES

DATA LINK CONTROL

Frame Format

Each frame in HDLC may contain up to six fields, a beginning flag field, an address field, a control field, an information field, a frame check sequence (FCS) field, and an ending flag field. In multiple-frame transmissions, the ending flag of one frame can serve as the beginning flag of the next frame.

- **Flag field** The flag field of an HDLC frame is an 8-bit sequence with the bit pattern 01111110 that identifies both the beginning and the end of a frame and serves as a synchronization pattern for the receiver.
- **Address field** It contains the address of the secondary station. If a primary station created the frame, it contains to address. If a secondary creates the frame, it contains from address. An address field can be 1 byte or several bytes long, depending on the needs of the network. One byte can identify up to 128 stations. Larger networks require multiple-byte address fields. If the address field is only 1 byte, the last bit is always a 1. If the address is more than 1 byte, all bytes but the last one will end with 0; only the last will end with 1. Ending each intermediate byte with 0 indicates to the receiver that there are more address bytes to come.
- **Control field** The control field is a 1- or 2-byte segment of the frame used for flow and error control. The interpretation of bits in this field depends on the frame type.
- **Information field** The information field contains the user's data from the network layer or management information. Its length can vary from one network to another.
- **FCS field** The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 2- or 4-byte ITU-T CRC.
- **Control Field** The control field determines the type of frame and defines its functionality. The first bit defines the type. If the first bit of the control field is 0, this means the frame is an I-frame. The next 3 bits, called N(S), define the sequence number of the frame. Note that with 3 bits, we can define a sequence number between 0 and 7; but in the extension format, in which the control field is 2 bytes, this field is larger. The last 3 bits, called N(R), correspond to the acknowledgment number when piggybacking is used. The single bit between N(S) and N(R) is called the PIF bit. The PIP field is a single bit with a dual purpose. It has meaning only when it is set (bit = 1) and can mean poll or final. It means poll when the frame is sent by a primary station to a secondary (when the address field contains the address of the receiver). It means final when the frame is sent by a secondary to a primary (when the address field contains the address of the sender).

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Name the types of HDLC frames and give a brief description of each. In HDLC, what is bit stuffing and why is it needed?	Dec 2010	7
Q.2	Draw the frame format of HDLC protocol. Explain the technique of bit stuffing for data transparency. Explain the use of control, data checksum and address fields of HDLC protocol.	Dec 2009	7
Q.3	Explain about HDLC.	Dec 2013	7
Q.4	What are the transfer modes supported by the HDLC? Describe each.	Dec 2012	7
Q.5	Explain any two of the following data link layer protocols giving characteristics features, frame format and applications: (1) HDLC (2) IEE 802.2 LLC	Jun 2014	14

	(3) PPP		

Unit-02/Lecture-08/ Lecture-09

Logical link control/ Media access control

IEEE STANDARDS

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 does not seek to replace any part of the OSI or the Internet model. Instead, it is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

The standard was adopted by the American National Standards Institute (ANSI). In 1987, the International Organization for Standardization (ISO) also approved it as an international standard under the designation ISO 8802.

The IEEE has subdivided the data link layer into two sub layers:

- logical link control (LLC)
- media access control (MAC)

IEEE has also created several physical layer standards for different LAN protocols.

IEEE standard for LANs

- LLC: Logical link control
- MAC: Media access control

the data link layer in the IEEE standard is divided into two sub layers:

- LLC
- MAC

Logical Link Control (LLC) [RGPV/Dec 2009, Jun 2010, Jun 2013, Jun 2014]

Data link control handles framing, flow control, and error control. In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sublayer called the logical link control. Framing is handled in both the LLC sublayer and the MAC sublayer.

The LLC provides one single data link control protocol for all IEEE LANs. In this way, the LLC is different from the media access control sublayer, which provides different protocols for different LANs. A single LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent. One single LLC protocol serving several MAC protocols. Framing LLC defines a protocol data unit (PDU) that is somewhat similar to that of HDLC. The header contains a control field like the one in HDLC; this field is used for flow and error control. The two other header fields define the upper-layer protocol at the source and destination that uses LLC. These fields are called the destination service access point (DSAP) and the source service access point (SSAP). The other fields defined in a typical data link control protocol such as HDLC are moved to the MAC sublayer. In other words, a frame defined in HDLC is divided into a PDU at the LLC sublayer and a frame at the MAC sublayer

Need for LLC The purpose of the LLC is to provide flow and error control for the upper-layer protocols that actually demand these services. For example, if a LAN or several LANs are used in an isolated system, LLC may be needed to provide flow and error control for the application layer protocols. However, most upper-layer protocols media access control that defines the specific access method for each LAN. For example, it defines CSMA/CD as the media access method for Ethernet LANs and the token passing method for Token Ring and Token Bus LANs. Part of the framing function is also handled by the MAC layer.

In contrast to the LLC sublayer, the MAC sublayer contains a number of distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol.

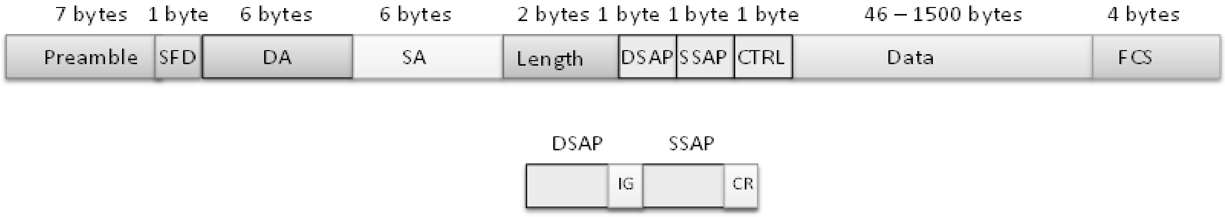


FIGURE 2.22: FRAME FORMAT MAC

Physical Layer

The physical layer is dependent on the implementation and type of physical media used. IEEE defines detailed specifications for each LAN implementation. For example, although there is only one MAC sublayer for Standard Ethernet,

MAC Sublayer [RGPV/Jun 2014]

In Standard Ethernet, the MAC sublayer governs the operation of the access method. It also frames data received from the upper layer and passes them to the physical layer.

Frame Format

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU) and upper-layer data. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium. Acknowledgments must be implemented at the higher layers.

- **Preamble** The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0's and 1's that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not (formally) part of the frame.
- **Start frame delimiter (SFD)** The second field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.
- **Destinations address (DA)** The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.
- **Sources address (SA)** The SA field is also 6 bytes and contains the physical address of the sender of the packet.
- **Length or type** This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field. Both uses are common today.
- **Data** This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes CRC. The last field contains error detection information, in this case a CRC-32
- **Frame Length** Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame,
  Minimum payload length: 46 bytes
  Maximum payload length: 1500 bytes-1

  Minimum frame length: 512 bits or 64 bytes
  Maximum frame length. 12,144 bits or 1518 bytes

  An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. Part of this length is the header and the trailer. If we count 18 bytes of header and trailer (6 bytes of source address, 6 bytes of destination address, 2 bytes of length or type, and 4 bytes of

CRC), then the minimum length of data from the upper layer is 64 - 18 = 46 bytes. If the upper-layer packet is less than 46 bytes, padding is added to make up the difference.

The standard defines the maximum length of a frame (without preamble and SFD field) as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes. The maximum length restriction has two historical reasons. First, memory was very expensive when Ethernet was designed: a maximum length restriction helped to reduce the size of the buffer. Second, the maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.

- **Frame length:**
  Minimum: 64 bytes (512 bits) Maximum: 1518 bytes (12,144 bits)

- **Addressing**
  Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6-byte physical address. As shown in Figure 13.6, the Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.
- Unicast
- Multicast
- Broadcast Addresses

A source address is always a unicast address-the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast.

If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.

If the bit is 0, the address is unicast; otherwise, it is multicast.

A unicast destination address defines only one recipient; the relationship between the sender and the receiver is one-to-one. A multicast destination address defines a group of addresses; the relationship between the sender and the receivers is one-to-many. The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN. A broadcast destination address is forty-eight 1's. The broadcast destination address is a special case of the multicast address in which all bits are 1's.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain the concept of Ethernet frame and explain the meaning of each field in the frame?	Jun 2014	7
Q.2	Explain the following: IEEE 802.2 LLC frame format	Dec 2009 Jun 2010 Jun 2013	7
Q.3	Explain any two of the following data link layer protocols giving characteristics features, frame format and applications: (1) HDLC (2) IEE 802.2 LLC (3) PPP	Jun 2014	14
Q.4	Explain IEE 802.3/ ether net frame format justifying utility of each field in the frame.	Jun 2014	3.5

UNIT 2/LECTURE 010

SERIAL LINE INTERNET PROTOCOL (SLIP)

Serial Line Internet Protocol (SLIP)

SLIP Basic Data Framing Method and General Operation

An IP datagram is passed down to SLIP, which breaks it into bytes and sends them one at a time over the link. After the last byte of the datagram, a special byte value is sent that tells the receiving device that the datagram has ended. This is called the SLIP END character, and has a byte value of 192 decimal (C0 hexadecimal, 11000000 binary). And that's basically it: take the whole datagram, send it one byte at a time, and then send the byte 192 to delimit the end of the datagram.

A minor enhancement to this basic operation is to **precede** the datagram by an END character as well. The benefit of this is that it clearly separates the start of the datagram from anything that preceded it. To see why this might be needed, suppose at a particular time we have only one datagram to send, datagram #1. So, we send #1, and then send the END character to delimit it. Now, suppose there is a pause before the next datagram shows up. During that time we aren't transmitting, but if there is line noise, the other device might pick up spurious bytes here and there. If we later receive datagram #2 and just start sending it, the receiving device might think the noise bytes were part of datagram #2.

Starting datagram #2 off with an END character tells the recipient that anything received between this END character and the previous one is a separate datagram. If that's just noise, then this “noise datagram” is just gibberish that will be rejected at the IP layer. Meanwhile, it doesn't corrupt the real datagram we wish to send. If no noise occurred on the line between datagrams then the recipient will just see the END at the start of datagram #2 right after the one at the end of #1, and will ignore the “null datagram” between the two.

Escaping Special Characters

There is only one other issue SLIP deals with. If the END character is 192 decimal, what happens if the byte value 192 appears in the datagram itself? Transmitting it “as is” would fool the recipient into thinking the datagram ended prematurely. To avoid this, a special Escape character (ESC) is defined, which has a decimal value of 219 (DB in hex, 11011011 in binary). The term “escape” means that this symbol conveys the meaning “this byte and the next one have a special meaning”. When a value of 192 appears in the datagram, the sending device replaces it by the ESC character (219 decimal) followed by the value 220 decimal. Thus, a single “192” becomes “219 220” (or “DB DC” in hexadecimal). The recipient translates back from “219 220” to “192”.

This leaves one final problem: what happens if the **escape character itself** is in the original datagram? That is, what if there's a byte value of 219 in the IP datagram to be sent? This is handled by a similar substitution: instead of “219” we put “219 221”.

So in summary, this is basically everything SLIP does:

- Break an IP datagram into bytes.
- Send the END character (value “192”) after the last byte of the datagram; in better implementations, send the END character before the first byte as well.
- If any byte to be sent in the datagram is “192”, replace it with “219 220”.
- If any byte to be sent is “219”, replace it with “219 221”.

Figure shows an example of how SLIP works, including the escaping of special characters, using a mock IP datagram.

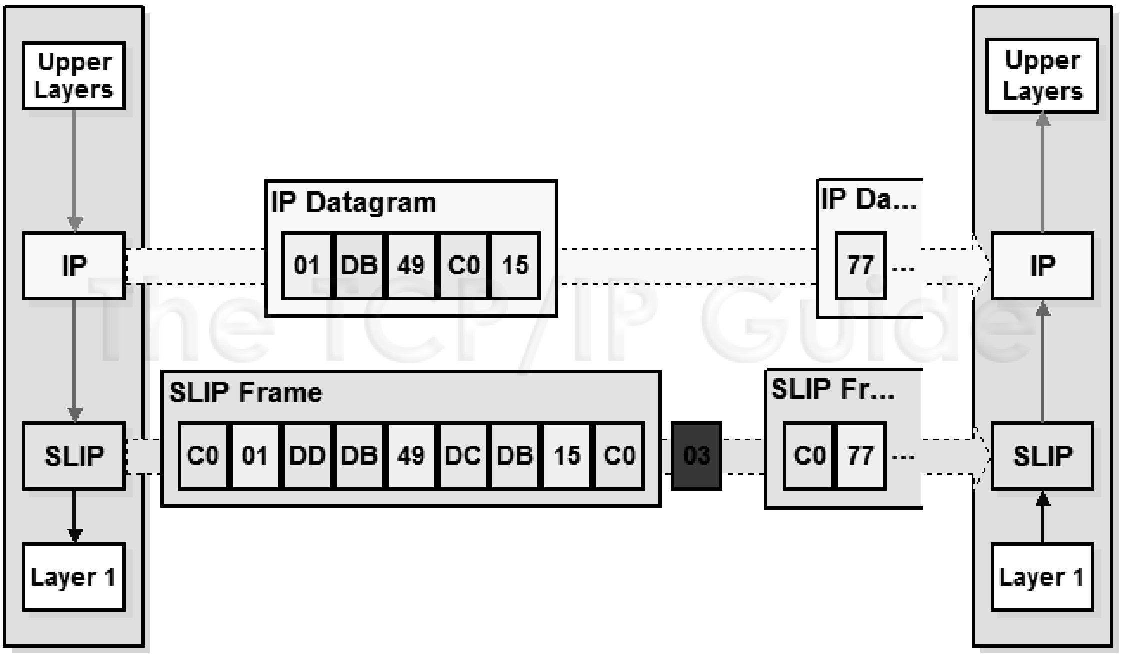


FIGURE 2.23: OPERATION OF THE SERIAL LINE INTERNET PROTOCOL (SLIP)

IP datagrams are passed down to the SLIP software at layer two (a simplified one with only five bytes is shown here). There, they are framed by surrounding them with END characters (hexadecimal value C0h, shown in orange). Special characters with hexadecimal values DBh and C0h are replaced by two-byte sequences. Note that the presence of the bracketing END characters forces the receiving device to see the noise byte (03h, in red) as a separate IP datagram, rather than part of either of the real ones. It will be rejected when passed up to the IP layer.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain the SLIP	June 2010	7

POINT-TO-POINT PROTOCOL

POINT-TO-POINT PROTOCOL[RGPV/[Dec 2004, Dec 2009, Jun 2010, Jun 2014]

Although HDLC is a general protocol that can be used for both point-to-point and multipoint configurations, one of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP). Today, millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP. The majority of these users have a traditional modem; they are connected to the Internet through a telephone line, which provides the services of the physical layer, manage the transfer of data; there is a need for a point-to-point protocol at the data link layer.

PPP provides several services:

- PPP defines the format of the frame to be exchanged between devices.
- PPP defines how two devices can negotiate the establishment of the link and the exchange of data.
- PPP defines how network layer data are encapsulated in the data link frame.
- PPP defines how two devices can authenticate each other.
- PPP provides multiple network layer services supporting a variety of network layer protocols.
- PPP provides connections over multiple links.
- PPP provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

On the other hand, to keep PPP simple, several services are missing:

- PPP does not provide flow control. A sender can send several frames one after another with no concern about overwhelming the receiver.
- PPP has a very simple mechanism for error control. A CRC field is used to detect errors. If the frame is corrupted, it is silently discarded; the upper-layer protocol needs to take care of the problem. Lack of error control and sequence numbering may cause a packet to be received out of order.
- PPP does not provide a sophisticated addressing mechanism to handle frames in a multipoint configuration.

Framing

PPP is a byte-oriented protocol.

Frame Format

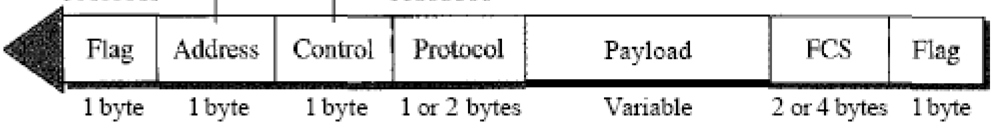


FIGURE 2.24: FRAME FORMAT PPP

- **Flag** A PPP frame starts and ends with a 1-byte flag with the bit pattern 01111110. Although this pattern is the same as that used in HDLC, there is a big difference. PPP is a byte-oriented protocol; HDLC is a bit-oriented protocol. The flag is treated as a byte
- **Address** The address field in this protocol is a constant value and set to 11111111 (broadcast address). During negotiation, the two parties may agree to omit this byte.
- **Control** This field is set to the constant value 11000000 (imitating unnumbered frames in HDLC). PPP does not provide any flow control.
- **Error control** is also limited to error detection. This means that this field is not needed at all,

and again, the two parties can agree, during negotiation, to omit this byte.

- **Protocol** The protocol field defines what is being carried in the data field: either user data or other information. This field is by default 2 bytes long, but the two parties can agree to use only I byte.
- **Payload field** This field carries either the user data or other information .The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation. The data field is byte stuffed if the flag byte pattern appears in this field. Because there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value or the maximum negotiated value.
- **FCS** The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC.

Byte Stuffing

The similarity between PPP and HDLC ends at the frame format. PPP is a byte-oriented protocol totally different from HDLC. As a byte-oriented protocol, the flag in PPP is a byte and needs to be escaped whenever it appears in the data section of the frame. The escape byte is 01111101, which means that every time the flag like pattern appears in the data, this extra byte is stuffed to tell the receiver that the next byte is not a flag.

PPP is a byte-oriented protocol using byte stuffing with the escape byte 01111101.

Transition Phases

A PPP connection goes through phases which can be shown in a transition phase

- Failed
- Carrier
- Dropped
- Terminate
- Done
- Carrier
- Detected
- Failed

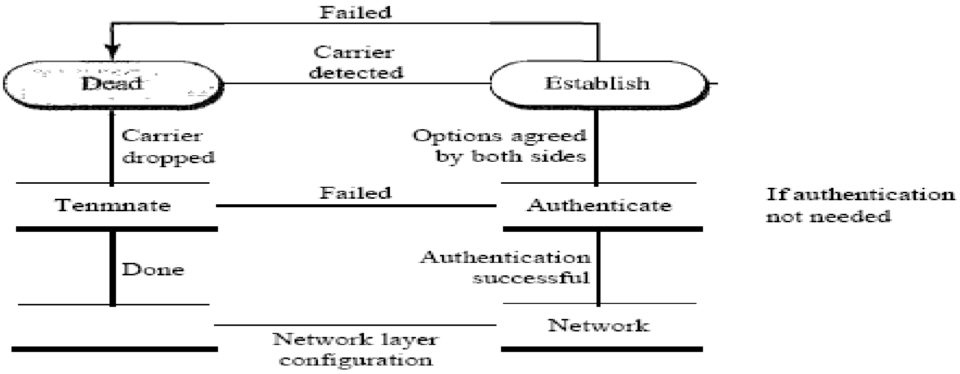


FIGURE 2.25: TRANSITION PHASE PPP

- **Dead** In the dead phase the link is not being used. There is no active carrier (at the physical layer) and the line is quiet.
- **Establish** When one of the nodes starts the communication, the connection goes into this phase. In this phase, options are negotiated between the two parties. If the negotiation is successful, the system goes to the authentication phase (if authentication is required) or directly to the networking phase. The link control protocol packets are used for this purpose. Several packets may be exchanged here.
- **Authenticate** The authentication phase is optional; the two nodes may decide, during the establishment phase, not to skip this phase. However, if they decide to proceed with authentication, they send several authentication packets, If the result is successful, the connection goes to the networking phase; otherwise, it goes to the termination phase.

- **Network** In the network phase, negotiation for the network layer protocols takes place. PPP specifies that two nodes establish a network layer agreement before data at the network layer can be exchanged. The reason is that PPP supports multiple protocols at the network layer. If a node is running multiple protocols simultaneously at the network layer, the receiving node needs to know which protocol will receive the data.
- **Open** In the open phase, data transfer takes place. When a connection reaches this phase, the exchange of data packets can be started. The connection remains in this phase until one of the endpoints wants to terminate the connection.
- **Terminate** In the termination phase the connection is terminated. Several packets are exchanged between the two ends for house cleaning and closing the link.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	What is PPP?	Jun 2010	7
Q.2	Write a brief note on point to point protocol.	Dec 2004 Dec 2009	7
Q.3	Explain any two of the following data link layer protocols giving characteristics features, frame format and applications: (1) HDLC (2) IEE 802.2 LLC (3) PPP	Jun 2014	14

UNIT 2/LECTURE 012/ADDITIONAL TOPIC

Project 802

IEEE802 refers to a family of IEEE standards dealing with local area networks and metropolitan area networks.

More specifically, the IEEE 802 standards are restricted to networks carrying variable-size packets. (By contrast, in cell relay networks data is transmitted in short, uniformly sized units called cells. Isochronous networks, where data is transmitted as a steady stream of octets, or groups of octets, at regular time intervals, are also out of the scope of this standard.) The number 802 was simply the next free number IEEE could assign, though “802” is sometimes associated with the date the first meeting was held — February 1980.

The services and protocols specified in IEEE 802 map to the lower two layers (Data Link and Physical) of the seven-layer OSI networking reference model. In fact, IEEE 802 splits the OSI Data Link Layer into two sub-layers named Logical Link Control (LLC) and Media Access Control (MAC), so that the layers can be listed like this:

- Data link layer
    - LLC Sublayer
    - MAC Sublayer
- Physical layer

The IEEE 802 family of standards is maintained by the IEEE 802 LAN/MAN Standards Committee (LMSC). The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs. An individual Working Group provides the focus for each area.

Working groups[edit]

Name	Description	Note
IEEE 802.1	Bridging (networking) and Network Management	
IEEE 802.2	LLC	inactive
IEEE 802.3	Ethernet	
IEEE 802.4	Token bus	disbanded
IEEE 802.5	Defines the MAC layer for a Token Ring	inactive
IEEE 802.6	MANs (DQDB)	disbanded
IEEE 802.7	Broadband LAN using Coaxial Cable	disbanded
IEEE 802.8	Fiber Optic TAG	disbanded
IEEE 802.9	Integrated Services LAN (ISLAN or isoEthernet)	disbanded
IEEE 802.10	Interoperable LAN Security	disbanded
IEEE 802.11	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	
IEEE 802.12	100BaseVG	disbanded

IEEE 802.13	Unused	Reserved for Fast Ethernet development
IEEE 802.14	Cable modems	disbanded
IEEE 802.15	Wireless PAN	
IEEE 802.15.1	Bluetooth certification	
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	
IEEE 802.15.3	High-Rate wireless PAN (e.g., UWB, etc.)	
IEEE 802.15.4	Low-Rate wireless PAN (e.g., ZigBee, WirelessHART, MiWi, etc.)	
IEEE 802.15.5	Mesh networking for WPAN	
IEEE 802.15.6	Body area network	
IEEE 802.16	Broadband Wireless Access (WiMAX certification)	
IEEE 802.16.1	Local Multipoint Distribution Service	
IEEE 802.17	Resilient packet ring	
IEEE 802.18	Radio Regulatory TAG	
IEEE 802.19	Coexistence TAG	
IEEE 802.20	Mobile Broadband Wireless Access	
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Network	
IEEE 802.23	Emergency Services Working Group	
IEEE 802.24	Smart Grid TAG	New (November, 2012)
IEEE 802.25	Omni-Range Area Network	Not yet ratified

ADDRESSES Four levels of addresses are used in an internet employing the TCP/IP protocols:

- physical (link) addresses
- logical (IP) addresses
- port addresses
- specific addresses

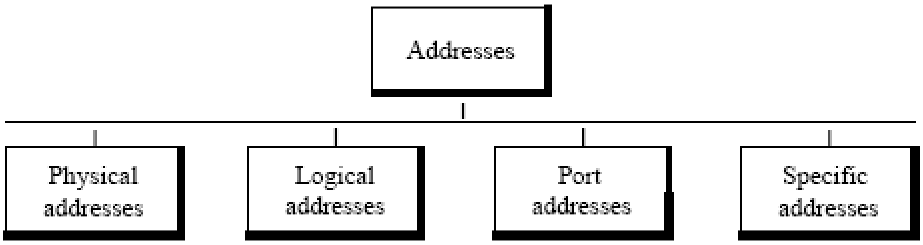


FIGURE 2.26: ADDRESS

- **Physical Addresses** The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address.
  The physical addresses have authority over the network (LAN or WAN). The size and format of these addresses vary depending on the network.

- **Logical Addresses** Logical addresses are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address.

- **Port Addresses** The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet. A system that sends nothing but data from one computer to another is not complete. Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process. For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes.
  In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a port address. A port address in TCP/IP is 16 bits in length.

- **Specific Addresses**
  Some applications have user-friendly addresses that are designed for that specific address. Examples include the e-mail address and the Universal Resource Locator (URL).The first defines the recipient of an e-mail, the second is used to find a document on the World Wide Web. These addresses, however, get changed to the corresponding port and logical addresses by the sending computer.

UNIT –0 3

ALOHA

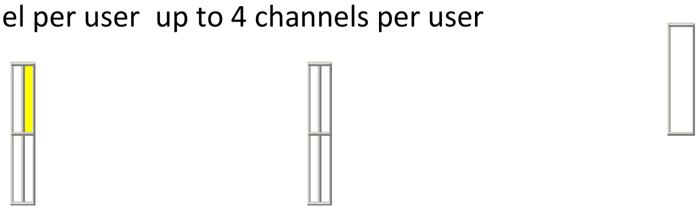
Unit-03/Lecture-01/ Lecture-02

Static Channel Allocation in LANs and MANs[RGPV/Jun 2010, Jun2014]

- **Frequency Division Multiplexing -** Frequency of one channel divided (usually evenly) among n users. Each user appears to have full channel of full frequency/n. Wastes bandwidth when user has nothing to send or receive, which is often the case in data communications. Other users cannot take advantage of unused bandwidth.
- **Time Division Multiplexing** - Time of one channel divided (usually evenly) among n users. Each user appears to have full channel for time/n. same problems as FDM.
- **Analysis of Static Channel Allocation -** Static allocation is intuitively a bad idea when considering that for an n divisions of a channel, any one user is limited to only 1/n channel bandwidth whether other users where accessing the channel or not. By limiting a user to only a fraction of the available channel, the delay to the user is increased over that if the entire channel were available.

  Intuitively, static allocation results in restricting one user to one channel even when other channels are available. Consider the following two diagrams, each with one user wanting to transmit 400 bits over a 1 bit per second channel. The left diagram would have a delay 4 times greater than the diagram on the right, delaying 400 seconds using 1 channel versus 100 second delay using the 4 channels.

  Static Allocation 1 channel per user Dynamic Allocation up to 4 channels per user One user with entire channel



  Generally we want delay to be small. More formally the mean time delay for one channel, T is:

  C = Channel capacity bps (constant). Larger capacity reduces T.
  l = input rate, frames/sec. Smaller input rate reduces T.
  m = average bits per frame. Larger frames reduces T.
  T = 1/ (mC-l) mean time delay

  For each of n sub channels, the mean delay time using FDM (T_{FDM}) is:

  C/n = Channel capacity bps (constant)
  l/n = input rate, frames/sec.
  m = average bits per frame
  T_{FDM} = 1/ (m(C/n)-(l/n)) = n/(mC-l) = nT

  Generally, dividing a channel statically into n channels increases the average delay by a factor of n agreeing with the intuitive result from the diagrams.

Dynamic Channel Allocation in LANs and MANs - Obviously static allocation of a multi-access channel is not generally desirable when overall channel usage is low. Note that channel use is bursty with long periods of inactivity punctuated by short bursts of activity.

Dynamic Channel Allocation Assumptions

- **Station model -** n independent stations each generating frames for transmission. One frame is generated and successfully transmitted at a time.

- **Single channel -** A single channel is shared with other stations.
- **Collision -** Overlapping transmissions destroy the frames, can be detected, and require retransmission. Collisions are the only errors.
- **Time**
    - **Continuous time -** No master clock dividing time, transmissions can begin at any time.
    - **Slotted time -** Master clock, time is divided into discrete intervals (slots), transmissions can only begin at the start of a slot. Slots may contain 0 frames (idle), 1 (a successful transmission), or 2 (a collision).
- **Carrier**
    - **Carrier sense -** Stations can detect whether the channel is in use prior to transmitting. If in use waits for channel to become available.
    - **No carrier sense -** Stations cannot detect whether the channel is in use prior to transmitting. Transmits and later determines whether successful.

ALOHA [RGPV/ Dec 2009,Jun 2010, Dec 2010,Dec 2013,Jun 2014]

ALOHA, the earliest random access method was developed at the University of Hawaii in early 1970. It was designed for a radio (wireless) LAN, but it can be used on any shared medium.
It is obvious that there are potential collisions in this arrangement. The medium is shared between the stations. When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

Pure ALOHA

The original ALOHA protocol is called pure ALOHA. The idea is that each station sends a frame whenever it has a frame to send.
However, since there is only one channel to share, there is the possibility of collision between frames from different stations. Figure shows an example of frame collisions in pure ALOHA.

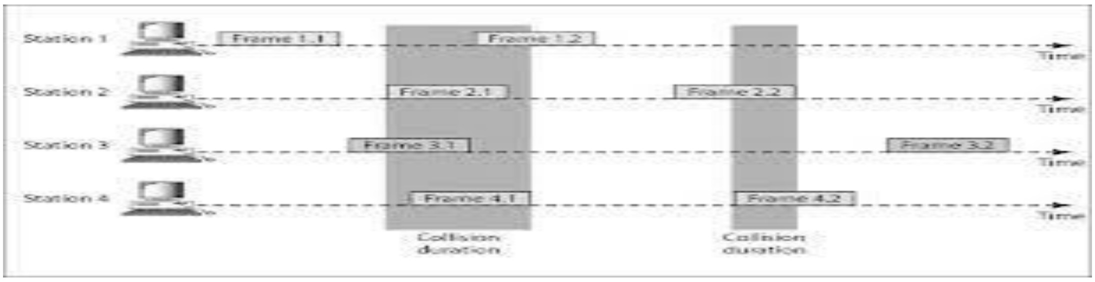


FIGURE 3.1: PURE ALOHA

There are four stations (unrealistic assumption) that contend with one another for access to the shared channel. The figure shows that each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames survive: frame 1.1 from station 1 and frame 3.2 from station 3. We need to mention that even if one bit of a frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed.
It is obvious that we need to resend the frames that have been destroyed during transmission. The pure ALOHA protocol relies on acknowledgments from the receiver.
When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.
A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again. Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the back-off time TB.

Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames. After a maximum number of retransmission attempts Kmax' a station must give up and try later. The time-out period is equal to the maximum possible round-trip propagation delay, which is twice the amount of time required to send a frame between the two most widely separated stations (2 x Tp)' The back-off time TB is a random value that normally depends on K (the number of attempted unsuccessful transmissions). The formula for TB depends on the implementation. One common formula is the **binary exponential back-off.** In this method, for each retransmission, a multiplier in the range 0 to 2K - 1 is randomly chosen and multiplied by Tp (maximum propagation time) or Tfr (the average time required to send out a frame) to find TB' Note that in this procedure, the range of the random numbers increases after each collision. The value of Kmax is usually chosen as 15.

Vulnerable time Let us find the length of time, the **vulnerable time,** in which there is a possibility of collision. We assume that the stations send fixed-length frames with each frame taking Tfr S to send. Figure 12.5 shows the vulnerable time for station A.

Vulnerable time = 2 X Tfr

Station A sends a frame at time t. Now imagine station B has already sent a frame between t - Tfr and t. This leads to a collision between the frames from station A and station B. The end of B's frame collides with the beginning of A's frame. On the other hand, suppose that station C sends a frame between t and t + Tfr . Here, there is a collision between frames from station A and station C. The beginning of C's frame collides with the end of A's frame.

We see that the vulnerable time, during which a collision may occur in pure ALOHA, is 2 times the frame transmission time.

Pure ALOHA vulnerable time = 2 x Tfr

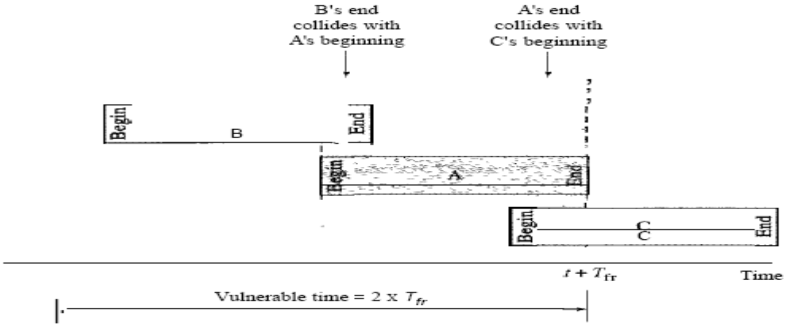

B's end collides with A's beginning
A's end collides with C's beginning
Begin
B
End
Begin
A
End
Begin
C
End
$t + T_{fr}$
Time
Vulnerable time = 2 x T_{fr}

FIGURE 3.2: VULNERABLE TIME PURE ALOHA

Throughput Let us call G the average number of frames generated by the system during one frame transmission time. Then it can be proved that the average number of successful transmissions for pure ALOHA is S = G x e-2G.
he maximum throughput Smax is 0.184, for G = 1.
In other words, if one-half a frame is generated during one 2 frame transmission time (in other words, one frame during two frame transmission times), then 18.4 percent of these frames reach their destination successfully. This is an expected result because the vulnerable time is 2 times the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time (and no other stations generate a frame during this time), the frame will reach its destination successfully.
The throughput for pure ALOHA is S =G x e-2G.
The maximum throughput Smax =0.184 when G = (1/2).

Slotted ALOHA

Pure ALOHA has a vulnerable time of 2 x Tfr . This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
In slotted ALOHA we divide the time into slots of Tfr s and force the station to send only at the beginning of the time slot. Figure shows an example of frame collisions in slotted ALOHA.

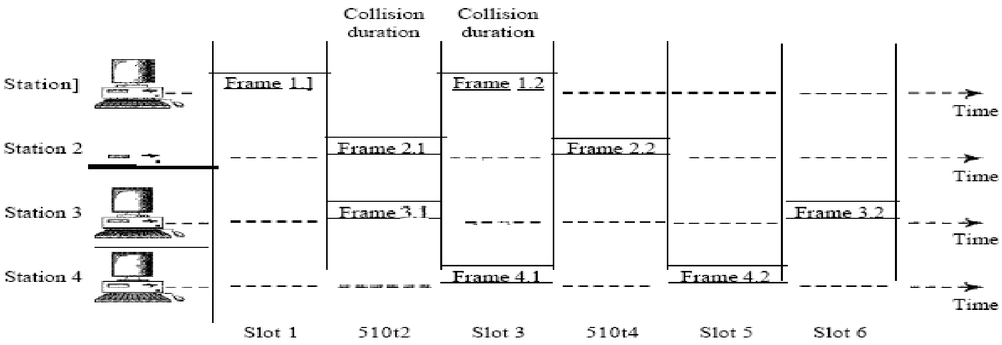
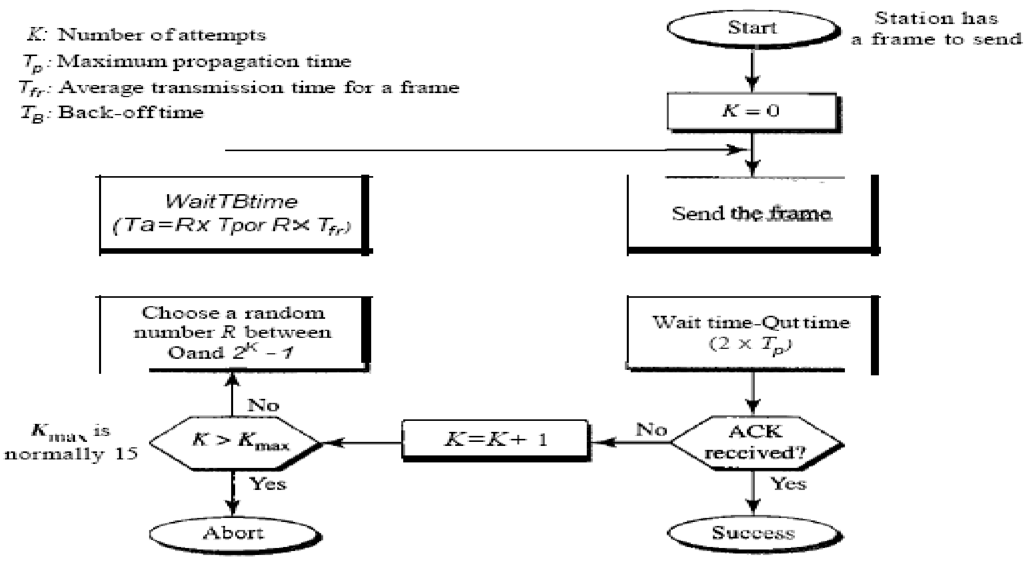


FIGURE 3.3: SLOTTED ALOHA

Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame. Of course, there is still the possibility of collision if two stations try to send at the beginning of the same time slot. However, the vulnerable time is now reduced to one-half, equal to Tfr.
It shows that the vulnerable time for slotted ALOHA is one-half that of pure ALOHA.

Slotted ALOHA vulnerable time = Tfr
Throughput It can be proved that the average number of successful transmissions for slotted ALOHA is S = G x e-G. The maximum throughput Smax is 0.368, when G = 1.
In other words, if a frame is generated during one frame transmission time, then 36.8 percent of these frames reach their destination successfully. This result can be expected because the vulnerable time is equal to the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time (and no other station generates a frame during this time), the frame will reach its destination successfully.
The throughput for slotted ALOHA is S =: G x e-G.
The maximum throughput Smax == 0.368 when G=1.

Vulnerable time for slotted ALOHA protocol= Tfr



K: Number of attempts
Tp: Maximum propagation time
Tfr: Average transmission time for a frame
TB: Back-off time
Start
Station has a frame to send
K = 0
Send the frame
WaitTBtime (Ta=Rx Tpor R× Tfr)
Choose a random number R between Oand 2^K - 1
Wait time-Qut time (2 × Tp)
No
Kmax is normally 15
K > Kmax
K=K+ 1
No
ACK received?
Yes
Yes
Abort
Success

FIGURE 3.4: ALOHA FLOW DIAGRAM

Comparison between pure and slotted aloha

ALOHA is a medium access protocol that was originally designed for ground based radio broadcasting
however it is applicable to any system in which uncoordinated users are competing for the use of a shared channel. Pure ALOHA and slotted ALOHA are the two versions of ALOHA.

