ADVANCED COMPUTER NETWORKS

Geetha G
Shashikala H.K

BOOKS ARCADE

Advanced Computer Networks

Advanced Computer Networks

Geetha G
Shashikala H.K

BOOKS ARCADE
KRISHNA NAGAR, DELHI

Advanced Computer Networks

Geetha G
Shashikala H.K

BOOKS ARCADE

Regd. Office:
F-10/24, East Krishna Nagar, Near Vijay Chowk, Delhi-110051
Ph. No: +91-11-79669196, +91-9899073222
E-mail: info@booksarcade.co.in, booksarcade.pub@gmail.com
Website: www.booksarcade.co.in

Year of Publication 2023

International Standard Book Number-13: 978-81-19199-88-4

CONTENTS

CHAPTER 1

INTRODUCTION TO NETWORKS

Geetha G, Director,
School of Computer Science and Engineering, School of Sciences, Jain (Deemed to be University) Bangalore, India
Email Id- geetha.g@jainuniversity.ac.in

Networking is an intellectually and technically exciting area because of the technology that makes it possible for people and their computers to communicate with one another. It is a collection of transmission nodes and computers channels (links) that enable communication across all types of distances. Your home computer's peripherals might easily be connected to a Bluetooth personal area network. An ocean may be crossed with an underwater fibre optic cable. Worldwide telephone and Internet networks exist. In particular, networking is a late 20th-century invention. During the last 40 years or more, the Internet has evolved. Local area networks, SONET fibre networks, and ATM backbones all developed and expanded throughout the 1980s and 1990s. The growth and development of WDM fibre multiplexing occurred in the 1990s and the first decade of the new century. There are always new wireless protocols emerging. The world of networking and computing today is increasingly relying on data centres and cloud computing.

The goal of the book is to provide a brief introduction of several important networking issues. An introduction to the practical features of networking will now be given. There are several cable and wireless transmission techniques available today to link computers, networks, and users. Fiber optics, twisted pair wiring, and coaxial cable are examples of wired transmission medium. Microwave line of sight, satellites, cellular systems, ad hoc networks, and wireless sensor networks are all examples of wireless technology. We'll now discuss these tools of the trade.

Coaxial Cable:

This is the thick wire that connects your home's cable TV setup box to the outside electrical system. This kind of wire is an established technology with a long history. It is still a common choice for cable TV systems today, but back in the 1980s, it was also a common option for wiring LANs. It was included into the first 10 Mbps Ethernet wire. A coaxial cable consists of four components: a copper inner core, an insulating layer, a metallic outer conductor, and a plastic outer cover. A coaxial cable consists of two wires (a copper inner core and an outer conductor), one of which is geometrically positioned within the other. With regard to other neighbouring wires, this design reduces interference to/from the coaxial cable.

A coaxial cable has a bandwidth of about 1 GHz. Can it carry how many bits per second? A digital stream is modulated to meet the cable's capacity for transporting spectrum. 1 bps needs between 1/14 and 4 Hz, depending on how well the modulation method is employed. A coaxial cable may employ 8 bits/Hz or transport 8 Gbps over short distances. There are also many varieties of coaxial cable. For digital transmissions, a 50 ohm termination is employed. For analogue broadcasts or cable TV systems, one with a 75 ohm termination is utilised.

I should say a few words about cable TV systems. These networks have a head end at the root node and are locally connected as tree networks. Programming is delivered through fibre or satellite to the head end. Cables (and perhaps fibre) extend out to dwellings from the head end. When there are significant gaps in the network, amplifiers may be added. Cable TV providers

have long been interested in offering two-way service. With the exception of Video on Demand, early limited experiments were mostly unsuccessful, but more lately, cable TV seems to be winning when it comes to transporting telephone traffic and broadband Internet access.

Twisted pair wiring:

Local area networks no longer often employ coaxial cable for wiring. Twisted pair wiring has been used as a substitute type. Traditionally, twisted pair wiring was used to connect phones to the telephone network. Two wires are twisted together along their length to form a pair. The twisted shape reduces crosstalk between neighbouring cables and electromagnetic leakage. Without amplification, twisted pairs may travel across a distance of many kilometres. The quantity of twists per inch determines a twisted pair's quality (carrying capacity). In 1990, 10 Mbps (for Ethernet) transmission via unshielded twisted pair became feasible (UTP). If the cable and connection parameters are correctly established, higher speeds may also be attainable. Category 3 UTP is one kind of unshielded twisted pair. It consists of a sheath around four sets of twisted pairs. It has a 16 MHz bandwidth. Category 3 wiring used to be utilised in a lot of workplaces.

There are more twists per inch in Category 5 UTP. As a result, its bandwidth is greater (100 MHz). Category 6 variants (250 MHz or greater) and category 7 versions are more recent specifications (600 MHz or more). The 1200 MHz version of Category 8 is under development (Wikipedia). Twisted pair's rapid adoption is due to the fact that it is lighter and thinner than coaxial wire.

Fiber Optics

As opposed to coaxial cables and twisted pair wire, which transmit electricity, fibre optic cable has a silicon glass core. A plastic jacket is placed over the cladding that surrounds the core. The maximum data carrying capability of any wired media is provided by fibre optic cables. 50 Tbps (terabits per second, or 50 1012 bits per second) is the standard capacity of a fibre. In actuality, this data rate has long exceeded the pace at which conventional electronics could fill the fibre. The electronic bottleneck is this mismatch between the speed of the nodal electronics and the fibre. The scenario was flipped decades ago, with connections being sluggish and nodes being quite quick. The paradigm change has caused procedures to be redesigned. Multi-mode and single mode fibre are the two main varieties. Single mode fibre more correctly preserves pulse forms, which increases the possible data rate. Yet, the price of single mode and multi-mode fibre is similar. The opto-electronics required at either end of the fibre account for the majority of the price difference. Dispersion is one of the factors contributing to multi-mode fibres' inferior performance. Square digital pulses have a tendency to disperse over time when there is dispersion, which reduces the maximum data rate. Research has focused on a certain class of pulse forms termed solitons, for which dispersion is reduced (e.g., hyperbolic cosines).

10% of the light that a fibre transports may be lost when two fibres are connected via mechanical fibre connectors. A reduced attenuation occurs when the fiber's two ends are fused together. Nowadays, fibre optic cables are stretched across the bottom of seas and across continents. Organizations also utilise them to transport phone, data, and video traffic internally.

Line of Sight for Microwaves

Radio waves in the microwave range generally go in straight lines. As a result, some network operators set up networks of tall towers spaced a few kilometres apart and installed microwave antennas on each tower at various heights. The benefit of not having to dig holes for cables must be balanced against the cost of building and maintaining towers.

Satellites

In the late 1940s, science fiction author Arthur C. Clarke popularised the idea of employing satellites as communication relays. Nowadays, satellites are widely employed for communication. They excel at filling certain technology voids, such as connecting mobile users, enabling wide-area broadcasts, and facilitating communications in underdeveloped regions. Geostationary satellites and low-earth orbit satellites are the two primary communication satellite designs (LEOS). Now we talk about both.

