1.Introduction & Physical Layer

Computer Network (Definition)

A collection of devices, or nodes, connected by communication lines is called a network. Any device that can send and/or receive data created by other nodes on the network is referred to as a node. Examples of such devices include printers and computers.If two computers can share data, then they are considered to be interconnected. Copper wires are one possible connecting method; other options include fiber optics, microwaves, infrared, and communication satellites. There are numerous sizes, forms, and shapes for networks.

Uses of Computer Networks

Resource Sharing: The objective of resource sharing is to facilitate the accessibility of equipment and data to all network users, regardless of the geographical location of the resource or the user. A group of individuals employed in an office environment collectively utilize a shared printing device. A networked printer with high volume capacity is frequently more cost-effective, efficient, and manageable in terms of maintenance compared to a large collection of individual printers.

Client-Server model: Information related to the organization is stored on servers, which are robust computers under the care of a system administrator. Employees utilize client devices, which are simple computers located on their workstations, to retrieve data from the servers. The server and client computers are linked together via a network.

Communication medium:A computer network can be an excellent means for workers to communicate to each other. Email, or electronic mail, is now available at almost every business with two or more computers. Employees use email for a lot of daily communication.It is possible for the computer network to handle phone calls between workers instead of the phone company. It's known as IP telephony or Voice over IP (VoIP) when it's used with the Internet. Video can be added to audio so that workers in different places can see and hear each other during a meeting. This method is very useful for cutting down on the time and money needed for travel.

E-commerce (electronic commerce): Many businesses use electronic means to conduct business. Retailers such as booksellers and airlines have found that a lot of their consumers prefer the ease of purchasing from home. As a result, a lot of businesses offer online catalogues featuring their products and services and even accept online orders.

Network Hardware

There is a lack of agreement over a universally accepted taxonomy that incorporates all computer networks.

However, two key elements emerge as significant factors: transmission technology and scalability. There are two main forms of transmission technologies that are extensively used: broadcast links and point-to-point links.

Point-to-point links establish direct connections between individual pairs of devices.

In a network made up of point-to-point links, packets may need to be routed through one or more intermediary devices before reaching their intended destination. In point-to-point networks, it is crucial to identify optimal routes due to the existence of multiple paths of varying lengths. The transmission method characterized by a single sender and a single recipient is sometimes referred to as unicasting.On the other hand, with a broadcast network, every machine on the network shares the communication channel, meaning that any machine can send and receive packets.

Each packet has an address field that identifies the intended recipient.A machine reads a packet and looks up the address field. When a packet is meant for the receiving machine, it is processed by that machine; when it is meant for another machine, it is simply ignored.

Broadcast systems typically allow a packet to be addressed to all destinations by using a special code in the address field. When a packet containing this code is sent, every machine on the network receives and processes it. This form of functioning is referred to as broadcasting. Some broadcast systems also offer multicasting, which is the transmitting of data to a subset of workstations.Networks can also be categorized in terms of scale. Distance is a metric used for this categorization.

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

Figure 1-6. Classification of interconnected processors by scale.

Network Software

In the early stages of computer network development, hardware predominated over software considerations. This approach is no longer effective. Presently, network software is heavily structured.Most

networks are set up as a stack of layers or levels, with each layer building on top of the one below it. This makes them easier to organize. From network to network, the number of levels, the name of each layer, the contents of each layer, and the job of each layer are all different.

The job of each layer is to provide certain services to the layers above it while keeping those layers from knowing the particulars of how the services are delivered.

Layer n on one machine has a conversation with layer n on another machine. The rules and conventions that these two machines follow are called the layer n protocol.A protocol is essentially an agreement between communicative parties on how communication should proceed. Peers are the entities that make up the matching layers on various machines. The protocols are used by the peers to communicate with one another.

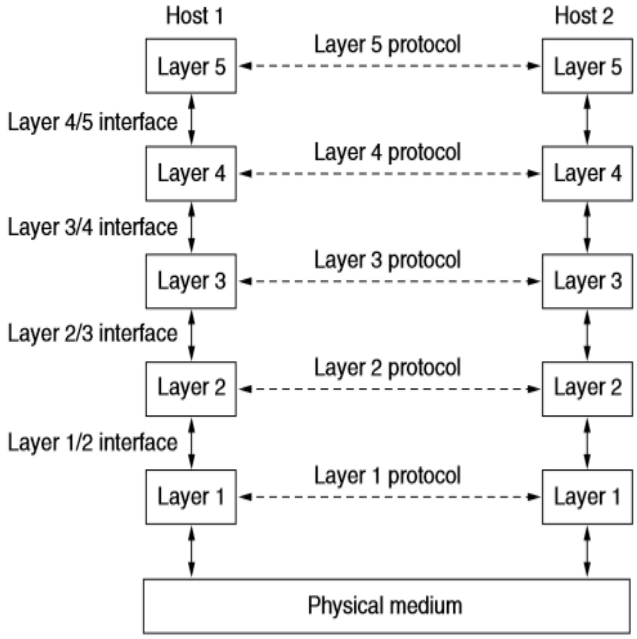


Figure 1-13. Layers, protocols, and interfaces.

There is no straight transfer of data from layer n on one machine to layer n on another machine.

Each layer instead sends control and data information to the layer below it, all the way down to the lowest layer. The physical medium that transmission actually takes place is below layer 1.Actual communication is shown by straight lines, and virtual communication is shown by dashed lines.An interface exists between each pair of neighboring layers. The interface specifies which primitive operations and services are made available to the upper layer by the lower layer. Each layer has an own set of functions. Interfaces that are clean and unambiguous also make it easier to replace one layer with an entirely different protocol or implementation. A network architecture is a collection of layers and protocols.

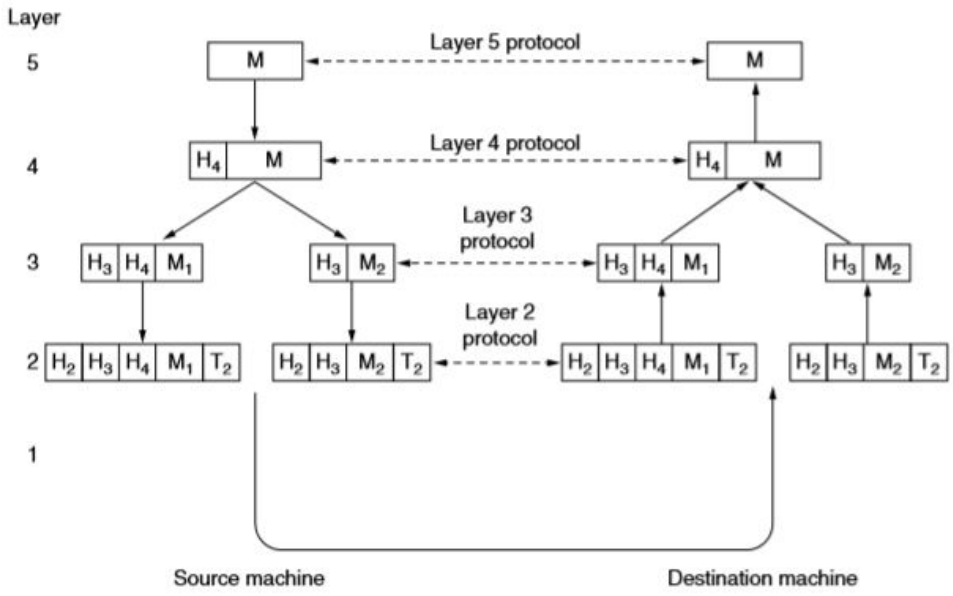


Figure 1-15. Example information flow supporting virtual communication in layer 5.