Pure ALOHA uses a very simple idea that is to let users transmit whenever they have data to send. Pure ALOHA is featured with the feedback property that enables it to listen to the channel and finds out whether the frame was destroyed. Feedback is immediate in LANs but there is a delay of 270 msec in the satellite transmission. It requires acknowledgment if listening to the channel is not possible due to some reason. It can provide a channel utilization of 18 percent that is not appealing but it gives the advantage of transmitting any time.

Slotted ALOHA divides time into discrete intervals and each interval corresponds to a frame of data. It requires users to agree on slot boundaries. It does not allow a system to transmit any time. Instead the system has to wait for the beginning if the next slot.

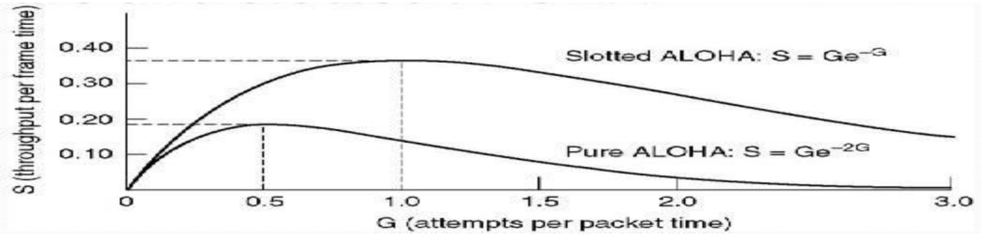


FIGURE 3.5: THROUGHPUT ALOHA

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	What is static & dynamic allocation?	Jun 2010	7
Q.2	Write short note on ALOHA?	Dec 2003 June2005	7
Q.3	Derive an expression to prove that throughput of Slotted Aloha is approximately twice than that of Pure Aloha?	JUN 2004 Dec 2006 Jun 2009 Dec 2010 Jun 2011	7
Q.4	Derive a relationship between offered traffic and throughput in Slotted Aloha.	Jun 2006	7
Q.5	A pure aloha network transmits 200 bits frames on a shared channel of 200 kbps. What is the throughput if the system produces 1000 frames/second?	Dec 2013	7
Q.6	Define the throughput of pure aloha? A pure aloha network transmits 200 bit frames on a shared channel of 200kbps. What is the throughput if the system(all station together) produces- (i) 1000 frames per second (ii) 500 frames per second (iii) 250 frames per second	Jun 2013	7
Q.7	Name different types of static and dynamic channel allocation policies of MAC sublayer. Compare static and dynamic channel allocation strategies under the heading of advantaged and disadvantages.	Jun 2014	7
Q.8	Explain giving neat sketches pure and slotted	Jun 2014	7

	ALOHA?		

Unit-03/Lecture-03

CSMA

Carrier Sense Multiple Access (CSMA)

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending. In other words, CSMA is based on the principle **"sense before transmit"** or **"listen before talk."**

CSMA can reduce the possibility of collision, but it cannot eliminate it. The reason is, a space and time model of a CSMA network. Stations are connected to a shared channel (usually a dedicated medium).

The possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (although very short) for the first bit to reach every station

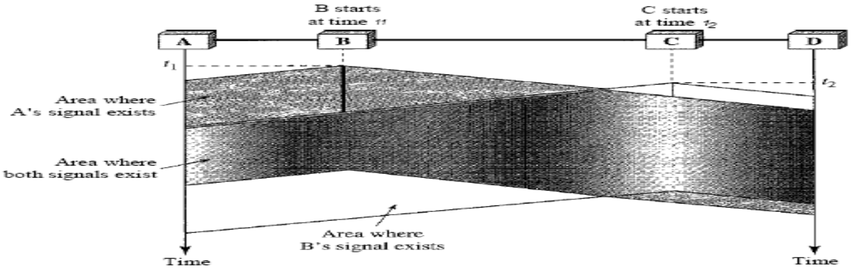

B starts at time t_1
C starts at time t_2
A
B
C
D
t_1
t_2
Area where A's signal exists
Area where both signals exist
Area where B's signal exists
Time
Time

FIGURE 3.6: CSMA

Vulnerable Time

The vulnerable time for CSMA is the propagation time Tp . This is the time needed for a signal to propagate from one end of the medium to the other. When a station sends a frame, and any other station tries to send a frame during this time, a collision will result. But if the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending.

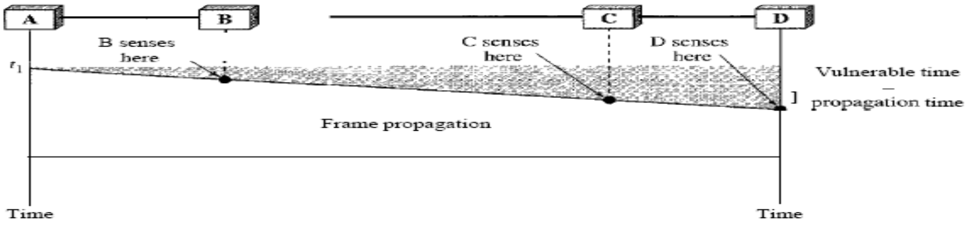


FIGURE 3.7: VULNERABLE TIME CSMA

Persistent Method

- **1-Persistent** 1-persistent method is simple and straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability 1). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

- **Nonpersistent** In the nonpersistent method**,** a station that has a frame to send senses the line. If the line is idle, it sends immediately.

- **P-Persistent The p-persistent method** is used if the channel has time slots with slot duration equal to or greater than the maximum propagation time. The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency. In this method, after the station finds the line idle it follows these steps:
  1. With probability p, the station sends its frame.
  2. With probability q = 1 - p, the station waits for the beginning of the next time slot and checks the line again.
     a. If the line is idle, it goes to step 1.
     b. If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.

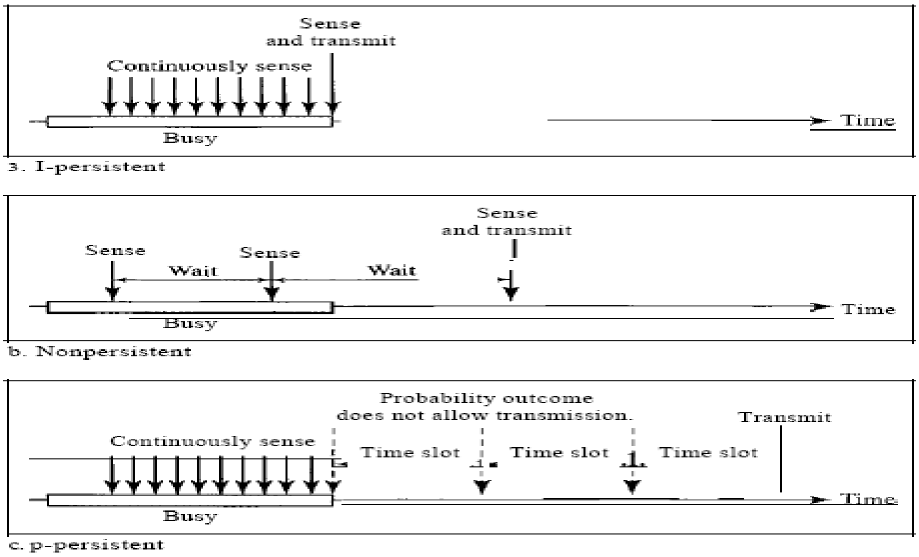


FIGURE 3.8: PERSISTENT METHOD CSMA

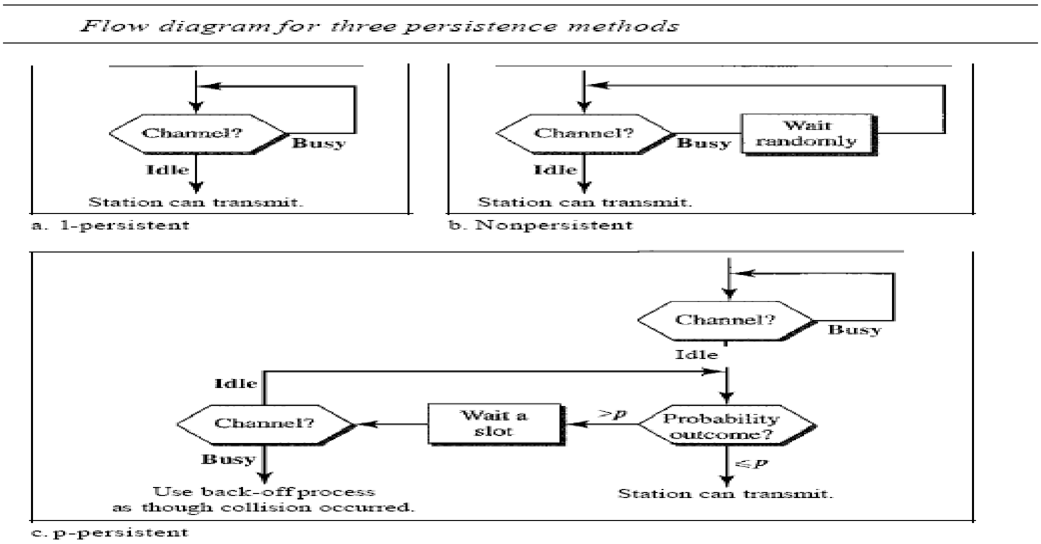


FIGURE 3.9: PERSISTENT METHOD FLOE DIAGRAM

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain the following CSMA protocol- (i)1 persistent (ii) p-persistent (iii) non-persistent	Dec.2003 Dec 2006 Dec 2011	7
Q.2	In p-persistent CSMA the value of p is wrongly estimated. How will it affected the network performance?	June.2013	7
Q.3	Explain CSMA protocols & give their best channel utilization.	Dec.2011	7

Unit-03/Lecture-04

CSMA / CD

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)[RGPV/Jun 2005, Jun 2007, Jun 2009, Jun 2011, Dec 2012, Dec 2013]

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

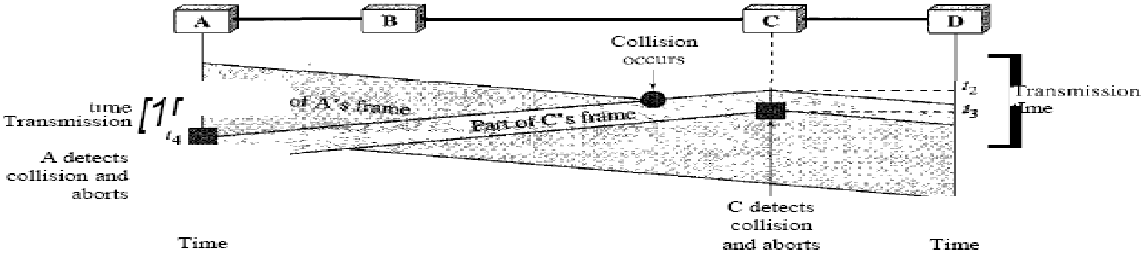


FIGURE 3.10: CSMA/CD

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.

To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision. Although each station continues to send bits in the frame until it detects the collision, we show what happens as the first bits collide. In stations A and C are involved in the collision.

At time t1, station A has executed its persistence procedure and starts sending the bits of its frame. At time t2, station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right. The collision occurs sometime after time t2' Station C detects a collision at time t3 when it receives the first bit of A's frame. Station C immediately (or after a short time, but we assume immediately) aborts transmission. Station A detects collision at time t4 when it receives the first bit of C's frame; it also immediately aborts transmission. Looking at the figure, we see that A transmits for the duration t4 – t1; C transmits for the duration t3 - t2. The length of any frame divided by the bit rate in this protocol must be more than either of these durations. At time t4, the transmission of A:s frame, though incomplete, is aborted; at time t3, the transmission of B's frame, though incomplete, is aborted. Now that we know the time durations for the two transmissions.

Minimum Frame Size

For CSMA/CD to work, we need a restriction on the frame size. Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission. This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection. Therefore, the frame transmission time Tfr must be at least two times the maximum propagation time Tp. To understand the reason, let us think about the worst-case scenario. If the two stations involved in a collision are the maximum distance apart, the signal from the first takes time Tp to reach

the second, and the effect of the collision takes another time Tp to reach the first. So the requirement is that the first station must still be transmitting after 2Tp.

CSMA/CD VS. ALOHA protocol

- The first difference is the addition of the persistence process. We need to sense the channel before we start sending the frame by using one of the persistence processes (non persistent, I-persistent, or p-persistent). The corresponding box can be replaced by one of the persistence processes.
- The second difference is the frame transmission. In ALOHA, we first transmit the entire frame and then wait for an acknowledgment. In CSMA/CD, transmission and collision detection is a continuous process. We do not send the entire frame and then look for a collision. The station transmits and receives continuously and simultaneously (using two different ports). We use a loop to show that transmission is a continuous process. We constantly monitor in order to detect one of two conditions: either transmission is finished or a collision is detected. Either event stops transmission. When we come out of the loop, if a collision has not been detected, it means that transmission is complete; the entire frame is transmitted. Otherwise, a collision has occurred.
- The third difference is the sending of a short jamming signal that enforces the collision in case other stations have not yet sensed the collision.

Throughput

The throughput of CSMA/CD is greater than that of pure or slotted ALOHA. The maximum throughput occurs at a different value of G and is based on the persistence method and the value of p in the p-persistent approach. For I-persistent method the maximum throughput is around 50 percent when G =1. For non persistent method, the maximum throughput can go up to 90 percent when G is between 3 and 8.

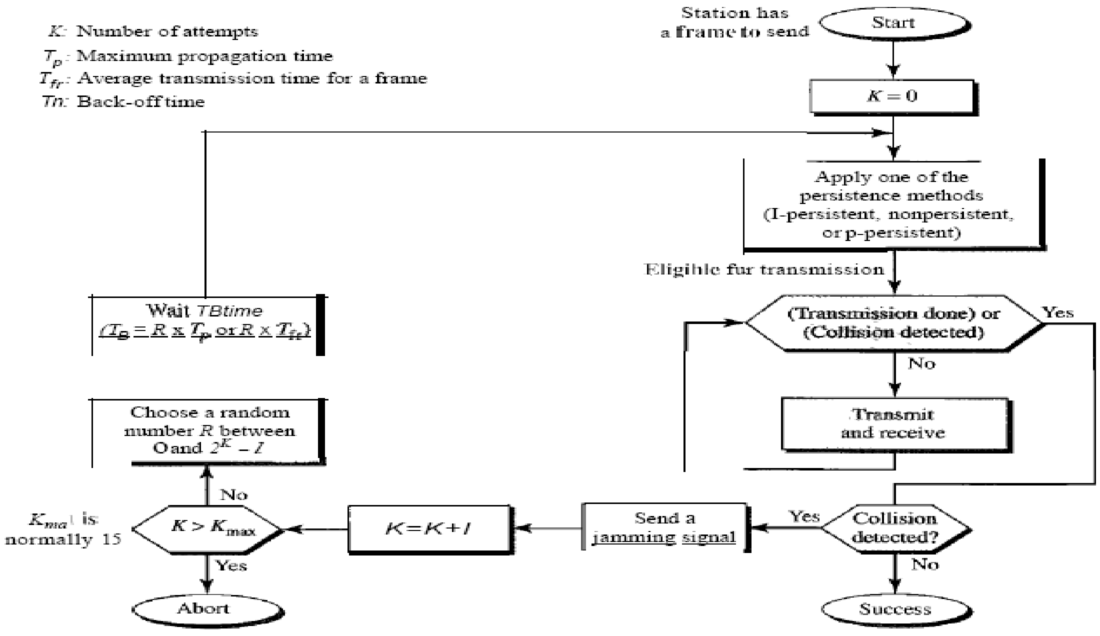

K: Number of attempts
T_p: Maximum propagation time
T_{fr}: Average transmission time for a frame
Tn: Back-off time
Station has a frame to send
Start
K = 0
Apply one of the persistence methods (I-persistent, nonpersistent, or p-persistent)
Eligible fur transmission
(Transmission done) or (Collision detected)
Yes
No
Transmit and receive
Collision detected?
Yes
No
Success
Send a jamming signal
K=K+I
K > Kmax
Kmax is normally 15
Yes
Abort
No
Choose a random number R between O and $2^K - I$
Wait TBtime ($T_B = R \times T_p$ or $R \times T_{fr}$)

FIGURE 3.11: CSMA/CD FLOW DIAGRAM

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Write short notes on CSMA/CD protocol. Discuss collision free protocol.	Jun 2005 Jun 2009, 11	7

Q.2	How does CSMA/CD protocol improve the performance over CSMA protocol for long frames?	Jun 2007	7
Q.3	Describe about CSMA/CD protocol.	Dec 2013	7
Q.4	With the aid of sketch, explain how a collision can occur with the CSMA/CD MAC method. Explain the meaning of the terms: (i) Interframe gap (ii) Jam sequence (iii) Slot time And hence, with the help of flow charts, describe the principle of operation of the transmit and receive sections of the MAC sublayer.	Dec 2012	7
Q.4	Explain how CSMA/CD works in Ethernet based LANs?	Jun 2014	3.5

Unit-03/Lecture-05

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

The basic idea behind CSMA/CD is that a station needs to be able to receive while transmitting to detect a collision. When there is no collision, the station receives one signal: its own signal. When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station. To distinguish between these two cases, the received signals in these two cases must be significantly different. In other words, the signal from the second station needs to add a significant amount of energy to the one created by the first station.

In a wired network, the received signal has almost the same energy as the sent signal because either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver. This means that in a collision, the detected energy almost doubles.

Collisions are avoided through the use of CSMA/CA's three strategies:

- The Interframe Space(IFS)
- The Contention Window
- Acknowledgments

Interframe Space (IFS)

First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS. Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting.

The distant station's signal has not yet reached this station. The IFS time allows the front of the transmitted signal by the distant station to reach this station. If after the IFS time the channel is still idle, the station can send, but it still needs to wait a time equal to the contention time (described next). The IFS variable can also be used to prioritize stations or frame types. For example, a station that is assigned shorter IFS has a higher priority.

In CSMA/CA, the IFS can also be used to define the priority of a station or a frame.

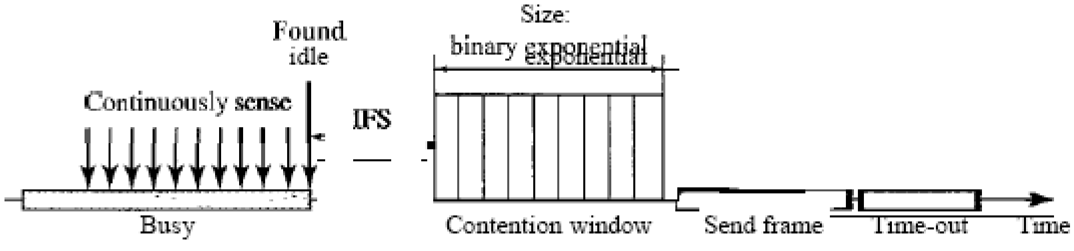


FIGURE 3.12: CSMA/CA

Contention Window

The 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. This means that it is set to 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. One interesting point about the contention window is that the station needs to sense the channel after each time slot. However, if the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time.

In CSMA/CA, if the station finds the channel busy, it does not restart the timer of the contention window; it stops the timer and restarts it when the channel becomes idle.

Acknowledgment

With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

Procedure

The channel needs to be sensed before and after the IFS. The channel also needs to be sensed during the contention time. For each time slot of the contention window, the channel is sensed. If it is found idle, the timer continues; if the channel is found busy, the timer is stopped and continues after the timer becomes idle again.

Figure 12.17 *Flow diagram for CSMA/CA*

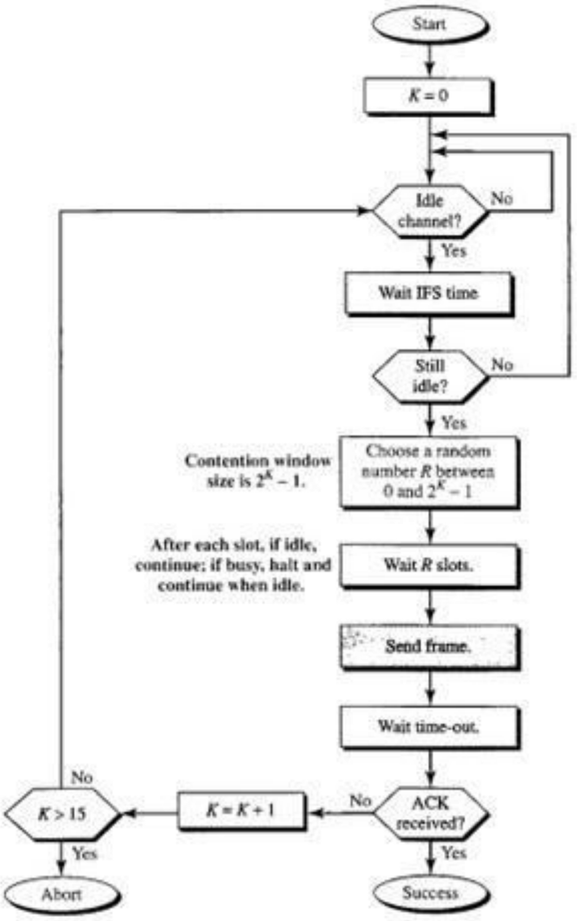

Start
$K = 0$
Idle channel?
No
Yes
Wait IFS time
Still idle?
No
Yes
Contention window size is $2^K - 1$.
Choose a random number R between 0 and $2^K - 1$
After each slot, if idle, continue; if busy, halt and continue when idle.
Wait R slots.
Send frame.
Wait time-out.
No
$K > 15$
$K = K + 1$
No
ACK received?
Yes
Yes
Abort
Success

FIGURE 3.13: CSMA/CA FLOW DIAGRAM

UNIT 03/LECTURE 06

IEEE 802.4 TOKEN BUS

Token bus network[RGPV/ Dec 2009, Dec 2012]

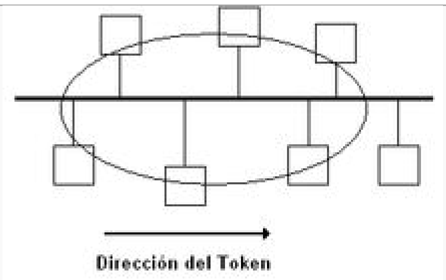


FIGURE 3.14: TOKEN PASSING IN A TOKEN BUS NETWORK

Token bus is a network implementing the token ring protocol over a "virtual ring" on a coaxial cable. A token is passed around the network nodes and only the node possessing the token may transmit. If a node doesn't have anything to send, the token is passed on to the next node on the virtual ring. Each node must know the address of its neighbor in the ring, so a special protocol is needed to notify the other nodes of connections to, and disconnections from, the ring.

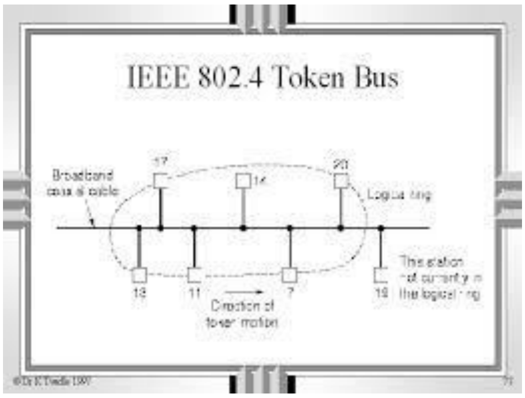

IEEE 802.4 Token Bus

FIGURE 3.15: TOKEN BUS

Token bus was standardized by IEEE standard 802.4. It is mainly used for industrial applications. This is an application of the concepts used in token ring networks. The main difference is that the endpoints of the bus do not meet to form a physical ring.

Due to difficulties handling device failures and adding new stations to a network, token bus gained a reputation for being unreliable and difficult to upgrade.

Frame format

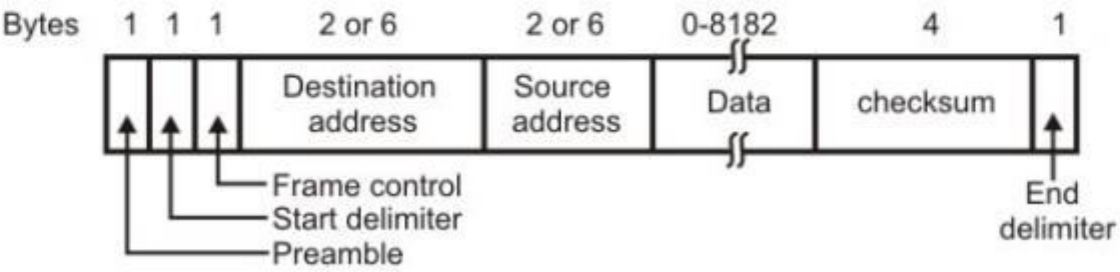


FIGURE 3.16: TOKEN BUS FRAME FORMAT

- Preamble – clock synchronization

• Starting and ending delimiter
• frame boundaries
– analog encoding symbols (other than 0 or 1)
– does not occur in analog dat
• no need of length field
• Frame Control
– Successors,
– predecessors
– Entry of new station
– Claim token
- Token lost, station with token dead
– Protocols to handle all issues
– Useful for real time traffic

Advantages and disadvantages of 802.4
Advantages

- Uses cable TV cables and parts readily and cheaply available.
- Deterministic and able to prioritize traffic.
- Short minimum frames.
- Excellent performance under conditions of high load.
- Broadband can support multiple channels (for example, video and voice)

Disadvantages

- Complex protocol and engineering of equipment.
- Expensive; requires modems and repeaters.
- Since node must wait for token to come around before transmitting, messages are delayed waiting for token even when network is idle.

S.NO	RGPV QUESTION	YEAR	MARKS
Q.1	What is 802.4? How token is passed in the ring? Give advantages and disadvantages of 802.4.	Dec 2009	7
Q.2	Write short notes on IEEE 802.4	Dec 2012	7

UNIT 03/LECTURE 07

IEEE 802.5 TOKEN RING

Star-wired ring topology

The star-wired ring topology is a circular connection of workstations. The star-wired ring is essentially a marriage of the earlier ring topology to the star-wired topology. Since star-wired ring topologies support baseband signals, the star-wired ring is capable of supporting only one channel of information. This channel of information flows in one direction around the ring, moving from workstation to workstation. Since the star-wired ring is a closed loop of wire, it is important for some device to remove a circling piece of data from the ring; otherwise, the piece of data will keep circling. The device that removes the data is the workstation that originally transmitted the data.

Although the logical organization of the workstations in a star-wired ring topology is circular, the physical organization of a star-wired ring is not circular. Physically, a star-wired ring looks much like a star-wired bus design, with all its workstations connected to a central device. This central device is not a hub but a multistation access unit. A Multistation Access Unit (MAU) accepts data from a workstation and transmits this data to the next workstation downstream in the ring.

An MAU is quite a bit different from a hub in that it does not send a copy of the incoming data immediately out to every connection. If a workstation is not connected to a particular port on the MAU, that port simply closes itself so that a continuous ring is maintained. Thus, a ring topology based on MAUs is commonly referred to as a star-wired ring topology. As with hubs in the star-wired bus design, it is possible to interconnect multiple MAUs to extend the size of a star-wired ring local area network. As the data passes around the ring in the first MAU, it encounters the connector to the second MAU. The signal then passes over the cable to the second MAU and begins its journey around the ring in the second MAU. When all workstations have been accessed on the second MAU, the signal passes again over the cable and returns to the first MAU.

The star-wired ring topology has many of the same advantages as the star-wired bus topology. The star-wired ring topology is based on twisted pair wiring, and because it makes installing new workstations easy, it is easy to maintain. Some of the disadvantages of star-wired rings include slower transmission speeds, higher costs, and more complex software. Because of these disadvantages, and the fact that star-wired buses have pretty much taken over the local area network market, the star-wired ring is close to extinction.

Token Ring

The token ring local area network uses the star-wired ring topology for the hardware and a round robin protocol for the software. It operates on the principle that to transmit data onto the ring, your workstation must be currently in possession of software token. There is typically only one token in the entire network, so only one workstation may transmit at a time. When a workstation has completed its transmission, it passes the token on to the downstream neighboring workstation. Only the workstation holding the token can transmit, so there is no need for any workstation to listen for a collision while transmitting, because collisions cannot occur.

As has been mentioned, collisions are one of the main problems of CSMA/CD. As the number of concurrent users rises, the number of collisions rises. As the collisions rise, more workstations are forced to retransmit their messages, and overall throughput declines. Since the token ring does not experience any collisions, overall throughput remains high even under heavy loads. This ability of token ring to give every workstation a turn is attractive and is valuable for applications that require uniform response times. Since the order of transmission by each workstation is known, the wait time to transmit can be determined (as opposed to being unpredictable); thus, token ring is a deterministic protocol.

Let's take a quick look at how the token ring protocol works. Consider, in which Station A has just released the token. Since Station B is the next downstream neighbor from Station A, and Station B has data to transmit on the ring, Station B seizes the token. After seizing the token, Station B transmits its data, which is destined for Station M. As Station M copies in the data frame, the data continues around the ring until it returns to Station B, which removes the data from the ring. After Station B has removed its data from the ring, it passes the token to Station C.

Frame format

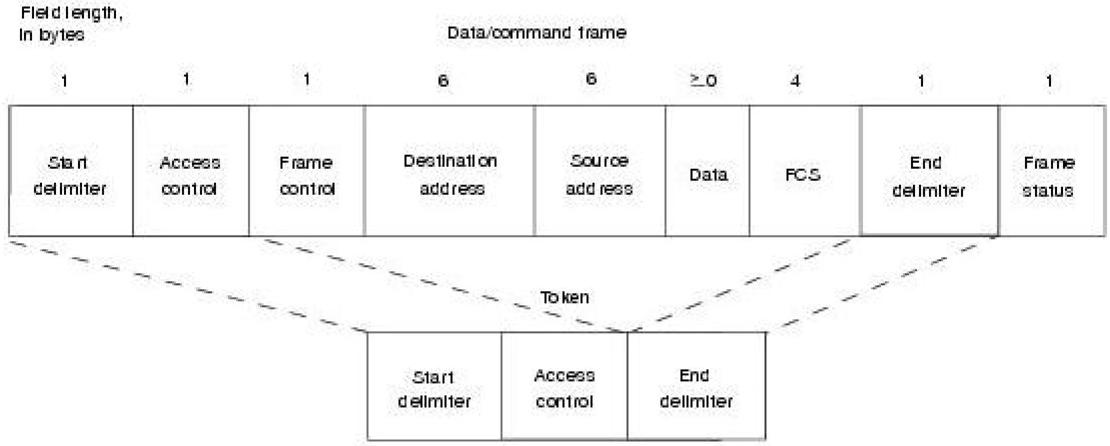


FIGURE 3.17: TOKEN RING FRAME FORMAT

Token Frame Fields

The three token frame fields are summarized in the descriptions that follow:

- **Start delimiter** Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control byte** Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
- **End delimiter** - Signals the end of the token or data/command frame. This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

Data/Command Frame Fields

Data/command frames have the same three fields as Token Frames, plus several others. The Data/command frame fields are described in the following summaries:

- **Start delimiter** Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.

- **Access-control byte** Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
- **Frame-control bytes** Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.
- **Destination and source addresses** Consists of two 6-byte address fields that identify the destination and source station addresses.
- **Data** Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.
- **Frame-check sequence (FCS)** is filed by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
- **End Delimiter** Signals the end of the token or data/command frame. The end delimiter also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.
- **Frame Status** is a 1-byte field terminating a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

Advantages and disadvantages of 802.5

A major disadvantage of the token ring access protocol is the complexity of the software needed to maintain the token. This software has to address important questions such as:

- What happens if the token disappears? (A workstation does not forward it)
- If the token disappears, who generates a new token?
- Is it possible for two stations to generate a token, thus resulting in two tokens on the ring?

Although token ring has the definite advantage of being a deterministic protocol and performing quite well under heavy loads, it has had a difficult time competing with CSMA/CD networks. An overwhelming majority of local area networks use CSMA/CD as the medium access control protocol of choice. Some reasons that CSMA/CD is more popular than token ring are:

- CSMA/CD was the first local area network medium access control method, and thus got a good jump on installations and support.
- Token ring local area networks have almost always lagged behind CSMA/CD networks with regard to transmission speed. When CSMA/CD first became popular, the typical transmission speed was 10 Mbps. Token ring, when it first appeared, had a transmission speed of only 4 Mbps. For a while, token ring jumped ahead with a 16-Mbps version, but CSMA/CD caught up with a 100-Mbps version, and then a 1000-Mbps version. Token ring finally announced a 100-Mbps version, but this was too late to save the protocol in the marketplace. Many people feel it will just be a matter of time before token ring fades into the history books.
- CSMA/CD is less expensive to implement, due in part to its widespread marketing and acceptance. CSMA/CD is a simpler protocol.

Comparison of IEEE 802.3, IEEE 802.4 and IEEE 802.5 Standards

Sr.No	Parameter of comparison	802.3 Ethernet	802 4Token Bus	802.5Token Ring
1	Physical	Linear	Linear	Ring

	topology			
2	Logical topology	None	Ring	Ring
3	Contention	Random chance	By token	By token
4	Adding stations	A new station can be added almost anywhere on the cable at any time.	Distributed algorithms are needed to add new stations.	Must be added between two specified stations.
5	Performance	Stations often transmit immediately under light loads, but heavy traffic can reduce the effective data to nearly 0.	Stations must wait for the token even if no other station is transmitting. Under heavy load, token passing provides fair access to all stations.	Stations must wait for the token even if no other station is transmitting. Under heavy loads, token passing provides fair access to all stations.
6	Maximum delay before transmitting	None	Bounded, depending on distance spanned and number of stations.	Bounded, depending on distance spanned and number of stations. However, if priorities are used, a low priority station may have no maximum delay.
7	Maintenance	No central maintenance	Distributed algorithm provide maintenance	A designated monitor station performs maintenance.
8	Cable used	Twisted pair, co-axial fiber optic	co axial	Twisted pair and fiber optic.
9	Cable length	50 to 2000 m	200 to 500 m	50 to 2000 m
10	Frame	l0Mbps to 100 Mbps	10Mbps	4 to l00Mbps
11	structure	1500 bytes	8191 bytes	5000 bytes

NO	RGPV QUESTION	YEAR	MARKS
Q.1	Explain the working of IEEE 802.5 with the help of neat diagram. Give two reasons why not to choose token ring.	Dec 2010	7
Q.2	Discuss the compare IEEE 802.3, IEEE 802.4 and IEEE 802.5 Standards	Jun 2004	7

UNIT 03/LECTURE 08

FDDI

Fiber Distributed Data Interface (FDDI)[RGPV/Dec 2009, Jun 2011, Dec 2011, Dec 2012, Jun 2013]

Fiber distributed data interface (FDDI) is a local area network protocol standardized by ANSI and the ITU- T (ITU- T X.3). It supports data rates of 100 Mbps and provides a high-speed alternative to Ethernet and Token Ring. When FDDI was designed, speeds of 100 Mbps required fiber-optic cable. Today, however, comparable speeds are available using copper cable. The copper version of FDDI is known as CDDI.

Access Method: Token Passing

In FDDI, access is limited by time. A station may send as many frames as it can within its allotted access period, with the proviso that real-time data be sent first.

To implement this access mechanism, FDDI differentiates between two types of data frames: synchronous and asynchronous. Synchronous here refers to information that is real-time, while asynchronous refers to information that is not. These frames are usually called S-frames and A-frames.

Each station that captures the token is required to send S-frames first. In fact, it must send its S-frames whether or not it's time allotment has run out. Any remaining time may then be used to send A-frames. To understand how this mechanism ensures fair and timely link access, it is necessary to understand the FDDI time registers and timers.

Time Registers

FDDI defines three time registers to control circulation of the token and distribute link access opportunities among the nodes equitably. Values are set when the ring is initialized and do not vary in the course of operation. The registers are called synchronous allocation (SA), target token rotation time (TTRT), and absolute maximum time (AMT).

- **Synchronous Allocation (SA)** The SA register indicates the length of time allowed each station for sending synchronous data. This value is different for each station and is negotiated during initialization of the ring.

- **Target Token Rotation Time (TTRT)** The TTRT register indicates the **average time required** for a token to circulate around the ring exactly once (the **elapsed time between a token's arrival at a given station and its next arrival at the same station**). Because it is an **average**, the actual time of any rotation may be greater or less than this value.

- **Absolute Maximum Time (AMT)** The AMT register holds a value equal to twice the TTRT. A token may not take longer than this time to make one rotation of the ring. If it does, some station or stations are monopolizing the network and the ring must be reinitialized.

Timers

Each station contains a set of timers that enable it to compare actual timings with the values contained in the registers. Timers can be set and" reset, and the_ values decremented or incremented at a rate set by the system clock. The two timers used by FDDI are called the token rotation timer (TRT) and token holding timer (THT).

- **Token Rotation Timer (TRT)** The TRT runs continuously and measures the **actual time** taken by the token to complete a cycle. In our implementation, we use an incrementing TRT for simplicity, although some implementations may use a decrementing timer.
- **Token Holding Timer (THT)** The THT begins running as soon as the token is received. Its function is to show how much time remains for sending asynchronous frames once the synchronous frames have been sent. In our implementation, we use a decrementing THT for simplicity, although some implementations may use an incrementing one. In addition, we allow the value of THT to become negative (to make the concept easier to understand) although a real timer may stay at zero.

Station Procedure

When a token arrives, each station follows this procedure:
1. THT is set to the difference between TTRT and TRT (THT = TIRT - TRT).
2. TRT is reset to zero (TRT = 0).
3. The station sends its synchronous data.
4. The station sends asynchronous data till the value of THT is positive.

Addressing

FDDI uses a six-byte address, which is imprinted on the NIC card similar to Ethernet addresses.

Electrical Specification

Signaling (Physical Layer)

FDDI uses a special encoding mechanism called four bits/five bits (4B/5B). In this system, each four-bit segment of data is replaced by a five-bit code before being encoded in NRZ-I. The NRZ-I used here inverts on the 1.