Satellites that are in orbit

A satellite in a low orbit (hundreds of kilometres) near the equator seems to move against the sky, as you may remember from a physics class. Its apparent velocity slows as its orbital height rises. It seems to remain stationary in the sky above the equator at a certain height of around 36,000 kilometres for a whole 24-hour period. The day of introduction to networks. The satellite seems to be floating in the sky even though it is really orbiting the earth at the same angular rate that the planet rotates.

It's quite helpful. For instance, a satellite TV provider may install inside antennas that only point in the direction of the satellite. As an alternative, a geostationary satellite may continuously transmit a signal across a vast region (its footprint). Geostationary satellites are positioned 2 degrees apart from one another near the equator by international agreement. Depending on the areas of the earth beneath a location, certain places are more economically advantageous than others.

Several hundred transponders (relay amplifiers), each with a bandwidth of 80 MHz, are typically found on a geostationary satellite (Tanenbaum 03). A spacecraft of this size may weigh several thousand kilos and use solar panels to generate several kilowatts of power. When the lower bands have gotten congested and technology has advanced, more microwave frequency bands have been utilized. The L (1.5/1.6 GHz), S (1.9/2.2 GHz), C (4/6 GHz), Ku (11/14 GHz), and Ka (20/30 GHz) bands are among the frequency ranges. Thus, the downlink band is represented by the first number, and the uplink band by the second. In the L band, a signal's real bandwidth may range from around 15 MHz to several GHz (Tanenbaum 03). It should be emphasised that in-depth research has been done on satellite signal transmission in various atmospheric and meteorological situations. Budgets for excess power to overcome rain attenuation often go over 11 GHz.

Satellites in Low Earth Orbit

Low-Earth Orbit Satellite Architecture is a more modern design. The most well-known of these systems was Motorola's Iridium. It got its name since the initial 77 satellite network had exactly as many satellites as the number 1 in the atomic structure. Low Earth Orbit Satellites (LEOS) of the element Iridium in polar orbits are shown in Figure 1.1. While there were really 66 satellites in the system's orbit, the name Iridium was retained.

Iridium was created with the intention of offering a worldwide mobile phone service. An Iridium phone may be used everywhere in the globe, including the Arctic and the ocean. In contrast to local terrestrial mobile phone service, which costs less than 25 cents per minute, chatting on Iridium unfortunately costs a dollar or more per minute after investing $5 billion to establish the infrastructure. Despite efforts to target business travellers, the system was not financially successful and was sold; it is currently run by a private corporation. Yet from a technological standpoint, the Iridium system is intriguing. Each of the six polar orbits, which

pass over the North Pole, south to the South Pole, and back up to the North Pole (see Figure 1.1), carries eleven satellites.

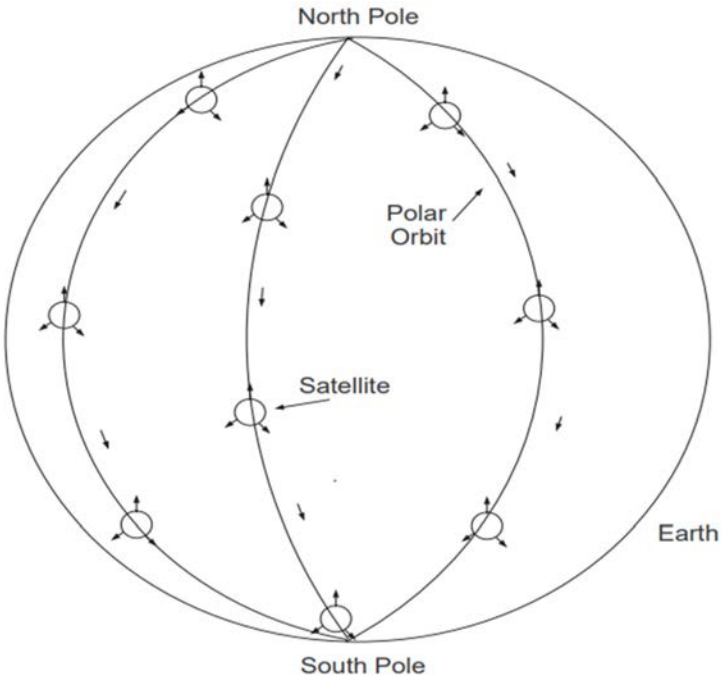


Figure 1.1: Low earth orbit satellites (LEOS) in polar orbits.

Above every area on earth, a number of satellites are constantly gliding around the sky. The device can accommodate roughly a quarter of a million chats using a number of dozen spot beams. From satellite to satellite, calls may be transmitted. It should be noted that various rivals to Iridium were suggested but never constructed. One used a bent pipe design in which, as opposed to being transmitted from satellite to satellite, a call to a satellite would be beamed down from the same satellite to a ground station and then delivered via the terrestrial phone network. In an attempt to save expenses and simplify the design, this was done.

Cellular Systems: Cellular phone networks, which link mobile phones to the public switched telephone network, have been in use since the early 1980s. Signals from/to mobile phones go through/to a nearby base station antenna that is hard linked into the public switched telephone network in such systems. Such a mechanism is shown in Figure 1.2. A geographic area, such as a city or suburb, is split up into smaller areas known as cells.

Cell centres are shown to be base stations: A switching computer (the mobile switching centre, or MSC) that offers a route to the phone network is connected to nearby base stations. While making a call, a mobile phone connects to the base station with the strongest signal that is closest to it. Received power levels are measured and transmitted by base stations and mobile devices.

Driving towards a new base station will eventually cause its signal to become stronger than the one of the one you are linked to, at which time the system will complete a handoff. Connectivity is switched from one base station to a nearby one during a handoff. Transparent handoffs happen without the talking user being aware of it. A paging-like device that activates (rings) the mobile phone during a call.

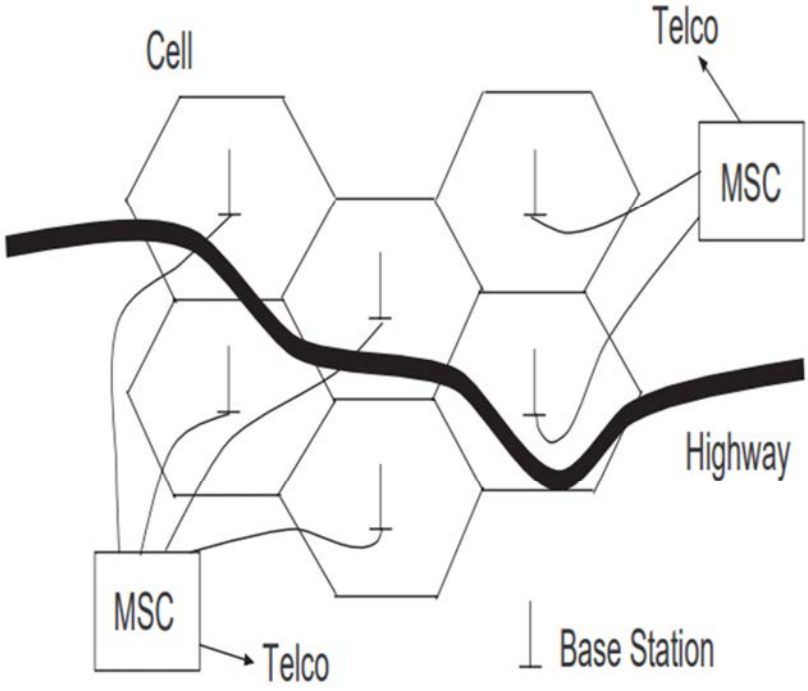


Figure 1.2: User's phone is a cellular network component.