Each process may include some information known as a header that is exclusively intended for its peer. This data is not transmitted to the layer above. Control information like as addresses, sequence numbers, sizes, and times are included in the header. An application process at layer 5 generates a message, M, which is sent to layer 4 for transmission.Layer 4 adds a header to the message and forwards the result to Layer 3.In many networks, there is no limit on the size of messages sent using the layer 4 protocol. However, the layer 3 protocol almost always has a limit.So, layer 3 has to separate the received messages into smaller pieces called packets and add a layer 3 header to each packet. M is split into two parts, M1 and M2, which will be sent separately in this case.Layer 3 selects which of the lines to use for sending data and sends the packets to Layer 2. Layer 2 gives each piece both header and a trailer, and then sends the whole thing to Layer 1 to be sent physically. At the recipient machine, the message moves from one layer to the next, and as it goes up, headers are stripped off. Below layer n, none of the headers are sent up to layer n.

Design Issues for the Layers

Reliability is a design issue of constructing a network that functions accurately in spite of having a collection of unreliable components. Consider the packet traverse in the network. It is possible that some of these bits may be received in an inverted state due to noise, hardware defects, software errors, and so forth. How do we manage to locate and rectify these errors? One approach to identifying errors in received data involves the use of **error detection codes**.

If information is received wrongly, it can be sent again until it is received correctly. Error correction is possible with stronger codes by adding redundant information.

There are often more than one way for transferring data from one place to another, and in a big network,

some links or routers may not work. The decision should be made immediately by the network. We call this subject "**routing**."

Due to the large number of computers comprising the network, every layer must incorporate a means of detecting the senders and receivers associated with a specific message. This process is called as addressing.It is a fact that some communication channels will not maintain the sequence of messages transmitted through them, requiring the implementation of message numbering solutions. Differences in the maximum message size that can be transmitted across networks are another example. As a consequence, mechanisms are developed to disassemble, transmit, and subsequently reassemble messages. The collective term for this subject is **internetworking**.

How can a quick sender avoid sending too much data at once to a slow receiver? It is common to employ feedback from the recipient to the sender. We refer to this topic as **flow control**.Oversubscriptions can occur when an excessive number of computers attempt to transmit an excessive amount of traffic, surpassing the network's capacity to deliver. The term used for this condition is called as **congestion**.

The final design consideration is the network's protection against various types of threats. One of such risk relates to the eavesdropping of communications. **Confidentiality**-preserving mechanisms serve as protection against this danger.The implementation of **authentication** mechanisms serves to prevent attempts at fraud identities. Additional **integrity** mechanisms serve to prevent modifications made to messages.

Connection-Oriented Versus Connectionless Service

Connection-oriented and connectionless services are the two forms of services that layers can provide to the layers above them. The telephone system serves as the example for connection-oriented service.To speak with someone, you pick up the phone, dial the number, speak with them, and then hang up. Similarly, to use a connection-oriented network service, the service user first establishes a connection, then uses it, and then releases it.In the majority of instances, the order of transmission is maintained to ensure that the bits are received in the same sequence as they were originally transmitted.The connectionless service is designed based on the conceptual framework of the postal system. Every individual message, in the form of a letter, contains the whole destination address. These messages are then directed through the intermediate nodes within the system, irrespective of subsequent messages.Each type of service can be further classified based on its level of reliability.Certain services can be considered reliable due to their ability to maintain data without any loss. Typically, the establishment of a reliable service requires the integration of a mechanism wherein the recipient acknowledges the receipt of every message, so providing assurance to the sender of its successful delivery. The process of being acknowledged involves additional costs and time delays, which are often considered reasonable, while occasionally considered undesirable.

File transfer is a common scenario where a reliable connection-oriented service is suitable.

The file owner wants to be sure that everything comes in the exact same sequence that it was sent in.

Two slight variations of reliable connection-oriented services are byte streams and message sequences.

The message boundaries are maintained in the former version. Two 1024-byte messages never arrive as a single 2048-byte message when they are transmitted; instead, they arrive as two separate 1024-byte messages.In the latter case, there are no message boundaries and the connection is just a stream of bytes. It is impossible to determine if 2048 bytes were sent as two 1024-byte messages or as a single 2048-byte message when they reach the recipient.The acknowledgement-induced transit delays are unacceptably long for some applications.For instance, a few incorrect pixels during a video conference won't affect the transmission; however, it will irritate the viewer if the image jerks as the flow stops and begins to rectify faults.Not every application needs to be connected. A method for sending a single message with a good chance of arriving but no guarantee is all that is required.Datagram service is a common term for connectionless services that are unreliable (i.e., not acknowledged).In certain cases, it is not desirable to connect in order to transmit a single message, but reliability is crucial.For these applications, the acknowledged datagram service can be offered.It functions similarly to obtaining a return receipt for a registered letter sent. The sender is certain that the letter was delivered to the appropriate recipient and wasn't misplaced when the receipt is returned.Particularly in real-time applications like multimedia, the inevitable delays in delivering reliable service would not be acceptable. These factors lead to the coexistence of reliable and unreliable communication.

OSI reference mode

The ISO proposed this concept as a first step towards international standardisation of layer protocols.

The ISO OSI (Open Systems Interconnection) Reference Model connects open-communication systems.

Physical Layer: Raw bits are sent via a communication channel by the physical layer.What electrical impulses indicate 1 and 0, and how long do bits last?Can two-way transmission occur simultaneously?How is the initial connection made and broken when both sides are done?Number and purpose of network connector pins. Mechanical, electrical, and timing connections and the physical transmission medium underlying the physical layer are the main design issues.

Data link Layer: Its primary responsibility is to provide error-free information transfer.In order to complete this task, the transmitter must divide the input data into data frames and deliver the frames one after the other sequentially. The receiver sends back an acknowledgement frame to verify that each frame was received correctly, indicating that the service is reliable.How to prevent a fast transmitter from drowning a slow receiver with data is another problem that occurs at the data link layer. In the data link layer, broadcast networks also face the problem of controlling access to the shared channel. This issue is addressed by the medium access control sublayer, a unique sublayer of the data link layer.