Encoding

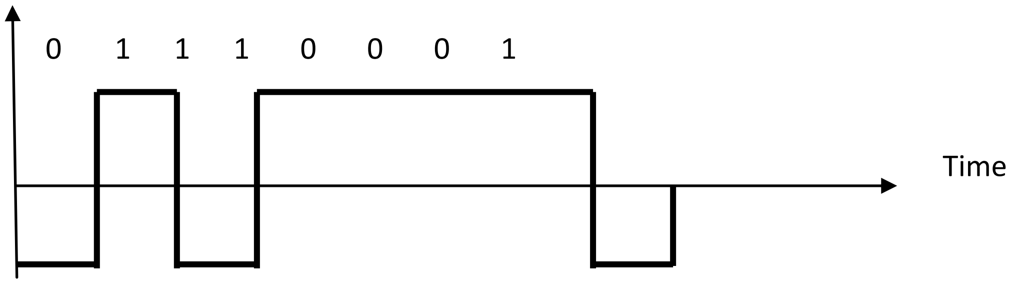


FIGURE 3.18: FDDI

The reason for this extra encoding step is that, although NRZ-I provides adequate synchronization under average circumstances, sender and receiver may go out of synchronization anytime the data includes a long sequence of 0s. 4B/5B encoding transforms each four-bit data segment into a five bit unit that contains no more than two consecutive 0s. Each of the 16 possible four-bit patterns is assigned a five-bit pattern to represent it. These five-bit patterns have been carefully selected so that even sequential data units cannot result in sequences of more than three 0s (none of the five-bit patterns start with more than one 0 or end with more than two 0s);

Data Rate

FDDI supports data rates up to 100 Mbps.

Frame Format

The FDDI standard divides transmission functions into four protocols: physical medium dependent (PMD), physical (PHY), media access control (MAC), and logical link control (LLC). These protocols correspond to the physical and data link layers of the OSI model. In addition, the standard specifies a fifth protocol (used for station management).

FDDI Layers

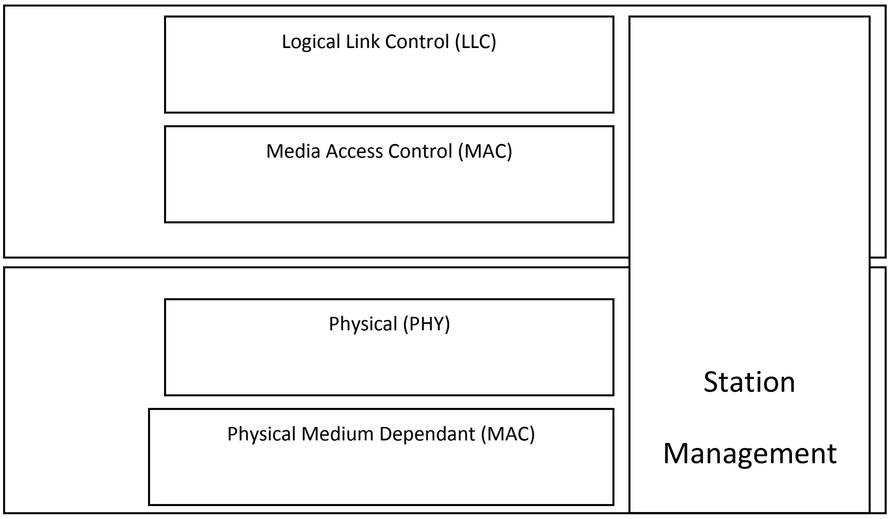

Logical Link Control (LLC)
Media Access Control (MAC)
Physical (PHY)
Physical Medium Dependant (MAC)
Station
Management

FIGURE 3.19: FDDI LAYER

Logical Link Control
The LLC layer is similar to that defined in the IEEE 802.2 protocols.

Media Access Control
The FDDI MAC layer is almost identical to that defined for Token Ring. However. although the functions are similar, the FDDI MAC frame itself is different enough to warrant an independent discussion of each field

Each frame is preceded by 16 idle symbols (1111), for a total of 64 bits to initialize clock synchronization with the receiver.

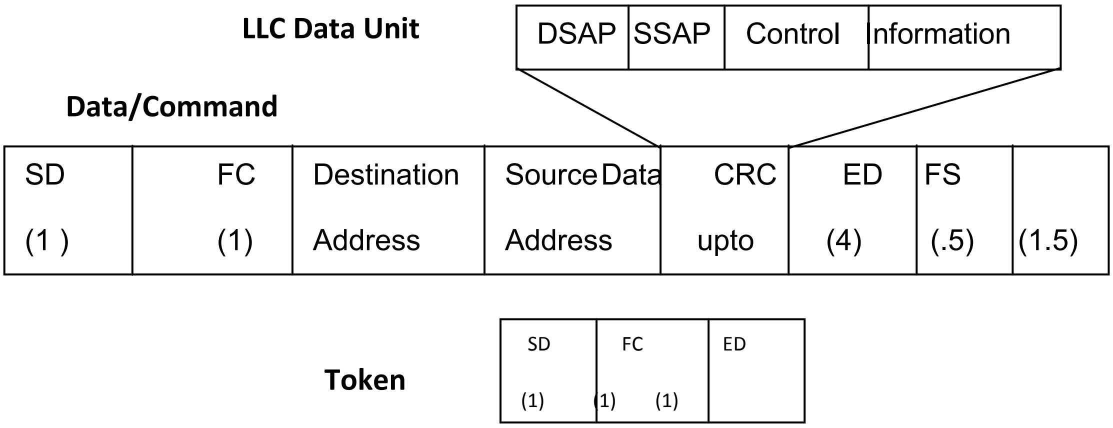


FIGURE 3.20: FDDI MAC LAYER

SD : Start Delimiter (flag)
FC : Frame Control (frame type)
ED : End Delimiter (flag)
CRC : Cyclic Redundancy Check

FS : Frame status

Frame Fields There are eight fields in the FDDI frame:

- **Start delimiter (SD)** The first byte of the field is the frame's starting flag. As in **Token Ring**, these bits are replaced in the physical layer by the control codes (violations) J and K (the five-bit sequences used to represent J and K are shown in Table 4B/5B Control Symbols.
- **Frame control (FC)** The second byte of the frame identifies the frame type.
- **Addresses** The next two fields are the destination and source addresses. Each address consists of two to six bytes.
- **Data** Each data frame can carry up to 4500 bytes of data.
- **CRC** FDDI uses the standard IEEE four-byte cyclic redundancy check.
- **End delimiter (ED)** This field consists of half a byte in the data frame or a full byte in the token frame. It is changed in the physical layer with one violation symbol in the data/command frame or two T symbols in the token frame. (Refer 4B/5B Control Symbols)
- **Frame status (FS)** The FDDI FS field is similar to that of Token Ring. It is included only in the data/command frame and consists of 1.5 bytes.

Implementation: Physical Medium Dependent (PMD) Layer

The physical medium dependent (PMD) layer defines the required connections and electronic components. Specifications for this layer depend on whether the transmission medium used is fiber-optic or copper cable.

Dual Ring

FDDI is implemented as a dual ring. In most cases, data transmission is confined to the primary ring. The secondary ring is provided in case the primary fails.

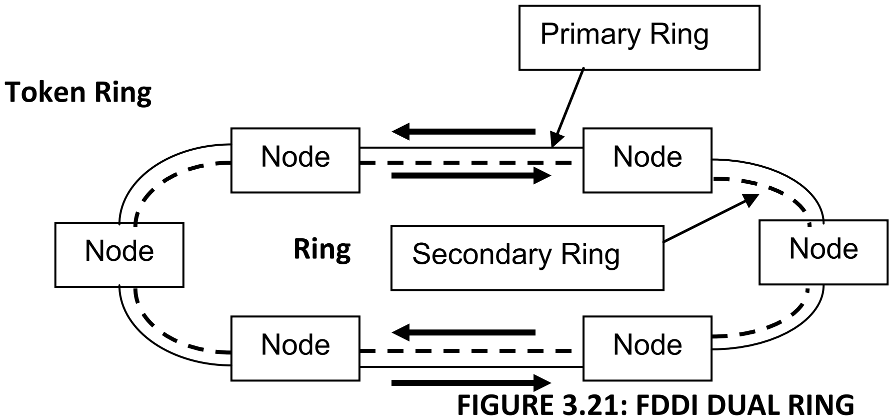


FIGURE 3.21: FDDI DUAL RING

The secondary ring makes FDDI self-healing. Whenever a problem occurs on tile primary ring, the secondary can be activated to complete data circuits and maintain service.

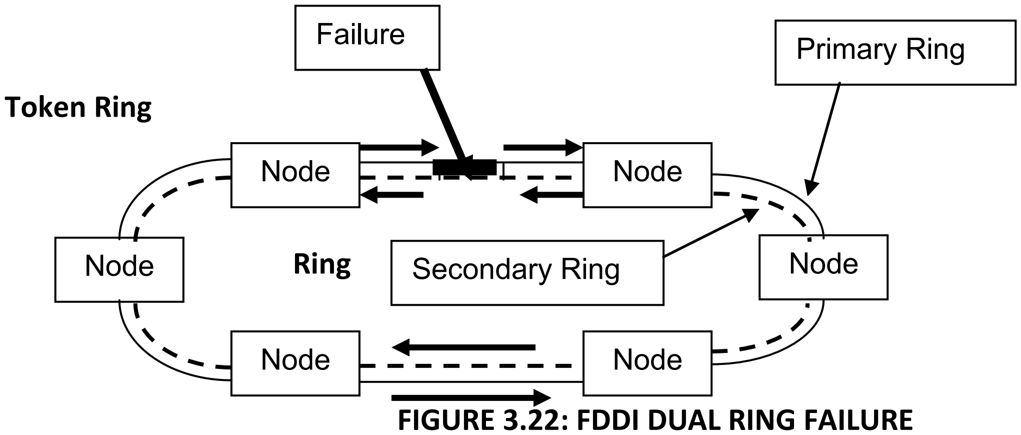


FIGURE 3.22: FDDI DUAL RING FAILURE

Nodes connect to one or both rings using a **media interface connector** (MIC) that can be either male or female depending on the requirements of the station.

Advantage and disadvantage of FDDI

Advantages:

- FDDI supports real-time allocation of network bandwidth.
- This allows you to use a wide array of different types of traffic.
- FDDI has a dual ring that is fault-tolerant. The benefit here is that if a station on the ring fails or if the cable becomes damaged, the dual ring is automaticaly doubled back onto itself into a single ring.
- The FDDI compensates for wiring failures. The stations wrap within themselves when the wiring fails.
- Optical bypass switches are used that can help prevent ring segmentation. The faild stations are eliminated from the ring.

Disadvantages:

- There's a potential for multiple ring failures.
- As the network grows, this possibility grows larger and larger.
- The use of fiber optic cables is expensive.
- This has kept many companies from deploying FDDI in a widespread manner. Instead, they have been using copper wire and the similar method of CDDI.

COMPARISON

Ethernet is good for low-level loads but collapses as the load increases due to collisions and retransmissions. Token Ring and fool perform equally well at low- and high-level loads.

Network	**Access Method**	**Signaling**	**Data Rate**	**Error Control**
Ethernet	CSMA/CD	Manchester	1,10 Mbps	No
Fast Ethernet	CSMA/CD	Several	100 Mbps	No
Gigabit Ethernet	CSMA/CD	Several	1 Gbps	No
Token Ring	Token passing	Differential Manchester	4, 16 Mbps	Yes
FDDI	Token passing	4B/5B, NRZ-I	100 Mbps	Yes

S.NO	RGPV QUESTION	YEAR	MARKS
Q.1	Write short notes on FDDI protocol.	Jun 2011 Dec 2012	7
Q.2	Compare the capacity allocation schemes	Dec 2011	7

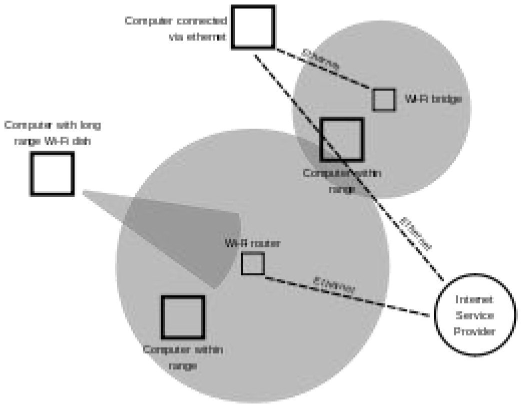
	for IEEE 802.5 token ring and FDDI. What are the relative pros & cons?		
Q.3	Explain FDDI network. What is the protocol used to MAC layer of FDDI LANS?	Dec 2009	7
Q.4	Explain the concept of FDDI wireless LAN in communication.	Jun 2013	7

UNIT 03/LECTURE- 09/ LECTURE- 10

WIRELESS LAN

Wireless LAN[RGPV/ Jun 2010, Jun 2011, Dec 2012, Dec 2013, Jun 2014]

A wireless local area network (WLAN) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider Internet. This gives users the ability to move around within a local coverage area and still be connected to the network. Most modern WLANs are based onIEEE 802.11 standards, marketed under the Wi-Fi brand name.


Computer connected via ethernet
Ethernet
Wi-Fi bridge
Computer with long range Wi-Fi dish
Computer within range
Ethernet
Wi-Fi router
Ethernet
Internet Service Provider
Computer within range

Wireless LANs have become popular in the home due to ease of installation, and in commercial complexes offering wireless access to their customers; often for free. New York City, for instance, has begun a pilot program to provide city workers in all five boroughs of the city with wireless Internet access.

Norman Abramson, a professor at the University of Hawaii, developed the world's first wireless computer communication network, ALOHAnet (operational in 1971), using low-cost ham-like radios. The system included seven computers deployed over four islands to communicate with the central computer on the Oahu Island without using phone lines.

WLAN hardware initially cost so much that it was only used as an alternative to cabled LAN in places where cabling was difficult or impossible. Early development included industry-specific solutions and proprietary protocols, but at the end of the 1990s these were replaced by standards, primarily the various versions of IEEE 802.11 (in products using the Wi-Fibrand name). An alternative ATM-like 5 GHz standardized technology, HiperLAN/2, has so far not succeeded in the market, and with the release of the faster 54 Mbit/s 802.11a (5 GHz) and 802.11g (2.4 GHz) standards, it is even more unlikely that it will ever succeed.

In 2009 802.11n was added to 802.11. It operates in both the 2.4 GHz and 5 GHz bands at a maximum data transfer rate of 600 Mbit/s. Most newer routers are able to utilize both wireless bands, known as dualband. This allows data communications to avoid the crowded 2.4 GHz band, which is also shared with Bluetooth devices and microwave ovens. The 5 GHz band is also wider than the 2.4 GHz band, with more channels, which permits a greater number of devices to share the space. Not all channels are available in all regions.

A HomeRF group formed in 1997 to promote a technology aimed for residential use, but it disbanded at the end of 2002.

Architecture

Stations

All components that can connect into a wireless medium in a network are referred to as stations. All stations are equipped with wireless network interface controllers(WNICs). Wireless stations fall into one of two categories: wireless access points, and clients. Access points (APs), normally wireless routers, are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with. Wireless clients can be mobile devices such as laptops,personal digital assistants, IP phones and other smartphones, or fixed devices such as desktops and workstations that are equipped with a wireless network interface.

Basic service set

The basic service set (BSS) is a set of all stations that can communicate with each other. Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.

There are two types of BSS: Independent BSS (also referred to as IBSS), and infrastructure BSS. An independent BSS (IBSS) is an ad hoc network that contains no access points, which means they cannot connect to any other basic service set.

Extended service set

An extended service set (ESS) is a set of connected BSSs. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string.

Distribution system

A distribution system (DS) connects access points in an extended service set. The concept of a DS can be used to increase network coverage through roaming between cells.

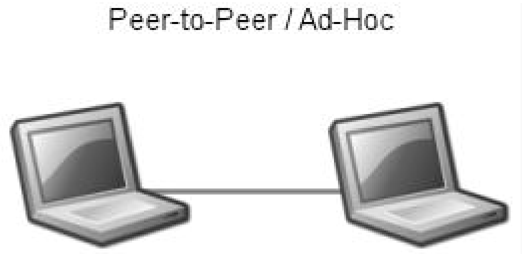
DS can be wired or wireless. Current wireless distribution systems are mostly based on WDS or MESH protocols, though other systems are in use.

Types of wireless LANs

The IEEE 802.11 has two basic modes of operation: ad hoc mode and infrastructure mode. In ad hoc mode, mobile units transmit directly peer-to-peer. In infrastructure mode, mobile units communicate through an access point that serves as a bridge to other networks (such as Internet or LAN).

Since wireless communication uses a more open medium for communication in comparison to wired LANs, the 802.11 designers also included encryption mechanisms:Wired Equivalent Privacy (WEP, now insecure), Wi-Fi Protected Access (WPA, WPA2), to secure wireless computer networks. Many access points will also offer Wi-Fi Protected Setup, a quick (but now insecure) method of joining a new device to an encrypted network.

Peer-to-peer



Peer-to-Peer or ad hoc wireless LAN

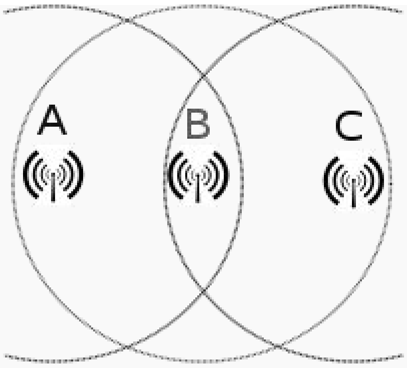
An ad hoc network (not the same as a WiFi Direct network) is a network where stations communicate only peer to peer (P2P). There is no base and no one gives permission to talk. This is accomplished using the Independent Basic Service Set (IBSS).

A WiFi Direct network is another type of network where stations communicate peer to peer.

In a Wi-Fi P2P group, the group owner operates as an access point and all other devices are clients. There are two main methods to establish a group owner in the Wi-Fi Direct group. In one approach, the user sets up a P2P group owner manually. This method is also known as Autonomous Group Owner (autonomous GO). In the second method, also called negotiation-based group creation, two devices compete based on the group owner intent value. The device with higher intent value becomes a group owner and the second device becomes a client. Group owner intent value can depend on whether the wireless device performs a cross-connection between an infrastructure WLAN service and a P2P group, remaining power in the wireless device, whether the wireless device is already a group owner in another group and/or a received signal strength of the first wireless device.

A peer-to-peer network allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network.

If a signal strength meter is used in this situation, it may not read the strength accurately and can be misleading, because it registers the strength of the strongest signal, which may be the closest computer.



Hidden node problem: Devices A and C are both communicating with B, but are unaware of each other

IEEE 802.11 defines the physical layer (PHY) and MAC (Media Access Control) layers based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). The 802.11 specification includes provisions designed to minimize collisions, because two mobile units may both be in range of a common access point, but out of range of each other.

Bridge[edit]

A bridge can be used to connect networks, typically of different types. A wireless Ethernet bridge allows the connection of devices on a wired Ethernet network to a wireless network. The bridge acts as the connection point to the Wireless LAN.

Wireless distribution system

A Wireless Distribution System enables the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them, as is traditionally required. The notable advantage of WDS over other solutions is that it preserves the MAC addresses of client packets across links between access points.

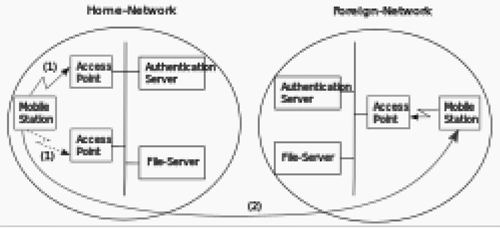
An access point can be either a main, relay or remote base station. A main base station is typically connected to the wired Ethernet. A relay base station relays data between remote base stations, wireless clients or other relay stations to either a main or another relay base station. A remote base station accepts connections from wireless clients and passes them to relay or main stations. Connections between "clients" are made using MAC addresses rather than by specifying IP assignments.

All base stations in a Wireless Distribution System must be configured to use the same radio channel, and share WEP keys or WPA keys if they are used. They can be configured to different service set identifiers. WDS also requires that every base station be configured to forward to others in the system as mentioned above.

WDS may also be referred to as repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging). It should be noted, however, that throughput in this method is halved for all clients connected wirelessly.

When it is difficult to connect all of the access points in a network by wires, it is also possible to put up access points as repeaters.

Roaming



Roaming among Wireless Local Area Networks

There are two definitions for wireless LAN roaming:

- Internal Roaming (1): The Mobile Station (MS) moves from one access point (AP) to another AP within a home network because the signal strength is too weak. An authentication server (RADIUS) performs the re-authentication of MS via 802.1x (e.g. with PEAP). The billing of QoS is in the home network. A Mobile Station roaming from one access point to another often interrupts the flow of data among the Mobile Station and an application connected to the network. The Mobile Station, for instance, periodically monitors the presence of alternative access points (ones that will provide a better connection). At some point, based on proprietary mechanisms, the Mobile Station decides to re-associate with an access point having a stronger wireless signal. The Mobile Station, however, may lose a connection with an access point before associating with another access point. In order to provide reliable connections with applications, the Mobile Station must generally include software that provides session persistence.[6]

- External Roaming (2): The MS (client) moves into a WLAN of another Wireless Internet Service Provider (WISP) and takes their services (Hotspot). The user can independently of his home network use another foreign network, if this is open for visitors. There must be special authentication and billing systems for mobile services in a foreign network.

Applications

Wireless LANs have a great deal of applications. Modern implementations of WLANs range from small in-home networks to large, campus-sized ones to completely mobile networks on airplanes and trains. Users can access the Internet from WLAN hotspots in restaurants, hotels, and now with portable devices that connect to 3G or 4G networks. Oftentimes these types of public access points require no registration or password to join the network. Others can be accessed once registration has occurred and/or a fee is paid.

Comparison of wired and wireless LAN

Wired Network

- Wired networking requires cables to be connected to each and every computer in the network

- Cost of a Wired network is less as compared to wireless network as Ethernet ,cables, switches are not expensive

- Wired LAN offers better performance as compared to wireless networks. Wired network can offer 100Mpbs bandwidth using Fast Ethernet technology.

- Ethernet cables, Switches are used in wired network are reliable.

- Security considerations for a wired network connected to the internet are firewalls. Firewall software can be installed on each computer.

Wireless Network

- Wireless network can be configured in two ways. I.e. Adhoc or infrastructure mode. Wireless devices require WLAN cards and access points for communication.

- Wireless networks require equipments like Wireless Adapters and access points which quite expensive.

- Cost of wireless networks is high as compared to wired networks.
  Maximum bandwidth provided by wireless network is about 11Mpbs.

- The reliability of wireless network is less as compared to wired network.

- WLANS use wired equivalent privacy (WEP) encryption to protect the data. This makes wireless networks as secure as wired networks.

- Laptops and other computing devices can be moved around freely within the wireless network because mobility of wireless network is better as compared to wired networks.

WLAN vs. LAN

LAN stands for Local Area Network, which is a collection of computers and other network devices in a certain location that are connected together by switches and/or routers that facilitate the communication of the network elements. Each computer or network element is connected to the switches/routers via a UTP cable. The added letter in WLAN stands for wireless. This is a type of network where the data is not transmitted via cables but over the air through the use of wireless transmitters and receivers.

WLANs are deployed in areas where a wide number of computers may connect to the network but not at the same time. Places like coffee shops often add WLAN to their shops to entice more customers who do not stay for extended periods. Even at home where you have a somewhat fixed number of computers that connect to the network, WLAN is also preferred as it gives users the freedom to move around the house and carry their laptops with them without needing to fuss with cables. For areas where the computers are pretty much fixed, a wired LAN is very desirable due to the advantages that it offers.

First off, a wired LAN is much faster compared to a WLAN. Most wireless routers nowadays are limited to a theoretical maximum speed of 54mbps while a contemporary wired LAN has a bandwidth of 100mbps. Gigabit network equipment can even ramp this up to 1000mbps or 1Gbps. This might not be such a big issue for browsing the internet or sending email but when you are copying large files, it can take a while with a WLAN.

WLANs are also vulnerable to attack as just about anyone with a strong enough transceiver is able to detect the signal. Access can then be achieved by breaking the encryption used by the router through certain software. The information that is being transmitted through the WLAN can also be collected by malicious person and used in a variety, often destructive, ways. In order to intercept data in a wired LAN, you need to physically connect to a switch or a router.

Summary:

- LAN refers to a wired network while WLAN is used to refer to a wireless network.
- LAN is commonly used in fixed networks while WLAN is common in areas where computers are moved quite often.
- WLAN is more convenient to users compared to LAN.
- LAN is much faster compared to WLAN.
- LAN is more secure compared to WLAN.

Computer networks for the home and small business can be built using either wired or wireless technology. Wired Ethernet has been the traditional choice in homes, but Wi-Fi and other wireless options are gaining ground fast. Both wired and wireless can claim advantages over each other; both represent viable options for home and other local area networks (LANs).

Below we compare wired and wireless networking in five key areas:

- ease of installation
- total cost
- reliability
- performance
- security

About Wired LANs

Wired LANs use Ethernet cables and networkadapters. Although two computers can be directly wired to each other using an Ethernet crossover cable, wired LANs generally also require central devices like hubs, switches, or routers to accommodate more computers.

For dial-up connections to the Internet, the computer hosting the modem must run Internet Connection Sharing or similar software to share the connection with all other computers on the LAN. Broadband routers allow easier sharing of cable modem or DSL Internet connections, plus they often include built-in firewall support.

Installation

Ethernet cables must be run from each computer to another computer or to the central device. It can be time-consuming and difficult to run cables under the floor or through walls, especially when computers sit in different rooms. Some newer homes are pre-wired with CAT5 cable, greatly simplifying the cabling process and minimizing unsightly cable runs.

The correct cabling configuration for a wired LAN varies depending on the mix of devices, the type of Internet connection, and whether internal or external modems are used. However, none of these options pose any more difficulty than, for example, wiring a home theater system.

After hardware installation, the remaining steps in configuring either wired or wireless LANs do not differ much. Both rely on standard Internet Protocol and network operating system configuration options. Laptops and other portable devices often enjoy greater **mobility** in wireless home network installations (at least for as long as their batteries allow).

Cost

Ethernet cables, hubs and switches are very inexpensive. Some connection sharing software packages, like ICS, are free; some cost a nominal fee. Broadband routers cost more, but these are optional components of a wired LAN, and their higher cost is offset by the benefit of easier installation and built-in security features.

Reliability

Ethernet cables, hubs and switches are extremely reliable, mainly because manufacturers have been continually improving Ethernet technology over several decades. Loose cables likely remain the single most common and annoying source of failure in a wired network. When installing a wired LAN or moving any of the components, be sure to carefully check the cable connections.

Broadband routers have also suffered from some reliability problems in the past. Unlike other Ethernet gear, these products are relatively new, multi-function devices. Broadband routers have matured over the past several years and their reliability has improved greatly.

Performance

Wired LANs offer superior performance. Traditional Ethernet connections offer only 10 Mbps and width, but 100 Mbps Fast Ethernet technology costs little more and is readily available. Although 100 Mbps represents a theoretical maximum performance never really achieved in practice, Fast Ethernet should be sufficient for home file sharing, gaming, and high-speed Internet access for many years into the future.

Wired LANs utilizing hubs can suffer performance slowdown if computers heavily utilize the network simultaneously. Use Ethernet switches instead of hubs to avoid this problem; a switch costs little more than a hub.

Security

For any wired LAN connected to the Internet, firewalls are the primary security consideration. Wired Ethernet hubs and switches do not support firewalls. However, firewall software products like ZoneAlarm can be installed on the computers themselves. Broadband routers offer equivalent firewall capability built into the device, configurable through its own software.

About Wireless LANs

Popular WLAN technologies all follow one of the three main Wi-Fi communication standards. The benefits of wireless networking depend on the standard employed:

- 802.11b was the first standard to be widely used in WLANs.
- The 802.11a standard is faster but more expensive than 802.11b; 802.11a is more commonly found in business networks.
- The newest standard, 802.11g, attempts to combine the best of both 802.11a and 802.11b, though it too is more a more expensive home networking option.

Installation

Wi-Fi networks can be configured in two different ways:

- "Ad hoc" mode allows wireless devices to communicate in peer-to-peer mode with each other.
- "Infrastructure" mode allows wireless devices to communicate with a central node that in turn can communicate with wired nodes on that LAN.

Most LANs require infrastructure mode to access the Internet, a local printer, or other wired services, whereas ad hoc mode supports only basic file sharing between wireless devices.
Both Wi-Fi modes require wireless network adapters, sometimes called WLAN cards. Infrastructure mode WLANs additionally require a central device called the access point. The access point must be installed in a central location where wireless radio signals can reach it with minimal interference. Although Wi-Fi signals typically reach 100 feet (30 m) or more, obstructions like walls can greatly reduce their range.

Cost
Wireless gear costs somewhat more than the equivalent wired Ethernet products. At full retail prices, wireless adapters and access points may cost three or four times as much as Ethernet cable adapters and hubs/switches, respectively. 802.11b products have dropped in price considerably with the release of 802.11g, and obviously, bargain sales can be found if shoppers are persistent.

Reliability
Wireless LANs suffer a few more reliability problems than wired LANs, though perhaps not enough to be a significant concern. 802.11b and 802.11g wireless signals are subject to interference from other home appliances including microwave ovens, cordless telephones, and garage door openers. With careful installation, the likelihood of interference can be minimized.

Wireless networking products, particularly those that implement 802.11g, are comparatively new. As with any new technology, expect it will take time for these products to mature.

Performance
Wireless LANs using 802.11b support a maximum theoretical bandwidth of 11 Mbps, roughly the same as that of old, traditional Ethernet. 802.11a and 802.11g WLANs support 54 Mbps, that is approximately one-half the bandwidth of Fast Ethernet. Furthermore, Wi-Fi performance is distance sensitive, meaning that maximum performance will degrade on computers farther away from the access point or other communication endpoint. As more wireless devices utilize the WLAN more heavily, performance degrades even further.

Overall, the performance of 802.11a and 802.11g is sufficient for home Internet connection sharing and file sharing, but generally not sufficient for home LAN gaming.

The greater mobility of wireless LANs helps offset the performance disadvantage. Mobile computers do not need to be tied to an Ethernet cable and can roam freely within the WLAN range. However, many home computers are larger desktop models, and even mobile computers must sometimes be tied to an electrical cord and outlet for power. This undermines the mobility advantage of WLANs in many homes.

Security
In theory, wireless LANs are less secure than wired LANs, because wireless communication signals travel through the air and can easily be intercepted. To prove their point, some engineers have promoted the practice of wardriving that involves travelling through a residential area with Wi-Fi equipment scanning the airwaves for unprotected WLANs. On balance, though, the weaknesses of wireless security are more theoretical than practical. WLANs protect their data through the Wired

Equivalent Privacy (WEP) encryption standard that makes wireless communications reasonably as safe as wired ones in homes.

No computer network is completely secure and homeowners should research this topic to ensure they are aware of and comfortable with the risks. Important security considerations for homeowners tend to not be related to whether the network is wired or wireless but rather ensuring:

- the home's Internet firewall is properly configured
- the family is familiar with the danger of Internet "spoof emails" and how to recognize them
- the family is familiar with the concept of "spyware" and how to avoid it
- babysitters, housekeepers and other visitors do not have unwanted access to the network

Advantages & disadvantages of wireless LAN

Advantages of WLAN:

- User mobility
- Voice and data services
- Scalable architecture
- Availability of all HiPath VoIP network services
- Access to central applications
- Handover between access points
- Robust model for industry
- Economical access points
- Plug-and-Play architecture
- Robust controller
- Security on the level of fixed networks
- “Small Enterprise” option with own controller
- “Branch Office” option for small branches where remote controller is used

Disadvantages of WLAN:

- As the number of computers using the network increases, the data transfer rate to each computer will decrease accordingly.
- As standards change, it may be necessary to replace wireless cards and/or access points.
- Lower wireless bandwidth means some applications such as video streaming will be more effective on a wired LAN.
- Security is more difficult to guarantee and requires configuration.
- Devices will only operate at a limited distance from an access point, with the distance determined by the standard used and buildings and other obstacles between the access point and the user.
- A wired LAN is most likely to be required to provide a backbone to the WLAN; a WLAN should be a supplement to a wired LAN and not a complete solution.
- Long-term cost benefits are harder to achieve in static environments that require few moves and changes.

S.NO	RGPV QUESTION	YEAR	MARKS
Q.1	Explain with diagram the architecture of wireless LAN	Jun 2011	7
Q.2	Compare wired & wireless LAN	Jun 2010	7
Q.3	Write comparison between wired LAN, wireless LAN and WIMAX?	Dec 2013	7
Q.4	Test and explain requirements of wireless LAN in detail.	Dec 2012	7
Q.5	Explain wireless LANs and their working	Jun 2014	3.5

UNIT 03/LECTURE 11

WIMAX

Introduction [RGPV/Jun 2011, Dec 2013, Jun 2014]

Worldwide Interoperability for Microwave Access (WiMAX) is currently one of the best technologies in wireless. The Institute of Electrical and Electronics Engineers (IEEE) 802 committee, which sets networking standards such as Ethernet (802.3) and WiFi (802.11), has published a set of standards that define WiMAX. IEEE 802.16-2004 (also known as Revision D) was published in 2004 for fixed applications; 802.16 Revision E (which adds mobility) is publicated in July 2005. The WiMAX Forum is an industry body formed to promote the IEEE 802.16 standard and perform interoperability testing. The WiMAX Forum has adopted certain profiles based on the 802.16 standards for interoperability testing and "WiMAX certification". These operate in the 2.5GHz, 3.5GHz and 5.8GHz frequency bands, whic typically are licensed by various government authorities. WiMAX, is based on an RF technology called Orthogonal Frequency Division Multiplexing (OFDM), which is a very effective means of transferring data when carriers of width of 5MHz or greater can be used. Below 5MHz carrier width, current CDMA based 3G systems are comparable to OFDM in terms of performance. WiMAX is a standard-based wireless technology that provides high throughput broadband connections over long distance. WiMAX can be used for a number of applications, including "last mile" broadband connections, hotspots and high-speed connectivity for business customers. It provides wireless metropolitan area network (MAN) connectivity at speeds up to 70 Mbps and the WiMAX base station on the average can cover between 5 to 10 km.

Typically, a WiMAX system consists of two parts:

- **A WiMAX Base Station** Base station consists of indoor electronics and a WiMAX tower. Typically, a base station can cover up to 10 km radius (Theoretically, a base station can cover up to 50 kilo meter radius or 30 miles, however practical considerations limit it to about 10 km or 6 miles). Any wireless node within the coverage area would be able to access the Internet.
- **A WiMAX receiver** The receiver and antenna could be a stand-alone box or a PC card that sits in your laptop or computer. Access to WiMAX base station is similar to accessing a Wireless Access Point in a WiFi network, but the coverage is more.

Several base stations can be connected with one another by use of high-speed backhaul microwave links. This would allow for roaming by a WiMAX subscriber from one base station to another base station area, similar to roaming enabled by Cellular phone companies.

Several topology and backhauling options are to be supported on the WiMAX base stations: wireline backhauling (typically over Ethernet), microwave Point-to-Point connection, as well as WiMAX backhaul. With the latter option, the base station has the capability to backhaul itself. This can be achieved by reserving part of the bandwidth normally used for the end-user traffic and using it for backhauling purposes.

Advantages over WIFI

WiMAX is similar to the wireless standard known as Wi-Fi, but on a much larger scale and at faster speeds. A nomadic version would keep WiMAX-enabled devices connected over large areas, much like today.s cell phones. We can compare it with Wi-Fi based on the following factors.

IEEE Standards Wi-Fi is based on IEEE 802.11 standard where as WiMAX is based on IEEE 802.16. However, both are IEEE standards.

Range Wi-Fi typically provides local network access for around a few hundred feet with speeds of up to 54 Mbps, a single WiMAX antenna is expected to have a range of up to 40 miles with speeds of 70 Mbps or more. As such, WiMAX can bring the underlying Internet connection needed to service localWi-Fi networks.

Scalability Wi-Fi is intended for LAN applications, users scale from one to tens with one subscriber for each CPE device. Fixed channel sizes (20MHz).

WiMAX is designed to efficiently support from one to hundreds of Consumer premises equipments (CPE)s, with unlimited subscribers behind each CPE. Flexible channel sizes from 1.5MHz to 20MHz.

Bit rate Wi-Fi works at 2.7 bps/Hz and can peak up to 54 Mbps in 20 MHz channel. WiMAX works at 5 bps/Hz and can peak up to 100 Mbps in a 20 MHz channel.

Quality of Service

Wi-Fi does not guarantee any QoS but WiMax will provide your several level of QoS. As such, WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks. Wi-Fi does not provide ubiquitous broadband while WiMAX does.

Comparison Table:

Freature	**WiMax (802.16a)**	**Wi-Fi (802.11b)**	**Wi-Fi (802.11a/g)**
Primary Application	Broadband Wireless Access	Wireless LAN	Wireless LAN
Frequency Band	Licensed/Unlicensed 2 G to 11 GHz	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Channel Bandwidth	Adjustable 1.25 M to 20 MHz	25 MHz	20 MHz
Half/Full Duplex	Full	Half	Half
Radio Technology	OFDM (256-channels)	Direct Sequence Spread Spectrum	OFDM (64-channels)
Bandwidth Efficiency	<=5 bps/Hz	<=0.44 bps/Hz	<=2.7 bps/Hz
Modulation	BPSK, QPSK, 16-, 64-, 256-QAM	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	Convolutional Code Reed-Solomon	None	Convolutional Code
Encryption	Mandatory- 3DES Optional- AES	Optional- RC4 (AES in 802.11i)	Optional- RC4 (AES in 802.11i)
Mobility	Mobile WiMax (802.16e)	In development	In development
Mesh	Yes	Vendor Proprietary	Vendor Proprietary

Access Protocol	Request/Grant	CSMA/CA	CSMA/CA

S.NO	RGPV QUESTION	YEAR	MARKS
Q.1	Whas is WIMAX? Give technical advantages over WIFI.	Jun 2011	7
Q.2	Explain WIMAX characteristics	Jun 2014	3.5

UNIT 03/LECTURE 12

ETHERNET CABLING

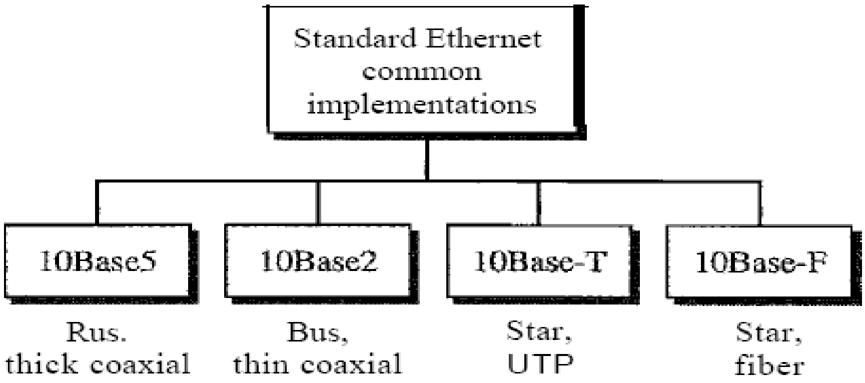


FIGURE 3.23: CATEGORY OF STANDARD ETHERNET

10Base5: Thick Ethernet

The first implementation is called **10BaseS, thick Ethernet, or Thicknet.** The nickname derives from the size of the cable. 10Base5 was the first Ethernet specification to use a bus topology with an external **transceiver** (transmitter/receiver) connected via a tap to a thick coaxial cable.