NTT introduced the first cellular network in Japan in 1979. AT&T's AMPS (Advanced Mobile Phone System) was the first cellular network in the United States. It was first used in 1983. These analogue systems were of the first generation. Systems from the second generation were digital. The most widely used GSM (Global System for Mobile), which was developed in Europe, is what has been placed all over the globe. Increased data rates are offered by third- and fourth-generation cellular networks for uses like Internet surfing and photo sending.

Ad hoc Networks:

Ad hoc networks are radio networks where (typically mobile) nodes may connect and transparently build a network without any user involvement. As long as the nodes are within range of one another and as long as the energy sources persist, will sustain the network. Messages in an ad hoc network hop from node to node before arriving at their final destination. In reality, using several tiny hops actually consumes significantly less energy than using a single big hop, sometimes by orders of magnitude, due to the nonlinear relationship of energy on transmission distance. Multi-hop transmission, potential mobility, and potential low energy to power the network nodes are all features of ad hoc networks. Mobile networks, emergency networks, wireless sensor networks, and ad hoc crowds of people, such those at convention centres, are a few examples of applications. For ad hoc networks, routing is a crucial problem. Topology-based routing and position-based routing are the two main subcategories of routing algorithms. Topology-based routing carries out the routing using knowledge of the present connections. Position-based routing uses the geographic position of each node as the basis for routing. A service like the Global Positioning System may provide the position data (GPS).

Proactive and reactive algorithms are subcategories of topology-based algorithms. Proactive algorithms provide traditional routing algorithms data about current pathways. Even if a route is idle, a significant amount of control message traffic is required to keep this information current. If there are several topology changes, this overhead issue is made worse (say due to movement of the nodes). Reactive algorithms, on the other hand, limit the amount of information and control overhead by maintaining routes only for active pathways, such as DSR, TORA, and AODV. Even Nevertheless, if there are several topology changes, more control traffic is produced. Positionn-based routing does not need the maintenance of routes, routing tables, or the creation of significant volumes of control traffic.

Spositions: It is simple to put into practise "Geocasting" to a particular region. Position-based routing may be implemented using a variety of heuristics.

Wireless Sensor Networks:

Networks of tiny components that can gather sensor data and convey the data to a human observer may be made practical by the combination of wireless, computer, and sensor technologies. Because of their potential to be a revolutionary technology and the technological difficulties that must be addressed in order for this to happen, wireless sensor networks have attracted the interest of researchers in academic institutions, government agencies, and private enterprise. Such wireless sensor networks are expected to transmit data in a multi-hop manner of operation using ad hoc radio networks.

A typical wireless sensor unit has dimensions between 1 millimetre and 1 centimetre, weighs less than 100 grammes, costs less than $1, and uses less than 100 microwatts of power. It also include computing and networking circuits (Shah 02). In comparison, a Bluetooth transceiver for a wireless personal area network uses more than 1000 microwatts. Using battery technology, a cubic millimetre wireless sensor can store 1 Joule, enabling a daily energy usage of 10 microwatts. Hence, the idea of capturing energy from light or vibration has been put out. Keep in mind that sensor data often has low data rates (100s bps to 100 Kbps).

Minimizing energy consumption in wireless sensor networks becomes crucial given these factors, of course. Although wireless sensor networks may only be required for a day or less in certain applications, there are numerous more uses for which a constant supply of electricity is required.

Moreover, communication consumes a lot more energy than computing. It may need as much energy to send one bit 100 metres across a network as it does to execute 3000 instructions on a microprocessor. Wireless sensor network uses in the military are quite evident. Beginning with Wireless sensor networks have a wide range of possible scientific and non-commercial uses. Geophysical, environmental, and planetary exploration are examples of scientific applications. Wireless sensor networks might be used to study volcanoes, gauge the weather, keep an eye on beach pollution, or document planetary surface conditions. Applications for biomedicine include things like retinal prostheses and glucose level monitoring. Manufacturing sensors that can live within the human body without having an adverse effect on it is especially challenging for these applications.

Sensors may be installed in rotating machines, semiconductor processing chambers, robots, engines, and other machinery (where vibration might sometimes provide energy). Telemetry for pollution control may employ wireless sensors in engines. Wireless sensors might be installed in houses and buildings for temperature management, among other possible uses. Be aware that wiring just one sensor in a structure might run into the hundreds of dollars. In the end, wireless sensors may be included into building materials.

Multiplexing

Sending many signals via a single media is known as multiplexing. A four-to-one telegraph multiplexer, created by Thomas Edison, and permitted the transmission of four telegraph signals over a single line. Frequency division multiplexing (FDM), time division multiplexing (TDM), and spread spectrum are the three main types of multiplexing used in networking today. Now each is examined (Figure 1.3).

Frequency Division Multiplexing

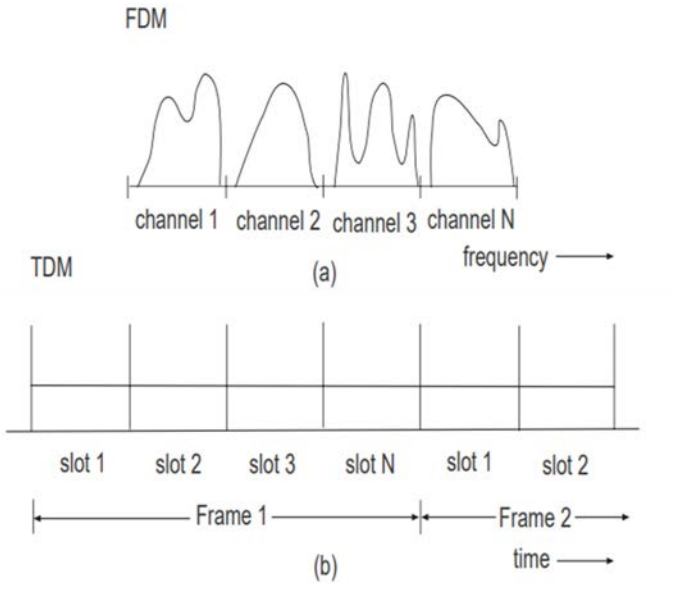


Figure 1.3: Time division multiplexing, as well as (a) frequency division multiplexing.

One channel can only be received at a time by the receiver. AM, FM, and analogue television signals are broadcast in this manner. Moreover, it refers to the wavelength division multiplexing (WDM) technique used to transport several optical signals through a fibre.

Time Division Multiplexing

A digital technique called time division multiplexing divides time into equal-duration slots on a serial connection (Figure 1.3(b)). In a telephone system, a slot may store a speech sample, but in a packet switching system, it may store a packet. There are N slots in a frame. Slots and frames both repeat. During a conversation, a telephone channel could, for example, employ slot 14 out of 24 slots in a frame. The GSM second-generation cellular system employs time division multiplexing. Digital telephone switches also use it. In reality, these switches operate by exchanging speech samples between slots using electrical devices called time slot interchangers.