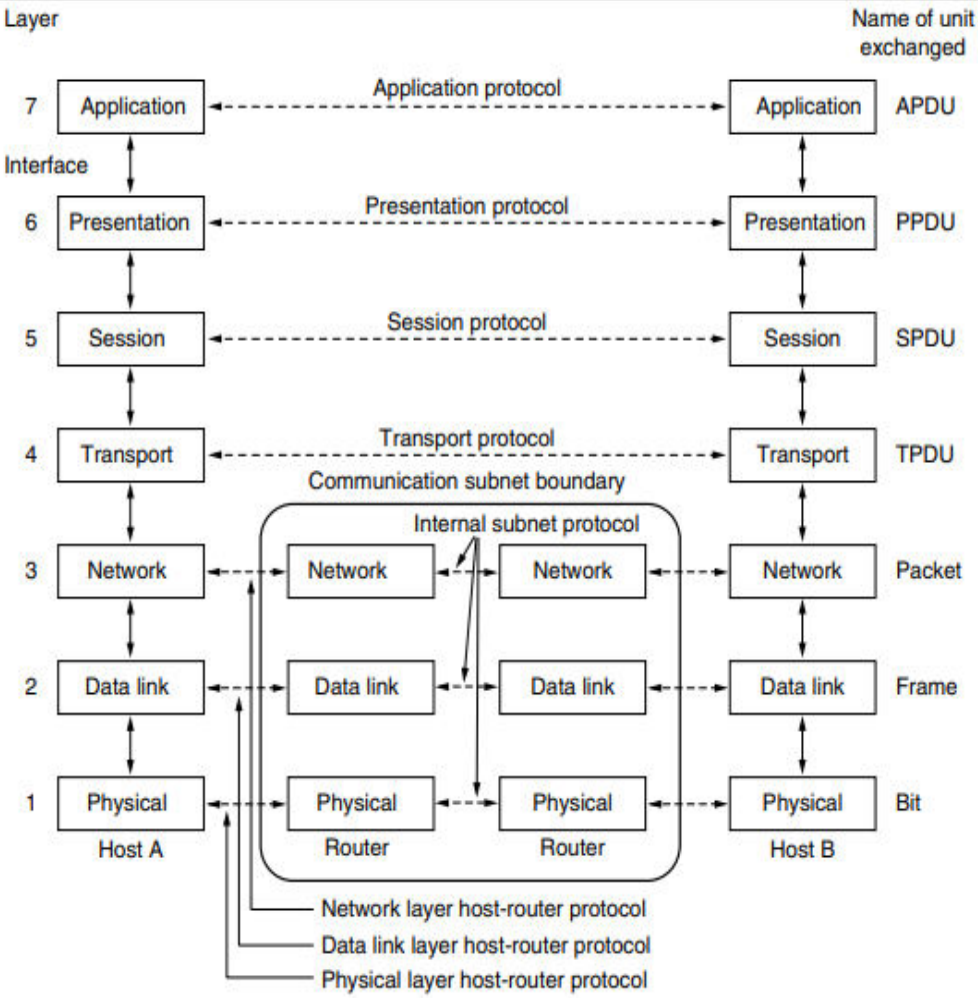


Figure 1-20. The OSI reference model.

Network Layer: Choosing the best route for packets to go from source to destination is an important design decision.Bottlenecks arise when there are too many packets in the network at once and they obstruct one another. The network layer is also in responsible for handling congestion. Numerous issues can occur when a packet needs to go across networks in order to reach its destination. It's possible that the addressing implemented by the two networks differs from one another. The packet might be too big for the second network to receive at all. The protocols could vary, and so on. The network layer is responsible for resolving each of these issues so that diverse networks can be joined. The network layer in broadcast networks is frequently minimal or non-existent since the routing problem is simple.

Transport Layer: The transport layer is a true end-to-end layer, carrying data from source to destination.

In other words, a programme on the source machine communicates with a programme on the destination system via message headers and control messages. Each protocol in the lower layers is between a machine and its near neighbours, rather than between the final source and destination machines, which may be separated by multiple routers.The transport layer also decides what kind of service to give to the session layer and, ultimately, to network users.

TCP is a reliable, error-free point-to-point transport connection that delivers messages in the order in which they were transmitted.UDP is another kind of transport service that carries individual messages with no guarantee of delivery order.

Session Layer: The session layer enables sessions to be established between users on multiple machines. Sessions provide a variety of services, such as dialogue control (keeping track of who is transmitting), token management (preventing two parties from attempting the same critical operation at the same time), and synchronisation (check pointing long transmissions to allow them to pick up where they left off in the event of a crash and subsequent recovery).

Presentation Layer: The presentation layer is concerned with the syntax and semantics of the information delivered, compared to the lower levels, which are largely concerned with moving bits around.The data structures must be exchanged in order for machines with various internal data representations to communicate.

Application Layer: The application layer contains a number of protocols that users frequently require.

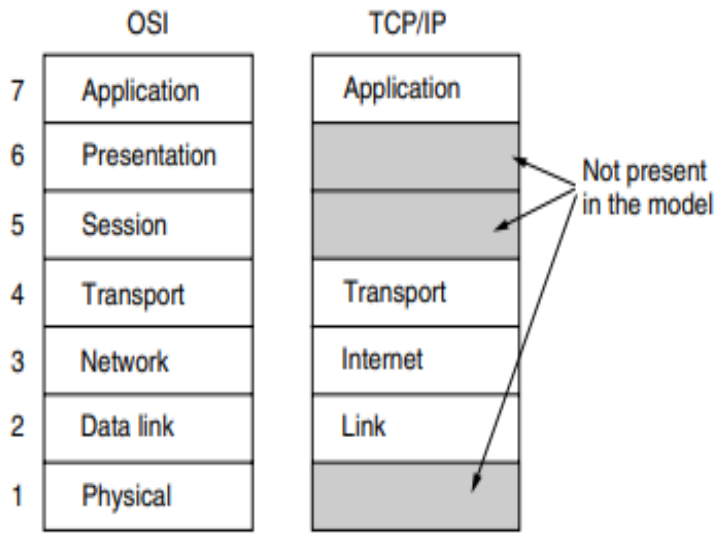
HTTP (Hypertext Transfer Protocol), the foundation of the World Wide Web, is a popular application protocol. When a browser requests a Web page, it uses HTTP to send the page's name to the server hosting the page. The page is then returned by the server. For file transfer, electronic mail, and network news, other application protocols are employed.

TCP/IP Reference Model

The ARPANET was a DoD-sponsored research network. It used leased telephone lines to connect hundreds of universities. When satellite and radio networks were added later, the current protocols had difficulty interacting with them, necessitating the creation of new reference architecture. One of the main design aims was to be able to integrate numerous networks in a seamless manner. This architecture came to be known as the TCP/IP Reference Model.Another key goal was for the network to be able to withstand the loss of subnet hardware without breaking up on-going communications.Furthermore, because applications with varying needs, ranging from file transfer to real-time speech transmission, a flexible architecture was required.