The transceiver is responsible for transmitting, receiving, and detecting collisions. The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable.

The maximum length of the coaxial cable must not exceed 500 m; otherwise, there is excessive degradation of the signal. If a length of more than 500 m is needed, up to five segments, each a maximum of 500-meter, can be connected using repeaters.

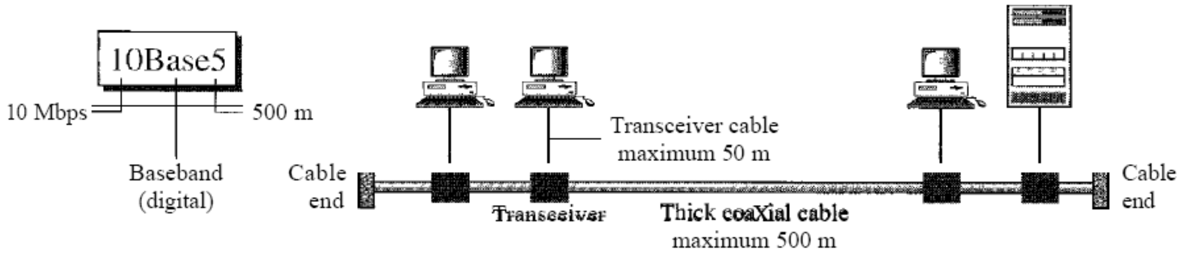


FIGURE 3.24: 10BASE5

10Base2: Thin Ethernet

The second implementation is called 10Base2, **thin** Ethernet, or Cheapernet. 10Base2 also uses a bus topology, but the cable is much thinner and more flexible. The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.

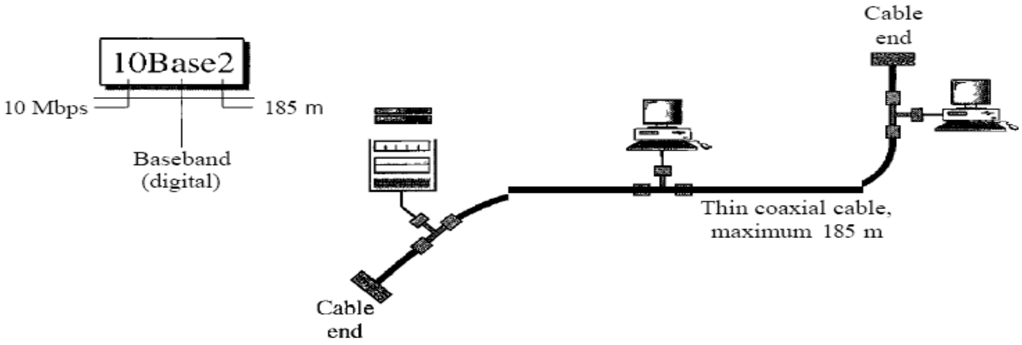


FIGURE3.25 : 10BASE2

Note that the collision here occurs in the thin coaxial cable. This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial and the tee connections are much cheaper than taps. Installation is simpler because the thin coaxial cable is very flexible. However, the length of each segment cannot exceed 185 m (close to 200 m) due to the high level of attenuation in thin coaxial cable.

10Base-T: Twisted-Pair Ethernet

The third implementation is called 10Base-T or twisted-pair Ethernet. 1OBase-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable Note that two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub. Any collision here happens in the hub. Compared to 10Base5 or 10Base2, we can see that the hub actually replaces the coaxial cable as far as a collision is concerned. The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.

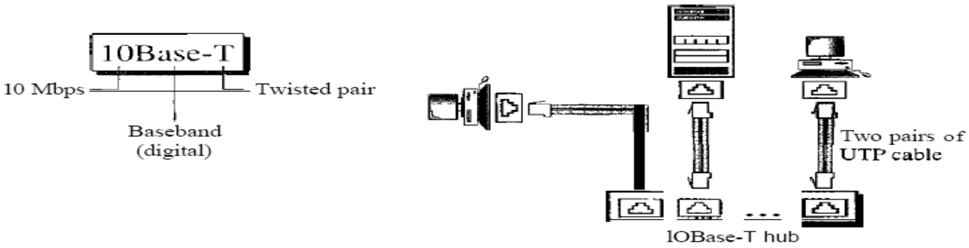


FIGURE 3.26: 10BASET

lOBase-F: Fiber Ethernet

Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called 10Base-F. 10Base-F uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables.

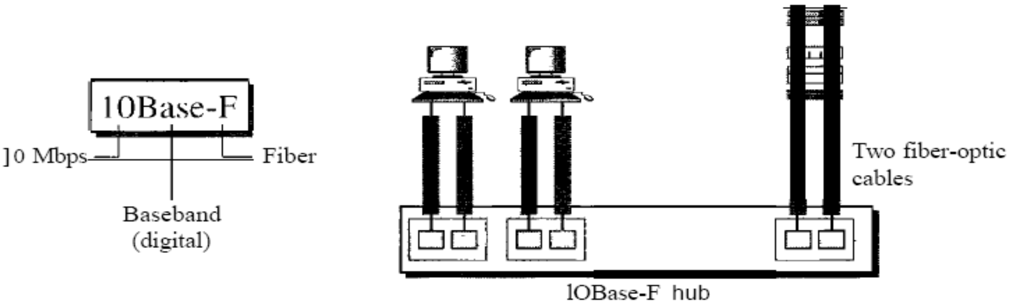
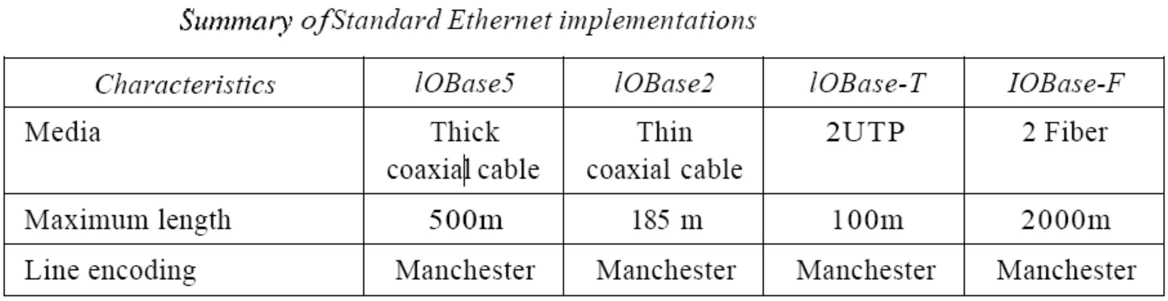


FIGURE 3.27: 10BASEF



Summary ofStandard Ethernet implementations

Characteristics	*lOBase5*	*lOBase2*	*lOBase-T*	*IOBase-F*
Media	Thick coaxial cable	Thin coaxial cable	2UTP	2 Fiber
Maximum length	500m	185 m	100m	2000m
Line encoding	Manchester	Manchester	Manchester	Manchester

FIGURE 3.28: SUMMRY OS STANDARD ETHERNET

UNIT – 4 /Lecture-01/ Lecture-02
logical addressing

Logical Addressing[RGPV/Jun 2014]

A person's name usually does not change. A person's address on the other hand, relates to where they live host NIC and is known as the physical address. The physical address remains the same regardless of where t

The IP address is similar to the address of a person. It is known as a logical address because it is assigned l each host by a network administrator based on the local network.

IP addresses contain two parts. One part identifies the local network. The network portion of the IP addres address identifies the individual host. Within the same local network, the host portion of the IP address is u

Both the physical MAC and logical IP addresses are required for a computer to communicate on a hierarchic

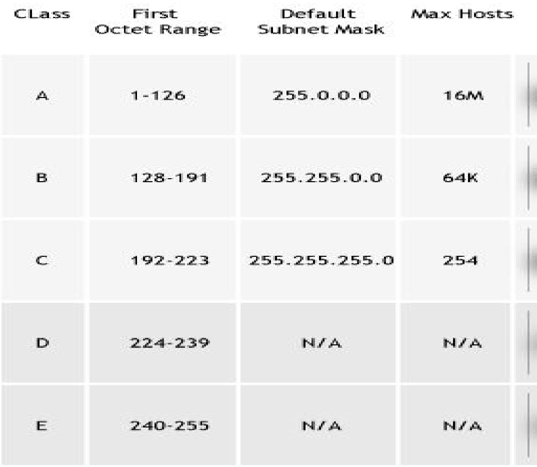
IPv4

Internet Protocol version 4 (**IPv4**) is the fourth version in the development of the Internet Protocol (IP) Inte

IPv4 Address Classes

The IPv4 address space can be subdivided into 5 **classes** –

- Class A
- Class B
- Class C
- Class D
- Class E



CLass	First Octet Range	Default Subnet Mask	Max Hosts
A	1-126	255.0.0.0	16M
B	128-191	255.255.0.0	64K
C	192-223	255.255.255.0	254
D	224-239	N/A	N/A
E	240-255	N/A	N/A

FIGURE : IP ADDRE

Each class consists of a contiguous subset of the overall IPv4 address range.

With a few special exceptions explained further below, the values of the leftmost four bits of an IPv4 addres

Class	Leftmost bits	Start addr
A	0xxx	0.0.0.0
B	10xx	128.0.0.
C	110x	192.0.0.
D	1110	224.0.0.
E	1111	240.0.0.

All Class C addresses, for example, have the leftmost three bits set to '110', but each of the remaining 29 bit

110xxxxx xxxxxxxx xxxxxxxx xxxxxxxx
Converting the above to dotted decimal notation, it follows that all Class C addresses fall in the range from 1

IP Address Class E and Limited Broadcast

The IPv4 networking standard defines Class E addresses as reserved, meaning that they should not be used
However, nodes that try to use these addresses on the Internet will be unable to communicate properly.

A special type of IP address is the limited broadcast address 255.255.255.255. A broadcast involves deliverin
255.255.255.255 to indicate all other nodes on the local network (LAN) should pick up that message. This br

Technically, IP reserves the entire range of addresses from 255.0.0.0 through 255.255.255.255 for broadcas

IP Address Class D and Multicast

The IPv4 networking standard defines Class D addresses as reserved for multicast. Multicast is a mechanism
on the LAN (broadcast) or just one other node (unicast).

Multicast is mainly used on research networks. As with Class E, Class D addresses should not be used by ord

IP Address Class A, Class B, and Class C

Class A, Class B, and Class C are the three classes of addresses used on IP networks in common practice, wit

IP Loopback Address

127.0.0.1 is the loopback address in IP. Loopback is a test mechanism of network adapters. Messages sent t
messages and returns them to the sending application. IP applications often use this feature to test the beh

As with broadcast, IP officially reserves the entire range from 127.0.0.0 through 127.255.255.255 for loopba
part of the normal Class A range.

Zero Addresses

As with the loopback range, the address range from 0.0.0.0 through 0.255.255.255 should not be considere
nodes attempting to use them will be unable to communicate properly on the Internet.

Private Addresses

The IP standard defines specific address ranges within Class A, Class B, and Class C reserved for use by privat

Class	Private start address
A	10.0.0.0
B	172.16.0.0
C	192.168.0.0

Nodes are effectively free to use addresses in the private ranges if they are not connected to the Internet, c

Classful network[RGPV/Dec 2009]

A **classful network** is a network addressing architecture used in the Internet from 1981 until the introductic Protocol Version 4 (IPv4) into five address classes. Each class, coded in the first four bits of the address, defi

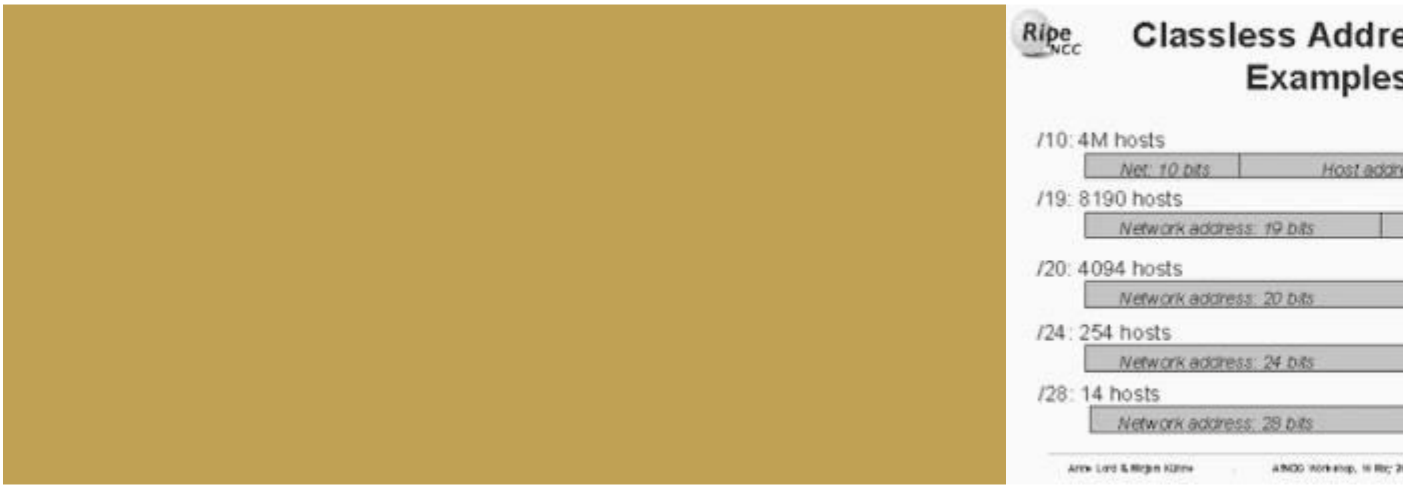
Special-use addresses

Reserved address blocks

Range	Description
0.0.0.0/8	Current network (only valid as source address)
10.0.0.0/8	Private network
100.64.0.0/10	Shared Address Space
127.0.0.0/8	Loopback
169.254.0.0/16	Link-local
172.16.0.0/12	Private network
192.0.0.0/24	IETF Protocol Assignments
192.0.2.0/24	TEST-NET-1, documentation and examples
192.88.99.0/24	IPv6 to IPv4 relay
192.168.0.0/16	Private network
198.18.0.0/15	Network benchmark tests
198.51.100.0/24	TEST-NET-2, documentation and examples
203.0.113.0/24	TEST-NET-3, documentation and examples
224.0.0.0/4	IP multicast (former Class D network)
240.0.0.0/4	Reserved (former Class E network)
255.255.255.255	Broadcast

Classless Addressing :[RGPV/Dec 2009]

Classless addressing uses a variable number of bits for the network and host portions of the address.



Classless Addre
Examples

/10: 4M hosts

/19: 8190 hosts

/20: 4094 hosts

/24: 254 hosts

/28: 14 hosts

Classless addressing treats the IP address as a 32 bit stream of ones and zeroes, where the boundary betwe system is also known as CIDR (Classless Inter-Domain Routing).Classless addressing is a way to allocate and system of Internet Protocol (IP) address classes. CIDR (Classless Internet Domain Routing) defines arbitrarily address of 192.168.0.0/24 defines a block of addresses in the range 192.168.0.0 through 192.168.0.255, wh 192.168.15.255.

Decimal	192	160	20
Binary	11000000	10100000	000
	<-------- 28 bits Network ------->		

What is the difference between classless and classful IP address?

Your default class addresses are Class A 0-127, Class B - 128-191, Class C - 192-223 for the 1st octet values

Classful IP addresses are IP addresses that follow this standard subnet ranges for class A, B, C so a classful 255.255.0.0 even if you want it to have a subnet of 255.255.255.0 so on a classful router protocol 172.16 octet falls in the Class B range of 128-191 and class B addresses have the subnet mask set to 255.255.0.0)

Classless IP addresses mean that the address range is determined by the subnet mask and hence the same because 255.255.255.0 corresponds to that range.

Public IP Address and Private IP Address

Public Host

Any computer accessing a public network like internet must have a unique ip address.Such a host is termec

Private Host

The total IP addresses available are very limited. So it is not possible to assign unique ip address to all comp addresses are reserved for private IP.

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

Inside a LAN or a private network computers can use these ip addresses. Two different private network may

These private hosts can access internet or a public network through a public host.That is the private host's i host through which it is connected to the internet. That is Private host shows the IP address of the public ho

A private network is typically a network that uses private IP address space.Private IP addresses were origina

Merging two Private Networks

Internal networks of two different organizations may use the same private IP addresses.Problem occurs wh

- One network must renumber
- A NAT router must be placed between the networks.

CIDR - Classless Inter-Domain Routing

IPv4 TCP/IP Subnet Table

While subnetting might be easy enough to grasp as a concept, it can be a bit involved, and even mind-boggl ideas behind subnetting, but find it hard to follow the actual steps required to subnet a network. The table l

Subnet Mask (Netmask)	Binary	CIDR	Hosts*	Inverse Mask**	Notes
255.255.255.255	11111111.11111111.11111111.11111111	/32	1	0.0.0.0	single host mask
255.255.255.254	11111111.11111111.11111111.11111110	/31	0		unusable mask, no host bits
255.255.255.252	11111111.11111111.11111111.11111100	/30	2	0.0.0.3	
255.255.255.248	11111111.11111111.11111111.11111000	/29	6	0.0.0.7	
255.255.255.240	11111111.11111111.11111111.11110000	/28	14	0.0.0.15	
255.255.255.224	11111111.11111111.11111111.11100000	/27	30	0.0.0.31	
255.255.255.192	11111111.11111111.11111111.11000000	/26	62	0.0.0.63	
255.255.255.128	11111111.11111111.11111111.10000000	/25	126	0.0.0.127	
255.255.255.0	11111111.11111111.11111111.00000000	/24	254	0.0.0.255	1 Class C network
255.255.254.0	11111111.11111111.11111110.00000000	/23	510	0.0.1.255	2 Class C networks

255.255.252.0	11111111.11111111.11111100.00000000	/22	1022	0.0.3.255	4 Class C
255.255.248.0	11111111.11111111.11111000.00000000	/21	2046	0.0.7.255	8 Class C
255.255.240.0	11111111.11111111.11110000.00000000	/20	4094	0.0.15.255	16 Class C
255.255.224.0	11111111.11111111.11100000.00000000	/19	8190	0.0.31.255	32 Class C
255.255.192.0	11111111.11111111.11000000.00000000	/18	16382	0.0.63.255	64 Class C
255.255.128.0	11111111.11111111.10000000.00000000	/17	32766	0.0.127.255	128 Class C
255.255.0.0	11111111.11111111.00000000.00000000	/16	65534	0.0.255.255	1 Class B Network (255 Class C)
255.254.0.0	11111111.11111110.00000000.00000000	/15	131070	0.1.255.255	2 Class B networks
255.252.0.0	11111111.11111100.00000000.00000000	/14	262142	0.3.255.255	4 Class B
255.248.0.0	11111111.11111000.00000000.00000000	/13	524286	0.7.255.255	8 Class B
255.240.0.0	11111111.11110000.00000000.00000000	/12	1M	0.15.255.255	16 Class B
255.224.0.0	11111111.11100000.00000000.00000000	/11	2M	0.31.255.255	32 Class B
255.192.0.0	11111111.11000000.00000000.00000000	/10	4M	0.63.255.255	64 Class B
255.128.0.0	11111111.10000000.00000000.00000000	/9	8M	0.127.255.255	128 Class B
255.0.0.0	11111111.00000000.00000000.00000000	/8	16M	0.255.255.255	1 Class A Network (255 Class B)

254.0.0.0	11111110.00000000.00000000.00000000	/7	32M	1.255.255.255	2 Class A
252.0.0.0	11111100.00000000.00000000.00000000	/6	64M	3.255.255.255	
248.0.0.0	11111000.00000000.00000000.00000000	/5	128M	7.255.255.255	
240.0.0.0	11110000.00000000.00000000.00000000	/4	256M	15.255.255.255	
224.0.0.0	11100000.00000000.00000000.00000000	/3	512M	31.255.255.255	
192.0.0.0	11000000.00000000.00000000.00000000	/2	1024M	63.255.255.255	
128.0.0.0	10000000.00000000.00000000.00000000	/1	2048M	127.255.255.255	
0.0.0.0	00000000.00000000.00000000.00000000	/0	4096M	255.255.255.255	

* Usable Hosts - (2^N-2) method.
** Inverse mask is calculated by subtracting each subnet mask octet value from 255. The inverse mask is
logical ANDing an inverse mask and an IP address gives the host portion of the address, instead of the ne
TCP/IP functions.

CIDR Example:
192.182.154.208/28
Determine the network # range of the host #'s
IP number in binary 11000000.10110110.10011010.11010000
Netmask:
11111111.11111111.11111111.11110000
And the two binary strings:
Result:
11000000.10110110.10011010.11010000 =
192.182.154.208
Host range:
192.182.154.11010000 can't use it's the network number
192.182.154.11010001 1st host number = 192.182.154.209
Last value:
192.182.154.11011111 can't use, it's the broadcast address

Last value for host #:
192.182.154.11011110 = 222
Number of possible hosts = 222-209+1=14
Written in subnet notation the address range is
192.182.154.208 with a subnet of 255.255.255.240

Introduction to Subnet Masks

Subnet masks are one of the most interesting aspects of TCP/IP. Subnet masks point out to IP which bits of
determine and use subnet masks.

What Is a Subnet Mask?

A subnet mask is a number that looks like an IP address. It shows TCP/IP how many bits are used for the net
As you learned in Chapter 6, an IP address is made up of two parts: the network portion and the host portio
local network or on a remote network. If the destination is local, then IP uses an ARP broadcast to find out t
network, then ARP broadcasts request for the hardware address of the router. Therefore, IP sends packets t
gateway. The router then sends the packet to the next network on its journey to the correct destination net
or long distance, TCP/IP uses the subnet mask to determine whether the destination of a packet is a host or
number must have an area code, every IP address must have a subnet mask. If, for example, your telephone
it is a local call. You know that because you can look at the numbers between the parentheses and see that
someone whose number is (213) 888-8146, it's a long distance call. You know that because the numbers ins
parentheses of a telephone number. Just as an area code determines a phone call's destination, a subnet m
remote. The following graphic shows Harry calling Amber. Since Amber has a different area code, the phone
does not need to go through the router. When determining if the packet is bound for the local network or a
number of bits from the destination's IP address. If the bit values are exactly the same, the packet's destina
any differences in the bit values, the packet's destination is determined to be remote. To know how many b
series of 1s, and then the rest of the bits are set to 0. When IP evaluates the subnet mask, it is looking speci
many bits are set to 1, it knows how many bits of the source host's IP address and the destination host's IP a
mask as the number of digits inside the parentheses in a telephone number—if that number could change (
parentheses include 4, 5, or 6 digits. You would
then evaluate the number to be local or long distance based on the digits that are in the arentheses. If there
8 bits of the destination. If there are 16 bits in the subnet mask that are set to 1, IP will compare the first 16
you want to type in the IP address for a host, the only two required elements are the IP address itself and th
correct area code for the phone number. You then
compare the first three characters of your phone number (your area code) with the first three characters of
the area code, nor do you have to pay for a long distance call, because it is a local call. If the area code is no
your call to their city. You'll see over the next several pages that IP looks at everything in binary. Subnet ma
binary, so begin now to think of IP addresses and subnet
masks as 32 bits. When thinking in binary, do not pay attention to the periods
that we use in the decimal representation. IP does not pay attention to the periods;
neither should we. Just consider the addresses as 32 1s and 0s.

Standard Subnet

For each class of address, there is a standard, or default, subnet mask. Each is discussed in the following sec

Class A Addresses

The standard subnet mask for a Class A address is 255.0.0.0. This tells IP that the first 8 bits are used for the
looks at the 32 bits and uses the subnet mask to mask out the network portion of the address: NNNN NNNN

Because 24 bits are left for the host portion of the address, there are almost 17 million unique host IP addre

Class B Addresses

A Class B address has a standard subnet mask of 255.255.0.0. This mask tells IP that the first 16 bits are usec
portion: NNNN NNNN.NNNN NNNN.HHHH HHHH.HHHH HHHH The 16 bits that are used for the host portio

Class C Addresses

A Class C address has a standard subnet mask of 255.255.255.0, which masks out the first 24 bits as the netv
NNNN NNNN.NNNN NNNN.NNNN NNNN. HHHH HHHH The 8 bits used for the host portion can uniquely ad

In Summary

Class Subnet Masks(decimal) Standard Masks (Binary)

A 255.0.0.0 1111 1111.0000 0000.0000 0000.0000 0000

B 255.255.0.0 1111 1111.1111 1111.0000 0000.0000 0000

C 255.255.255.0 1111 1111.1111 1111.1111 1111.0000 0000

Default Mask

When a router receives a packet with a destination address, it needs to route the packet. A router outside t
organization route the packet based on the subnetwork address.

- Network Address
- Sub Network Address
- Default Mask
- Subnet Mask

The router outside the organization has a routing table with one coulmn based on the network address. The

IP Default Subnet Masks For Address Classes A, B and C

Subnetting is the process of dividing a Class A, B or C network into subnets, as we've seen in the precedi
worth starting with a look at how the "whole" class A, B and C networks are represented in a subnetted er
unsubnetted network using subnetting notation.

This might seem like a strange concept—if you aren't going to bother creating subnets, why do you need t
subnetting became popular, most operating systems and networking hardware and software were designe
may need to express your unsubnetted network using a subnet mask.

In essence, a non-subnetted class A, B or C network can be considered the "default case" of the more gener
so that zero bits are used for the subnet ID and all the bits are used for the host ID. I realize that this seems

Just as is always the case, the subnet mask for a default, unsubnetted class A, B or C network has ones for
just said we aren't subnetting, so there **are** no subnet ID bits! Thus, the subnet mask for this default case h
mask for each of the IP address classes.

Since classes A, B and C divide the network ID from the host ID on octet boundaries, the subnet mask will
have 255s or 0s when expressed in decimal notation

Default Subnet Masks for Class A, Cla	
IP Address Class	**Total # Of Bits For Network ID / Host ID**
Class A	**8 / 24**
Class B	**16 / 16**
Class C	**24 / 8**

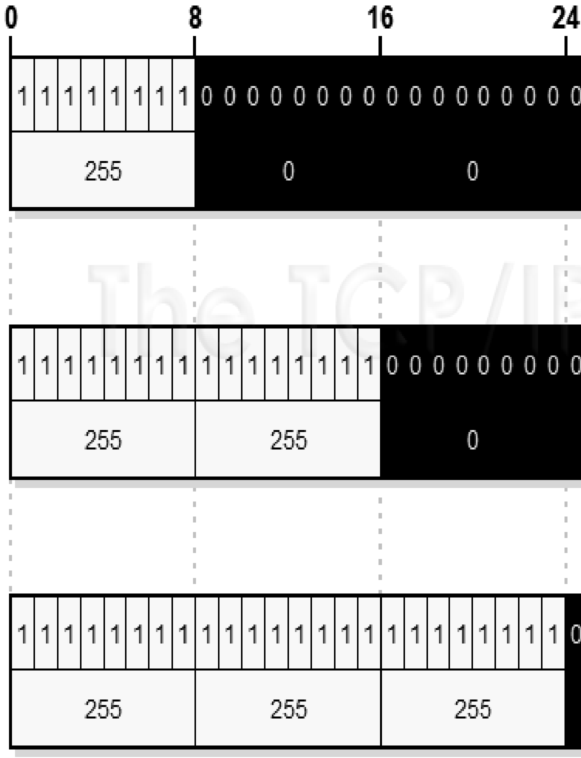


FIGURE : DEFAULT SUBNET MASKS FOR CLASS A

So, the three default subnet masks are 255.0.0.0 for Class A, 255.255.0.0 for class B, and 255.255.255.0 for with “255” and “0” are defaults. There are a small number of custom subnets that divide on octet boundari

- ○ **255.255.0.0:**,This is the default mask for Class B, but can also be the custom subnet mask for dividin
- ○ **255.255.255.0:** This is the default subnet mask for Class C, but can be a custom Class A with 16 bits f

Class	Default Mask
A	255.0.0.0

B	255.255.0.0
C	255.255.255.0

How to find the Subnet Mask? [RGPV/Jun 2010/Dec 2010]
Subnet Mask is a 32 bit binary number. The subnet mask contains all 1's in the network and subnet portion

Example.
200.129.41.0 is a Class C address . We need to create 14 subnet on this network. Find the Subnet Mask?
The default mask for this address is 255.255.255.0.To perform subnetting we need to borrow bits from the
200.129.41.00000000
If we borrow 4 bits from the host part can create 14 subnets.
That is $2^n - 2 = 2^4 - 2 = 16 - 2 = 14$
So from the host part of 200.129.41.00000000 we borrow 4 bits.
200.129.41 | 0000 | 0000
Network Address Subnet Bits Host bits

The 32 bit Subnet Mask is given by all 1's in the network and subnetwork portion and all 0's in the host port
11111111.11111111.11111111.11110000
255 .255 .255 .240
So the subnet mask is given by 255.255.255.240

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	What do you mean by classless and classful addressing? How many maximum network and host ids are there in class A, B and C networks?	Dec2009	7
Q.2	For the given data IP address 172.16.0.0 Subnet mask 255.255.248.0 Find the- (i) No of subnets (ii) No of host (iii) Subnet ip (iv) Range of ip address.	Jun 2010	7
Q.3	A host in an organization has an IP address 150.37.64.34 and a subnet mask 255.255.240.0. What is the address of this subnet? What is the range of IP address that a host can have on this subnet?	Dec 2010	7

Unit-04/Lecture-03

IPV4

IPV4 HEADER FORMAT[RGPV/Jun 2010, Jun 2011, Jun 2013,Dec 2012, Dec 2013]

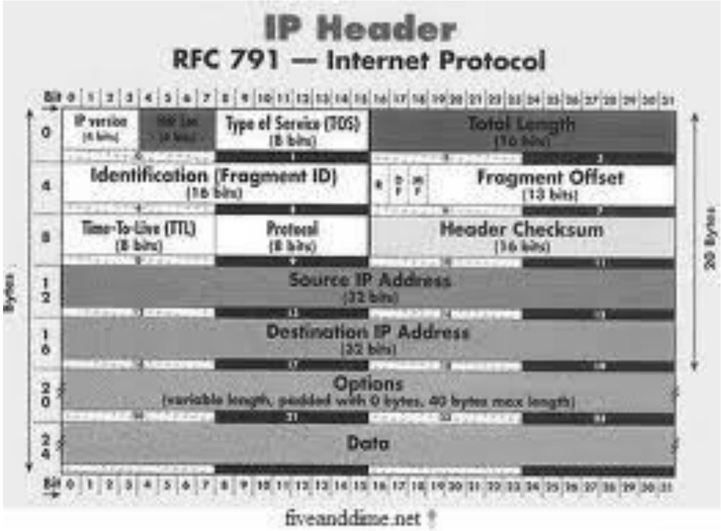

IP Header
RFC 791 — Internet Protocol
IP version (4 bits)
HDR Len (4 bits)
Type of Service (TOS) (8 bits)
Total Length (16 bits)
Identification (Fragment ID) (16 bits)
Fragment Offset (13 bits)
Time-To-Live (TTL) (8 bits)
Protocol (8 bits)
Header Checksum (16 bits)
Source IP Address (32 bits)
Destination IP Address (32 bits)
Options (variable length, padded with 0 bytes, 40 bytes max length)
Data
Bytes
20 Bytes
fiveanddime.net

FIGURE 4.1: IP HEADER

Version It defines the version of the IPv4 protocol. Currently the version is 4. However, version 6 (or IPng) may totally replace version 4 in the future. This field tells the IPv4 software running in the processing machine that the datagram has the format of version 4. All fields must be interpreted as specified in the fourth version of the protocol. If the machine is using some other version of IPv4, the datagram is discarded rather than interpreted incorrectly.

Header length (HLEN) This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes). When there are no options, the header length is 20 bytes, and the value of this field is 5 (5 x 4 = 20). When the option field is at its maximum size, the value of this field is 15 (15 x 4 = 60).

Services 8-bit field, this field, previously called service type, is now called differentiated services.

Service type or differentiated services

- D: Minimize delay
- R: Maximize reliability
- T: Maximize throughput
- C: Minimize cost

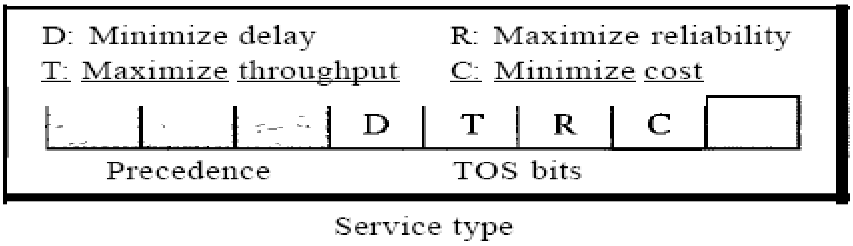


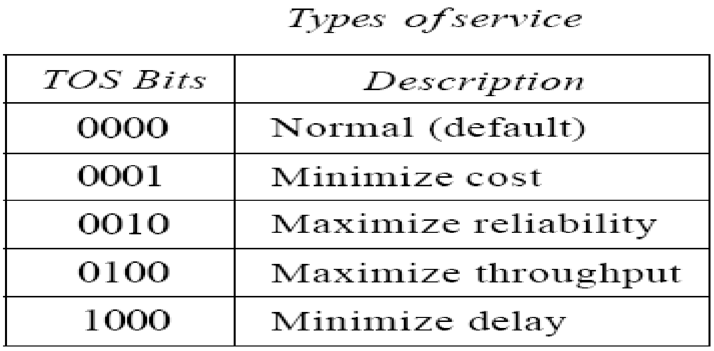
FIGURE : IP HEADER SERVICE TYPE

In this interpretation, the first 3 bits are called precedence bits. The next 4 bits are called type of service (TOS) bits, and the last bit is not used. a. Precedence is a 3-bit subfield ranging from 0 (000 in binary) to 7 (111 in binary). The precedence defines the priority of the datagram in issues such as congestion.

If a router is congested and needs to discard some datagrams, those datagrams with lowest precedence are discarded first. Some datagrams in the Internet are more important than others. For example, a datagram used for network management is much more urgent and important than a datagram containing optional information for a group.

The precedence subfield was part of version 4, but never used.

TOS bits is a 4-bit subfield with each bit having a special meaning. Although a bit can be either 0 or 1, one and only one of the bits can have the value of 1 in each datagram.



Types ofservice

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

FIGURE : IP HEADER TOS BITS DESCRIPTION

Total length This is a In-bit field that defines the total length (header plus data) of the IPv4 datagram in bytes. To find the length of the data coming from the upper layer, subtract the header length from the total length. The header length can be found by multiplying the value in the HLEN field by 4.

Length of data =total length - header length

Since the field length is 16 bits, the total length of the IPv4 datagram is limited to 65,535 (216 - 1) bytes, of which 20 to 60 bytes are the header and the rest is data from the upper layer. The total length field defines the total length of the datagram including the header. Though a size of 65,535 bytes might seem large, the size of the IPv4 datagram may increase in the near future as the underlying technologies allow even more throughput (greater bandwidth).

Fragmentation The datagram must be fragmented to be able to pass through those networks.

Identification This field is used in fragmentation

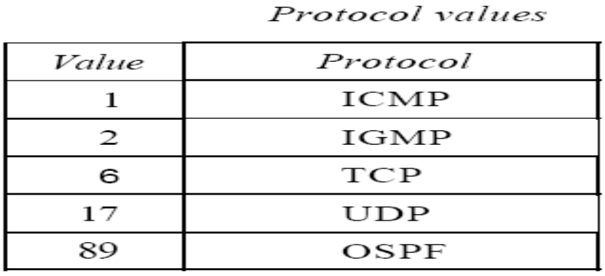
Flags This field is used in fragmentation

Fragmentation offset This field is used in fragmentation

Time to live A datagram has a limited lifetime in its travel through an internet. This field was originally designed to hold a timestamp, which was decremented by each visited router. The datagram was discarded when the value became zero. However, for this scheme, all the machines must have synchronized clocks and must know how long it takes for a datagram to go from one machine to another. Today, this field is used mostly to control the maximum number of hops (routers) visited by the datagram. When a source host sends the datagram, it stores a number in this
field. This value is approximately 2 times the maximum number of routes between any two hosts. Each router that processes the datagram decrements this number by 1. If this value, after being decremented, is zero, the router discards the datagram. This field is needed because routing tables in the Internet can become corrupted. A datagram may travel between two or more routers for a long time without ever getting delivered to the

destination host. This field limits the lifetime of a datagram. Another use of this field is to intentionally limit the journey of the packet. For example, if the source wants to confine the packet to the local network, it can store 1 in this field. When the packet arrives at the first router, this value is decremented to 0, and the datagram is discarded.

Protocol. This 8-bit field defines the higher-level protocol that uses the services of the IPv4 layer. An IPv4 datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP, and IGMP. This field specifies the final destination protocol to which the IPv4 datagram is delivered. In other words, since the IPv4 protocol carries data from different other protocols, the value of this field helps the receiving network layer know to which protocol the data belong



Protocol values

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

FIGURE : IP HEADER PROTOCOL

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

Fragmentation The fields that are related to fragmentation and reassembly of an IPv4 datagram are the identification, flags, and fragmentation offset fields.