Frequency Hopping:

One kind of spread spectrum technology is frequency hopping, which is often utilised on radio channels. A transmission's carrier (central) frequency alternates between them in a pseudo-random manner, as shown in Figure 1.4 (a) and Figure 1.4(b). Both the transmitter and the receiver are aware of the predictable, although seemingly random, manner in which the hopping is carried out. One has strong security if the hopping pattern is only known to the transmitter and receiver. Frequency hopping also offers strong interference suppression. If each

broadcast employs a sufficiently unique hopping pattern, numerous transmissions may be multiplexed in the same local area. Frequency hopping first appeared during World War Two.

Direct Sequence Spread Spectrum

Exclusive or (xor) gates are used in this alternative spread spectrum technology as scramblers and de-scramblers. Table 1.1. At the transmitter, a pseudo-random key stream and data are sent into opposite inputs of a xor gate.

Table 1.1: Truth Table for XOR

Key	Data	Output
0	0	0
0	1	1
1	0	1
1	1	0

The output bit equals the data bit if the key bit is zero, as shown by the xor truth table. The output bit is the complement of the data bit if the key bit is a one (0 becomes 1, 1 becomes 0). This action of scrambling is highly powerful.

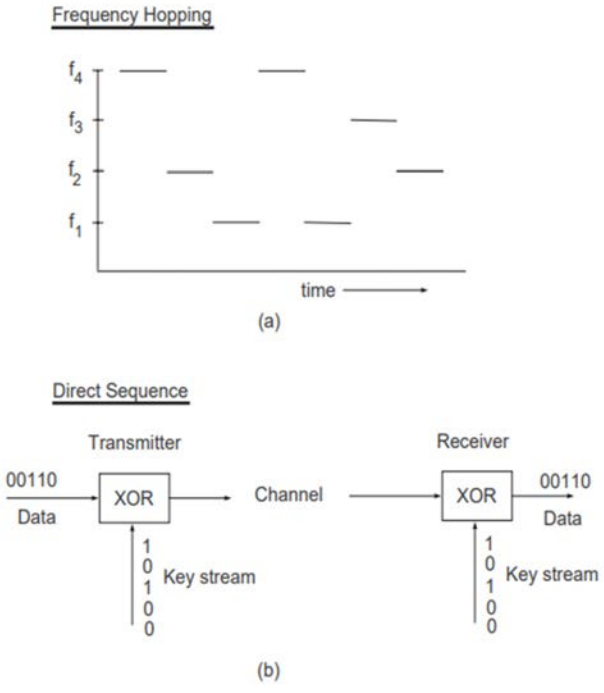


Figure 1.4: Direct sequence spread spectrum and frequency hopping spread spectrum, respectively.

An XOR gate at the receiver may be used to decode data. This works if the transmitter and receiver utilise the same (synchronised) key stream. Once again, if the key streams utilised for each broadcast are sufficiently diverse from one another, numerous transmissions may be multiplexed in a local area.

Comparing Circuit Switching with Packet Switching

Circuit switching and packet switching are the two main networking and telecommunications topologies. The earlier technique, circuit switching, dates to the decades after the late 1800s creation of the telephone. A physical route with the necessary resources, known as a circuit, is formed when a call has to be made from node A to node Z in a telephone network, as shown in Figure 1.5(a). Resources include connection bandwidth and switching resources. Before any communication can start, a circuit must be established. The circuit continues to work even if someone briefly stops speaking. Link and switching resources are made available for use by other callers when the call is over. A call is deemed blocked if insufficient resources are available to place it.

In the 1960s, packet switching was invented. A packet is a collection of bits that includes header and payload bits. The header includes all necessary information, including the source and destination addresses, priority levels, error check bits, and more. The actual information (data) to be transmitted is the payload. There is, however, a maximum packet size for many packet switching systems. Larger transmissions are thus divided into several packets and reconstructed at the receiver.

The illustration in Figure 1.5(b) depicts packets travelling through several pathways from node A to node Z, presumably from the same transmission. Datagram or connectionless focused service is what is meant by this. Given that nodal routing tables are routinely modified in the midst of, packets may in fact follow multiple paths while using this sort of service.

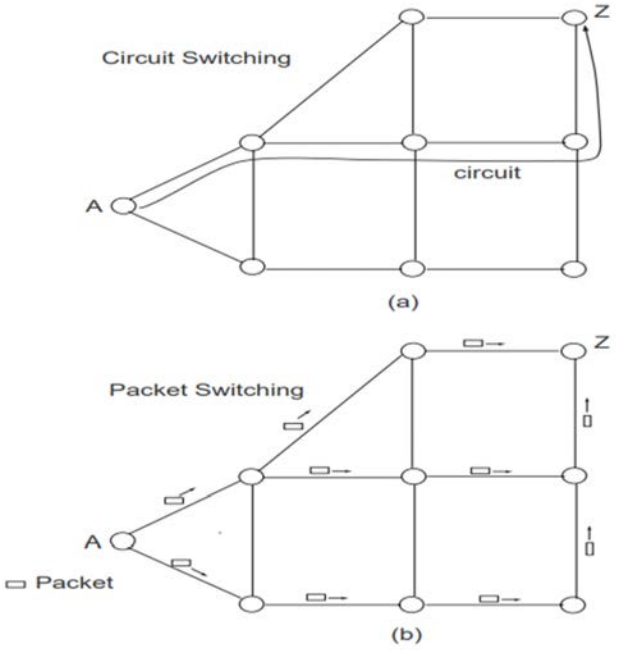


Figure 1.5: Circuit switching and packet switching are two examples of transmission.

The utilisation of virtual circuits or connection-oriented services is a hybrid service type. An identifying number for a virtual circuit is utilised at nodes to maintain the circuit's predetermined course. A virtual circuit has to be set up before it can be used for communication, much like with circuit switching. In other words, the routing tables that implement the virtual circuit must have entries created.

The fact that packets arrive at their destination in the same sequence they were transmitted is a benefit of using virtual circuits. By doing this, the requirement for reassembly buffers—which are required when packets arrive at the destination out of order, as in datagram service—is avoided. As we'll see, virtual circuits are employed by ATM, the high-speed packet switching technology used in Internet backbones. When communication is bursty (occurs at irregular intervals) and individual transmissions are brief, packet switching is desirable. When there are plenty of network transmissions, it is a highly effective technique to share them. Bursty and brief broadcasts are not well suited for circuit switching. It works well with reasonably lengthy transmissions that maintain a steady traffic flow and reduce setup time overhead.

CHAPTER 2

INCREASED USE OF COMPUTER NETWORKS

Krishnan Batri, Deputy Director,
Department of Computer Science and Engineering, School of Sciences, Jain (Deemed to be University) Bangalore, India
Email Id- krishnan.batri@jainuniversity.ac.in

The world of computer networking has developed rapidly. Computer communication has evolved from a specialised research area to a crucial component of the infrastructure since the 1970s. Every facet of company, including manufacturing, shipping, planning, invoicing, and accounting, uses networking. As a result, the majority of organisations have several networks. Computer networks are being used in schools at all grade levels, from elementary to post-graduate, to provide students and instructors immediate access to online resources. Military groups and federal, state, and municipal government agencies both utilise networks. Computer networks are, in short, present everywhere. One of the most fascinating and exciting developments in networking is the development and applications of the global Internet. The Internet was a research effort with a small number of sites in 1980. Now, the Internet has developed into a global production communication system that connects to all populous nations. Many people have access to high-speed Internet through wireless, DSL, or cable modems.