Link Layer: All of these needs lead to the selection of a packet-switching network based on a connectionless layer that spans many networks.The link layer, the model's lowest layer, explains which links suitable the requirements of this connectionless internet layer. The Link Layer serves as a bridge between hosts and transmission links.

Internet Layer: The internet layer is the linchpin that connects the entire architecture.Its purpose is to allow hosts to inject packets into any network and have them flow independently to the destination (which could be on a separate network).They may even arrive in a different order than when they were sent, in which case upper layers must rearrange them if in-order delivery is necessary.



The internet layer specifies an official packet format and protocol known as IP (Internet Protocol), as well as a companion protocol known as ICMP (Internet Control Message Protocol), which helps in its operation.

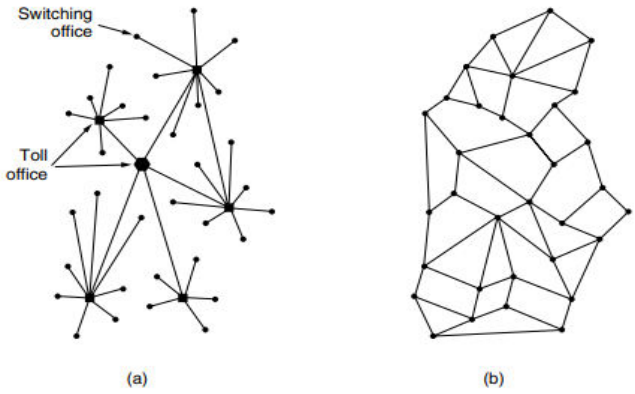
The internet layer's job is to get IP packets to where they need to go. Clearly, packet routing is a significant issue here.

Transport Layer: In the TCP/IP model, the layer above the internet layer is now commonly referred to as the transport layer.It is intended to allow peer entities on the source and destination hosts to converse in the same way that the OSI transport layer does.Here, two end-to-end transport protocols are defined. TCP (Transmission Control Protocol) is a reliable connection-oriented protocol that allows a byte stream from one machine to be sent without error to any other machine on the internet. It divides the incoming byte stream into discrete messages and forwards them to the internet layer.The receiving TCP process at the destination reassembles the received messages into the output stream. TCP also handles flow management to ensure that a fast sender does not overwhelm a slow receiver with messages that it cannot handle.UDP, the second protocol in this layer, is an unreliable, connectionless protocol designed for applications that do not require TCP's sequencing or flow control. Applications where speed is more critical than accuracy, such as transmitting speech or video.

Application Layer: There are no session or presentation levels in the TCP/IP architecture.The application layer stands above the transport layer. All of the higher-level protocols are included in it. The first ones were electronic mail (SMTP), file transfer (FTP), and virtual terminal (TELNET). The Domain Name System (DNS), which maps host names to their network addresses, HTTP, which retrieves pages from the World Wide Web, and RTP, which transfers real-time media like audio and video, are a few of the most important ones that we will examine.

Example Networks: Internet

The Internet is a huge collection of different networks that share many common protocols and services, but it is not actually a network at all. Because no one designed it and no one is in charge of it, it is an unusual system. Let's start from the beginning and examine how and why it has evolved in order to gain a deeper understanding of it.The story commences in the late 1950s, when the U.S. Department of Defence (DoD) sought a command-and-control network that could withstand a nuclear war. During that period, military communications relied on the public telephone network, which was considered vulnerable. The telephone switching offices, denoted by the black dots, were linked to thousands of phones through their connections, which in turn were connected to higher-level switching offices, or toll offices, forming a nationwide hierarchy.



One potential weakness of the system was that the destruction of several critical toll offices could result in its fragmentation into numerous isolated islands. To address this challenge ARPANET was designed.The subnet would be made up of 56-kbps transmission lines connecting minicomputers known as Interface

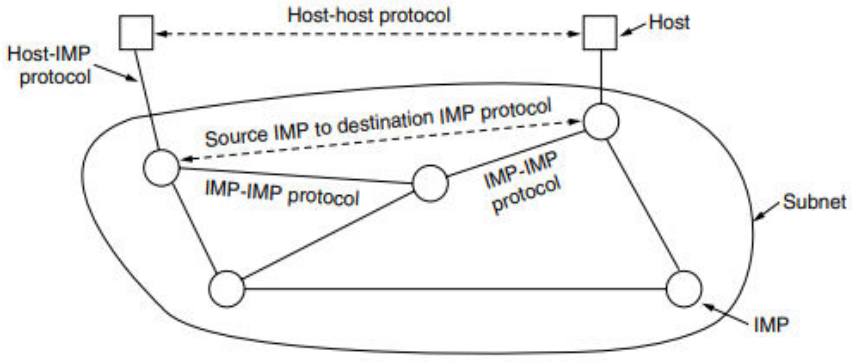


Figure 1-26. The original ARPANET design.

The software was divided into a host and subnet parts. The subnet software comprised the IMP-IMP protocol, the source IMP to destination IMP protocol, and the IMP end of the host-IMP connection, all of which were intended to increase reliability. In addition to the subnet, application software and the host-host protocol were required externally.

Message Processors or IMPs.Each IMP would be linked to at least two additional IMPs for maximum

reliability. Messages in a subnet may be automatically diverted along different paths even if some lines and IMPs were destroyed.Each network node was to be made up of an IMP and a host in the same room, linked by a short wire. A host could send up to 8063-bit messages to its IMP, which would then divide them into packets of no more than 1008 bits and forward them independently towards the destination.The subnet was the first electronic store and forward packet-switching network since each packet was received in its entirety before being forwarded.The ARPANET protocols that were in use at the time were not designed to run across several networks. The discovery of the TCP/IP model and protocols was the result of additional research on protocols motivated by this observation.TCP/IP was created specifically to manage internetwork communication, which became important as more and more networks were connected to the ARPANET.

Architecture of the Internet

An Internet Service Provider (ISP) is what connects a computer to the Internet. A user pays an ISP to get access to the Internet.People often use their home phone line to connect to an ISP. In this case, your phone company is your ISP.There is a DSL modem attached to the computer. This modem changes digital packets into analogue signals that can go over the phone line without any problems.A DSLAM (Digital Subscriber Line Access Multiplexer) makes the change between signals and packets at the other end.POP stands for "Point of Presence." This is the place where customer packets join the ISP network to be served. The system is now fully digitised and packet switched.ISP networks can cover an area, a country, or the whole world.The architecture of an ISP is made up of long-distance transmission lines that connect routers at POPs in different places. This equipment is called the backbone of the ISP.As long as the packet is going to a host that the ISP directly serves, it will be sent over the backbone and to that host. If not, it has to be given to another ISP.An IXP is a place where ISPs can connect their networks and exchange data.It is stated that the connected ISPs peer with one another. Globally, there are numerous IXPs located in cities.An IXP is essentially a room full of routers—at least one for each ISP. All of the routers in the room are connected by a LAN, allowing packets to be passed from one ISP backbone to another.The Amsterdam Internet Exchange is one of the biggest, connecting hundreds of ISPs and facilitating the exchange of hundreds of gigabits of traffic every second.A small number of corporations, such as AT&T and Sprint, run huge international backbone networks with thousands of routers linked by high-bandwidth fibre optic lines at the top of the food chain. These Internet service providers do not pay for transport. Tier 1 ISPs are commonly referred to as the Internet's backbone because everyone else must connect to them in order to access the whole Internet.Large content providers, such as Google and Yahoo!, house their computers in data centres that are well connected to the rest of the Internet.