Identification This 16-bit field identifies a datagram originating from the source host. The combination of the identification and source IPv4 address must uniquely define a datagram as it leaves the source host. To guarantee uniqueness, the IPv4 protocol uses a counter to label the datagrams. The counter is initialized to a positive number. When the IPv4 protocol sends a datagram, it copies the current value of the counter to the identification field and increments the counter by 1. As long as the counter is kept in the main memory, uniqueness is guaranteed. When a datagram is fragmented, the value in the identification field is copied to all fragments. In other words, all fragments have the same identification number, the same as the original datagram. The identification number helps the destination in reassembling the datagram. It knows that all fragments having the same identification value must be assembled into one datagram.

Flags This is a 3-bit field. The first bit is reserved. The second bit is called the do not fragment bit. If its value is 1, the machine must not fragment the datagram. If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host. If its value is 0, the datagram can be fragmented if necessary. The third bit is called the more fragment bit. If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one. If its value is 0, it means this is the last or only fragment

Flags used in fragmentation

- D: Don’t fragment

- M: More fragments

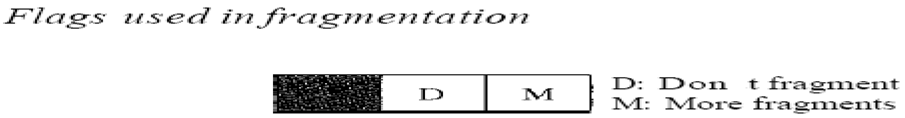
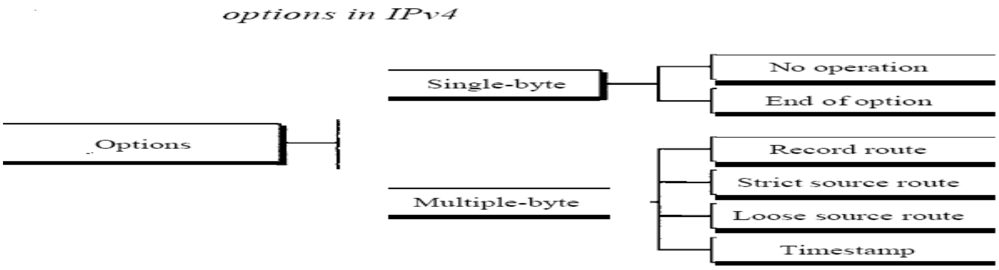


FIGURE : IP HEADER FLAGS

Fragmentation offset This 13-bit field shows the relative position of this fragment respect to the whole datagram. It is the offset of the data in the original data, measured in units of 8 bytes. Figure 20.11 shows a datagram with a data size of bytes fragmented into three fragments.

The bytes in the original datagram are numbered 0 to 3999. The first fragment ca bytes 0 to 1399. The offset for this datagram is 0/8 =O. The second fragment carries l 1400 to 2799; the offset value for this fragment is 1400/8 = 175. Finally, the fragment carries bytes 2800 to 3999. The offset value for this fragment is 2800/8 =35



FIG

: IP HEADER OPTIONS

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Write short note on IPv4.	Jun 2011	7
Q.2	Explain the frame format of IPv4.	Jun 2010	7
Q.3	Draw the frame format of IPv4	Dec 2013	7
Q.4	Discuss in detail the various aspects of IPV4?	Jun 2013	7
Q.5	Explain the function of 3 flags in the IPv4 header	Dec 2012	5
Q.6	How is the IPV4 header checksum calculated?	Dec 2012	5

Unit-04/Lecture-04

IPV6

Introduction to IPv6[RGPV/Dec 2009, Jun 2013]

There are legitimate reasons for designing and developing the new Internet Protocol IPv6:

- The recent exponential growth of the Internet and the impending exhaustion of the IPv4 address space. IPv4 addresses have become relatively scarce, forcing some organizations to use a network address translator (NAT) to map multiple private addresses to a single public IP address. While NATs promote reuse of the private address space, they do not support standards-based network layer security or the correct mapping of all higher layer protocols and can create problems when connecting two organizations that use the private address space. Additionally, the rising prominence of Internet-connected devices and appliances assures that the public IPv4 address space will eventually be depleted.

- The growth of the Internet and the ability of Internet backbone routers to maintain large routing tables. Because of the way in which IPv4 network IDs have been and are currently allocated, there are routinely over 70,000 routes in the routing tables of Internet backbone routers. The current IPv4 Internet routing infrastructure is a combination of both flat and hierarchical routing.
- The need for simpler configuration. Most current IPv4 implementations must be configured either manually or through a statefull address configuration protocol such as Dynamic Host Configuration Protocol (DHCP). With more computers and devices using IP, there is a need for a simpler and more automatic configuration of addresses and other configuration settings that do not rely on the administration of a DHCP infrastructure.
- The requirement for security at the IP level. Private communication over a public medium like the Internet requires encryption services that protect the data sent from being viewed or modified in transit. Although a standard now exists for providing security for IPv4 packets (known as Internet Protocol security or IPSec), this standard is optional and proprietary solutions are prevalent.
- The need for better support for real-time delivery of data (also known as quality of service). While standards for quality of service (QoS) exist for IPv4, real-time traffic support relies on the IPv4 Type of Service (TOS) field and the identification of the payload, typically using a UDP or TCP port. Unfortunately, the IPv4 TOS field has limited functionality and has different interpretations. In addition, payload identification using a TCP and UDP port is not possible when the IPv4 packet payload is encrypted.

IPv6 features

The following are the features of the IPv6 protocol:

- new header format;
- large address space;
- efficient and hierarchical addressing and routing infrastructure;
- stateless and state full address configuration;
- built-in security;
- better support for quality of service (QoS);
- new protocol for neighboring node interaction;
- Extensibility.

The IPv6 header has a new format that is designed to minimize header overhead. This is achieved by moving both nonessential fields and option fields to extension headers that are placed after the IPv6 header. The streamlined IPv6 header provides more efficient processing at intermediate routers.

IPv4 headers and IPv6 headers are not interoperable and the IPv6 protocol is not backward compatible with the IPv4 protocol. A host or router must use an implementation of both IPv4 and IPv6 in order to recognize and process both header formats. The new IPv6 header is only twice as large as the IPv4 header, even though IPv6 addresses are four times as large as IPv4 addresses.

Here is the IPv4 header. The red marked fields are removed in IPv6 and the black marked fields are changed.

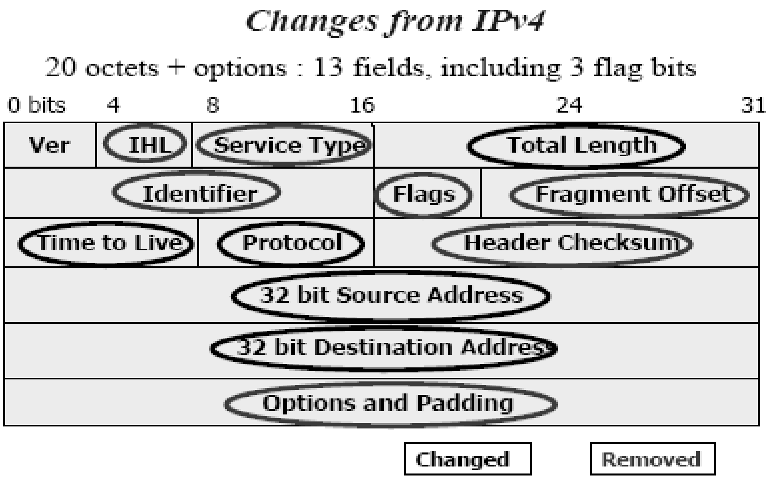


FIGURE: IPV4 HEADER

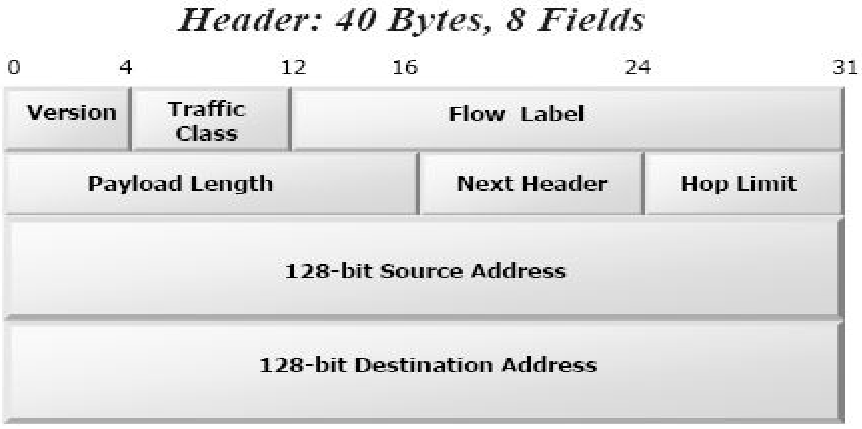
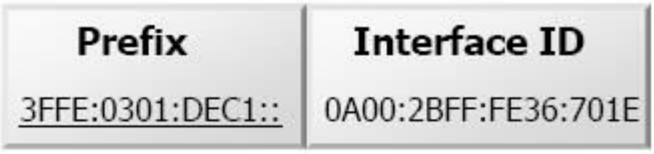


FIGURE: IPV6 HEADER

IPv6 has 128-bit (16-byte) source and destination addresses. Although 128 bits can provide over 3.4×10^{38} possible combinations, the large address space of IPv6 has been designed to allow for multiple levels of subnetting and address allocation from the Internet backbone to the individual subnets within an organization. Although only a small percentage of possible addresses are currently allocated for use by hosts, there are plenty of addresses available for future use. With a much larger number of available addresses, address-conservation techniques, such as the deployment of NATs, are no longer necessary.

An IPv6 address is formed by two entities: prefix and interface id, which separates “who you are” from “who you are connected to”.



Prefix	Interface ID
3FFE:0301:DEC1::	0A00:2BFF:FE36:701E

FIGURE : IPV6 FORMAT

The 48-bit Ethernet MAC address is mapped into a 64-bit Interface Id.
Let’s say that the MAC address of a host is 00-02-B3-1E-83-29. The first byte is modified from 00 in hexadecimal (00000000 in binary) to 02 in hexadecimal (00000010 in binary). After the third byte (B3) two bytes will be inserted: FF-FE (11111111:11111111:11111111:11111110 in binary). The interface id that is obtained will be 02:02:B3:FF:FE:1E:83:29.

IPv6 global addresses used on the IPv6 portion of the Internet are designed to create an efficient and hierarchical routing infrastructure that addresses the common occurrence of multiple levels of Internet service providers. On the IPv6 Internet, backbone routers have much smaller routing tables.

To simplify host configuration, IPv6 supports both state full address configuration, such as address configuration in the presence of a DHCP server, and stateless address configuration (address configuration in the absence of a DHCP server). With stateless address configuration, hosts on a link automatically configure themselves with IPv6 addresses for the link (link-local addresses) and with addresses that are derived from prefixes advertised by local routers. Even in the absence of a router, hosts on the same link can automatically configure themselves with link-local addresses and communicate without manual configuration.

Support for IPSec is an IPv6 protocol suite requirement. This requirement provides a standards-based solution for network security needs and promotes interoperability between different IPv6 implementations.

New fields in the IPv6 header define how traffic is handled and identified. Traffic identification, by using a Flow Label field in the IPv6 header, allows routers to identify and provide special handling for packets that belong to a flow. A flow is a series of packets between a source and destination. Because the traffic is identified in the IPv6 header, support for QoS can be easily achieved even when the packet payload is encrypted with IPSec.

The Neighbor Discovery protocol for IPv6 is a series of Internet Control Message Protocol for IPv6 (ICMPv6) messages that manage the interaction of neighboring nodes (that is, nodes on the same link). Neighbor Discovery replaces Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect messages with efficient multicast and unicast messages and provides additional functionality.

IPv6 can be extended for new features by adding extension headers after the IPv6 header. Unlike the IPv4 header, which can only support 40 bytes of options, the size of IPv6 extension headers is only constrained by the size of the IPv6 packet.

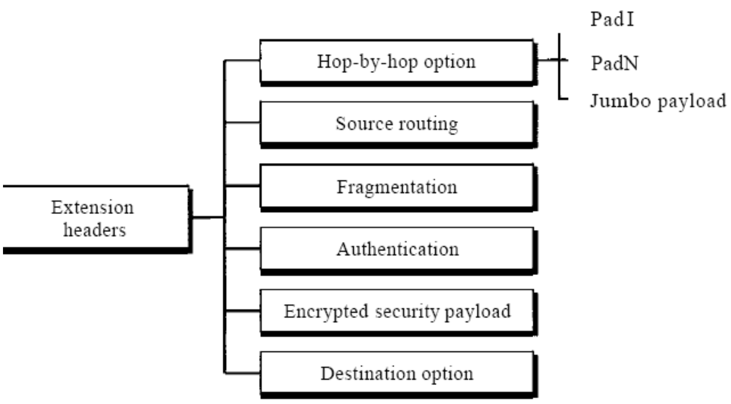
Security features in IPv6

The IPv6 protocol incorporates Internet Protocol security (IPSec), which provides protection of IPv6 data as it is sent over the network. IPSec is a set of Internet standards that uses cryptographic security services to provide the following:

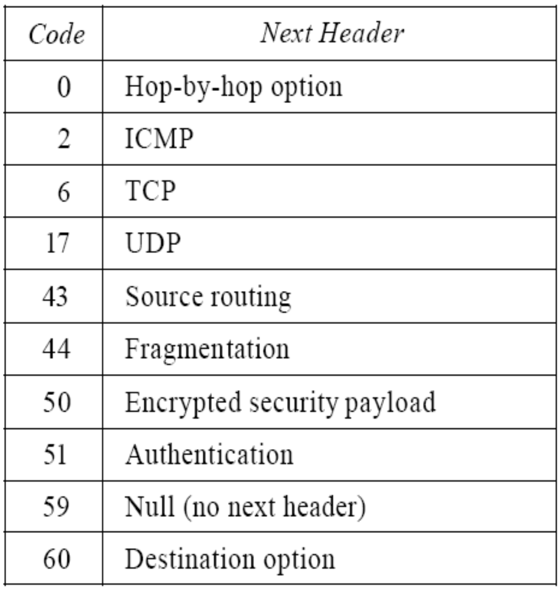
- Confidentiality: IPSec traffic is encrypted. Captured IPSec traffic cannot be deciphered without the encryption key.
- Authentication: IPSec traffic is digitally signed with the shared encryption key so that the receiver can verify that the IPSec peer sent it.
- Data integrity: IPSec traffic contains a cryptographic checksum that incorporates the encryption key. The receiver can verify that the packet was not modified in transit.

The IPv6 protocol for Windows XP also provides support for anonymous addresses. Anonymous addresses provide a level of anonymity when accessing Internet resources.

Extension header types



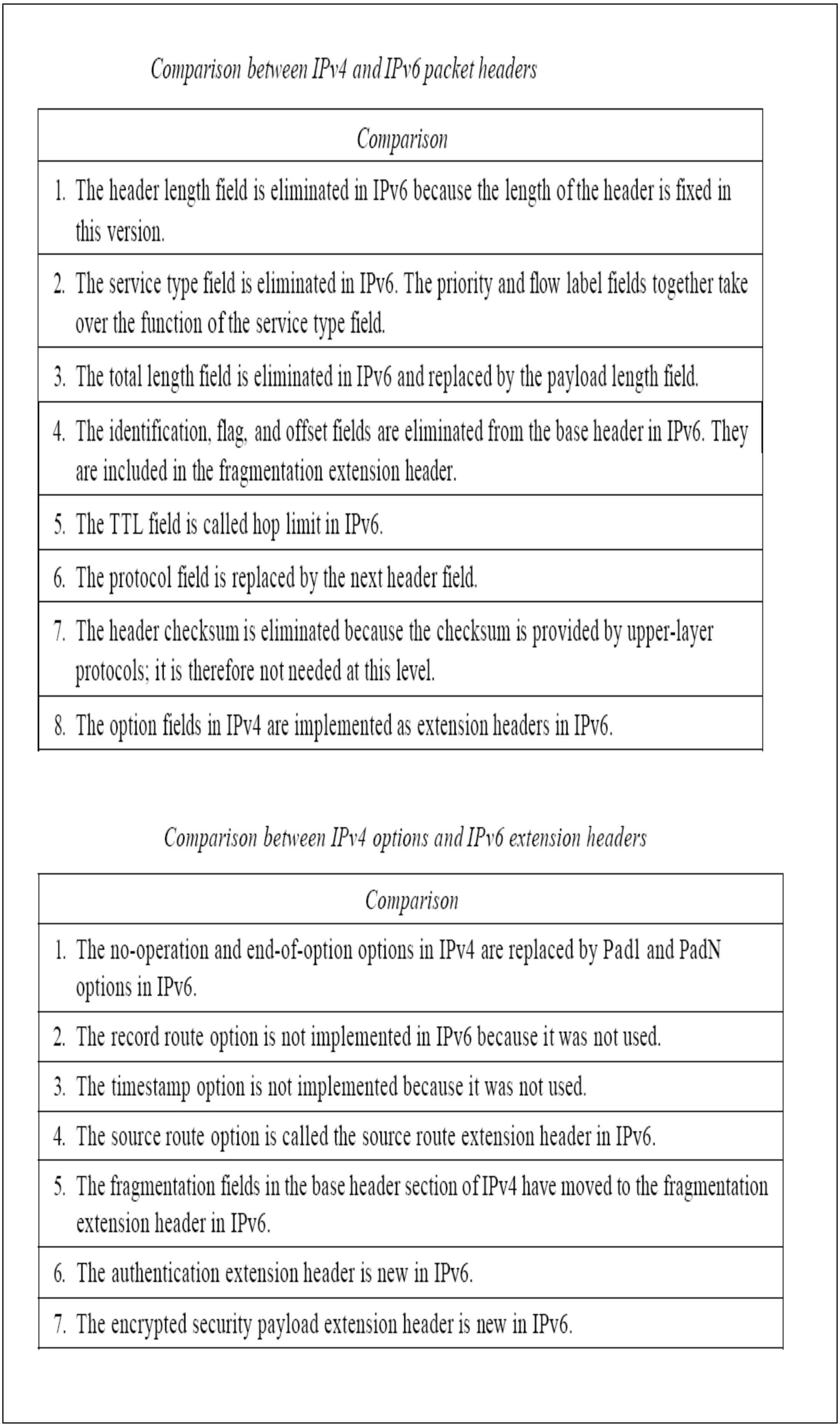
Next header codes for IPv6



Code	Next Header
0	Hop-by-hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null (no next header)
60	Destination option

IPv4	IPv6
Addresses are 32 bits (4 bytes) in length.	Addresses are 128 bits (16 bytes) in length

Address (A) resource records in DNS to map host names to IPv4 addresses.	Address (AAAA) resource records in DNS to map host names to IPv6 addresses.
Pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
IPSec is optional and should be supported externally	IPSec support is not optional
Header does not identify packet flow for QoS handling by routers	Header contains Flow Label field, which Identifies packet flow for QoS handling by router.
Both routers and the sending host fragment packets.	Routers do not support packet fragmentation. Sending host fragments packets
Header includes a checksum.	Header does not include a checksum.
Header includes options.	Optional data is supported as extension headers.
ARP uses broadcast ARP request to resolve IP to MAC/Hardware address.	Multicast Neighbor Solicitation messages resolve IP addresses to MAC addresses.
Internet Group Management Protocol (IGMP) manages membership in local subnet groups.	Multicast Listener Discovery (MLD) messages manage membership in local subnet groups.
Broadcast addresses are used to send traffic to all nodes on a subnet.	IPv6 uses a link-local scope all-nodes multicast address.
Configured either manually or through DHCP.	Does not require manual configuration or DHCP.
Must support a 576-byte packet size (possibly fragmented).	Must support a 1280-byte packet size (without fragmentation).

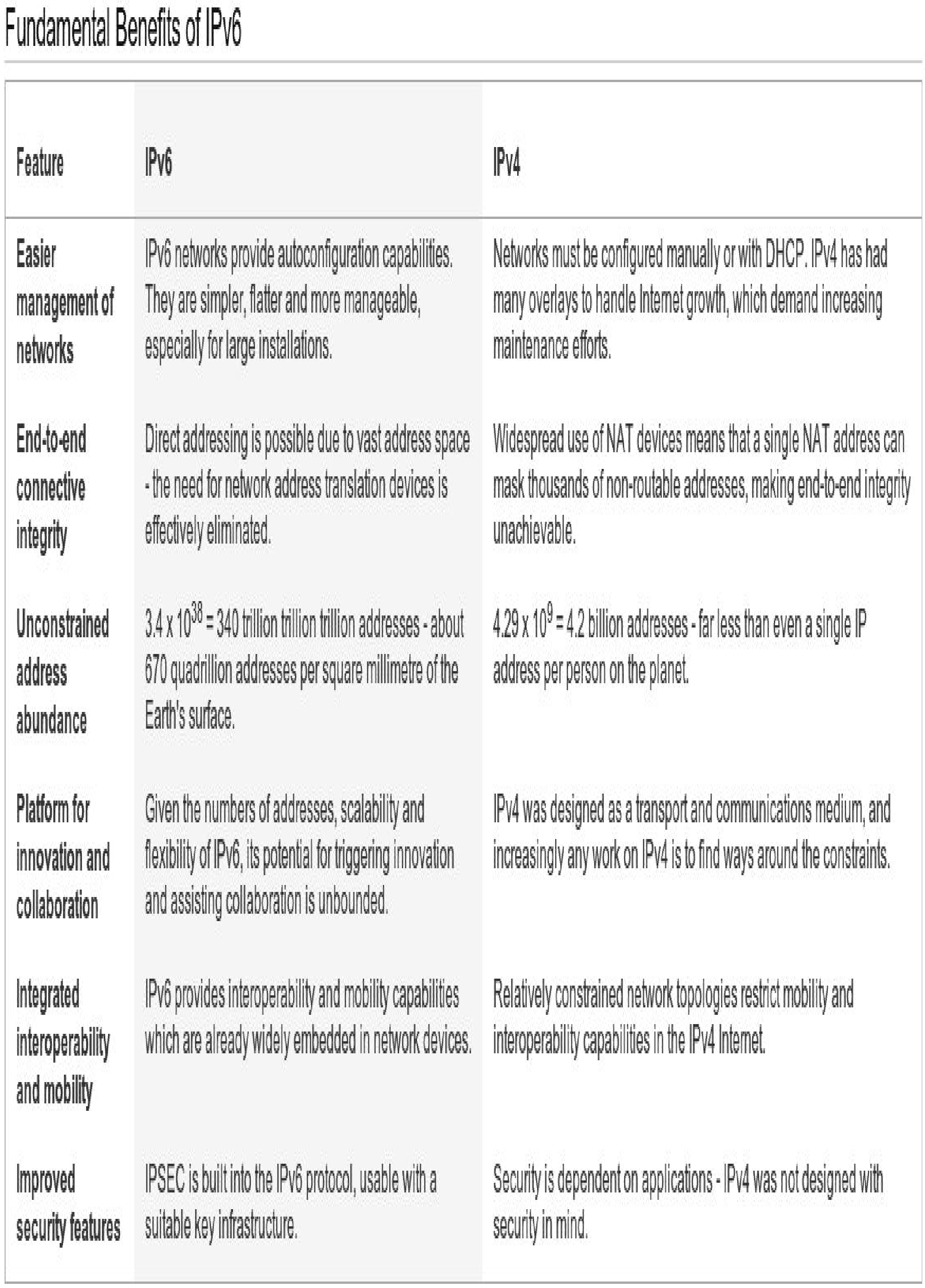


Comparison between IPv4 and IPv6 packet headers

Comparison
1. The header length field is eliminated in IPv6 because the length of the header is fixed in this version.
2. The service type field is eliminated in IPv6. The priority and flow label fields together take over the function of the service type field.
3. The total length field is eliminated in IPv6 and replaced by the payload length field.
4. The identification, flag, and offset fields are eliminated from the base header in IPv6. They are included in the fragmentation extension header.
5. The TTL field is called hop limit in IPv6.
6. The protocol field is replaced by the next header field.
7. The header checksum is eliminated because the checksum is provided by upper-layer protocols; it is therefore not needed at this level.
8. The option fields in IPv4 are implemented as extension headers in IPv6.

Comparison between IPv4 options and IPv6 extension headers

Comparison
1. The no-operation and end-of-option options in IPv4 are replaced by Pad1 and PadN options in IPv6.
2. The record route option is not implemented in IPv6 because it was not used.
3. The timestamp option is not implemented because it was not used.
4. The source route option is called the source route extension header in IPv6.
5. The fragmentation fields in the base header section of IPv4 have moved to the fragmentation extension header in IPv6.
6. The authentication extension header is new in IPv6.
7. The encrypted security payload extension header is new in IPv6.



Fundamental Benefits of IPv6

Feature	IPv6	IPv4
Easier management of networks	IPv6 networks provide autoconfiguration capabilities. They are simpler, flatter and more manageable, especially for large installations.	Networks must be configured manually or with DHCP. IPv4 has had many overlays to handle Internet growth, which demand increasing maintenance efforts.
End-to-end connective integrity	Direct addressing is possible due to vast address space - the need for network address translation devices is effectively eliminated.	Widespread use of NAT devices means that a single NAT address can mask thousands of non-routable addresses, making end-to-end integrity unachievable.
Unconstrained address abundance	3.4×10^{38} = 340 trillion trillion trillion addresses - about 670 quadrillion addresses per square millimetre of the Earth's surface.	4.29×10^{9} = 4.2 billion addresses - far less than even a single IP address per person on the planet.
Platform for innovation and collaboration	Given the numbers of addresses, scalability and flexibility of IPv6, its potential for triggering innovation and assisting collaboration is unbounded.	IPv4 was designed as a transport and communications medium, and increasingly any work on IPv4 is to find ways around the constraints.
Integrated interoperability and mobility	IPv6 provides interoperability and mobility capabilities which are already widely embedded in network devices.	Relatively constrained network topologies restrict mobility and interoperability capabilities in the IPv4 Internet.
Improved security features	IPSEC is built into the IPv6 protocol, usable with a suitable key infrastructure.	Security is dependent on applications - IPv4 was not designed with security in mind.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Differentiate IPv4 & IPv6.	Dec 2009	7
Q.2	Define the type of the following destination addresses: (i) 4A:30:10:21:10:1A (ii) 47:20:1B:2E:08:EE (iii) FF:FF:FF:FF:FF:FF	Jun 2013	7

CONGESTION CONTROL

CONGESTION

An important issue in a packet-switched network is **congestion.** Congestion in a network may occur if the **load** on the network-the number of packets sent to the network-is greater than the *capacity* of the network-the number of packets a network can handle.

Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

We may ask why there is congestion on a network. Congestion happens in any system that involves waiting. For example, congestion happens on a freeway because any abnonnality in the flow, such as an accident during rush hour, creates blockage.

Congestion in a network or internetwork occurs because routers and switches have queues-buffers that hold the packets before and after processing. A router, for example, has an input queue and an output queue for each interface.

Delay Versus Load

Note that when the load is much less than the capacity of the network, the delay is at a minimum. This minimum delay is composed of propagation delay and processing delay, both of which are negligible. However, when the load reaches the network capacity, the delay increases sharply because we now need to add the waiting time in the queues (for all routers in the path) to the total delay. Note that the delay becomes infinite when the load is greater than the capacity. If this is not obvious, consider the size of the queues when almost no packet reaches the destination, or reaches the destination with infinite delay; the queues become longer and longer. Delay has a negative effect on the load and consequently the congestion. When a packet is delayed, the source, not receiving the acknowledgment, retransmits the packet, which makes the delay, and the congestion, worse.

Throughput Versus Load

We defined throughput as the number of bits passing through a point in a second. We can extend that definition from bits to packets and from a point to a network. We can define throughput in a network as the number of packets passing through the network in a unit of time. Notice that when the load is below the capacity of the network, the throughput increases proportionally with the *load.* We expect the throughput to remain constant after the load reaches the capacity, but instead the throughput declines sharply. The reason is the discarding of packets by the routers. When the load exceeds the capacity, the queues become full and the routers have to discard some packets. Discarding packet does not reduce the number of packets in the network because the sources retransmit the packets, using time-out mechanisms, when the packets do not reach the destinations.

CONGESTION CONTROL[RGPV/Dec 2003, Dec 2010,Jun 2013, Dec 2013]

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. In general, we can divide congestion control mechanisms into two broad categories:

- **open-loop congestion control (prevention)**

- **closed-loop congestion control (removal)**

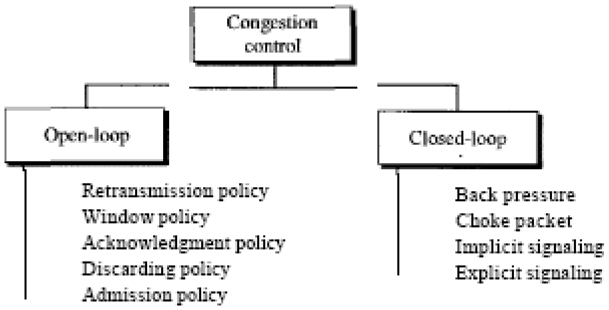


FIGURE : CONGESTION CONTROL

Open-Loop Congestion Control

In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination. We give a brief list of policies that can prevent congestion.

Retransmission Policy

Retransmission is sometimes unavoidable. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion. The retransmission policy and the retransmission timers must be designed to optimize efficiency and at the same time prevent congestion. For example, the retransmission policy used by TCP (explained later) is designed to prevent or alleviate congestion.

Window Policy

The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control. In the *Go-Back-N* window, when the timer for a packet times out, several packets may be resent, although some may have arrived safe and sound at the receiver. This duplication may make the congestion worse. The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted.

Acknowledgment Policy

The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion. Several approaches are used in this case. A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires. A receiver may decide to acknowledge only *N* packets at a time. We need to know that the acknowledgments are also part of the load in a network. Sending fewer acknowledgments means imposing less load on the network.

Discarding Policy

A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission. For example, in audio transmission, if the policy is to discard less sensitive packets when congestion is likely to happen, the quality of sound is still preserved and congestion is prevented or alleviated.

Admission Policy

An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks. Switches in a flow first check the resource requirement of a flow before admitting it to the network. A router can deny establishing a virtual circuit connection if there is congestion in the network or if there is a possibility of future congestion.

Closed-Loop Congestion Control

Closed-loop congestion control mechanisms try to alleviate congestion after it happens. Several mechanisms have been used by different protocols. We describe a few of them here.

Backpressure

The technique of *backpressure* refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. This may cause the upstream node or nodes to become congested, and they, in turn, reject data from their upstream nodes or nodes. And so on. Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source. The backpressure technique can be applied only to virtual circuit networks, in which each node knows the upstream node from which a flow of data is corning.

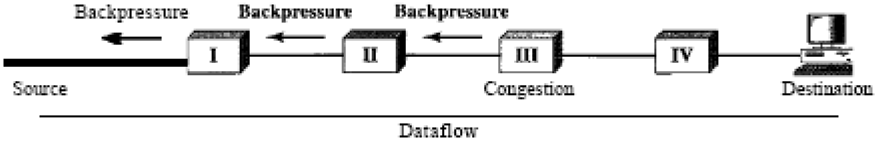


FIGURE : BACKPRESSURE

Node III in the figure has more input data than it can handle. It drops some packets in its input buffer and informs node II to slow down. Node II, in turn, may be congested because it is slowing down the output flow of data. If node II is congested, it informs node I to slow down, which in turn may create congestion. If so, node I inform the source of data to slow down. This, in time, alleviates the congestion. Note that the *pressure* on node III is moved backward to the source to remove the congestion. None of the virtual-circuit networks we studied in this book use backpressure. It was, however, implemented in the first virtual-circuit network, X.25. The technique cannot be implemented in a datagram network because in this type of network, a node (router) does not have the slightest knowledge of the upstream router.

Choke Packet[RGPV/Jun 2003,Dec 2010, Dec 2006, Jun 2013]

A choke packet is a packet sent by a node to the source to inform it of congestion. Note the difference between the backpressure and choke packet methods. In backpressure, the warning is from one node to its upstream node, although the warning may eventually reach the source station. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly. The intermediate nodes through which the packet has traveled are not warned. When a router in the Internet is overwhelmed with IP datagram's, it may discard some of them; but it informs the source host, using a source quench ICMP message. The warning message goes directly to the source station; the intermediate routers, and does not take any action. Figure shows the idea of a choke packet.

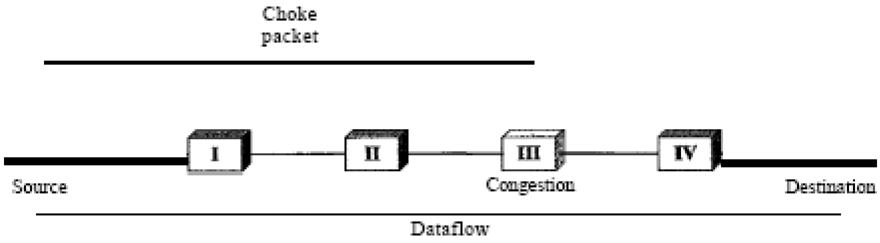


FIGURE 4.1: CHOKE PACKET

Implicit Signaling

In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is a congestion somewhere in the network from other symptoms. For example, when a source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested. The delay in receiving an acknowledgment is interpreted as congestion in the network; the source should slow down.

Explicit Signaling

The node that experiences congestion can explicitly send a signal to the source or destination. The explicit signaling method, however, is different from the choke packet method. In the choke packet method, a separate packet is used for this purpose; in the explicit signaling method, the signal is included in the packets that carry data. Explicit signaling can occur in either the forward or the backward direction.

Backward Signaling

A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.

Forward Signaling

A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the congestion.

Congestion Control in TCP[RGPV/Dec 2012/ Jun 2014]

How TCP uses congestion control to avoid congestion or alleviate congestion in the network.

Congestion Window

The sender window size is determined by the available buffer space in the receiver *(rwnd).* In other words, we assumed that it is only the receiver that can dictate to the sender the size of the sender's window. We totally ignored another entity here-the network. If the network cannot deliver the data as fast as they are created by the sender, it must tell the sender to slow down. In other words, in addition to the receiver, the network is a second entity that determines the size of the sender's window. Today, the sender's window size is determined not only by the receiver but also by congestion in the network. The sender has two pieces of information: the receiver-

advertised window size and the congestion window size. The actual size of the window is the minimum of these two.
Actual window size;;;;;; minimum (rwnd, cwnd)

Congestion Policy
TCP's general policy for handling congestion is based on three phases:

- slow start
- congestion avoidance
- congestion detection

In the slow-start phase, the sender starts with a very slow rate of ransmission, but increases the rate rapidly to reach a threshold. When the threshold is reached, the data rate is reduced to avoid congestion. Finally if congestion is detected, the sender goes back to the slow-start or congestion avoidance phase based on how the congestion is detected.

Slow Start: Exponential Increase
One of the algorithms used in TCP congestion control is called slow start. This algorithm is based on the idea that the size of the congestion window *(cwnd)* starts with one maximum segment size (MSS). The MSS is determined during connection establishment by using an option of the same name. The size of the window increases one MSS each time an acknowledgment is received. As the name implies, the window starts slowly, but grows exponentially. We have used segment numbers instead of byte numbers (as though each segment contains only 1 byte). We have assumed that *rwnd* is much higher than *cwnd,* so that the sender window size always equals *cwnd.* We have assumed that each segment is acknowledged individually. The sender starts with *cwnd* =1 MSS. This means that the sender can send only one segment. After receipt of the acknowledgment for segment 1, the size of the congestion window is increased by 1, which means that *cwnd* is now 2. Now two more segments can be sent. When each acknowledgment is received, the size of the window is increased by 1 MSS. When all seven segments are acknowledged, *cwnd* = 8.

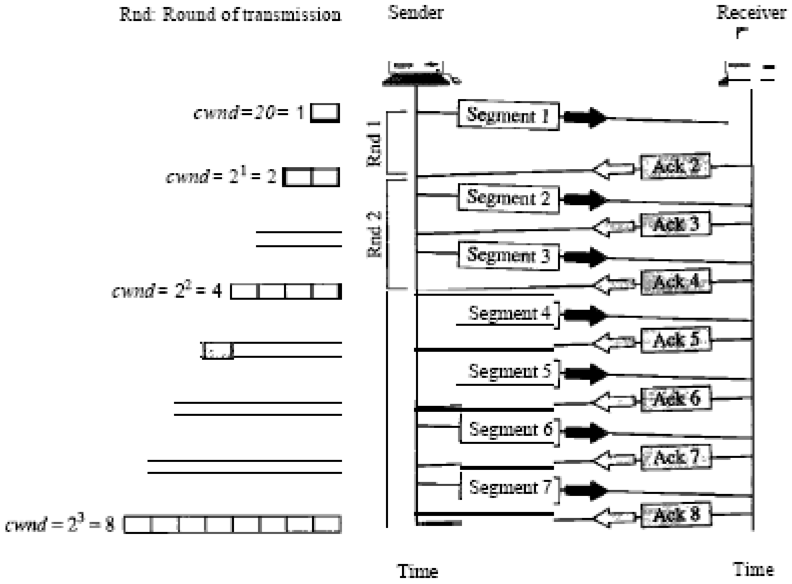


FIGURE : CONGESTION CONTROL,SLOW START

Congestion Avoidance: Additive Increase
If we start with the slow-start algorithm, the size of the congestion window increases exponentially. To avoid congestion before it happens, one must

slow down this exponential growth. TCP defines another algorithm called congestion avoidance, which undergoes an additive increase instead of an exponential one. When the size of the congestion window reaches the slow-start threshold, the slow-start phase stops and the additive phase begins. In this algorithm, each time the whole window of segments is acknowledged (one round), the size of the congestion window is increased by 1. To show the idea, we apply this algorithm to the same scenario as slow start, although we will see that the congestion avoidance algorithm usually starts when the size of the window is much greater than 1.