Networking's development and benefits have led to significant changes in the economy. Digital networking has transformed company communication and made telecommuting possible for people. Also, a whole sector of the economy that creates networking technologies, goods, and services has arisen. Due to the significance of computer networking, greater networking knowledge is in demand across all sectors. To design, get, install, run, and manage the hardware and software systems that make up computer networks and the internet, businesses require employees. Moreover, network programming is replacing the once-exclusive practise of individual computer programming.

Networking Feels Complicated

The topic looks complicated because computer networking is a vibrant, fascinating discipline. There are several technologies, and each one stands out from the others thanks to certain characteristics. Commercial networking goods and services are still being developed by businesses, often by using emerging technology in novel, unusual ways. Lastly, the fact that technologies may be merged and integrated in a variety of ways makes networking seem complicated. Since there isn't a single underlying theory that describes how all the components relate to one another, computer networking may be particularly perplexing to a novice. Networking standards have been developed by several organisations, however some of them are incompatible with one another. Because the set of technologies is diverse and changes quickly, many organisations and research groups have made an effort to define conceptual models that capture the essence and explain the subtleties among network hardware and software systems. However, these models are either too simplistic to distinguish between details or too complex to aid in the simplification of the topic.

Another difficulty for newcomers is the absence of a standard nomenclature for networking ideas due to the lack of uniformity in the area. Several organisations have all made an effort to develop their own terminology. Researchers insist on using exact scientific language. Corporate

marketing teams often equate a product with a general technical word or coin new terminologies in an effort to set their goods apart from those of rivals. As a result, technical jargon and names of well-known items are often confused. Professionals sometimes refer to an equivalent characteristic of one technology using a technical word from another, which only serves to increase misunderstanding. As a result, networking jargon also includes a vast number of phrases and acronyms that are often misused, shortened, or linked to specific products. To comprehend networking's complexity, it's crucial to get a wide background in the five main areas of the field:

Network Programming and Applications Technologies for Data Communications Packet Switching Further Networking Concepts and Technologies for TCP/IP Internetworking.

Network Programming and Applications

Application software is responsible for providing the network services and facilities that user's access. An application programme operating on one computer may connect with another application programme running on another machine through a network. Email, file transfer, online surfing, voice telephony, distributed databases, and audio and video teleconferencing are just a few of the many network application services available. All programmes may connect over a single, shared network, even if each application delivers a unique service and uses a different user interface. A programmer's job is significantly simplified by the availability of a unified underpinning network that supports all applications because there is only one interface to the network and one fundamental set of functions that must be learned because these functions are used by all application programmes that communicate over a network.

As we will see, it is not necessary to be familiar with the hardware and software technologies used to move data from one application to another in order to comprehend network applications or even to build code that talks over a network. It can seem that once a programmer learns the interface, more network expertise is not required. Network programming is comparable to traditional TV, however. While though a traditional programmer may write applications without having a thorough understanding of compilers, operating systems, or computer architecture, having this expertise can help a programmer produce more accurate, efficient, and dependable code. Similar to this, understanding the underlying network architecture enables programmers to produce better code.

Data Communications

The study of low-level techniques and technologies used to transmit data through a physical communication channel, such as a wire, radio wave, or laser beam, is known as data communications. Electrical engineering, which focuses on the design and construction of a variety of communication systems, is largely responsible for data transmission. The transport of information through physical events is the focus of data communications. Hence, a lot of the fundamental concepts come from the qualities of matter and energy that physicists have explored. For instance, we will see that the high-speed data transmission optical fibres depend on the characteristics of light and its reflection at a border between two kinds of matter.

Data communications may appear somewhat unrelated to our knowledge of networking since it deals with physical ideas. Particularly, the topic may appear relevant exclusively for engineers since many of the phrases and ideas pertain to physical events engineers who provide infrastructure for low-level transmission. For instance, it would seem that protocols cannot be designed or used with modulation techniques that transport information using physical forms of energy, such as electromagnetic radiation. Yet as we'll see, the design of many protocol layers is influenced by a number of fundamental ideas that come from data communications.

The idea of bandwidth in modulation has a direct connection to network throughput. Data communications, in particular, introduce the concept of multiplexing, which enables data from several sources to be joined for transmission via a common channel and then divided for delivery to various destinations. We'll see that multiplexing is not only for physical transmission the majority of protocols use multiplexing in some capacity. Similar to this, the majority of network security is built on the idea of encryption that was first used in data transmission.

Networking and packet switching technologies:

Data communications underwent a revolution in the 1960s thanks to a novel idea called packet switching. Early communication methods linked a physical pair of wires between two parties to create a communication circuit, such as telegraph and telephone systems. Electronic switches have taken the role of mechanical connections between wires, but the fundamental idea of creating a circuit and then sending information across it has not changed. By allowing several senders to transmit data across a common network rather than constructing a separate circuit, packet switching fundamentally altered networking and laid the groundwork for the current Internet. The basic data communications technologies that underlie both the phone system and packet switching are used in innovative ways. Data is divided into tiny blocks, or packets, through packet switching, and each packet contains a recipient identity. The network's devices are all equipped with knowledge on how to go to any potential location. When a packet reaches one of the devices, that device decides which route to send the packet down so that it finally gets to its intended location.

Theoretically, packet switching is simple. Nonetheless, depending on the answers to fundamental concerns, a wide range of designs are feasible. How should a destination be named, and where can a sender look up a destination's name? How big of a package should it be? How does a network distinguish between the conclusion of one packet and the start of another? How can a network of numerous computers coordinate to ensure that everyone has an equal chance to transmit while they are all sending data? How can wireless networks be modified to support packet switching? What design principles may be used to fulfil diverse demands for distance, speed, and cost effectively? There have been several solutions put forward and numerous packet switching systems developed. In fact, a key finding may be made while researching packet switching networks:

TCP/IP Internetworking: Another revolution in computer networking emerged in the 1970s with the invention of the Internet. While researching packet switching, several researchers searched for a single technique that could meet all requirements. Vinton Cerf and Robert Kahn noted that no one packet switching technology would ever meet all requirements in 1973, particularly given that low-capacity solutions for homes or workplaces might be created at very cheap costs. For such an interconnection, they suggested that a set of standards be created. These standards are known as the TCP/IP Internet Protocol Suite (sometimes shortened as TCP/IP). The idea behind inter-networking is quite potent. It serves as the foundation for the worldwide Internet and is crucial to the study of computer networking.

The acceptance of heterogeneity by TCP/IP standards is one of the main factors contributing to their success. TCP/IP adopts a virtualization approach, which defines a network-independent packet and a network-independent identification scheme, and then specifies how the virtual packets are mapped onto each potential underlying network. This approach avoids trying to impose details about packet switching technologies, such as packet sizes or the method used to identify a destination.