These data centres are intended for computers and can be filled with rack after rack of machines, referred to as a server farm.

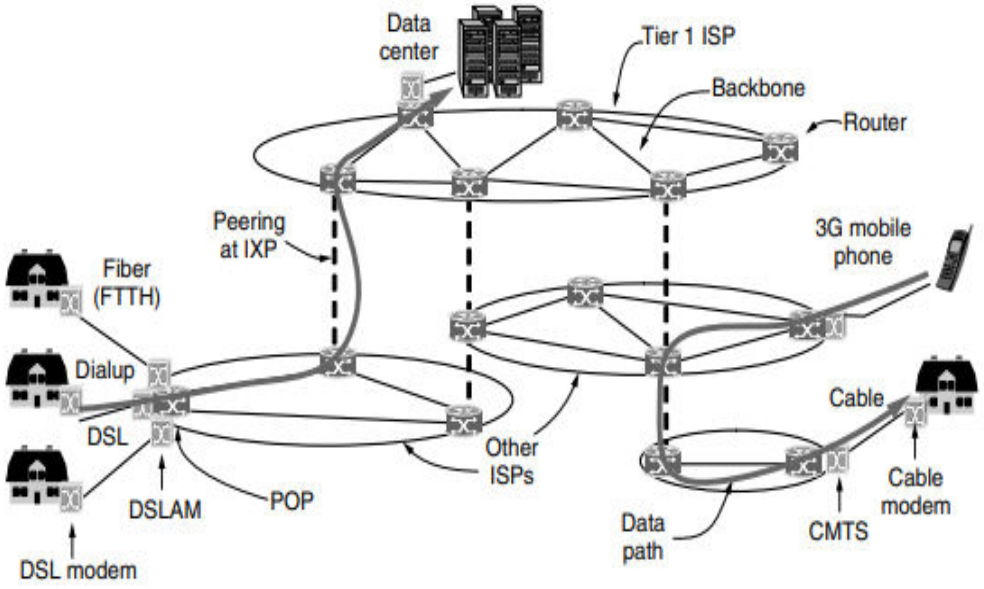


Figure 1-29. Overview of the Internet architecture.

If a machine: (1) ran the TCP/IP protocol stack; (2) had an IP address; and (3) could send IP packets to all other machines on the Internet, it was on the Internet. However, ISPs frequently reuse IP addresses based on which computers are currently in use, and they frequently share a single IP address among many computers.

Guided Transmission Media

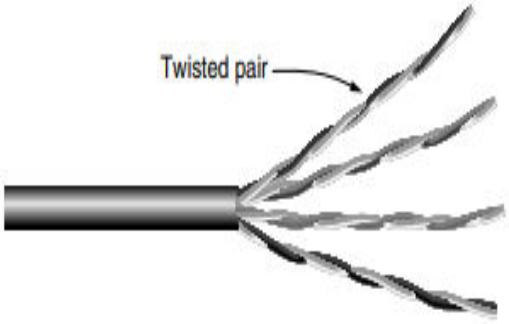
For the actual transmission, many physical mediums can be employed. Each has its own niche in terms of bandwidth, delay, cost, and simplicity of installation and maintenance. Broadly speaking, media can be divided into two categories: **unguided media** (such satellites, terrestrial wireless, and airborne lasers) and **guided media** (like fibre optics and copper wire).

Magnetic Media: Writing data to magnetic tape or removable media (like DVDs), moving the tape or discs to the destination computer, and then reading them back in again is one of the most popular ways to move data from one computer to another.It is usually cheaper, has a high speed, or costs less per bit sent.Even though magnetic tape has great capacity, the time it takes to send data is measured in minutes or hours, not milliseconds.

Twisted Pairs:A connection is needed for many applications. Twisted pair is one of the oldest and most popular ways to send data. A twisted pair is made up of two copper wires that are shielded and are usually about 1 mm thick. The wires are twisted together in a helical form, just like a DNA molecule.Twisting is done because two parallel wires make an excellent antenna. When wires are twisted, the waves from different twists cancel each other out, causing the wire to radiate less effectively. The telephone system is the most prevalent application of the twisted pair.Twisted pairs can be utilized to convey both analogue and digital

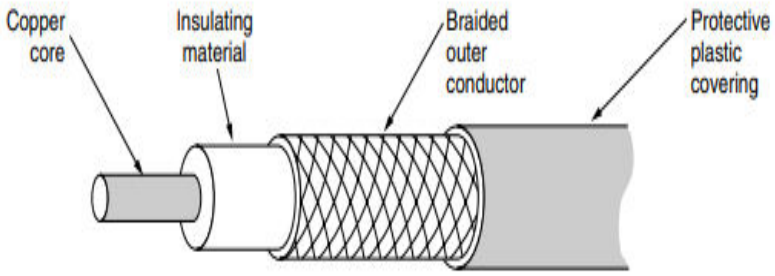
data. The bandwidth is determined by the wire's thickness and the distance travelled.There are various types of twisted-pair cabling. Category 5 cabling is the common type seen in many office buildings.

A category 5 twisted pair is made up of two insulated wires that have been gently twisted together. To protect the wires and keep them together, four such pairs are commonly combined in a plastic sheath.



Cat 5 cables replaced previous Category 3 cables with a similar cable that has more twists per metre but utilises the same connector. More twists result in reduced crosstalk and higher signal quality over longer distances, making the cables more suitable for high-speed computer connection.

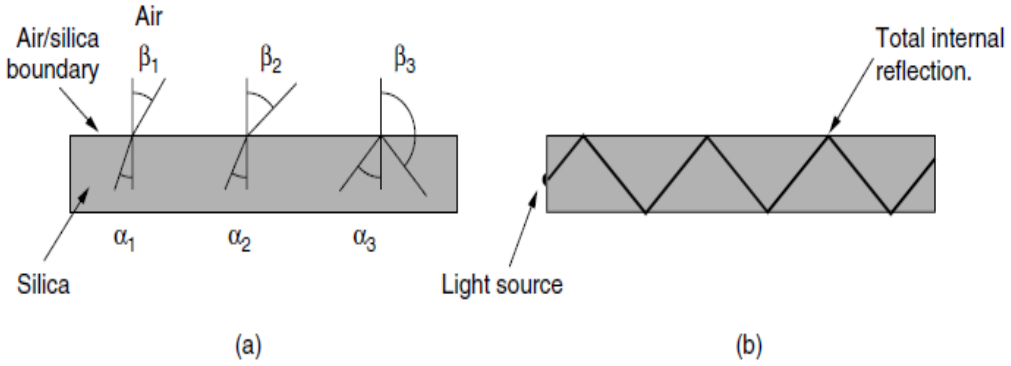
Coaxial cable: It can cover farther at faster rates than unshielded twisted pairs because it has stronger shielding and a wider bandwidth.In general, two types of coaxial cable are utilised. If the purpose of the cable is for digital transmission, 50-ohm cable is frequently utilised. Cable television and analogue transmission are two common uses for 75 ohm cable.A coaxial cable is made up of a strong copper wire core that is surrounded by an insulating layer. A cylindrical conductor, commonly in the form of a tightly woven braided mesh, surrounds the insulator. The outside conductor is protected by a plastic sheath.