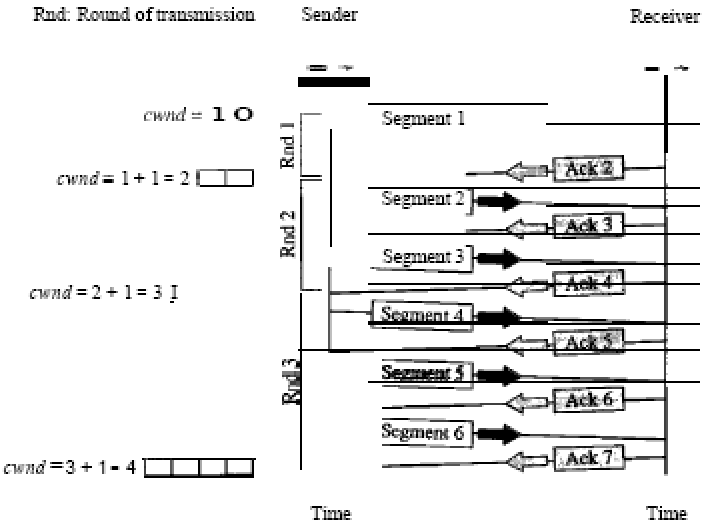


FIGURE : CONGESTION CONTROL ADDITIVE INCREASE

Congestion Detection: Multiplicative Decrease

If congestion occurs, the congestion window size must be decreased. The only way the sender can guess that congestion has occurred is by the need to retransmit a segment. However, retransmission can occur in one of two cases: when a timer times out or when three ACKs are received. In both cases, the size of the threshold is dropped to one-half, a multiplicative decrease. Most TCP implementations have two reactions:

I. If a time-out occurs, there is a stronger possibility of congestion; a segment has probably been dropped in the network, and there is no news about the sent segments.

In this case TCP reacts strongly:

a. It sets the value of the threshold to one-half of the current window size.

b. It sets *cwnd* to the size of one segment.

c. It starts the slow-start phase again.

2. If three ACKs are received, there is a weaker possibility of congestion; a segment may have been dropped, but some segments after that may have arrived safely since three ACKs are received. This is called fast transmission and fast recovery. In this case, TCP has a weaker reaction:

a. It sets the value of the threshold to one-half of the current window size.

b. It sets *cwnd* to the value of the threshold (some implementations add three segment sizes to the threshold).

c. It starts the congestion avoidance phase.

An implementations reacts to congestion detection in one of the following ways:

o If detection is by time-out, a new *slow-start* phase starts.

o If detection is by three ACKs, a new *congestion avoidance* phase starts.

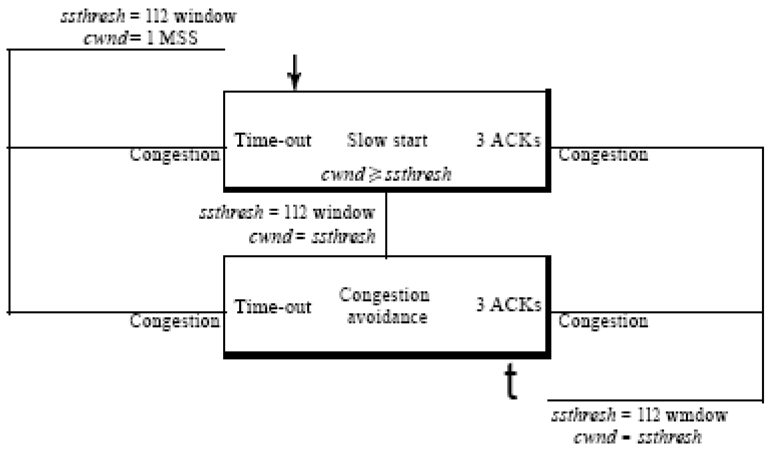


FIGURE : CONGESTION CONTROL

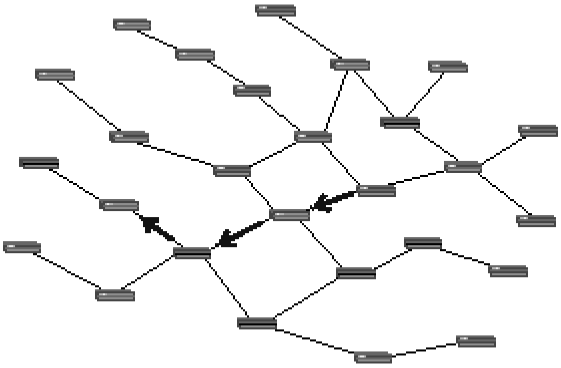
S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain various congestion control techniques.	Dec 2003	7
Q.2	Explain congestion control by choke packet method.	Jun 2003	7
Q.3	Explain leaky bucket algorithms in congestion control.	Dec 2003	7
Q.4	What are the policies and algorithm used for prevention of congestion? What are the policies that affect congestion?	Dec 2002	7
Q.5	Give an argument why the leaky bucket algorithm should allow just one packet per tick, independent of how large the packet is?	Dec 2010	7
Q.6	Explain congestion control in virtual circuit.	Dec 2013	7
Q.7	What is congestion control and how it is implemented in network layer? What is the role of choke packet in managing congestion?	Jun 2013	7
Q.8	How can TCP used to deal with network or internet congestion?	Dec 2012	7
Q.9	Enumerate various measures taken by TCP to avoid congestion on networks.	Jun 2014	7

11

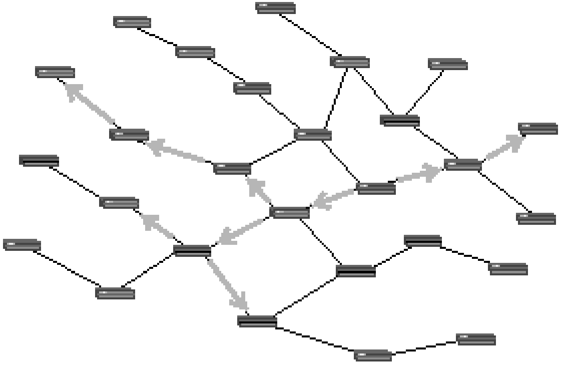
ROUTING PROTOCOLS

Packet forwarding

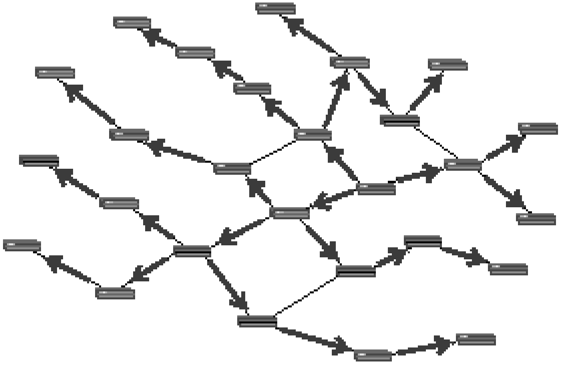
Packet forwarding is the relaying of packets from one network segment to another by nodes in a computer network.



A unicast forwarding pattern, typical of many networking technologies including the overwhelming majority of Internet traffic



A multicast forwarding pattern, typical of PIM



A broadcast forwarding pattern, typical of bridged Ethernet

The Network Layer of the OSI Layer is responsible for Packet Forwarding. The simplest forwarding model — unicasting — involves a packet being relayed from link to link along a chain leading from the packet's source to its destination. However, other forwarding strategies are commonly used. Broadcasting requires a packet to be duplicated and copies sent on multiple links with the goal of delivering a copy to every device on the network. In practice, broadcast packets are not forwarded everywhere on a network, but only to devices within a broadcast domain, making *broadcast* a relative term. Less common than broadcasting, but perhaps of greater utility and theoretical significance, is multicasting, where a packet is selectively duplicated and copies delivered to each of a set of recipients.

Direct Versus Indirect Delivery

The delivery of a packet to its final destination is accomplished by using two different methods of delivery

- direct
- indirect

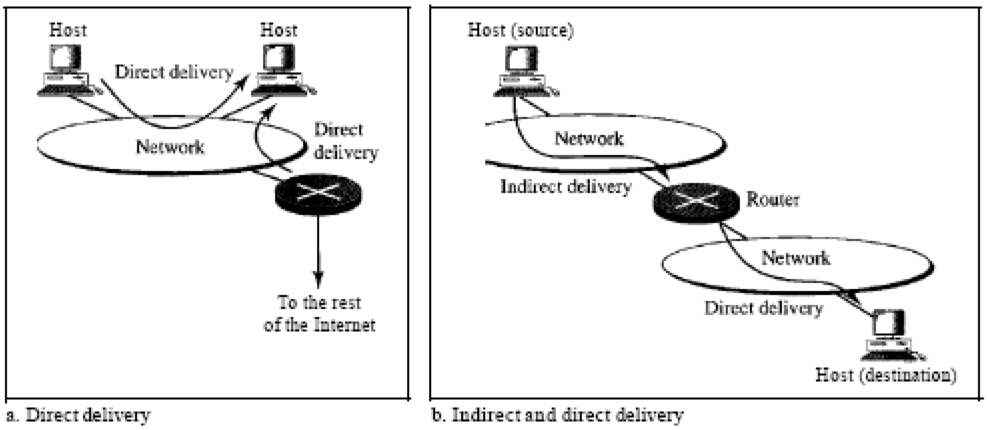
Direct Delivery

In a direct delivery, the final destination of the packet is a host connected to the same physical network as the deliverer. Direct delivery occurs when the source and destination of the packet are located on the same physical network or when the delivery is between the last router and the destination host.

The sender can easily determine if the delivery is direct. It can extract the network address of the destination (using the mask) and compare this address with the addresses of the networks to which it is connected. If a match is found, the delivery is direct.

Indirect Delivery

If the destination host is not on the same network as the deliverer, the packet is delivered indirectly. In an indirect delivery, the packet goes from router to router until it reaches the one connected to the same physical network as its final destination. Note that a delivery always involves one direct delivery but zero or more indirect deliveries.



a. Direct delivery

b. Indirect and direct delivery

FIGURE : DIRECT DELIVERY

FORWARDING

Forwarding means to place the packet in its route to its destination. Forwarding requires a host or a router to have a routing table. When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination. However, this simple solution is impossible today in an internetwork such as the Internet because the number of entries needed in the routing table would make table lookups inefficient.

Forwarding Techniques

Several techniques can make the size of the routing table manageable and also handle issues such as security. We briefly discuss these methods here.

Next-Hop Method Versus Route Method

One technique to reduce the contents of a routing table is called the next-hop method. In this technique, the routing table holds only the address of the next hop instead of information about the complete route (route method). The entries of a routing table must be consistent with one another.

Network-Specific Method Versus Host-Specific Method

A second technique to reduce the routing table and simplify the searching

process is called the network-specific method. Here, instead of having an entry for every destination host connected to the same physical network (host-specific method), we have only one entry that defines the address of the destination network itself. In other words, we treat all hosts connected to the same network as one single entity. For example, if 1000 hosts are attached to the same network, only one entry exists in the routing table instead of 1000.
Host-specific routing is used for purposes such as checking the route or providing security measures.

Default Method
Another technique to simplify routing is called the default method. Host A is connected to a network with two routers. Router Rl routes the packets to hosts connected to network N2. However, for the rest of the Internet, router R2 is used. So instead of listing all networks in the entire Internet, host A can just have one entry called the *default* (normally defined as network address 0.0.0.0).

Routing protocol [RGPV/ Dec 2012, Dec 2013, Jun 2014]

A **routing protocol** specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network

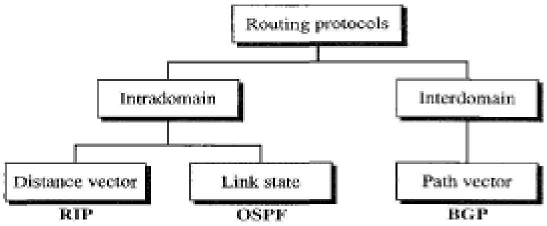


FIGURE : ROUTING PROTOCOL

Routing table

In computer networking a **routing table**, or **routing information base (RIB)**, is a data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The routing table contains information about the topology of the network immediately around it. The construction of routing tables is the primary goal of routing protocols. Static routes are entries made in a routing table by non-automatic means and which are fixed rather than being the result of some network topology "discovery" procedure.

Contents of routing tables

The routing table consists of at least three information fields:

1. the network id: i.e. the destination subnet
2. cost/metric: i.e. the cost or metric of the path through which the packet is to be sent
3. next hop: The next hop, or gateway, is the address of the next station to

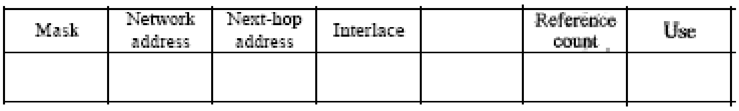
which the packet is to be sent on the way to its final destination

Depending on the application and implementation, it can also contain additional values that refine path selection:

1. quality of service associated with the route. For example, the U flag indicates that an IP route is up.
2. links to filtering criteria/access lists associated with the route
3. interface: such as eth0 for the first Ethernet card, eth1 for the second Ethernet card, etc.

Routing tables are also a key aspect of certain security operations, such as unicast reverse path forwarding (uRPF) In this technique, which has several variants, the router also looks up, in the routing table, the source address of the packet. If there exists no route back to the source address, the packet is assumed to be malformed or involved in a network attack, and is dropped.

Network id	**Cost**	**Next hop**
……..	……..	……..
……..	……..	……..



Mask	Network address	Next-hop address	Interlace		Reference count	Use

FIGURE : ROUTING TABLE

Static Routing Table

A **static routing table** contains information entered manually. The administrator enters the route for each destination into the table. When a table is created, it cannot update automatically when there is a change in the Internet. The table must be manually altered by the administrator.

A static routing table can be used in a small internet that does not change very often, or in an experimental internet for troubleshooting. It is poor strategy to use a static routing table in a big internet such as the Internet.

Dynamic Routing Table

A dynamic routing table is updated periodically by using one of the dynamic routing protocols such as RIP, OSPF, or BGP. Whenever there is a change in the Internet, such as a shutdown of a router or breaking of a link, the dynamic routing protocols update all the tables in the routers (and eventually in the host) automatically. The routers in a big internet such as the Internet need to be updated dynamically for efficient delivery of the IP packets.

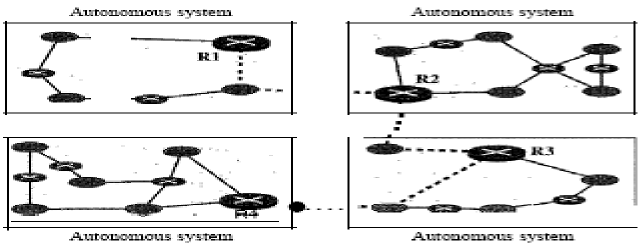


FIGURE : AUTONOMOUS SYSTEM

Autonomous System

Within the Internet, an **autonomous system** (**AS**) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the Internet.

Originally the definition required control by a single entity, typically an Internet service provider or a very large organization with independent connections to multiple networks, that adhere to a single and clearly defined routing policy, as originally defined in RFC 1771. The newer definition in RFC 1930 came into use because multiple organizations can run BGP using private AS numbers to an ISP that connects all those organizations to the Internet. Even though there may be multiple autonomous systems supported by the ISP, the Internet only sees the routing policy of the ISP. That ISP must have an officially registered **autonomous system number** (**ASN**).

Intra- and Interdomain Routing

Today, an internet can be so large that one routing protocol cannot handle the task of updating the routing tables of all routers. For this reason, an internet is divided into autonomous systems. An autonomous system (AS) is a group of networks and routers under the authority of a single administration. Routing inside an autonomous system is referred to as intradomain routing. Routing between autonomous systems is referred to as interdomain routing. Each autonomous system can choose one or more intradomain routing protocols to handle routing inside the autonomous system. However, only one interdomain routing protocol handles routing between autonomous systems.

Distance-vector routing protocol [RGPV/Dec 2010]

In computer communication theory relating to packet-switched networks, a **distance-vector routing protocol** is one of the two major classes of routing protocols, the other major class being the link-state protocol. Distance-vector routing protocols use the Bellman–Ford algorithm to calculate paths.

A distance-vector routing protocol requires that a router informs its neighbors of topology changes periodically. Compared to link-state protocols, which require a router to inform all the nodes in a network of topology changes, distance-vector routing protocols have less computational complexity and message overhead.

The term distance vector refers to the fact that the protocol manipulates vectors (arrays) of distances to other nodes in the network. The vector distance algorithm was the original ARPANET routing algorithm and was also used in the internet under the name of RIP (routing internet protocol).

Examples of distance-vector routing protocols include RIPv1 and RIPv2 and IGRP.

Method

Routers using distance-vector protocol do not have knowledge of the entire path to a destination. Instead they use two methods:

1. Direction in which router or exit interface a packet should be forwarded.
2. Distance from its destination

Distance-vector protocols are based on calculating the direction and distance to any link in a network. "Direction" usually means the next hop address and the exit interface. "Distance" is a measure of the cost to reach a certain node. The least cost route between any two nodes is the route with minimum distance. Each node maintains a vector (table) of minimum distance to every node. The cost of reaching a destination is calculated using various route metrics. RIP uses the hop count of the destination whereas IGRP takes into account other information such as node delay and available bandwidth.

Updates are performed periodically in a distance-vector protocol where all or part of a router's routing table is sent to all its neighbors that are configured to use the same distance-vector routing protocol. RIP supports cross-platform distance vector routing whereas IGRP is a Cisco Systems proprietary distance vector routing protocol. Once a router has this information it is able to amend its own routing table to reflect the changes and then inform its neighbors of the changes. This process has been described as ‘routing by rumor’ because routers are relying on the information they receive from other routers and cannot determine if the information is actually valid and true. There are a number of features which can be used to help with instability and inaccurate routing information.

EGP and BGP are not pure distance-vector routing protocols because a distance-vector protocol calculates routes based only on link costs whereas in BGP, for example, the local route preference value takes priority over the link cost.

Count-to-infinity problem

The Bellman–Ford algorithm does not prevent routing loops from happening and suffers from the **count-to-infinity problem**. The core of the count-to-infinity problem is that if A tells B that it has a path somewhere, there is no way for B to know if the path has B as a part of it. To see the problem clearly, imagine a subnet connected like A–B–C–D–E–F, and let the metric between the routers be "number of jumps". Now suppose that A is taken offline. In the vector-update-process B notices that the route to A, which was distance 1, is down – B does not receive the vector update from A. The problem is, B also gets an update from C, and C is still not aware of the fact that A is down – so it tells B that A is only two jumps from C (C to B to A), which is false. This slowly propagates through the network until it reaches infinity (in which case the algorithm corrects itself, due to the relaxation property of Bellman–Ford).

Workarounds and solutions

RIP uses the split horizon with poison reverse technique to reduce the chance of forming loops and uses a maximum number of hops to counter the 'count-to-infinity' problem. These measures avoid the formation of routing loops in some, but not all, cases. The addition of a *hold time* (refusing route updates for a few minutes after a route retraction) avoids loop formation in virtually all cases, but causes a significant increase in convergence times.

More recently, a number of loop-free distance vector protocols have been developed — notable examples are EIGRP, DSDV and Babel. These avoid loop formation in all cases, but suffer from increased complexity, and their deployment has been slowed down by the success of link-state routing protocols such as OSPF.

BELLMAN FORD ALGORITHM [RGPV/Jun 2006 / Dec 2008/Jun 2011/ Dec 2012/ Dec 2013]

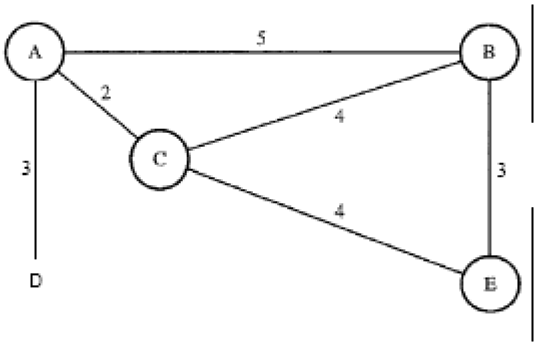
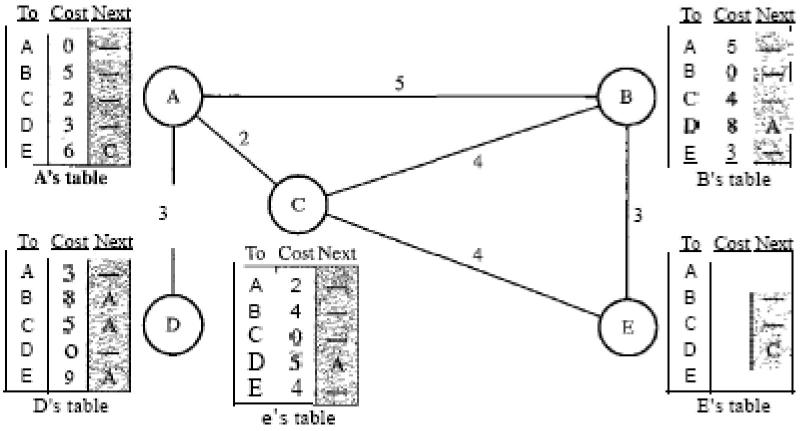


FIGURE : NETWORK



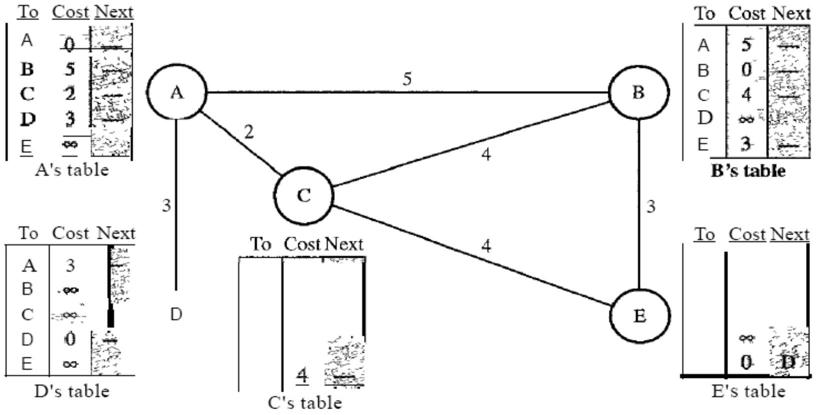
The table for node A shows how we can reach any node from this node. For example, our least cost to reach node E is 6. The route passes through C.

Initialization

The tables in Figure are stable; each node knows how to reach any other node and the cost. At the beginning, however, this is not the case. Each node can know only the distance between itself and its immediate neighbors, those directly connected to it.

So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors. Figure shows the initial tables for each node. The distance for any entry that is not a neighbor is marked as infinite (unreachable).

Initialization oftables in distance vector routing



Sharing

The whole idea of distance vector routing is the sharing of information between neighbors. Although node A does not know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E. On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C, node C also knows how to reach node D. In other words, nodes A and C, as immediate neighbors, can improve their routing tables if they help each other. There is only one problem. How much of the table must be shared with each neighbor? A node is not aware of a neighbor's table. The best solution for each node is to send its entire table to the neighbor and let the neighbor decide what part to use and what part to discard. However, the third column of a table (next stop) is not useful for the neighbor. When the neighbor receives a table, this column needs to be replaced with the sender's name. If any of the rows can be used, the next node is the sender of the table. A node therefore can send only the first two columns of its table to any neighbor. In other words, sharing here means sharing only the first two columns.

Updating

When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps:

1. The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear. If node C claims that its distance to a destination is *x* mi, and the distance between A and C is *y* mi, then the distance between A and that destination, via C, is *x* + *y* mi.

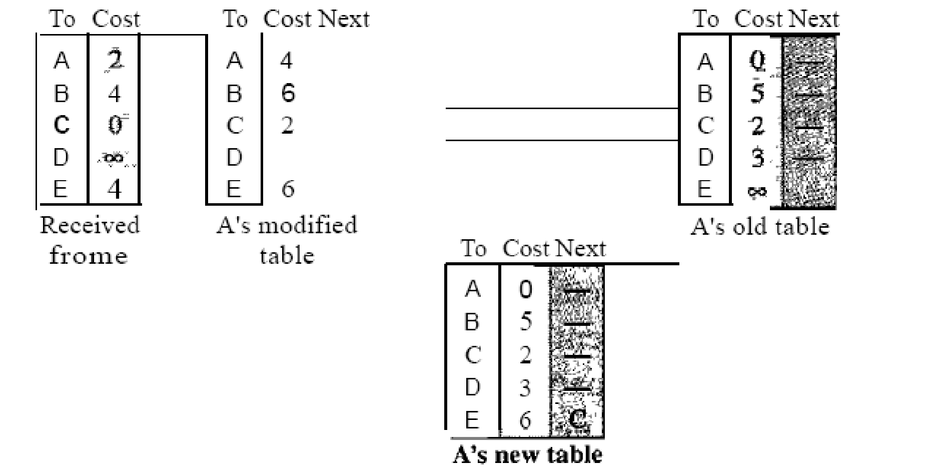
2. The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row. The sending node is the next node in the route.

3. The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

a. If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.

b. If the next-node entry is the same, the receiving node chooses the new row. For example, suppose node C has previously advertised a route to node X with distance 3. Suppose that now there is no path between C and X; node C now advertises this route with a distance of infinity. Node A must not ignore this value even though its old entry is smaller. The old route does not exist any more. The new route has a distance of infinity.

Updating in distance vector routing



Received frome

To	Cost
A	2
B	4
C	0
D	∞
E	4

A's modified table

To	Cost	Next
A	4	
B	6	
C	2	
D		
E	6	

A's old table

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	∞	—

A's new table

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

FIGURE : BELLMAN FORD ALGORITHM

There are several points we need to emphasize here. First, as we know from mathematics, when we add any number to infinity, the result is still infinity. Second, the modified table shows how to reach A from A via C. If A needs to reach itself via C, it needs to go to C and come back, a distance of 4. Third, the only benefit from this updating of node A is the last entry, how to reach E. Previously, node A did not know how to reach E (distance of infinity); now it knows that the cost is 6 via C.

Each node can update its table by using the tables received from other nodes. In a short time, if there is no change in the network itself, such as a failure in a link, each node reaches a stable condition in which the contents of its table remains the same.

When to Share

The question now is, When does a node send its partial routing table (only two columns) to all its immediate neighbors? The table is sent both periodically and when there is a change in the table.

Periodic Update

A node sends its routing table, normally every 30 s, in a periodic update. The period depends on the protocol that is using distance vector routing.

Triggered Update

A node sends its two-column routing table to its neighbors anytime there is a change in its routing table. This is called a triggered update. The change can result from the following.

1. A node receives a table from a neighbor, resulting in changes in its own table after updating.
2. A node detects some failure in the neighboring links which results in a distance change to infinity.

RIP

The Routing Information Protocol (RIP) is an intradomain routing protocol used inside an autonomous system. It is a very simple protocol based on distance vector routing. RIP implements distance vector routing directly with some considerations:

1. In an autonomous system, we are dealing with routers and networks (links). The routers have routing tables; networks do not.
2. The destination in a routing table is a network, which means the first column defines a network address.
3. The metric used by RIP is very simple; the distance is defined as the number of links (networks) to reach the destination. For this reason, the metric in RIP is called a hop count.
4. Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.
5. The next-node column defines the address of the router to which the packet is to be sent to reach its destination.

Figure shows an autonomous system with seven networks and four routers. The table of each router is also shown. Let us look at the routing table for Rl. The table has seven entries to show how to reach each network in the autonomous system. Router Rl is directly connected to networks 130.10.0.0 and 130.11.0.0, which means that there are no next-hop entries for these two networks. To send a packet to one of the three networks at the far left, router Rl needs to deliver the packet to R2. The next-node entry for these three networks is the interface of router R2 with IP address 130.10.0.1. To send a packet to the two networks at the far right, router Rl needs to send the packet to the interface of router R4 with IP address 130.11.0.1.

Link State Routing [RGPV/Dec 2009/ Jun 2010]

Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)-the node can use Dijkstra's algorithm to build a routing table.

Concept oflink state routing

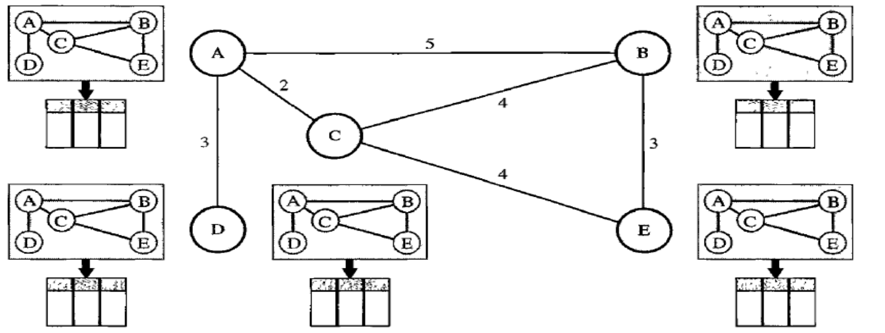


FIGURE: LINK STATE ROUTING

The figure shows a simple domain with five nodes. Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology. This is analogous to a city map. While each person may have the same map, each needs to take a different route to reach her specific destination.

The topology must be dynamic, representing the latest state of each node and each link. If there are changes in any point in the network (a link is down, for example), the topology must be updated for each node.

How can a common topology be dynamic and stored in each node? No node can know the topology at the beginning or after a change somewhere in the network. Link state routing is based on the assumption that, although the global knowledge about the topology is not clear, each node has partial knowledge: it knows the state (type, condition, and cost) of its links. In other words, the whole topology can be compiled from the partial knowledge of each node. Figure shows the same domain as in Figure, indicating the part of the knowledge belonging to each node.

Link state knowledge

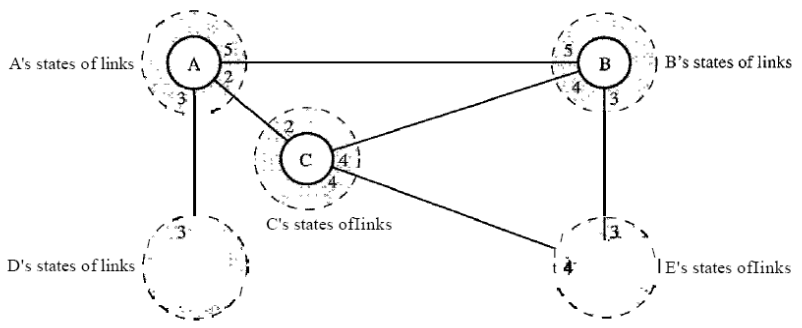


FIGURE: LINK STATE KNOWLEDGE

Node A knows that it is connected to node B with metric 5, to node C with metric 2, and to node D with metric 3. Node C knows that it is connected to node A with metric 2, to node B with metric 4, and to node E with metric 4. Node D knows that it is connected only to node A with metric 3. And so on. Although there is an overlap in the knowledge, the overlap guarantees the creation of a common topology-a picture of the whole domain for each node.

Dijkstra Algorithm[RGPV/Dec 2007, Dec 2010,Dec 2012]

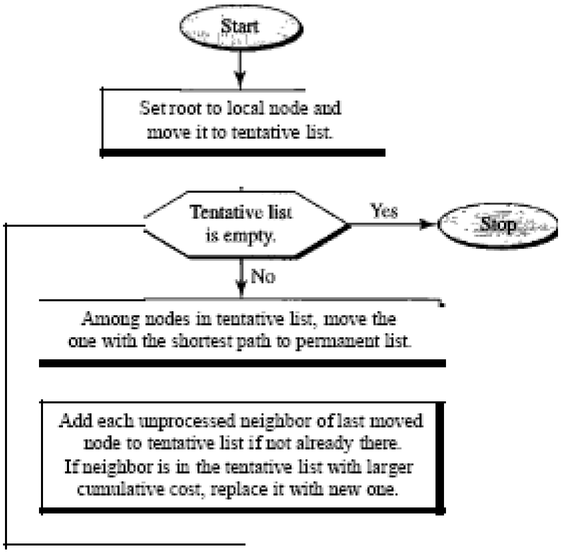
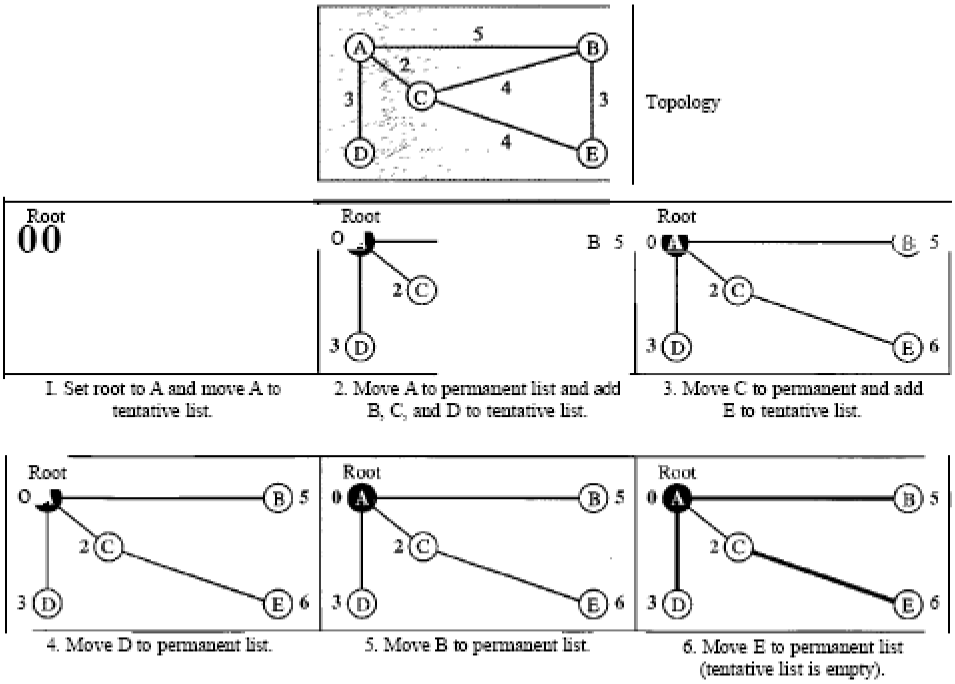

Start
Set root to local node and move it to tentative list.
Tentative list is empty.
Yes
Stop
No
Among nodes in tentative list, move the one with the shortest path to permanent list.
Add each unprocessed neighbor of last moved node to tentative list if not already there. If neighbor is in the tentative list with larger cumulative cost, replace it with new one.

FIGURE : DIJKSTRA ALGORITHM FLOW CHART



1. Set root to A and move A to tentative list.

2. Move A to permanent list and add B, C, and D to tentative list.

3. Move C to permanent and add E to tentative list.

4. Move D to permanent list.

5. Move B to permanent list.

6. Move E to permanent list (tentative list is empty).

FIGURE : DIJKSTRA ALGORITHM

1. We make node A the root of the tree and move it to the tentative list. Our two lists are Permanent list: empty Tentative list: A(O)
2. Node A has the shortest cumulative cost from all nodes in the tentative list. We move A to the permanent list and add all neighbors of A to the tentative list.

Our new lists are

Permanent list: A(O) Tentative list: B(5), C(2), D(3)

3. Node C has the shortest cumulative cost from all nodes in the tentative list. We move C to the permanent list. Node C has three neighbors, but node A is already processed, which makes the unprocessed neighbors just B and E. However, B is already in the tentative list with a cumulative cost of 5. Node A could also reach node B through C with a cumulative cost of 6. Since 5 is less than 6, we keep node B with a cumulative cost of 5 in the tentative list and do not replace it. Our new lists are

Permanent list: A(O), e(2) Tentative list: B(5), 0(3), E(6)

4. Node D has the shortest cumulative cost of all the nodes in the tentative list. We move D to the permanent list. Node D has no unprocessed neighbor to be added to the tentative list. Our new lists are

Permanent list: A(O), C(2), 0(3) Tentative list: B(5), E(6)

5. Node B has the shortest cumulative cost of all the nodes in the tentative list. We move B to the permanent list. We need to add all unprocessed neighbors of B to the tentative list (this is just node E). However, E(6) is already in the list with a smaller cumulative cost. The cumulative cost to node E, as the neighbor of B, is 8. We keep node E(6) in the tentative list. Our new lists are

Permanent list: A(O), B(5), C(2), 0(3) Tentative list: E(6)

6. Node E has the shortest cumulative cost from all nodes in the tentative list. We move E to the permanent list. Node E has no neighbor. Now the tentative list is empty. We stop; our shortest path tree is ready. The final lists are Permanent list: A(O), B(5), C(2), D(3), E(6) Tentative list: empty

OSPF

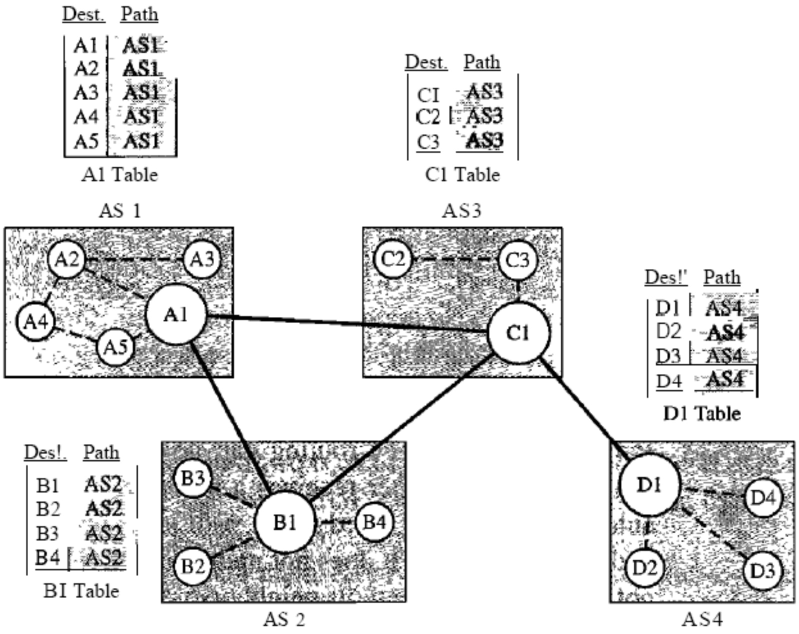
The Open Shortest Path First or OSPF protocol is an intradomain routing protocol based on link state routing. Its domain is also an autonomous system.

Areas To handle routing efficiently and in a timely manner, OSPF divide an autonomous system into areas. An area is a collection of networks, hosts, and routers all contained within an autonomous system. An autonomous system can be divided into many different areas. All networks inside an area must be connected. Routers inside an area flood the area with routing information. At the border of an area, special routers called area border routers summarize the information about the area and send it to other areas. Among the areas inside an autonomous system is a special area called the *backbone;* all the areas inside an autonomous system must be connected to the backbone. In other words, the backbone serves as a primary area and the other areas as secondary areas. This does not mean that the routers within areas cannot be connected to each other, however. The routers inside the backbone are called the backbone routers. Note that a backbone router can also be an area border router. If, because of some problem, the connectivity between a backbone and an area is broken, a virtual link between routers must be created by an administrator to allow continuity of the functions of the backbone as the primary area. Each area has area identification. The area identification of the backbone is zero.