An interesting reason for the ongoing development of packet switching technologies is TCP/tolerance IP's of new packet switching networks. Computers becoming more powerful as the internet expands, and apps transfer more data overall, especially visual pictures and video. Engineers create innovative technologies that can send more data and analyse more packets in a given amount of time to handle increases in use. New technologies are added to the Internet alongside existing ones as they are developed. In other words, engineers may experiment with new networking technologies without damaging the current networks since the Internet tolerates heterogeneity.

Internet Areas that are Public and Private

The Internet is made up of elements that are owned and run by different people or organisations, despite the fact that it works as a single communication system. The networking industry uses the words public network and private network to assist define ownership and function.

Public Network

A public network is operated as a paid service for users. Anybody who pays the membership cost and wants to utilise the network may do so. A service provider is a business that provides communication services. A lot more than only Internet service providers are included in the definition of a service provider (ISPs). In actuality, organisations who provided analogue voice telephone service were the ones who first used the name. It is crucial to realise that the word "public" does not relate to the data communicated but rather to the wide availability of the service. Several public networks, in particular, adhere to stringent government laws that demand the service provider safeguard communications against unintentional spying.

Private Network

One single organisation has control over a private network. The boundary between the public and private portions of the Internet may be complicated even though it may appear obvious since control does not necessarily imply ownership. For instance, if a business rents a data circuit from a provider and limits its usage to business traffic, the circuit joins the business' private network. Vendors of networking hardware classify private networks into the following four groups:

Consumer

Home office or small office (SOHO) Small to medium-sized businesses (SMB) Large Business. The language is vague since the categories are related to sales and marketing. While each category may be qualitatively described, a precise definition cannot be found. So, rather of giving specific measurements, the paragraphs following provide a general description of size and function. One of the most affordable types of private network is a LAN that is controlled by an individual. If a person buys a cheap LAN switch and uses it to connect a printer to a PC, they have established a private network. Similarly, a wireless router represents a private network that a customer may pur- chase and install.

Home office or small office (SOHO)

A consumer network is marginally bigger than a SOHO network. Two or more computers, one or more printers, a router that connects to the Internet, and maybe other devices, such a cash register, are all connected by a standard SOHO network. A battery-backup power supply and other features that enable uninterrupted operation are often included in SOHO systems.

Small to medium-sized businesses (SMB)

An SMB network may link several computers in various offices around a building, as well as PCs in a manufacturing facility (e.g., in a shipping department). An SMB network often employs a broadband Internet connection, has numerous Layer-2 switches linked by routers, and might include wireless access points.

Large Corporation

The IT infrastructure required by a significant organisation is provided by a big enterprise network. In a typical big corporate network, there are two or more high-speed Internet connections, several Layer-2 switches and routers are used, and there are multiple buildings at each of the various geographic locations that make up the network's connections. Wired and wireless networking components are often used in enterprise networks.

Standards, Networks, and Interoperability

There are always at least two parties involved in communication—one gives information, the other receives it. In actuality, we will see that the majority of packet switching communication systems include intermediary entities (i.e., devices that forward packets). It is crucial to keep in mind that all network participants must agree on how information will be represented and delivered in order for communication to be effective. Communication agreements have various aspects. For instance, in order for two organisations to communicate via a wired network, both parties must agree on the voltages to be utilised, the precise method in which electrical signals are used to represent data, the processes for initiating and carrying out communication, and the message format.

The capacity of two entities to communicate is referred to as interoperability, and we state that two entities are said to interoperate successfully if they can do so without miscommunication. An precise set of requirements is spelled down in writing to ensure that all parties interacting can agree on specifics and adhere to the same set of guidelines. Following diplomatic etiquette, we refer to a specification for network communication as a protocol, network protocol, or specification. A specific protocol either explains a high-level method, such as the messages that two application programmes exchange, or it specifies low-level features, such as the kind of radio transmission utilised in a wireless network. We said that a protocol might specify the steps to be taken during an exchange. One of the most significant components of a protocol covers circumstances in which an error or unexpected event arises. As a result, a protocol often specifies the proper course of action for each potential aberrant circumstance (e.g., a response is expected, but no response arrives). To sum it up:

Protocol Suites and Layering Models

To guarantee that the final communication system is both comprehensive and effective, a set of protocols must be carefully built. Each protocol should, for instance, handle a portion of communication that is not handled by other protocols in order to minimise duplication of effort. How can the compatibility of protocols be ensured? The solution may be found in a comprehensive design strategy, where protocols are defined in whole, cohesive groups called suites or families rather than individually. The protocols in a suite work together to manage all elements of communication, including hardware failures and other extraordinary circumstances. Each protocol in a suite handles one component of communication. Moreover, the complete suite is built to make it possible for the protocols to cooperate effectively. layering model is the underlying abstraction that is utilised to group protocols into a single, cohesive entity, a model of the current condition of the current situation of the current state of the current

of anda para By enabling them to focus on one component of communication at a time, layering protocols enables both protocol designers and implementors to handle the complexity.

Figure 2.1 provides an illustration of the idea by displaying the layering model applied to Internet protocols. The word "stack" has become commonplace due to the visual look of representations used to depict stacking. Does that computer run the TCP/IP stack? is a common phrase used to refer to a machine's protocol software.

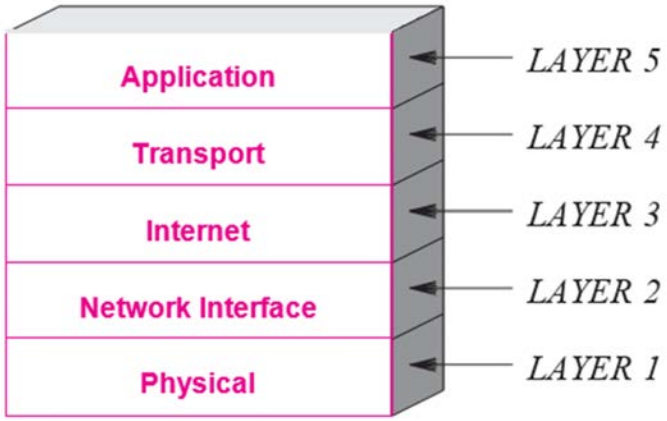


Figure 2.1: The layering paradigm for the TCP/IP Internet protocols.

Subsequent will define protocols in more depth to help us grasp layering. It is necessary for now to understand how protocols are used for communication as well as the functions of each layer. The following sections provide an overview of the function of the layers; a subsequent part looks at how data travels across the levels during computer communication.

Physical

The physical layer protocols provide information about the hardware and underlying transmission media. Layer 1 should include all parameters pertaining to electrical characteristics, radio frequencies, and transmissions.

Network Interface

The Network Interface layer protocols define the specifics of communication between the underlying network, which is implemented in hardware, and higher layers of protocols, which are often implemented in software. Protocols required to access the underlying media, hardware addressing, network address specifications, and the largest packet size a network may allow all belong under layer 2.

Internet

The Internet's core building blocks are protocols found at the Internet layer. Layer 3 protocols define Internet-based communication between two computers (i.e., across multiple interconnected networks). Layer 3 should include the Internet addressing scheme, Internet packet format, technique of breaking up big Internet packets into smaller packets for transmission, and systems for error reporting.

Transportation

Communication between an application programme on one machine and an application programme on another is made possible by protocols at the transport layer. Layer 4 is the proper

place for specifications that regulate the maximum pace at which a receiver may take data, prevent network congestion, and ensure that all data is received in the proper sequence.