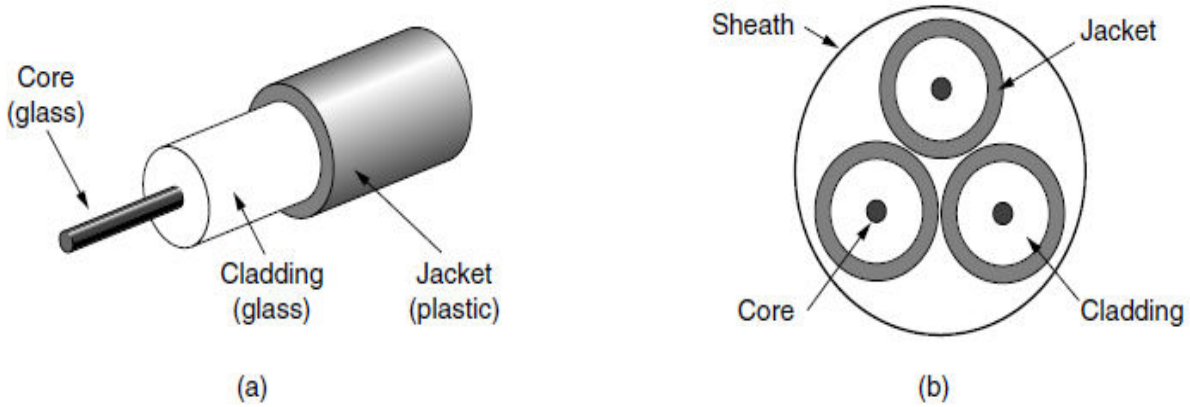
The bandwidth is determined by the cable's quality and length. Modern cables have bandwidths of many GHz. Cable television and metropolitan area networks continue to depend heavily on coax.

Fiber Optics: Fibre optics are used in network backbones, high-speed LANs, and high-speed Internet access like FttH (Fibre to the Home).The light source, transmission medium, and detector are the three main components of an optical transmission system. A light pulse represents a 1 bit, whereas the absence of light represents a 0 bit. The transmission medium is a glass fibre that is extremely thin.When light strikes the detector, it generates an electrical pulse.By connecting a light source to one end of an optical fibre and a

detector to the other, we can make a one-way data transfer system that takes an electrical signal, changes it into light pulses, sends them, and then changes the output back to an electrical signal at the receiving end. The path of a light ray changes when it goes from one material to another, like silica to air.Here we see a light ray incident on the boundary at an angle α1 emerging at an angle β1. The amount of refractiondepends on the properties of the two media.



When the angle of incidence is above a certain critical angle, the light is bent back into the silica and doesn't get out into the air. So, a light ray that hits the fibre at or above the critical angle gets stuck inside it and can travel for many kilometres with almost no loss.The glass core through which light propagates is located in the centre.To keep all of the light in the core, the core is surrounded by a glass cladding with a lower index of refraction than the core.The cladding is then protected by a thin plastic jacket. Fibres are normally bundled together and protected by an outer sheath.



Comparison of Fiber Optics and Copper Wire:

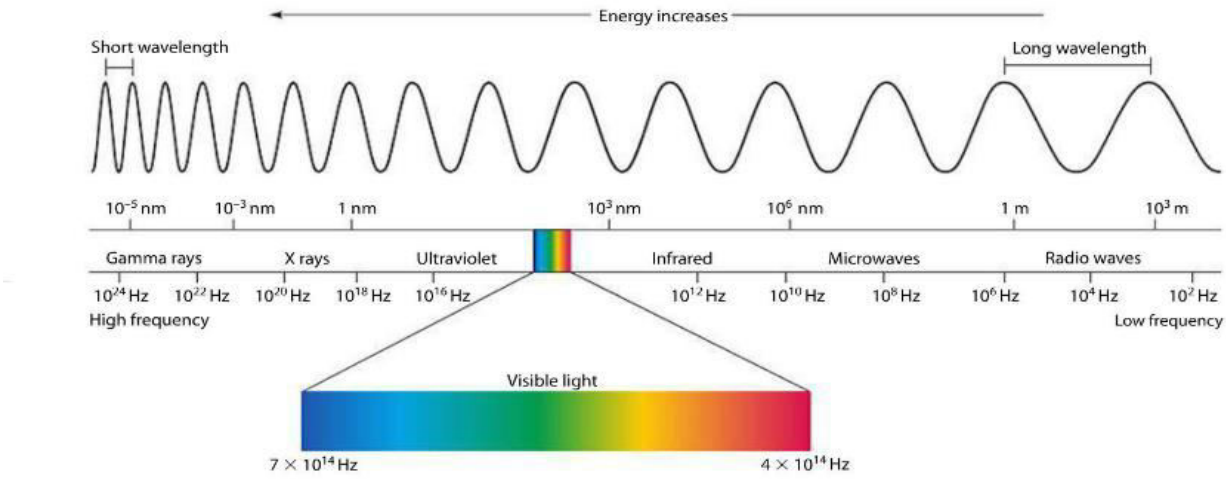
Fibre offers a lot of benefits. It can tolerate significantly larger bandwidths than copper, to start.Because there isn't much loss, repeaters are only needed every 50 km on long lines, compared to every 5 km for copper. This saves a lot of money.Fibre is also better because it doesn't get damaged by power spikes, electromagnetic interference, or power outages.It is important for harsh factory environments that it is not

affected by chemicals in the air that erode away at metal. Copper is a lot heavier than fibre. It costs considerably less to install. Fibres are hard to tap and never allow light through. Because of these features, fibre is very safe from individuals who might try to tap.Finally, fibre interfaces cost more than electrical interfaces.

Wireless Transmission

Twisted pair, coax, and fibre optics are useless to mobile users. They require data without being bound to terrestrial communication infrastructure. Wireless communication is the solution for these consumers. In some cases, wireless has advantages over fixed equipment. If running fibre to a building is difficult because of the geography (mountains, jungles, etc.), wireless may be preferable.