Path Vector Routing

Distance vector and link state routing are both intradomain routing protocols. They can be used inside an autonomous system, but not between autonomous systems. These two protocols are not suitable for interdomain routing mostly because of scalability. Both of these routing protocols become intractable when the domain of operation becomes large. Distance vector routing is subject to instability if there are more than a few hops in the domain of operation. Link state routing needs a huge amount of resources to calculate routing tables. It also creates heavy traffic because of flooding. There is a need for a third routing protocol which we call path vector routing. Path vector routing proved to be useful for interdomain routing. The principle of path vector routing is similar to that of distance vector routing. In path vector routing, we assume that there is one node (there can be more, but one is enough for our conceptual discussion) in each autonomous system that acts on behalf of the entire autonomous system. Let us call it the speaker node. The speaker node in an AS creates a routing table and advertises it to speaker nodes in the neighboring ASs. The idea is the same as for distance vector routing except that only speaker nodes in each AS can communicate with each other. However, what is advertised is different. A speaker node advertises the path, not the metric of the nodes, in its autonomous system or other autonomous systems

Initial routing tables in path vector routing



Dest.	Path
A1	AS1
A2	AS1
A3	AS1
A4	AS1
A5	AS1

A1 Table

Dest.	Path
CI	AS3
C2	AS3
C3	AS3

C1 Table

Des!'	Path
D1	AS4
D2	AS4
D3	AS4
D4	AS4

D1 Table

Des!.	Path
B1	AS2
B2	AS2
B3	AS2
B4	AS2

BI Table

BGP

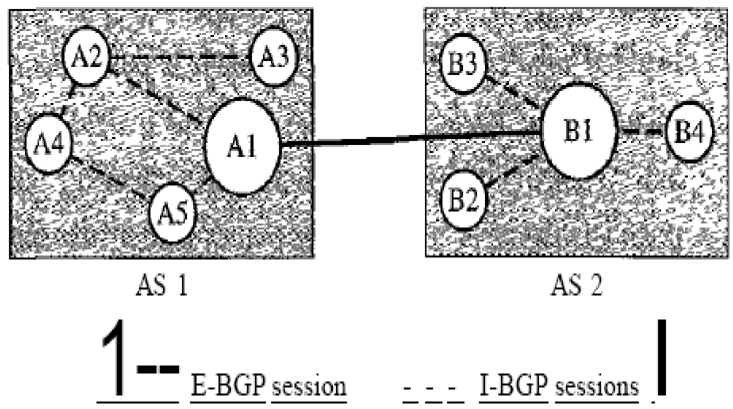
Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing. It first appeared in 1989 and has gone through four versions. Types **of Autonomous** Systems As we said before, the Internet is divided into hierarchical domains called autonomous systems. For example, a large corporation that manages its own network and has full control over it is an autonomous system. A local ISP that provides services to local customers is an autonomous system. We can divide autonomous systems into three categories: stub, multihomed, and transit.

Stub AS. A stub AS has only one connection to another AS. The interdomain data traffic in a stub AS can be either created or terminated in the AS. The hosts in the AS can send data traffic to other ASs. The hosts in the AS can receive data coming from hosts in other ASs. Data traffic, however, cannot pass through a stub AS. A stub AS is either a source or a sink. A good example of a stub AS is a small corporation or a small local ISP.

Multihomed AS. A multihomed AS has more than one connection to other ASs, but it is still only a source or sink for data traffic. It can receive data traffic from more than one AS. It can send data traffic to more than one AS, but there is no transient traffic. It does not allow data coming from one AS and going to another AS to pass through. A good example of a multihomed AS is a large corporation that is connected to more than one regional or national AS that does not allow transient traffic.

Transit AS. A transit AS is a multihomed AS that also allows transient traffic. Good examples of transit ASs are national and international ISPs (Internet backbones).

Internal and external BGP sessions



S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain distance vector routing with suitable example.	Dec 2012	7
Q.2	Write a short note on bellman-ford routing algorithm. Explain the drawback of count to infinity in bellman-ford algorithm.	Jun 2006 Dec 2008 Jun 2011	7
Q.3	Explain the two classes of routing algorithm- (i) Adaptive algorithm (ii) Non-adaptive algorithm Discuss about multipath routing.	Dec 2011	7
Q.4	compare the following- (i) Adaptive vs. non-adaptive routing (ii) Centralized, isolated and distributed routing.	Jun 2011	7
Q.5	Explain least cost routing algorithm with example.	Jun 2010	7
Q.6	What is optimality principle? Why it is used in routing? Explain the shortest path routing algorithm.	Dec 2008 Dec 2009	7
Q.7	Apply dijkstra routing algorithm to calculate shortest path with source vertex	Dec 2007 Dec 2010	7
Q.8	Describe about unicast routing protocol and multicast routing protocol.	Dec 2013	7
Q.9	Explain bellman ford algorithm with example.	Dec 2012 Dec 2013	7
Q.10	Describe the different adaptive routing	Dec 2012	7

	strategies. What are the advantages and disadvantages of adaptive routing strategies?		
Q.11	State and Describe the dijkstra algorithm with example.	Dec 2012	7
Q.12	Name different unicast routing protocols any explain any of them in details	Jun 2014	7
Q.13	Name different multicast routing protocols any explain any of them in details	Jun 2014	7

UNIT 4/LECTURE 12

Internetworking Device

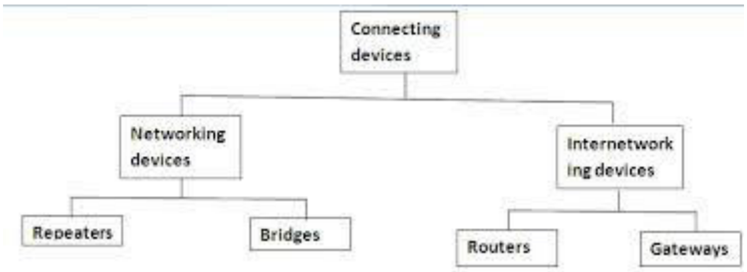


FIGURE: INTERNETWORKING DEVICE

Internetworking Device [RGPV/Dec 2011, Jun 2013]

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.

Based on designs developed in the 1960s, the Advanced Research Projects Agency Network (ARPANET) was created in 1969 by the U.S. Department of Defense. This early network design was based on circuit switching. The first device to function as a router was the Interface Message Processors that made up ARPANET to form the first data packet network.

The initial idea for a router, which was then called a gateway, came from a group of computer networking researchers who formed an organization called the International Network Working Group, which became a subcommittee of the International Federation for Information Processing in 1972.

In 1974, the first true router was developed and by 1976, three PDP-11-based routers were used to form a prototype experimental version of the Internet. From the mid-1970s to the 1980s, mini-computers were used as routers. Today, high-speed modern routers are actually very specialized computers with extra hardware for rapid data packet forwarding and specialized security functions such as encryption.

When several routers are used in a collection of interconnected networks, they exchange and analyze information, and then build a table of the preferred routes and the rules for determining routes and destinations for that data. As a network interface, routers convert computer signals from one standard protocol to another that's more appropriate for the destination network. Large routers determine interconnectivity within an enterprise, between enterprises and the Internet, and between different internet service providers (ISPs); small routers determine interconnectivity for office or home networks. ISPs and major enterprises exchange routing information using border gateway protocol (BGP).

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 network bridge device is primarily used in local area networks because they can potentially flood and clog a large network thanks to their ability to broadcast data to all the nodes if they don’t know the destination node's MAC address.

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.[1] 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[2]

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 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.[*citation needed*]

Both the computers of Internet users and the computers that serve pages to users are host nodes, while the nodes that connect the networks in between are gateways. For example, the computers that control traffic between company networks or the computers used by internet service providers (ISPs) to connect users to the internet are gateway nodes.

In the network for an enterprise, a computer server acting as a gateway node is often also acting as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.

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 into 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 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.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Write short notes on the following networking devices- (iv) Switches (v) Bridges (vi) Hubs (vii) gateway	Dec 2011	7
Q.2	Explain the following: (i) Bridges (ii) Routers (iii)Gateways	Jun 2013	7

UNIT – 5

Transport Layer Services

Unit-05/Lecture-01/ Lecture-02

Transport Layer Services [RGPV/ Jun 2013, Dec 2013, Jun 2014]

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 through the use of 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, so as 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 3-WAY HANDSHAKE (SYN,SYN-ACK,ACK)

The TCP three-way handshake in Transmission Control Protocol (also called the TCP-handshake; three message handshake and/or SYN-SYN-ACK) is the method used by TCP set up a TCP/IP connection over an Internet Protocol based network. TCP's three way handshaking technique is often referred to as "SYN-SYN-ACK" (or more accurately SYN, SYN-ACK, ACK) because there are three messages transmitted by TCP to negotiate and start a TCP session between two computers. The TCP handshaking mechanism is designed so that two computers attempting to communicate can negotiate the parameters of the network TCP socket connection before transmitting data such as SSH and HTTP web browser requests.

This 3-way handshake process is also designed so that both ends can initiate and negotiate separate TCP socket connections at the same time. Being able to negotiate multiple TCP socket connections in both directions at the same time allows a single physical network interface, such as ethernet, to be multiplexed to transfer multiple streams of TCP data simultaneously.

Below is a (very) simplified diagram of the TCP 3-way handshake process. Have a look at the diagram on the right as you examine the list of events on the left.

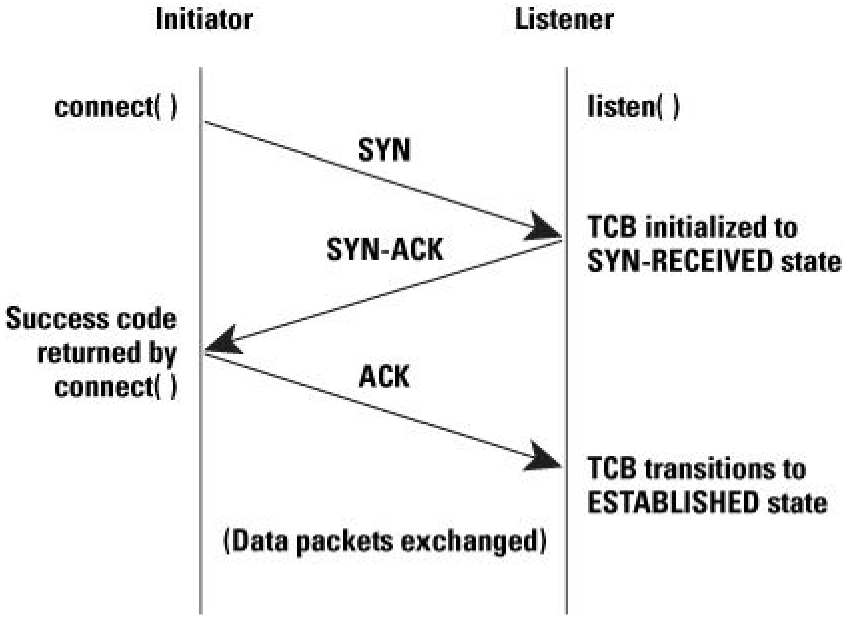

Initiator
Listener
connect( )
listen( )
SYN
TCB initialized to SYN-RECEIVED state
SYN-ACK
Success code returned by connect( )
ACK
TCB transitions to ESTABLISHED state
(Data packets exchanged)

FIGURE: TCP 3-WAY HANDSHAKE DIAGRAM

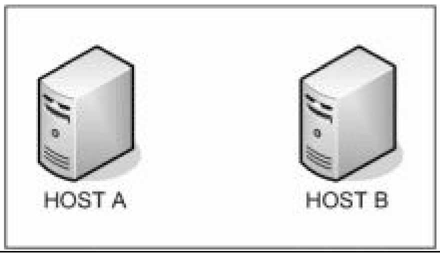


FIGURE: EVENT DIAGRAM

Host A sends a TCP SYNchronize packet to Host B
Host B receives A's SYN
Host B sends a SYNchronize-ACKnowledgement
Host A receives B's SYN-ACK
Host A sends ACKnowledge
Host B receives ACK.
TCP socket connection is ESTABLISHED.
TCP Three Way Handshake
(SYN,SYN-ACK,ACK)

SYNchronize and ACKnowledge messages are indicated by a either the SYN bit, or the ACK bit inside the TCP header, and the SYN-ACK message has both the SYN and the ACK bits turned on (set to 1) in the TCP header.

TCP knows whether the network TCP socket connection is opening, synchronizing, established by using the SYNchronize and ACKnowledge messages when establishing a network TCP socket connection.

When the communication between two computers ends, another 3-way communication is performed to tear down the TCP socket connection. This setup and teardown of a TCP socket connection is part of what qualifies TCP a reliable protocol. TCP also acknowledges that data is successfully received and guarantees the data is reassembled in the correct order.

UDP is connectionless. That means UDP doesn't establish connections as TCP does, so UDP does not perform this 3-way handshake and for this reason, it is referred to as an unreliable protocol. That doesn't mean UDP can't transfer data, it just doesn't negotiate how the connection will work, UDP just transmits and hopes for the best.

PROTOCOLS ENCAPSULATED IN TCP

FTP, Telnet, HTTP, HTTPS, SMTP, POP3, IMAP, SSH and any other protocol that rides over TCP also has a three way handshake performed as connection is opened. HTTP web requests, SMTP emails, FTP file transfers all manage the messages they each send. TCP handles the transmission of those messages.

TCP 'rides' on top of Internet Protocol (IP) in the protocol stack, which is why the combined pair of Internet protocols is called TCP/IP (TCP over IP). TCP segments are passed inside the payload section of the IP packets. IP handles IP addressing and routing and gets the packets from one place to another, but TCP manages the actual communication sockets between endpoints (computers at either end of the network or internet connection).

Process to Process Delivery

* UDP and TCP are transport-layer protocols that create a process-to-process communication.
* UDP is an unreliable and connectionless protocol that requires little overhead and offers fast delivery.
* In the client-server paradigm, an application program on the local host, called

the client, needs services from an application program on the remote host, called a server.

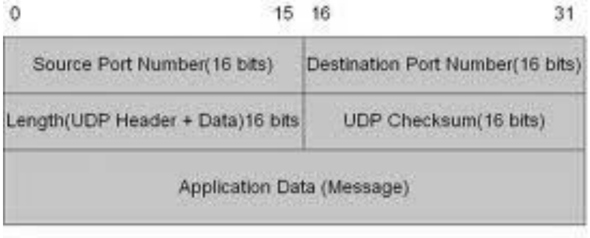
* Each application program has a unique port number that distinguishes it from other programs running at the same time on the same machine.
* The client program is assigned a random port number called the ephemeral port number.
* The server program is assigned a universal port number called a well-known port number.
* The combination of the IP address and the port number, called the socket address, uniquely defines a process and a host.
* The UDP packet is called a user datagram.
* UDP has no flow control mechanism.
* Transmission Control Protocol (TCP) is a connection-oriented, reliable, stream transport-layer protocol in the Internet model.
* The unit of data transfer between two devices using TCP software is called a segment; it has 20 to 60 bytes of header, followed by data from the application program.
* TCP uses a sliding window mechanism for flow control.
* Error detection is handled in TCP by the checksum, acknowledgment, and time-out.
* Corrupted and lost segments are retransmitted, and duplicate segments are discarded.
* TCP uses four timers—retransmission, persistence, keep-alive, and time-waited—in its operation.
* Connection establishment requires three steps; connection termination normally requires four steps.
* TCP software is implemented as a finite state machine.
* The TCP window size is determined by the receiver.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	With neat sketch explain connection establishment and release using 3-way handshaking in transport layer.	Dec 2007	7
Q.2	Explain the issue of addressing, multiplexing and flow control in connection-oriented transport protocol mechanisms.	Dec 2011	7
Q.3	Write short notes on transport services.	Dec 2013	5
Q.4	Explain how the connection is released in a TCP.	Jun 2013	7
Q.5	Explain the following terms in the context of transport layer: Three way handshake	Jun 2013	7
Q.6	How flow control is managed in TCP? Explain in detail.	Jun 2013	7
Q.7	Enlist various services provided by transport layer to its upper layer and explain why they are required.	Jun 2014	7

UDP

Unit-05/Lecture-03

UDP [RGPV/Dec 2009/ Jun 2010/ Dec 2010/ Jun 2011/Dec 2011 / Dec 2012/ Dec 2013]



0 15	16 31
Source Port Number(16 bits)	Destination Port Number(16 bits)
Length(UDP Header + Data)16 bits	UDP Checksum(16 bits)
Application Data (Message)	

FIGURE : UDP HEADER

General Header

The general header (packet header) defines the endpoints of each association to which the packet belongs, guarantees that the packet belongs to a particular association, and preserves the integrity of the contents of the packet including the header itself. There are four fields in the general header:

- **Source port address** This is a 16-bit field that defines the port number of the process sending the packet.

- **Destination port address** This is a 16-bit field that defines the port number of the process receiving the packet.

- **Verification tag** This is a number that matches a packet to an association. This prevents a packet from a previous association from being mistaken as a packet in this association. It serves as an identifier for the association; it is repeated in every packet during the association. There is a separate verification used for each direction in the association.

- **Checksum** This 32-bit field contains a CRC-32 checksum. Note that the size of the checksum is increased from 16 (in UDP, TCP, and IP) to 32 bits to allow the use of the CRC-32 checksum.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Why UDP does exist? Would it not have been enough to just let user processes send raw IP packets?	Jun 2011	7
Q.2	Why is UDP needed? why can't user program directly access IP?	Dec 2011	7
Q.3	Give the format of UDP datagram and explain the semantics of every field. How is the checksum in the header computed?	Dec 2010	7
Q.4	What is UDP? In case where reliability is not a primary importance, UDP would make a good transport protocol. Give example of specific	Dec 2009	7

	case.		
Q.5	What does UDP provide that is not provided by IP?	Dec 2012	7

Unit-05/Lecture-04

TCP

TCP SEGMENT[RGPV/Dec 2009/ Jun 2010/ Dec 2011/Dec 2012/ Dec 2013]
The segment consists of a 20- to 60-byte header, 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.

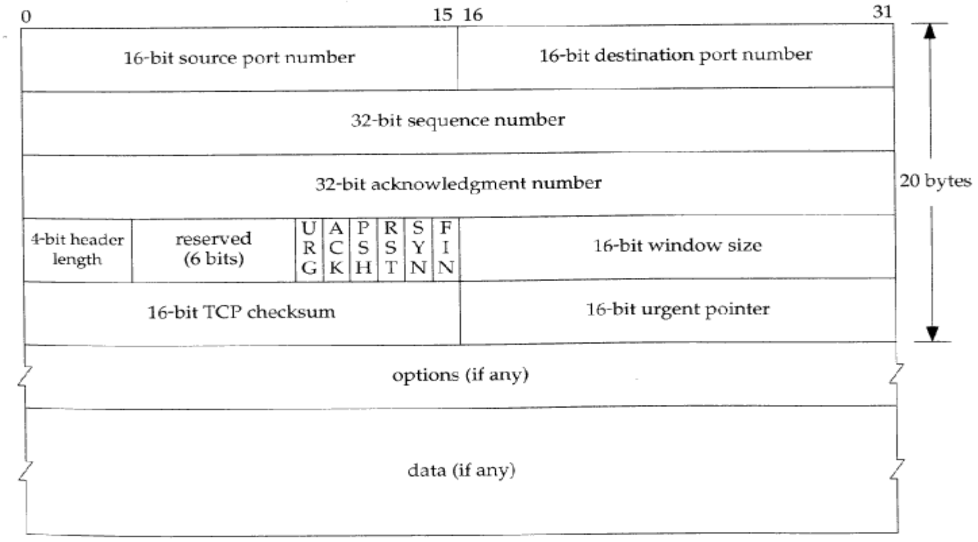


FIGURE : TCP HEADER

- **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. This serves the same purpose as the source port address in the UDP header.

- **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. This serves the same purpose as the destination port address in the UDP header.

- **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. The sequence number tells the destination which byte in this sequence comprises the first byte in the segment. During connection establishment, each party uses a random number generator to create an initial sequence number (ISN), which is usually different in each direction.

- **Acknowledgment number** This 32-bit field defines the byte number that the receiver of the segment is expecting to receive from the other party. If the receiver of the segment has successfully received byte number x from the other party, it defines x + I as the acknowledgment number. Acknowledgment and data can be piggybacked together.

- **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. Therefore, the value of this field can be between 5 (5 x 4 =20) and 15 (15 x 4 =60).

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

- **Control** This field defines 6 different control bits or flags. One or more of these bits can be set at a time.

Control field

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

These bits enable flow control, connection establishment and termination, connection abortion, and the mode of data transfer in TCP.

Flag Description

- **URG** The value of the urgent pointer field is valid.
- **ACK** The value of the acknowledgment field is valid.
- **PSH** Push the data.
- **RST** Reset the connection.
- **SYN** Synchronize sequence numbers during connection.
- **FIN** Terminate the connection.

- **Window size** This field defines the size of the window, in bytes, that the other party must maintain. Note that the length of this field is 16 bits, which means that the maximum size of the window is 65,535 bytes. This value is normally referred to as the receiving window (rwnd) and is determined by the receiver. The sender must obey the dictation of the receiver in this case.

- **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. However, the inclusion of the checksum in the UDP datagram is optional, whereas the inclusion of the checksum for TCP is mandatory. The same pseudoheader, serving the same purpose, is added to the segment. For the TCP pseudoheader, the value for the protocol field is 6.

- **Urgent pointer** This l6-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data. It defines the number that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.

- **Options** There can be up to 40 bytes of optional information in the TCP header. We will not discuss these options here; please refer to the reference list for more information.

A TCP Connection

TCP is connection-oriented. A connection-oriented transport protocol establishes a virtual path between the source and destination. All 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. You may wonder how TCP, which uses the services of IP, a connectionless protocol, can be connection-oriented. The point is that a TCP connection is virtual, not physical. TCP operates at a higher level. TCP uses the services of IP to deliver individual segments to the receiver, but it controls the connection itself. If a segment is lost or corrupted, it is retransmitted. Unlike TCP, IP is unaware of this retransmission. If a segment arrives out of order, TCP holds it until the missing segments arrive; IP is unaware of this reordering.

In TCP, connection-oriented transmission requires three phases: connection establishment, data transfer, and connection termination.

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.

Three-Way Handshaking The connection establishment in TCP is called three way handshaking. In our example, an application program, called the client, wants to make a connection with another application program, called the server, using TCP as the transport layer protocol.

The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This is called a request for a passive open. Although the server TCP is ready to accept any connection from any machine in the world, it cannot make the connection itself. The client program issues a request for an active open. A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server. TCP can now start the three-way handshaking process. To show the process, we use two time lines: one at each site. Each segment has values for all its header fields and perhaps for some of its option fields, too.

The three steps in this phase are as follows.

1. The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence numbers. It consumes one sequence number. When the data transfer starts, the sequence number is incremented by 1. We can say that the SYN segment carries no real data, but we can think of it as containing 1 imaginary byte.

A SYN segment cannot carry data, but it consumes one sequence number.

2. The server sends the second segment, a SYN +ACK segment, with 2 flag bits

set: SYN and ACK. This segment has a dual purpose. It is a SYN segment for communication in the other direction and serves as the acknowledgment for the SYN segment. It consumes one sequence number.
A SYN +ACK segment cannot carry data, but does consume one sequence number.

3. The client sends the third segment. This is just an ACK segment. It acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field. Note that the sequence number in this segment is the same as the one in the SYN segment; the ACK segment does not consume any sequence numbers. An ACK segment, if carrying no data, consumes no sequence number. Simultaneous Open A rare situation, called a simultaneous open, may occur when both processes issue an active open. In this case, both TCPs transmit a SYN + ACK segment to each other, and one single connection is established between them. SYN Flooding Attack The connection establishment procedure in TCP is susceptible to a serious security problem called the SYN flooding attack. This happens when a malicious attacker sends a large number of SYN segments to a server, pretending that each of them is corning from a different client by faking the source IP addresses in the datagrams. The server, assuming that the clients are issuing an active open, allocates the necessary resources, such as creating communication tables and setting timers. The TCP server then sends the SYN +ACK segments to the fake clients, which are lost. During this time, however, a lot of resources are occupied without being used. If, during this short time, the number of SYN segments is large, the server eventually runs out of resources and may crash. This SYN flooding attack belongs to a type of security attack known as a denial-of-service attack, in which an attacker monopolizes a system with so many service requests that the system collapses and denies service to every request.
Some implementations of TCP have strategies to alleviate the effects of a SYN attack. Some have imposed a limit on connection requests during a specified period of time. Others filter out datagrams coming from unwanted source addresses. One recent strategy is to postpone resource allocation until the entire connection is set up, using what is called a cookie. SCTP, the new transport layer protocol that we discuss in the next section, uses this strategy.

Data Transfer
After connection is established, bidirectional data transfer can take place. The client and server can both send data and acknowledgments. We will study the rules of acknowledgment later in the chapter; for the moment, it is enough to know that data traveling in the same direction as an acknowledgment are carried on the same segment. The acknowledgment is piggybacked with the data.

Urgent Data TCP is a stream-oriented protocol. This means that the data are presented from the application program to TCP as a stream of bytes. Each byte of data has a position in the stream. However, on occasion an application program needs to send urgent bytes. This means that the sending application program wants a piece of data to be read out of order by the receiving application program. As an example, suppose that the sending application program is sending data to be processed by the receiving application program. When the result of processing comes back, the sending application program finds that everything is wrong. It wants to abort the process, but it has already sent a huge amount of data. If it issues an abort command (control +C), these two characters will be stored at the end of the receiving TCP buffer. It will be delivered to the receiving application program after all the data have been processed. The solution is to send a segment with the URG bit set. The sending application program tells the sending TCP that the piece of data is urgent. The sending TCP creates a segment and inserts the urgent data at the beginning of the segment. The rest of the segment can contain normal data from the buffer. The urgent pointer field in the header defines the end of the urgent data and the start of normal data. When the receiving TCP receives a segment with the URG bit set, it extracts the urgent data from the segment, using the value of the urgent pointer, and delivers them, out of order, to the receiving application program.

Connection Termination
Any of the two parties involved in exchanging data (client or server) can close the connection, although it is usually initiated by the client. Most implementations today allow two options for connection termination: three-way handshaking and four-way handshaking with a half-close option.

Three-Way Handshaking Most implementations today allow three-way handshaking for connection termination. In a normal situation, the client TCP, after receiving a close command from the client process, sends the first segment, a FIN segment in which the FIN flag is set. Note that a FIN segment can include the last chunk of data sent by the client. Connection termination using three-way handshaking can be just a control segment as shown in Figure 23.20. If it is only a control segment, it consumes only one sequence number.

The FIN segment consumes one sequence number ifit does not carry data. 2. The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN +ACK segment, to confirm the receipt of the FIN segment from the client and at the same time to announce the closing of the connection in the other direction. This segment can also contain the last chunk of data from the server. If it does not carry data, it consumes only one sequence number.
The FIN +ACK segment consumes one sequence number if it does not carry data.

3. The client TCP sends the last segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server. This segment contains the acknowledgment number, which is 1 plus the sequence number received in the FIN segment from the server. This segment cannot carry data and consumes no sequence numbers. Half-Close In TCP, one end can stop sending data while still receiving data. This is called a half-close. Although either end can issue a half-close, it is normally initiated by the client. It can occur when the server needs all the data before processing can begin. A
good example is sorting. When the client sends data to the server to be sorted, the server needs to receive all the data before sorting can start. This means the client, after sending all the data, can close the connection in the outbound direction. However, the inbound direction must remain open to receive the sorted data. The server, after receiving the data, still needs time for sorting; its outbound direction must remain open. By sending a FIN segment. The server accepts the half-close by sending the ACK segment. The data transfer from the client to the server stops. The server, however, can still send data. When the server has sent all the processed data, it sends a FIN segment, which is acknowledged by an ACK from the client.

After half-closing of the connection, data can travel from the server to the client and acknowledgments can travel from the client to the server. The client cannot send any more data to the server. Note the sequence numbers we have used. The second segment (ACK) consumes no sequence number. Although the client has received sequence number y - 1 and is expecting y, the server sequence number is still y - 1. When the connection finally closes, the sequence number of the last ACK segment is still x, because no sequence numbers are consumed during data transfer in that direction.

Flow Control

TCP uses a sliding window to handle flow control. The sliding window protocol used by TCP, however, is something between the Go-Back-N and Selective Repeat sliding window.

the Go-Back-N protocol because it does not use NAKs; it looks like Selective Repeat because the receiver holds the out-of-order segments until the missing ones arrive. There are two big differences between this sliding window and the one we used at the data link layer. First, the sliding window ofTCP is byte-oriented; the one we discussed in the data link layer is frame-oriented. Second, the TCP's sliding window is of variable size; the one we discussed in the data link layer was of fixed size.

the sliding window n TCP. The window spans a portion of the buffer containing bytes received from the process. The bytes inside the window are the bytes that can be in transit; they can be sent without worrying about acknowledgment. The imaginary window has two walls: one left and one right. The window is opened, closed, or shrunk. These three activities, as we will see, are in the control of the receiver (and depend on congestion in the network), not the sender.

The sender must obey the commands of the receiver in this matter. Opening a window means moving the right wall to the right. This allows more new bytes in the buffer that are eligible for sending. Closing the window means moving the left wall to the right. This means that some bytes have been acknowledged and the sender need not worry about them anymore. Sluinking the window means moving the right wall to the left. This is strongly discouraged and not allowed in some implementations because it means revoking the eligibility of some bytes for sending. This is a problem if the sender has already sent these bytes. Note that the left wall cannot move to the left because this would revoke some of the previously sent acknowledgments. A sliding window is used to make transmission more efficient as weD as to control the flow of data so that the destination does not become overwhelmed with data. TCP sliding windows are byte-oriented. The size of the window at one end is determined by the lesser of two values: receiver window (rwnd) or congestion window (cwnd). The receiver window is the value advertised by the opposite end in a segment containing acknowledgment. It is the number of bytes the other end can accept before its buffer overflows and data are discarded. The congestion window is a value determined by the network to avoid congestion.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Compare TCP and OSI class 4 transport protocol	Dec 2011	7
Q.2	Differentiate between TCP & UDP?	Jun 2010 Dec 2013	7
Q.3	How does reliability in data transmission? explain	Dec 2012	7

Q.4	How does fast retransmission improve TCP's overall utilization of network resources?	Dec 2010	7
Q.5	Draw and explain the TCP header. Explain each field in detail.	Dec 2012	7
Q.6	What is window management in TCP?	Dec 2012	7

Unit-05/Lecture-05/Lecturer- 06

Integrated Services & Differentiated Services

INTEGRATED SERVICES [RGPV/Dec 2009/Dec 2013/Jun 2014]

Two models have been designed to provide quality of service in 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 IntServ, 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

In the Integrated Services model, an application program needs resource reservation. As we learned in the discussion of the IntServ model, the resource reservation is for a flow. This means that if we want to use IntServ 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 in 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 travelled 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 a 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 in the Internet:

- scalability
- service-type limitation

Scalability

The Integrated Services model requires that each router keep 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-load. Those opposing this model argue that applications may need more than these two types of services.

DIFFERENTIATED SERVICES [RGPV/Dec 2009/ Jun 2014]

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.

Differentiated Services is a class-based QoS model designed for IP.

DS Field

In Diffserv, each packet contains a field called the DS field. The value of this field is set at the boundary of the network by the host or the first router designated as the boundary router. IETF proposes to replace the existing TOS (type of service) field in IPv4 or the class field in IPv6 by the DS field

The DS field contains two subfields: DSCP and CU. The DSCP (Differentiated Services Code Point) is a 6-bit subfield that defines the per-hop behavior (PHB). The 2-bit CU (currently unused) subfield is not currently used.

The Diffserv capable node (router) uses the DSCP 6 bits as an index to a table defining the packet-handling mechanism for the current packet being processed.

Per-Hop Behavior

The Diffserv model defines per-hop behaviors (PHBs) for each node that receives a packet. So far three PHBs are defined: DE PHB, EF PHB, and AF PHB. DE PHB The DE PHB (default PHB) is the same as best-effort delivery, which is compatible with TOS.

- Low latency
- Ensured bandwidth

This is the same as having a virtual connection between the source and destination. AF PHB The AF PHB (assured forwarding PHB) delivers the packet with a high assurance as long as the class traffic does not exceed the traffic profile of the node. The users of the network need to be aware that some packets may be discarded.

Traffic Conditioner

To implement Oiffserv, the OS node uses traffic conditioners such as meters, markers, shapers, and droppers

Meters

The meter checks to see if the incoming flow matches the negotiated traffic profile. The meter also sends this result to other components. The meter can use several tools such as a token bucket to check the profile.

Marker

A marker can remark a packet that is using best-effort delivery (OSCP: 000000) or down-mark a packet based on information received from the meter. Downmarking (lowering the class of the flow) occurs if the flow does not match the profile. A marker does not up-mark (promote the class) a packet.

Shaper

A shaper uses the information received from the meter to reshape the traffic if it is not compliant with the negotiated profile.

Dropper

A dropper, which works as a shaper with no buffer, discards packets if the flow severely violates the negotiated profile.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain the following- (iv) Integrated services (v) Differentiated services	Dec 2009	7
Q.2	Write short notes on integrated service.	Dec 2013	5
Q.3	compare integrated service and differentiated service.	Jun 2014	7

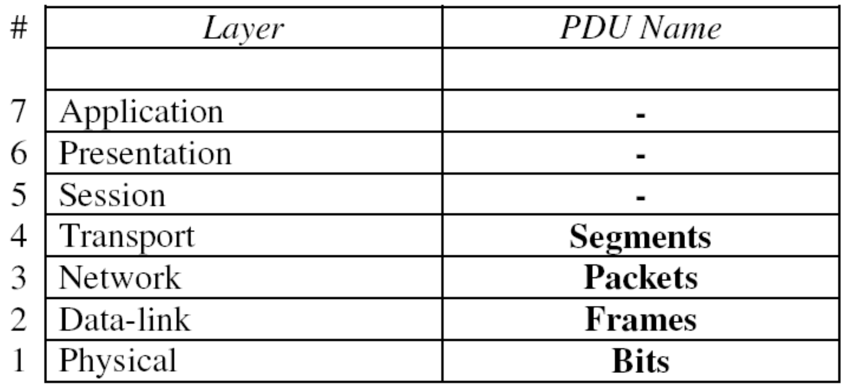
Unit-05/Lecture-07

INTERNETWORKING DEVICE

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:



#	*Layer*	*PDU Name*
7	Application	-
6	Presentation	-
5	Session	-
4	Transport	**Segments**
3	Network	**Packets**
2	Data-link	**Frames**
1	Physical	**Bits**

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).

However, the strict definitions of the terms switch and router have blurred over time, which can result in confusion. For example, the term switch can now refer to devices that operate at layers higher than Layer-2. This will be explained in greater detail in this guide.

Icons for Network Devices

The following icons will be used to represent network devices

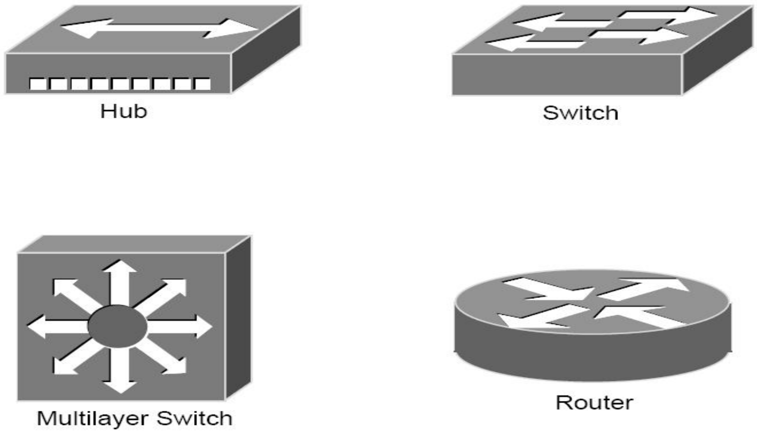


FIGURE: NETWORK DEVICES

Layer-1 Hubs [RGPV/Jun 2011]

Hubs are Layer-1 devices that physically connect network devices together for communication. Hubs can also be referred to as repeaters. Hubs provide no intelligent forwarding whatsoever. Hubs are incapable of processing either Layer-2 or Layer-3 information, and thus cannot make decisions based on hardware or logical addressing.

Thus, hubs will always forward every frame out every port, excluding the port originating the frame. Hubs do not differentiate between frame types, and thus will always forward unicasts, multicasts, and broadcasts out every port but the originating port.

Ethernet hubs operate at half-duplex, which allows a device to either transmit or receive data, but not simultaneously. Ethernet utilizes Carrier Sense Multiple Access with Collision Detect (CSMA/CD) to control media access. Host devices monitor the physical link, and will only transmit a frame if the link is idle.

However, if two devices transmit a frame simultaneously, a collision will occur. If a collision is detected, the hub will discard the frames and signal the host devices. Both devices will wait a random amount of time before resending their respective frames.

Remember, if any two devices connected to a hub send a frame simultaneously, a collision will occur. Thus, all ports on a hub belong to the same collision domain. A collision domain is simply defined as any physical segment where a collision can occur.

Multiple hubs that are uplinked together still all belong to one collision domain. Increasing the number of host devices in a single collision domain will increase the number of collisions, which can significantly degrade performance.

Hubs also belong to only one broadcast domain – a hub will forward both broadcasts and multicasts out every port but the originating port. A broadcast domain is a logical segmentation of a network, dictating how far a broadcast (or multicast) frame can propagate. Only a Layer-3 device, such as a router, can separate broadcast domains.

Layer-2 Switching[RGPV/ Jun 2014]

Layer-2 devices build hardware address tables, which will contain the following at a minimum:

- Hardware addresses for host devices
- The port each hardware address is associated with

Using this information, Layer-2 devices will make intelligent forwarding decisions based on frame (Data-Link) headers. A frame can then be forwarded

out only the appropriate destination port, instead of all ports. Layer-2 forwarding was originally referred to as bridging. Bridging is a largely deprecated term (mostly for marketing purposes), and Layer-2
forwarding is now commonly referred to as switching.

There are some subtle technological differences between bridging and switching. Switches usually have a higher port-density, and can perform forwarding decisions at wire speed, due to specialized hardware circuits called ASICs (Application-Specific Integrated Circuits). Otherwise, bridges and switches are nearly identical in function.