Application Layer

The TCP/IP stack's top-level protocols define how two programmes should cooperate while communicating. Layer 5 protocols include specifics on the structure and content of messages that applications may exchange, as well as the steps that must be taken while communicating. Layer 5 should include the specifications for email exchange, file transfer, online surfing, phone services, and video teleconferencing.

Information Transfer via Layers

Layering is more than just a theoretical idea that clarifies procedures. Instead, protocol implementations adhere to the layering paradigm by sending the output from one layer's protocol to the input of the following layer's protocol. Also, two protocols in neighbouring layers send a pointer to the packet in order to maximise efficiency rather than copying the complete packet. Consequently, data travels between layers efficiently. Consider two computers that are linked to a network to comprehend how protocols function. Layered protocols on the two computers are shown in Figure 2.2. Each computer has a set of layered protocols, as shown in the image. Each layer of protocols is traversed by an outgoing packet that is created when an application delivers data. The packet leaves the computer and is transferred through the underlying physical network after completing all protocol levels on the sending machine. The packet ascends via the layers of protocols until it reaches the receiving machine. The procedure is reversed if the programme on the machine receiving the message sends a reply. In other words, a response travels up through the layers on the computer that sends it and down through the layers on the machine that receives it.

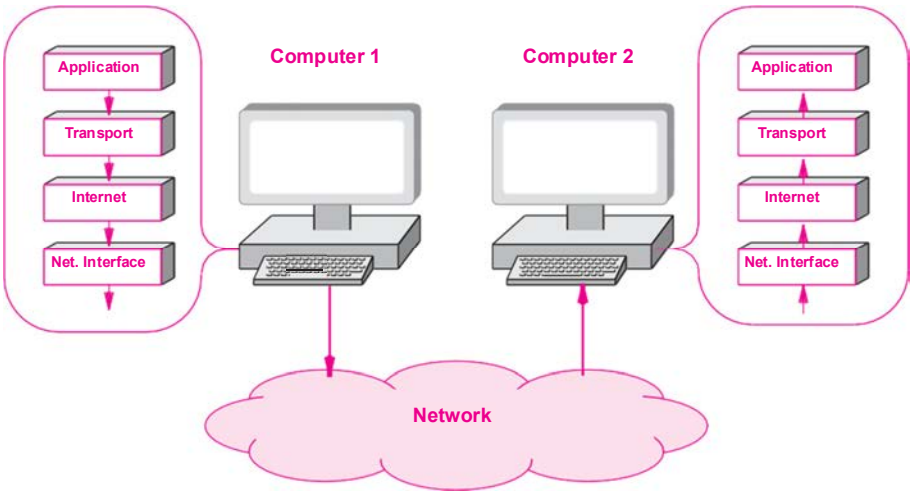


Figure 2.2 shows an illustration of the data flow across protocol levels during computer-to-computer communication via a network. Data travels via each layer of the tiered protocols that each computer possesses.

Headers and Layers

We shall discover that the calculations done by each layer of the protocol software ensure that the messages arrive as intended. The two computers' protocol software must communicate data in order to complete this calculation. Each layer on the transmitting computer prepends

additional data to the packet in order to do this; the matching protocol layer on the receiving computer removes the extra data and makes use of it.

A header is additional data that is added by a protocol. When the data moves through the layers on the transmitting computer, protocol software adds headers. In other words, the Transport layer prepends a header, followed by a header prepended by the Internet layer, and so on. Hence, if we watch a packet go via the network, the headers will show up in the sequence shown in Figure 2.3.

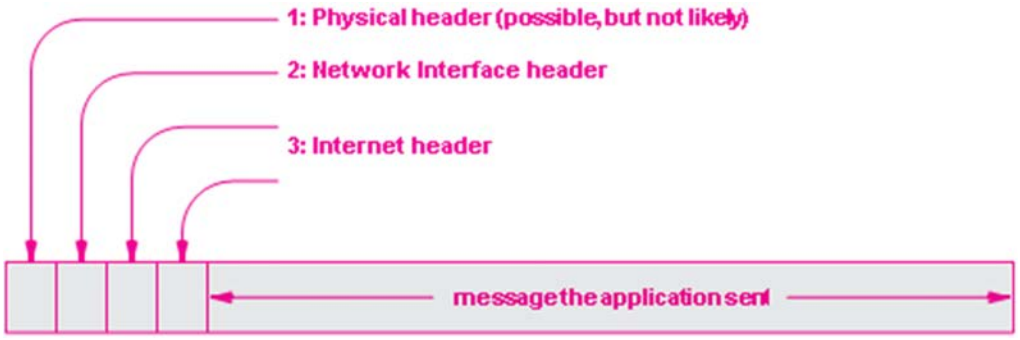


Figure 2.3 the layered protocol headers that show up on a packet when it moves between two machines via a network.

The initial bit transmitted over the underlying network is depicted on the left of the diagram as the commencement of the packet. The physical layer often describes how signals are utilized to transport data, as we will see in a later section. The presence of a Physical layer header is thus unexpected.

ISO and the OSI Seven Layer Reference Model

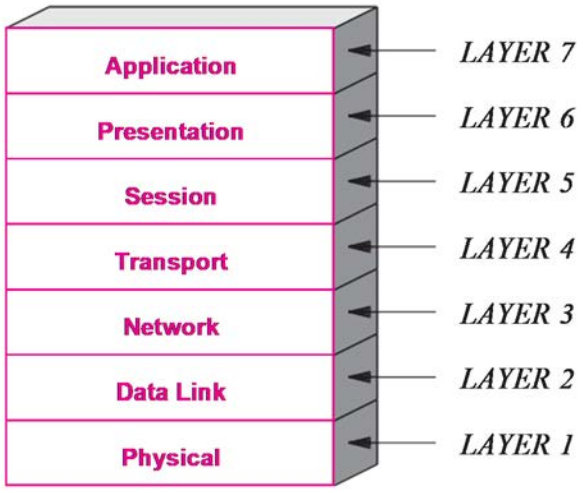


Figure 2.4 The OSI seven-layer model established by ISO.

At the same time the Internet protocols were being established, two significant standards groups together produced an alternative reference model. They also established a series of inter-networking protocols. The organizations are: International Organization for Standardization

(ISO), International Telecommunications Union, Telecommunication Standardization Sector (ITU-T).

The ISO layering model is known as the Open Systems Interconnection Seven-Layer Reference Model. The similarity between the acronyms for the organization and the proto-cols, OSI and ISO, causes ambiguity in terminology. Both the OSI seven-layer model and the ISO seven-layer model are likely to be mentioned. Figure 2.4 illustrates the seven layers in the model.

The Inside Scoop:

Like the majority of standards bodies, ISO and the ITU follow a procedure that takes into account as many points of view as is practical while developing a standard. As a consequence, rather than being the work of engineers and scientists, certain standards might give the impression that they were created by a committee that made political concessions. The seven-layer reference model is controversial. It did indeed start as a political compromise. Additionally, the model and the OSI protocols were developed as rivals for the Internet protocols. The Internet protocols and reference model were built by a small group of approximately a dozen researchers. It is understandable why the standards bodies would feel confidence in their ability to impose a set of rules, leading to a widespread abandonment of research-based procedures. At one point, even the U.S. government was convinced that TCP/IP should be replaced by OSI proto- cols.