Electromagnetic Spectrum: Electrons generate electromagnetic waves that can travel over space.These waves were predicted in 1865 by British physicist James Clerk Maxwell and first observed in 1887 by German scientist Heinrich Hertz.The frequency, f, of a wave is measured in hertz (Hz) and is defined as the number of oscillations per second. The wavelength is defined as the distance between two successive maxima (or minima).When an appropriate-sized antenna is connected to an electrical circuit, electromagnetic waves can be broadcast efficiently and received by a receiver located some distance away. This idea drives all wireless communication.



In a vacuum, all electromagnetic waves, regardless of frequency, travel at the same speed. This is commonly referred to as the speed of light.The fundamental relation between f, λ, and c (in a vacuum) is $\lambda f = c$

100-MHz waves, for example, are around 3 metres long, 1000-MHz waves are roughly 0.3 metres long, and 0.1-meter waves have a frequency of 3000 MHz.By changing the waves' amplitude, frequency, or phase, information can be sent through radio waves, microwaves, infrared light, and visible light.Due to their higher frequencies, ultraviolet light, X-rays, and gamma rays would be even more ideal; however, they are hazardous to living organisms, difficult to generate and modulate, and do not transmit effectively through buildings.

Radio Transmission: Radio frequency (RF) waves are often used for communication both indoors and outdoors because they are simple to produce, can travel great distances, and can easily penetrate walls. Additionally, because radio waves are omnidirectional—that is, they can travel in any direction from their source—physical alignment between the transmitter and receiver is not necessary.The characteristics of radio waves vary with frequency. Radio waves can easily go through obstructions at low frequencies.Radio waves at high frequencies typically bounce off obstacles and go in straight lines.As the distance from the source increases, the RF signal's energy abruptly decreases. We refer to this attenuation as "path loss." Rain also absorbs radio signals at high frequencies.Radio waves in the VLF, LF, and MF bands follow the earth. These bands allow radio waves to readily pass through buildings.Ground waves are absorbed by the earth in the HF and VHF frequencies. However, waves that reach the ionosphere, a layer of charged particles that circles Earth at a height of 100 to 500 km, are refracted and returned to the

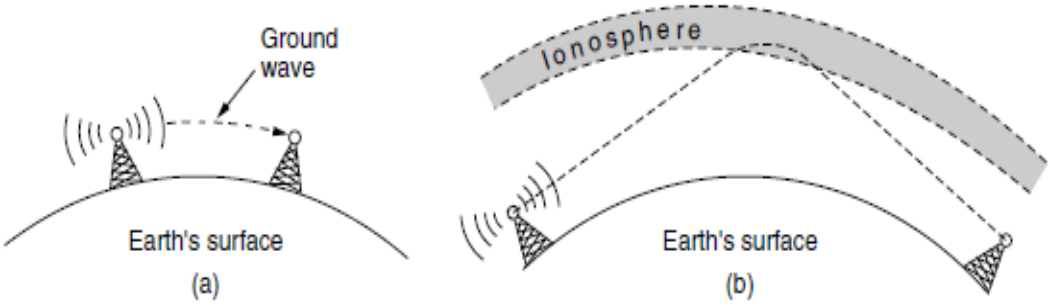
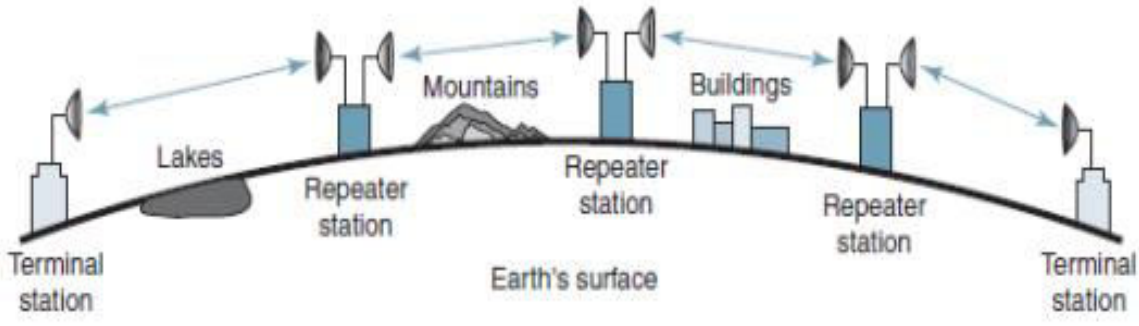


Figure 2-12. (a) In the VLF, LF, and MF bands, radio waves follow the curvature of the earth. (b) In the HF band, they bounce off the ionosphere.

earth.

Microwave Transmission: Because these waves travel in roughly straight lines, they can be narrowly directed. Using a parabolic antenna to concentrate all of the energy into a narrow beam. Both the transmitting and receiving antennas must be precisely aligned. Multiple transmitters lined up in a row can communicate with multiple receivers in a row without interfering, as long as specific minimum spacing restrictions are followed.Since microwaves move in a straight line, the earth will obstruct the path if the towers are too far apart. Repeaters are therefore occasionally required. The maximum distance between towers increases with height.



Microwaves, unlike lower-frequency radio waves, do not travel well through buildings. Furthermore, even if the beam is well concentrated at the transmitter, there is still some divergence in space. Some waves may be refracted off low-lying air layers and thus arrive slightly later than direct waves. When the delayed waves come out of phase with the direct wave, the signal is cancelled. This is known as multipath fading, and it is frequently a major issue.Microwave transmission is used for like long-distance phones, cell phones, and TV distribution.It's better than fibre in many ways. The main one is that you don't need to lay down wires. Every 50 km, buy a small piece of land and put a radio tower on it. The microwave is also not too expensive. Burying 50 km of fibre cable through a busy city or up over a mountain might cost more than putting up two simple towers with antennas on each one.

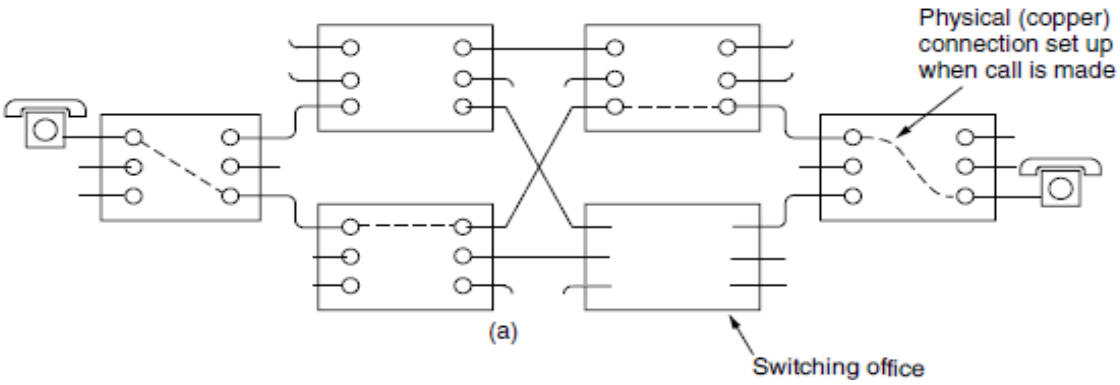
Infrared Transmission: Infrared waves are often used for short-range contact. Infrared is used for contact between TV, VCR, and stereo remote controls.They are cheap, easy to make, and good at pointing in the right direction, but they can't go through solid things, which is a big problem.On the other hand, it's a good thing that infrared waves don't easily pass through concrete walls. It means that an infrared system in one room of a building won't affect a similar system in rooms or buildings next door. For example, you can't use your remote to control your neighbour's TV.An infrared system does not need a licence from the government to work. Radio systems, on the other hand, need a licence to work outside of the ISM bands.