Ethernet switches build MAC-address tables through a dynamic learning process. A switch behaves much like a hub when first powered on. The switch will flood every frame, including unicasts, out every port but the originating port.

The switch will then build the MAC-address table by examining the source MAC address of each frame. Consider the following diagram:

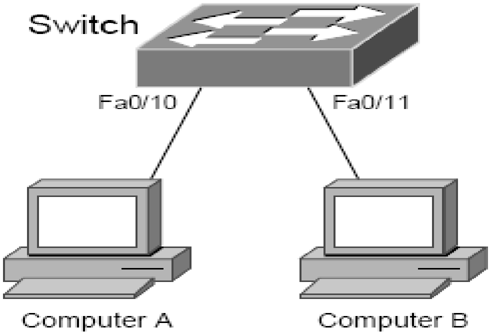


FIGURE: SWITCH

Switches always learn from the source MAC address.

A switch is in a perpetual state of learning. However, as the MAC-address table becomes populated, the flooding of frames will decrease, allowing the switch to perform more efficient forwarding decisions.

While hubs were limited to half-duplex communication, switches can operate in full duplex. Each individual port on a switch belongs to its own collision domain. Thus, switches create more collision domains, which results in fewer collisions.

Like hubs though, switches belong to only one broadcast domain. A Layer- 2 switch will forward both broadcasts and multicasts out every port but the originating port. Only Layer-3 devices separate broadcast domains. Because of this, Layer-2 switches are poorly suited for large, scalable networks. The Layer-2 header provides no mechanism to differentiate one
network from another, only one host from another. This poses significant difficulties. If only hardware addressing existed, all devices would technically be on the same network. Modern internetworks like the Internet could not exist, as it would be impossible to separate my
network from your network. Imagine if the entire Internet existed purely as a Layer-2 switched environment. Switches, as a rule, will forward a broadcast out every port.

Even with a conservative estimate of a billion devices on the Internet, the resulting broadcast storms would be devastating. The Internet would simply collapse.

Both hubs and switches are susceptible to switching loops, which result in destructive broadcast storms. Switches utilize the Spanning Tree Protocol (STP) to maintain a loop-free environment.

Remember, there are three things that switches do that hubs do not:

- Hardware address learning

- Intelligent forwarding of frames
- Loop avoidance

Hubs are almost entirely deprecated – there is no advantage to using a hub over a switch. At one time, switches were more expensive and introduced more latency (due to processing overhead) than hubs, but this is no longer the case.

Layer-2 Forwarding Methods

Switches support three methods of forwarding frames. Each method copies all or part of the frame into memory, providing different levels of latency and reliability. Latency is delay - less latency results in quicker forwarding. The Store-and-Forward method copies the entire frame into memory, and performs a Cycle Redundancy Check (CRC) to completely ensure the integrity of the frame. However, this level of error-checking introduces the highest latency of any of the switching methods. The Cut-Through (Real Time) method copies only enough of a frame's header to determine its destination address. This is generally the first 6 bytes following the preamble. This method allows frames to be transferred at wire speed, and has the least latency of any of the three methods. No error checking is attempted when using the cut-through method. The Fragment-Free (Modified Cut-Through) method copies only the first 64 bytes of a frame for error-checking purposes. Most collisions or corruption occur in the first 64 bytes of a frame. Fragment-Free represents a compromise between reliability (store-and-forward) and speed (cut-through).

Layer-3 Routing

Layer-3 routing is the process of forwarding a packet from one network to another network, based on the Network-layer header. Routers build routing tables to perform forwarding decisions, which contain the following:

- The destination network and subnet mask
- The next hop router to get to the destination network
- Routing metrics and Administrative Distance

Note that Layer-3 forwarding is based on the destination network, and not the destination host. It is possible to have host routes, but this is less common.

The routing table is concerned with two types of Layer-3 protocols:

- Routed protocols - assigns logical addressing to devices, and routes packets between networks. Examples include IP and IPX.
- Routing protocols - dynamically builds the information in routing tables. Examples include RIP, EIGRP, and OSPF.

Each individual interface on a router belongs to its own collision domain.

Thus, like switches, routers create more collision domains, which results in fewer collisions.

Unlike Layer-2 switches, Layer-3 routers also separate broadcast domains. As a rule, a router will never forward broadcasts from one network to another network.

Routers will not forward multicasts either, unless configured to participate in a multicast tree.

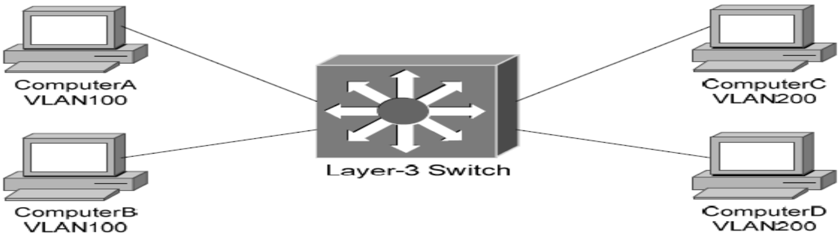
Traditionally, a router was required to copy each individual packet to its buffers, and perform a route-table lookup. Each packet consumed CPU cycles as it was forwarded by the router, resulting in latency. Thus, routing was generally considered slower than switching.

It is now possible for routers to cache network-layer flows in hardware, greatly reducing latency. This has blurred the line between routing and switching, from both a technological and marketing standpoint.

VLANs – A Layer-2 or Layer-3 Function?

a switch will forward both broadcasts and multicasts out every port but the originating port.

However, a switch can be logically segmented into multiple broadcast domains, using Virtual LANs (or VLANs).



Each VLAN represents a unique broadcast domain:

- Traffic between devices within the same VLAN is switched (forwarded at Layer-2).
- Traffic between devices in different VLANs requires a Layer-3 device to communicate.

Broadcasts from one VLAN will not be forwarded to another VLAN. This separation provided by VLANs is not a Layer-3 function. VLAN tags are inserted into the Layer-2 header.

Thus, a switch that supports VLANs is not necessarily a Layer-3 switch. However, a purely Layer-2 switch cannot route between VLANs. Remember, though VLANs provide separation for Layer-3 broadcast domains, and are often associated with IP subnets, they are still a Layer-2 function.

Layer-3 Switching

In addition to performing Layer-2 switching functions, a Layer-3 switch must also meet the following criteria:

- The switch must be capable of making Layer-3 forwarding decisions (traditionally referred to as routing).
- The switch must cache network traffic flows, so that Layer-3 forwarding can occur in hardware.

Many older modular switches support Layer-3 route processors – this alone does not qualify as Layer-3 switching. Layer-2 and Layer-3 processors can act independently within a single switch chassis, with each packet requiring a route-table lookup on the route processor.

Layer-3 switches leverage ASICs to perform Layer-3 forwarding in hardware. For the first packet of a particular traffic flow, the Layer-3 switch will perform a standard route-table lookup. This flow is then cached in hardware – which preserves required routing information, such as the destination network and the MAC address of the corresponding next-hop.

Subsequent packets of that flow will bypass the route-table lookup, and will be forwarded based on the cached information, reducing latency. This concept is known as route once, switch many. Layer-3 switches are predominantly used to route between VLANs:

Traffic between devices within the same VLAN, such as Computer A and Computer B, is switched at Layer-2 as normal. The first packet between devices in different VLANs, such as Computer A and Computer D is routed.

The switch will then cache that IP traffic flow, and subsequent packets in that flow will be switched in hardware.

Layer-3 Switching vs. Routing – End the Confusion!

The evolution of network technologies has led to considerable confusion over the terms switch and router. Remember the following:

- The traditional definition of a switch is a device that performs Layer-2 forwarding decisions.
- The traditional definition of a router is a device that performs Layer-3 forwarding decisions.

switching functions were typically performed in hardware, and routing functions were typically performed in software. This resulted in a widespread perception that switching was fast, and routing was slow (and expensive).

Once Layer-3 forwarding became available in hardware, marketing gurus muddied the waters by distancing themselves from the term router. Though Layer-3 forwarding in hardware is still routing in every technical sense, such devices were rebranded as Layer-3 switches.

Ignore the marketing noise. A Layer-3 switch is still a router.

Compounding matters further, most devices still currently referred to as routers can perform Layer-3 forwarding in hardware as well. Thus, both Layer-3 switches and Layer-3 routers perform nearly identical functions at the same performance.

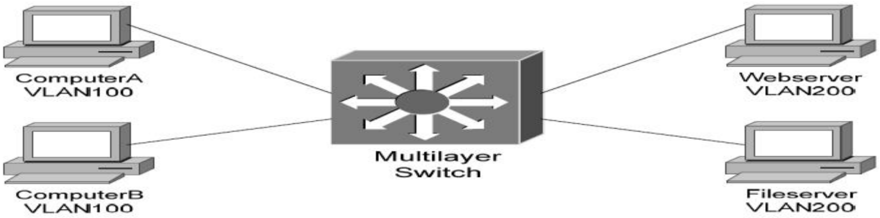
There are some differences in implementation between Layer-3 switches and routers, including (but not limited to):

- Layer-3 switches are optimized for Ethernet, and are predominantly used for inter-VLAN routing. Layer-3 switches can also provide Layer-2 functionality for intra-VLAN traffic.
- Switches generally have higher port densities than routers, and are considerably cheaper per port than routers (for Ethernet, at least).
- Routers support a large number of WAN technologies, while Layer-3 switches generally do not.
- Routers generally support more advanced feature sets.

Layer-3 switches are often deployed as the backbone of LAN or campus networks. Routers are predominantly used on network perimeters, connecting to WAN environments.

Multilayer Switching

Multilayer switching is a generic term, referring to any switch that forwards traffic at layers higher than Layer-2. Thus, a Layer-3 switch is considered a multilayer switch, as it forwards frames at Layer-2 and packets at Layer-3.



A Layer-4 switch provides the same functionality as a Layer-3 switch, but will additionally examine and cache Transport-layer application flow information, such as the TCP or UDP port. By caching application flows, QoS (Quality of Service) functions can be applied to preferred applications.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	What is hub? Explain various types of hub? How hub is different from switch?	Jun 2011	7
Q.2	What do you mean by bridges?	Jun 2006 Jun 2007	7
Q.3	List and discuss advantages & disadvantages of bridges relative to a repeater.	Jun 2005	7
Q.4	Distinguish between the functions of the following networking devices: hub, l2 switch,	Jun 2014	7

	routers and gateways. Explain giving neat sketches.		

Unit-05/Lecture-08

Configuring TCP/IP

Configuring TCP/IP

This chapter describes configuring TCP/IP for the Microsoft Windows platforms that are supported by the Oracle Transparent Gateway for DRDA. TCP/IP is a communications facility that is already part of the operating system. No third-party protocol software is required. Read this chapter to learn more about configuring TCP/IP.

Port Number

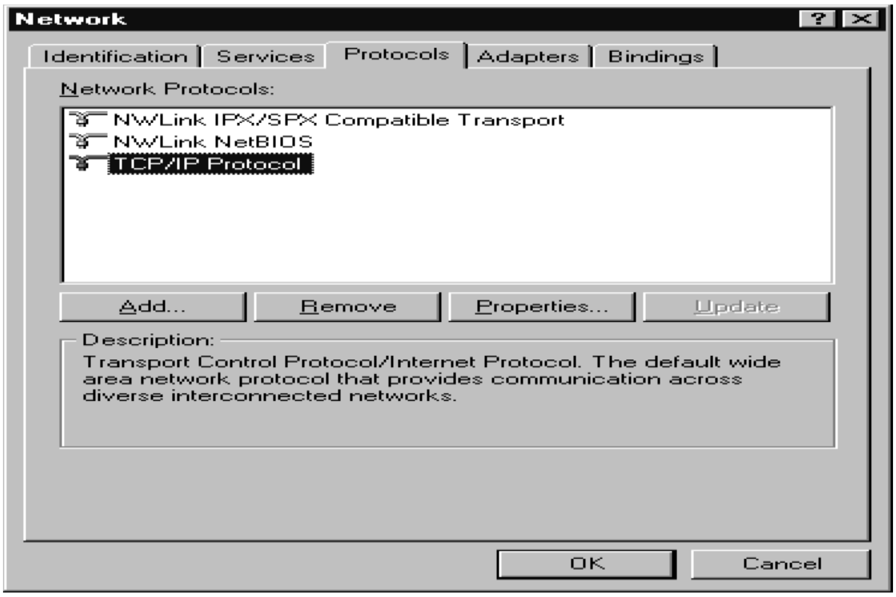
The DRDA standard specifies that port 446 be used for DRDA services. However, if several DRDA Servers are operating on the same system, then they will need to provide service on different ports. Therefore, the port number that is used by each DRDA Server will need to be extracted from the configuration of each individual DRDA Server. DB2 for OS/390 and DB2/400 typically use the DRDA standard port number, 446, whereas DB2/UDB typically uses 50000 as the port number. Refer to IBM DB2 Administrator and Installation guides for locating and changing these port numbers for your DRDA Server. For additional information, consult your DB2 DBA or System Administrator.

Configuring TCP/IP

The following configuration example is for Microsoft Windows NT 4.0. Other Microsoft Windows operating systems may have these panels in a different location or may present them differently, but the required contents will be essentially the same.

You configure TCP/IP from the network configuration tool in the Microsoft Windows Control Panel.

Click the Protocol tab and select TCP/IP Protocol. Then click the Properties button to display the Properties panel.



Network Protocols:

- NWLink IPX/SPX Compatible Transport
- NWLink NetBIOS
- TCP/IP Protocol

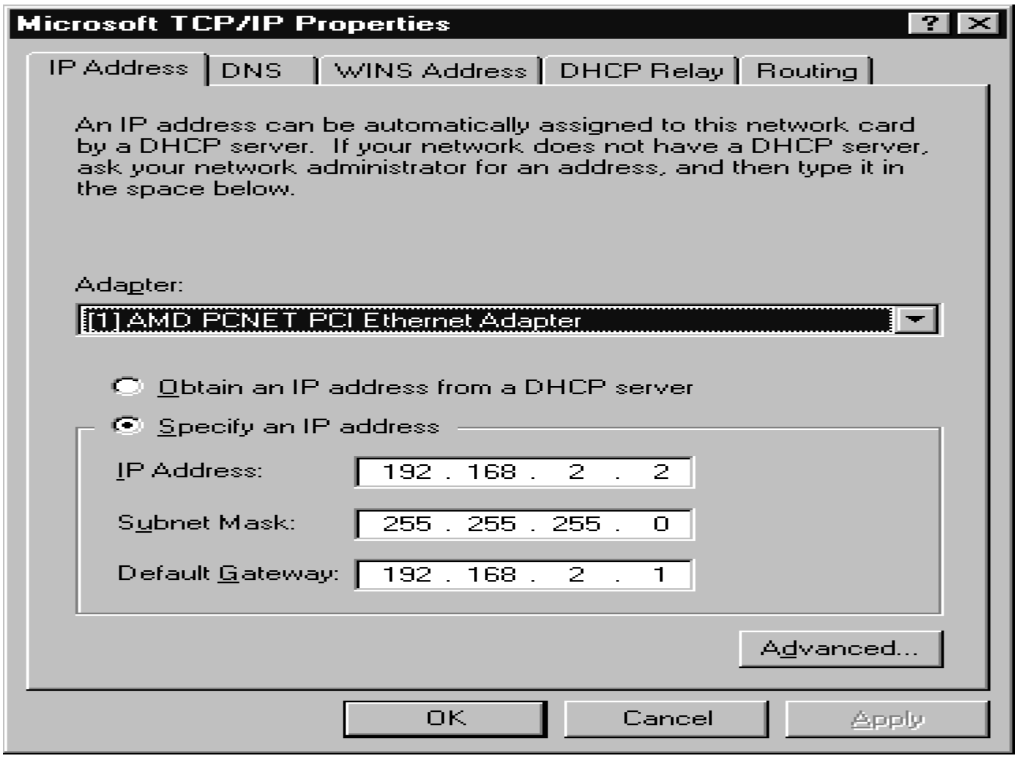
Description:
Transport Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

FIGURE: NETWORK CONFIGURATION TOOL

If the TCP/IP Protocol is not already installed, click Add and then select the TCP/IP Protocol.

Configuration consists of assigning a Hostname, an IP Address, and a Network Mask to a given network interface.

In the IP Address tab, use the pull-down list to choose the Adapter you will use. Your network administrator can tell you whether you will be using DHCP or a static IP address. If using a static IP, then you must enter the appropriate values for IP Address, Subnet Mask, and Default Gateway.



An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter: [1] AMD PCNET PCI Ethernet Adapter

○ Obtain an IP address from a DHCP server

● Specify an IP address

IP Address: 192 . 168 . 2 . 2

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 2 . 1

FIGURE: TCP/IP PROPERTIES PANEL

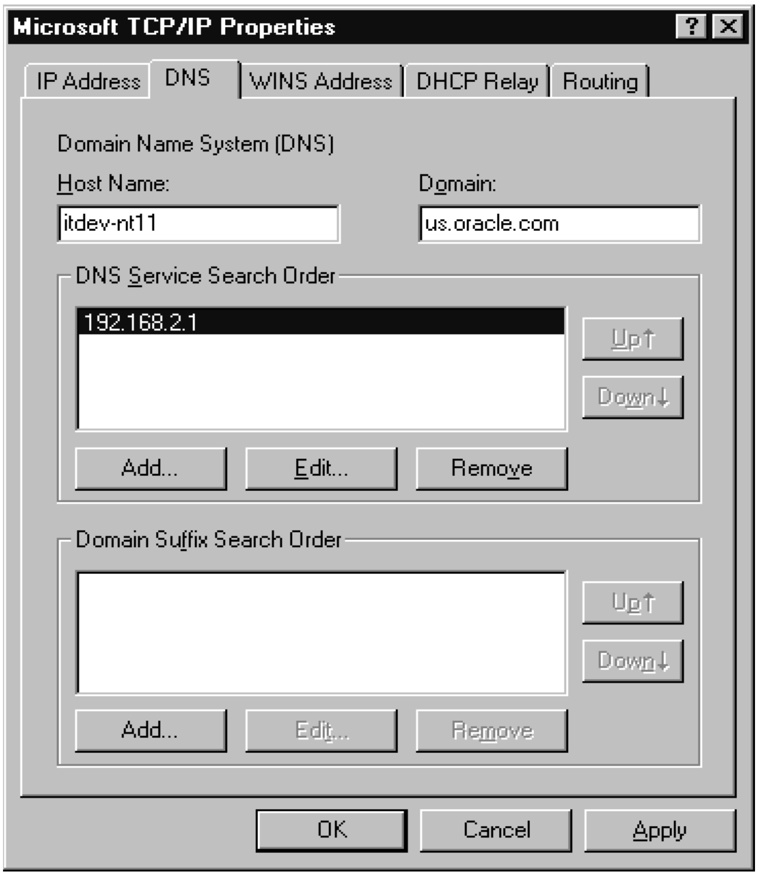
Additional configuration consists of defining a Name Server IP Address or creating entries in the Hosts file on the local machine. Name Servers translate host names into IP Addresses when queried on a particular host name. The Hosts file provides this same functionality, but in a non-network participating manner.

The Hosts file may be edited with a text editor of your choosing. For example, in Microsoft Windows NT, the file is located in:

C:\winnt\system32\drivers\etc\hosts

where C:\winnt is your Windows NT system root.

In order to use a Name Server, you must configure the TCP/IP to use DNS. Click on the DNS tab and enter a Host Name and Domain Name. Your network administrator will provide these values. Click the Add button below the Domain Suffix Search Order box and enter the IP Address of the Name Server. You may enter up to three name servers. Click [OK].



Microsoft TCP/IP Properties

Domain Name System (DNS)

Host Name: itdev-nt11

Domain: us.oracle.com

DNS Service Search Order: 192.168.2.1

Domain Suffix Search Order:

FIGURE :DEFINE A NAME SERVER

For local configuration (in other words, the gateway and the DRDA Server are on the same machine), it may be desirable to use the loop-back address. The IP address is 127.0.0.1 and is typically given the local name ("localhost" or "loopback") in the Hosts file. Using the loop-back address reduces the amount of network overhead by handling the traffic internally without actually talking to the network.

The gateway is configured for TCP/IP using the DRDA_CONNECT_PARM initialization file parameter. In an SNA configuration, this parameter would be set to the Side Information Profile name (name set). In a TCP/IP configuration, this parameter should be set to the IP address or Host name of the DRDA Server, which should be followed by the Service Port number of that server.

The rest of the DRDA-specific parameters are unrelated to the communications protocol and may be set the same for either SNA or TCP/IP installations.

Example #1: Configuration for a DRDA Server on a host named 'mvs01.domain.com' (or IP address of 192.168.1.2) with a Service Port number of 446.

```
DRDA_CONNECT_PARM=mvs01.domain.com:446
or
DRDA_CONNECT_PARM=192.168.1.2:446
```

Example #2: Configuration for a DRDA Server on the same host as the gateway with a Service Port number of 446.

```
DRDA_CONNECT_PARM=localhost:446
or
DRDA_CONNECT_PARM=127.0.0.1:446
```

UNIT 5/LECTURE 09

ipconfig, ping command

Commands [RGPV/Jun 2010/ Jun 2011/ Dec 2013]

To test a TCP/IP configuration by using the ping command

1. To quickly obtain the TCP/IP configuration of a computer, open Command Prompt, and then type **ipconfig**. From the display of the **ipconfig** command, ensure that the network adapter for the TCP/IP configuration you are testing is not in a **Media disconnected** state.

   At the command prompt, pings the loopback address by typing **ping 127.0.0.1**.
3. Ping the IP address of the computer.
4. Ping the IP address of the default gateway.

   If the **ping** command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.
5. Ping the IP address of a remote host (a host that is on a different subnet).

   If the **ping** command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.
6. Ping the IP address of the DNS server

   If the **ping** command fails, verify that the DNS server IP address is correct, that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

To open command prompt, click **Start**, point to **All Programs**, point to **Accessories**, and then click **Command Prompt**.

- If the **ping** command is not found or the command fails, you can use Event Viewer to check the System Log and look for problems reported by Setup or the Internet Protocol (TCP/IP) service.
- The ping command uses Internet Control Message Protocol (ICMP) Echo Request and Echo Reply messages. Packet filtering policies on routers, firewalls, or other types of security gateways might prevent the forwarding of this traffic.

- The ipconfig command is the command-line equivalent to the winipcfg command, which is available in Windows Millennium Edition, Windows 98, and Windows 95. Windows XP does not include a graphical equivalent to the winipcfg command; however, you can get the equivalent functionality for viewing and renewing an IP address by opening Network Connections, right-clicking a network connection, clicking **Status**, and then clicking the **Support** tab.

  Used without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters.
- To run ipconfig, open the command prompt, and then type **ipconfig**.
- To open Network Connections, click **Start**, click **Control Panel**, click **Network and Internet Connections**, and then click **Network Connections**.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain ipconfig and ping?	Jun 2010 Jun 2011	7
Q.2	Write short notes on ip configuration	Dec 2013	7

UNIT 2/ lecturer 10

Configuration of internetworking device

Configuration of internetworking device [RGPV/Dec 2009/ Jun 2010/ Dec 2011/Dec 2013]

Networking **Switch** is a awesome device, if you want to connect multiple computers to each other, thereby creating your own LAN Network. After this file transfers and chatting between all these computers becomes a piece of cake.

Requirements

1. Networking Switch. A basic switch of 300 to 600 should do the job. I am using D-Link 10/100Mbps 5 Ethernet Port Switch.
2. Few computers. Be it Mac OS X, Windows or Linux.
3. Ethernet cables. One for each computer. A Fast Ethernet cable (CAT5 and Untwisted pair) should be good enough.
4. Applications like IPMessenger or Dukto. Both are cross platform softwares.

Procedure

Read the instructions and then see the video for a better understanding.

1. Connect the Networking Switch to a power supply and Turn it on.
2. Connect all the computers you want on the LAN Network to the switch via Ethernet cables.
3. Now download an application like IPMessenger or Dukto. Both are cross platform softwares. However IPMessenger doesn’t work well with linux, so I would suggest Dukto.
4. Once you have installed the application on all your computers, the next step is the IP Configuration. This is the most important step. All computers will get an IP in sequential order.
5. Turn off the Wi-fi if it is ON.
6. The PC connected to port 1 on the Networking Switch will get an IP – 10.0.0.1, Router/Gateway – 255.255.255.0, DNS – 10.0.0.10
7. The PC connected to port 2 on the Networking Switch will get an IP – 10.0.0.2, Router/Gateway – 255.255.255.0, DNS – 10.0.0.10
8. The PC connected to port 3 on the Networking Switch will get an IP – 10.0.0.3, Router/Gateway – 255.255.255.0, DNS – 10.0.0.10
9. Do this till the IP Configuration is complete on all the computers.

10. Now open IPMessenger/Dukto.
11. All the computers connected to the switch should show up. Now go ahead and do some file transfers and chatting on your own LAN Network.

How to Set up an Ethernet Hub

When expanding an existing computer network or building a new one, one of the many devices that can be used in the process is an Ethernet hub. A hub is a simple device that connects multiple computers together and to the rest of the network, allowing communication to occur between all connected devices. When there is no need for the enhanced functions available on a router or the higher communications speed of a switch, an Ethernet hub can be an efficient way to create or expand a network at a lower cost when compared to a router or switch.

Instructions

Hardware Setup

1 Find the WAN or uplink port of the Ethernet hub. Typically, it is located on the rear of the unit, and it is often separate from the LAN ports.

2 Connect an Ethernet cable from the WAN port of the hub to either the Ethernet port of the internet modem or, if expanding a network, to an empty LAN port on the existing network’s router, switch or hub.

3 Plug an Ethernet cable into one of the LAN ports on the Ethernet hub and connect the other end of cable to the computer or device that will be added to the network. Repeat for any other devices that will need to be on the network.

4 Power up the Ethernet hub and the computers or other devices attached to it. On the front of the hub will be a series of LEDs that correspond to each LAN and WAN port on the hub. Every port that has a cable plugged into it should have one or more of the LEDs lit that represent that port. If not, check the connections and swap out the Ethernet cable if necessary.

Software Setup

5 Configure the network settings on each connected computer. If you are expanding a network and the network uses DCHP, or dynamic IP addressing, no configuration will be necessary. On networks using static IP addressing or on a new network setup using the Ethernet hub, each computer or device must be assigned a unique IP address. Local IP addresses must use the allowed “private” address pools that will not interfere with internet addresses. Acceptable addresses include 192.168.x.x, 172.16.x.x to 172.31.x.x, or 10.x.x.x. The “x” represents a number that is chosen by the user, from 0 to 254. All computers on the network should share the first three numbers in the address, with the final number representing the individual computer. In a network with three computers, for example, the first could be 192.168.1.1, the second could be 192.168.1.2 and the third could be 192.168.1.3, though the final number does not need to be sequential.

6 Click the “Start” button in Windows, select “Control Panel" and double-click the icon labeled “Network Connections.”

7 Right-click the icon for the Ethernet adapter and select “Properties.” Click on the check box marked “Internet Protocol (TCP/IP)” and press the “Properties” button.

8 Select the radio button labeled “Use the following IP address.” Enter a unique IP address for the computer and the applicable subnet mask. If a router is used on the network, enter the router’s IP address as the default gateway. Press the

“OK” button and reboot if necessary.

9 Enable file and printer sharing from the “Properties” dialog for the Ethernet card if files will be transferred between the networked computers.

10 Click the “Start” button, select “Control Panel” and double-click on the “System” icon. Select the “Computer Name” tab and click on the button labeled “Change” to set the computer’s network name. In the “Computer Name” box, enter a unique name for the computer. In the “Member of” section, choose the radio button marked “Workgroup” and enter the workgroup of the network. If setting up a new network, this name can be change but all computers on the network must share the same workgroup name.

11 Verify that all computers can access the network and the Internet if connected.

How to Setup a Network Bridge

A network bridge in Windows is a software method to connect two networks together so that they can communicate with each other. For example, in a small office with both a wired and wireless network, users on each network can only see other users on the same network: wired users cannot communicate with wireless users, and vice versa. By creating a network bridge, you can enable users of both networks to communicate with each other. These instructions will show you how to setup a network bridge in Windows XP and Windows Vista.

Instructions

Setup a Network Bridge in Windows XP

1 Click on "Start" and select "Control Panel."

2 Double-click "Network Connections."

3 Hold down "CTRL" and click each of the network connections you wish to bridge.

4 Right-click one of the network connections and select "Bridge Connections."

Setup a Network Bridge in Windows Vista

5 Click "Start" and select "Control Panel."

6 Double-click on "Network and Sharing Center."

7 Click "Manage Network Connections."

8 Hold down "CTRL" and click each of the network connections you wish to bridge.

9 Right-click one of the network connections and select "Bridge Connections."

Set Up a WiFi Router

A Wi-Fi router, also called a wireless router, is a networking device that acts as a gateway that joins your computer and your high-speed modem. A Wi-Fi router also acts as a wireless access point, allowing your wireless-enabled devices, such as a laptop, to communicate with it and connect to your network wirelessly. In order to use your W-iFi router, you must connect your computer, modem and router using Ethernet cables. You must also configure the router's settings.

Instructions

1 Disconnect your high-speed modem's power cord. Connect your high-speed modem to the Wi-Fi router using an Ethernet cable. Also disconnect the Ethernet cable that connected the modem to your computer. Insert the Ethernet cable that was connected to your modem into the "Internet" (or "Modem") port on the back of your router. This port is usually next to the Wi-Fi router's power port and is distinguished by a color or label.

2 Turn off your computer. Using another Ethernet cable, connect your Wi-Fi router to your computer; the Ethernet jack is on the back of your computer. Plug the other end of the Ethernet cable into one of the numbered LAN ports on the back of your Wi-Fi router. It does not matter which LAN port you use.

3 Turn on the high-speed modem, router and computer, in that order. First, plug the power cable back into your high-speed modem, and turn it on. Wait at least two minutes to allow the modem time to connect to your Internet service provider's server. Make sure that your modem's status indicators (the lights on the front of the modem) show that it has successfully connected. Next, plug the Wi-Fi router's power adapter into the router's power port and into a power outlet. Wait another two minutes for the Wi-Fi router to connect to the modem. You will know that it has successfully connected when all of the lights on the front of the Wi-Fi router are on. Lastly, turn on your computer. If you plug in and power on the devices out of this order, you may not be able to connect to the Internet.

4 Log on to the Wi-Fi router's URL. Open a web browser on your computer and type the Wi-Fi router's URL in the browser's address bar. This address can be found in the documentation that came with your Wi-Fi router or on the manufacturer's website. After typing in the URL, press "Enter." This will take you to the Wi-Fi router's settings page.

5 Enter the user name and password for the Wi-Fi router. After entering the router's URL, a dialog box will appear requiring you to enter a user name and password for the router. For most Wi-Fi routers, the default user name is "admin" and the default password is "password" or there is no password. Remember that the text boxes are case sensitive.

6 Configure the Wi-Fi router's settings and wireless settings. On the main page of the router's setup menu, you will find links to change several settings. You

can change the default SSID (wireless network name) to a custom name, and you can select the type of encryption you want to secure your wireless network. When you finish changing your settings, click "Apply" or "Save."

How to Install Wired Routers

Routers share a single Internet connection between computers.
Wired routers allow you to extend your home network and share a single Internet connection with multiple wired devices. With a router implemented in your network, you can easily share a single connection with multiple computers. You can also network computers and devices together to share files, folders, media and printers. Wired routers are simple to install and set up on your network. They connect to your Internet modem with an Ethernet cable, essentially acting to split a single Ethernet port into multiple ports to expand a network.

Instructions

1 Shut down your computer and any other devices connected to your current network configuration. Turn off your cable modem and disconnect its power cable from the wall outlet.

2 Unplug the Ethernet cable connecting your computer to the cable modem. Place the wired router in your chosen location and plug an Ethernet cable into the router's first port. This port is sometimes labeled "Uplink." Attach the other end of the router's Ethernet cable to your modem.

3 Attach your network's devices to the available router ports. Each device should be powered off before you connect the Ethernet cables to the router's available ports.

4 Plug your modem back into its power source and turn it on. Plug your router's power cable into an available outlet and turn the router on if your router model has an external power switch.

5 Start your computer and allow your operating system to boot up. In most cases, the Internet connection is automatically recognized.

Tips & Warnings

- If you cannot connect to the Internet after connecting your computer to your router, check all of the wired connections.
- Some routers will require you to install additional software to configure settings for your router, such as port forwarding, IP settings and security settings.
- To configure advance options for most routers, you can navigate to your router's configuration utility using your web browser. Most routers use a

default address of "192.168.0.1" or "192.168.1.1".

How to Configure a Computer as a Gateway

Configuring a computer as a gateway makes Internet connection sharing possible without a router.

A gateway provides access for computers inside the local network to send and receive information through the firewall to and from the Internet. Most home networks use a gateway, a modem, router and switch all-in-one device or a router for two computers to access the Internet simultaneously. However, if a router or gateway is not available, one computer inside the local network can be configured to act as a gateway or host for another computer or client to access the Internet.

Instructions

1 Set-up the host computer. Note that the host computer needs two network adapters to act as a host. Connect an Ethernet cable to the Ethernet port on the modem. Connect the other end of the Ethernet cable to one of the Ethernet ports on the host computer.

2 Set-up the client computer. Connect a second Ethernet cable to the other Ethernet port on the host computer. Connect the other end of the Ethernet cable to the Ethernet port on the client computer.

3 Enable Internet connections sharing on the host computer. "Click the "Start" (Windows logo) button, then "Control Panel" and then "Network and Sharing Center." Click "Manage network connections" in the task pane to the upper left of the window. Right-click the network adapter you wish to share and select "Properties" in the short-cut menu that appears. Next, click the "Sharing" tab. Place a check mark in the box next to the words "Allow other network users to connect through this computer's Internet connection." Un-check the box next to the words "Allow other network users to control or disable the shared Internet connection" and then click "OK." Close out of "Network Connections" and "Network and Sharing Center."

4 Configure the client computer. Click the "Start" (Windows logo) button, then "Control Panel" and then "Network and Sharing Center." Click "Manage network connections" in the task pane to the upper left of the window. Right-click the network adapter connected to the host computer and select "Properties" in the short-cut menu that appears. Click "Internet Protocol Version 4 (TCP-IPv4)" and then click the "Properties" button. Make sure the radio buttons next to "Obtain an IP address automatically" and "Obtain DNS Server address automatically" is selected. Click "OK."

Click the "Close" button on the "Local Area Connection Properties" window. Close out of "Network Connections" and "Network and Sharing Center."

5 Open a web browser on the client computer and connect to the Internet.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain different types of internetworking devices. Also briefly explain configuration of switches and bridges.	Dec 2009	7
Q.2	Explain various internetworking devices. Where are they used?	Jun 2010	7
Q.3	Write procedure for configuring the internetworking device like switches, hubs routers.	Dec 2013	7

UNIT 2/LECTURE 10

Quality of service

Quality of service (**QoS**) **[RGPV/Jun 2006/Dec 2008]**

QoS is the overall performance of telephony or computer network, particularly the performance seen by the users of the network.

To quantitatively measure quality of service, several related aspects of the network service are often considered, such as error rates, bandwidth, throughput, transmission delay, availability, jitter, etc.

Quality of service is particularly important for the transport of traffic with special requirements. In particular, much technology has been developed to allow computer networks to become as useful as telephone networks for audio conversations, as well as supporting new applications with even stricter service demands.

Qualities of traffic

In packet-switched networks, quality of service is affected by various factors, which can be divided into “human” and “technical” factors. Human factors include: stability of service, availability of service, delays, user information. Technical factors include: reliability, scalability, effectiveness, maintainability, grade of service, etc.

Many things can happen to packets as they travel from origin to destination, resulting in the following problems as seen from the point of view of the sender and receiver:

Low throughput

Due to varying load from disparate users sharing the same network resources, the bit rate (the maximum throughput) that can be provided to a certain data stream may be too low for real-time multimedia services if all data streams get the same scheduling priority.

Dropped packets

The routers might fail to deliver (drop) some packets if their data is corrupted or they arrive when their buffers are already full. The receiving application may ask for this information to be retransmitted, possibly causing severe delays in the overall transmission.

Errors

Sometimes packets are corrupted due to bit errors caused by noise and interference, especially in wireless communications and long copper wires. The receiver has to detect this and, just as if the packet was dropped, may ask for this information to be retransmitted.

Latency

It might take a long time for each packet to reach its destination, because it gets held up in long queues, or takes a less direct route to avoid congestion. This is different from throughput, as the delay can build up over time, even if the throughput is almost normal. In some cases, excessive latency can render an application such as VoIP or online gaming unusable.

Jitter

Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably. This variation in delay is known as jitter and can seriously affect the quality of streaming audio and/or video.

Out-of-order delivery

When a collection of related packets is routed through a network, different packets may take different routes, each resulting in a different delay. The result is that the packets arrive in a different order than they were sent. This problem requires special additional protocols responsible for rearranging out-of-order packets to an isochronous state once they reach their destination. This is especially important for video and VoIP streams where quality is dramatically affected by both latency and lack of sequence.

Applications

A defined quality of service may be desired or required for certain types of network traffic, for example:

- Streaming media specifically
  - Internet protocol television (IPTV)
  - Audio over Ethernet
  - Audio over IP
- IP telephony also known as Voice over IP (VoIP)
- Videoconferencing

- Telepresence
- Storage applications such as iSCSI and FCoE
- Circuit Emulation Service
- Safety-critical applications such as remote surgery where availability issues can be hazardous
- Network operations support systems either for the network itself, or for customers' business critical needs
- Online games where real-time lag can be a factor
- Industrial control systems protocols such as Ethernet/IP which are used for real-time control of machinery

These types of service are called inelastic, meaning that they require a certain minimum level of bandwidth and a certain maximum latency to function. By contrast, elastic applications can take advantage of however much or little bandwidth is available. Bulk file transfer applications that rely on TCP are generally elastic.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Why does transport layer regard QoS as a primary function provided by the network layer? Summarize the parameters.	Jun 2006 Dec 2008	7
Q.2	Write short notes on quality of services.	Dec 2010	7
Q.3	What is meant by quality of service, compare integrated service and differentiated service.	Jun 2014	7

REFERENCE

BOOK	**AUTHOR**	**PRIORITY**
Data Communication and Computer Networks	Forouzan	1
Computer Networks	Tanenbaum	2