Light Transmission: Free-space optics, also known as unguided optical signalling, has been used for a very long time. Lasers on the roofs of two buildings can be used to join their LANs, which is a more modern use. Laser-based optical signalling can only go in one direction, so each end needs its own laser and photo detector. This plan has a very wide bandwidth for a very low price. It is also pretty safe because it is hard to tap a narrow laser beam.It is also relatively simple to set up and does not necessitate an FCC licence.

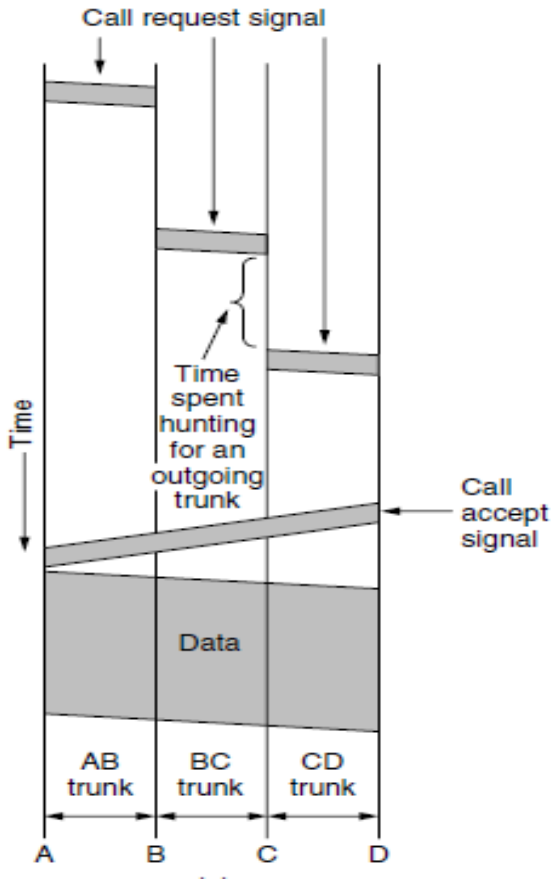
The laser's advantage, an extremely narrow beam, but also its disadvantage here.Aiming a laser beam 1 mm broad at a 500-meter-away target the size of a pin head necessitates precision.Wind and temperature variations can cause the beam to distort, and laser beams cannot penetrate rain or severe fog, even on sunny days.

Switching-Circuit switching

The phone system is made up of two main parts: the outside plant, which includes the local loops and trunks because they are not inside the switching offices and the inside plant, which includes the switches that are inside the switching offices. There are two types of switching that are used by networks today: packet switching and circuit switching.When you make a phone call, the telephone system's switching equipment searches for a physical path from your phone to the receiver's phone. This is referred to as circuit switching.

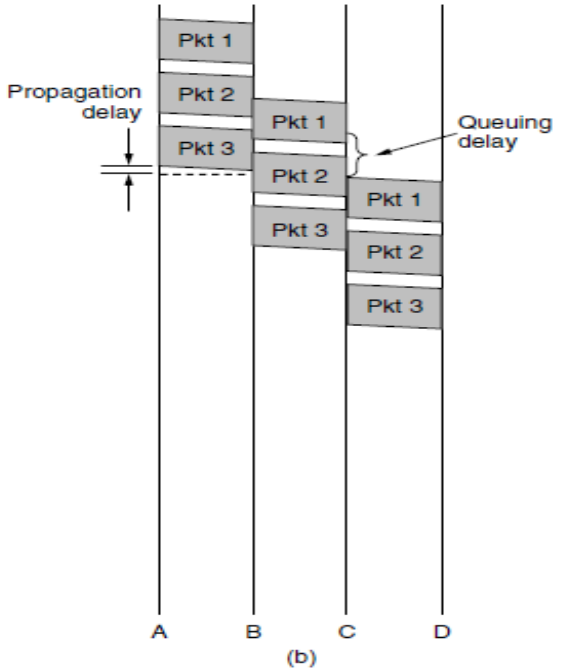


A carrier switching office is represented by each of the six rectangles.Each office has three incoming and three outgoing telephone lines. A physical connection is formed between the line on which the call came in and one of the output lines when a call travels through a switching office.Once a call is set up, there is a fixed path between both ends that will stay open until the call is over.There can be up to 10 seconds between when the phone stops dialling and when it starts to ring. This can be longer for foreign or long-distance calls. During this time, the phone system is looking for a path to connect.The one and only delay after setup is the electromagnetic signal propagation time, roughly 5 ms per 1000 kilometres. The established path prevents congestion—once the call is made, you never get busy signals. Full bandwidth is reserved from sender to receiver. Data that follows the same path cannot arrive out of order.



Switching: Packet Switching

Packets are sent as soon as they are available using this method. There is no need to plan ahead of time for a particular route. Routers must use store-and-forward transmission to transmit each packet on its own path to the destination. With packet switching there is no fixed path, thus distinct packets can travel various routes, depending on network conditions at the time they are transmitted, and they may arrive out of order. Packet-switching networks place a tight upper limit on the size of packets.The first packet of a long message can be forwarded before the second one has fully arrived.However, the store-and-forward delay of accumulating a packet in the router's memory before it is sent on to the next router exceeds that of circuit switching. Because no bandwidth is reserved with packet switching, packets may have to wait to be forwarded.If multiple packets are sent at the same time, this causes queuing delay and congestion. If a circuit is dedicated for a certain user but there is no traffic, the bandwidth is wasted. It can't be used for anything else. Because packet switching does not waste bandwidth, it is more efficient from a system viewpoint.Circuit switching is less tolerant of errors than packet switching. All circuits that are utilising a failed switch are terminated, preventing the transmission of any further traffic on any of them.Packet switching facilitates the bypassing of dead switches for packets.



(b)

Item	Circuit switched	Packet switched
Call setup	Required	Not needed
Dedicated physical path	Yes	No
Each packet follows the same route	Yes	No
Packets arrive in order	Yes	No
Is a switch crash fatal	Yes	No
Bandwidth available	Fixed	Dynamic
Time of possible congestion	At setup time	On every packet
Potentially wasted bandwidth	Yes	No
Store-and-forward transmission	No	Yes
Charging	Per minute	Per packet