Over time, it became evident that TCP/IP technology was more advanced than OSI, and within a few years, efforts to create and implement OSI protocols were abandoned. Standards bodies were left with the seven-layer model, which did not in- clude an Internet layer. Hence, for many years, proponents for the seven-layer paradigm have sought to expand the definitions to meet TCP/IP. They argue that layer three could be considered an Internet layer and that a few support protocols might be placed into layers five and six. The story's most amusing aspect may be how many engineers continue to refer to applications as layer 7 protocols despite knowing that layers five and six are empty and superfluous.

Users who have access to a computer are urged to create and utilise application programmes that use the Internet as they read the text. The functioning of the underlying technologies is covered in the following four sections. The second portion discusses data communications and the transmis- sion of information. It demonstrates how data is transported and discusses how electrical and electromagnetic energy may be utilised to send information through cables or across the air.

The third portion of the essay concentrates on packet switching and packet technology. It defines the overall structure of packets, looks at how they are encoded for transmission, and demonstrates how each packet is sent through a network to its destination. It also explains why computer networks employ packets. The third portion of book also discusses fundamental types of computer networks, such as Local Area Networks (LANs) and Wide Area Networks (WANs). It outlines the qualities of each category and covers example technology.

The fourth part of the text covers internetworking and the associated TCP/IP Inter- net Protocol Suite. The text explains the TCP/IP protocols and the structure of the Internet. It describes the mapping between Internet addresses and underlying hardware addresses as well as the IP addressing scheme. Additionally, routing protocols and Internet routing are covered. The description of several key ideas, such as encapsulation, fragmentation, congestion and flow control, virtual connections, address translation, bootstrapping, IPv6, and various support protocols, can be found in the fourth section.

The remaining subjects are covered in the text's fifth section, which addresses the network as a whole rather than its component pieces. Emerging technologies, network security.

CHAPTER 3

WEBSITE TRENDS

N Sengottaiyan, Deputy Director,
Department of Computer Science and Engineering, School of Sciences, Jain (Deemed to be University) Bangalore, India
Email Id- sengottaiyan.n@jainuniversity.ac.in

This analyses how data networking and the Internet have developed since its creation. A short history of the Internet is presented at the beginning and highlighting some of the first driving forces. It represents a change in focus from completely dispersed information systems to shared centralised facilities. This section of the book continues the debate by exploring certain Internet applications. The programming interface that Internet apps utilise to communicate in addition to outlining the various Internet communication paradigms. Since computers were still big and costly, resource sharing was the fundamental driving force behind the creation of early computer networks. For instance, networks were developed to link several people to a large centralised computer, each having a screen and keyboard. Later networks made it possible for numerous users to share peripherals like printers.

The U.S. Department of Defense's Advanced Research Projects Agency (ARPA) was particularly interested in resource sharing in the 1960s. Computers were very expensive and researchers required powerful computers. There weren't enough computers to be funded under the ARPA budget. As a result, ARPA started looking into data networking; rather than purchasing a computer for each project, ARPA intended to link all computers to a data network and develop software that would enable a researcher to choose whatever machine was most appropriate for a particular job. The brightest brains in networking research were assembled by ARPA, who then contracted contractors to implement the plans in the form of the AR-PANET. The study proved to be groundbreaking. The research team decided to use the packet switching method, which served as the foundation for data networks and the Internet. By providing financing for the Internet research project, ARPA sustained the effort. The Internet developed as a research project throughout the 1980s, and it achieved commercial success in the 1990s.

Internet Use Has Increased

The Internet has evolved from an early research prototype connecting a few sites to a worldwide communication system spanning every nation in the globe in less than 30 years. The growth rate has been astonishing. A graph showing the number of computers connected to the Internet as a function of the years from 1981 to 2008 is shown in Figure 3.1 to show the rise.

Sharing Resources and Communication

The Internet saw two key changes as it expanded. A backbone connection in the Internet may transport 100,000 times as many bits per second as a backbone link in the original Internet, which is the first sign of the huge improvement in communication speeds. Second, new uses emerged that were appealing to a wide swath of society. The second argument is also obvious: access to computing resources, scientific applications, and engineers and scientists no longer dominate the Internet. Resource sharing gave door to new applications as a result of two technical developments. On the one hand, faster connection rates allowed for the speedy transmission of enormous amounts of data by apps. The development of strong, reasonably priced personal computers, on the other hand, supplied the computing power required for

intricate calculations and graphical presentations, largely removing the need for shared resources.

Text to multimedia transition

The data that is transferred through the internet has undergone one of the most visible changes. The change is shown in one aspect in Figure 3.1.

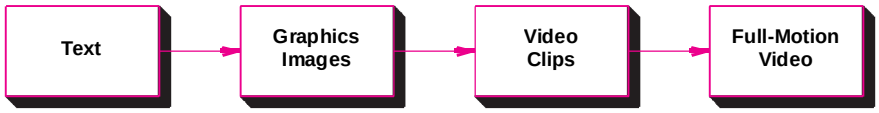


Figure 3.1: A change in the kind of data consumers transfer through the Internet.

The graphic shows that textual data was first used in Internet communication. In particular, email communications were confined to content shown in fixed-width font. By the In the 1990s, apps were developed that made it simple for users to share photographs, and computers had colour displays that could show graphics. Users started sending video snippets during the late 1990s, and full-motion videos were then practical. A similar change may be seen in the audio in Figure 3.2.

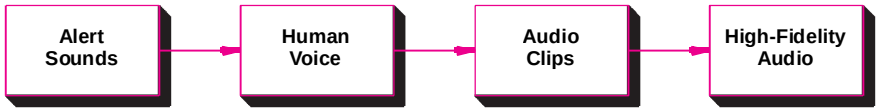


Figure 3.2: a change in the audio people are sending online.

For describing data that combines text, pictures, audio, and video, we use the phrase "multimedia". Nowadays, multimedia documents make up a large portion of the material that is accessible on the Internet.

Also, because greater bandwidths have made it feasible to transmit high-definition video and high-fidelity audio, quality has increased. Unexpectedly, new networking techniques and Internet applications keep appearing. The voice telephone network and cable television have seen some of the most important transformations as they switched from analogue to digital and embraced Internet technologies. Also, support for mobile users is growing quickly. Some of the modifications are shown in Table 3.1.

Table 3.1: Examples of changes in networking and the Internet

Topic	Transition
Telephone system	Switch from analog to Voice over IP (VoIP)
Cable television	Switch from analog delivery to Internet Protocol (IP)
Cellular	Switch from analog to digital cellular services (3G)
Internet access	Switch from wired to wireless access (Wi-Fi)
Data access	Switch from centralized to distributed services (P2P)

One of the most fascinating things about the Internet is how its applications evolve while the underlying technology fundamentally stays the same. Table 3.2 for instance, illustrates some emerging application kinds.

Table 3.2: Popular application examples.

Application	Significant For
High-quality teleconferencing	Business-to-business communication
Navigation systems	Military, shipping industry, consumers
Sensor networks	Environment, security, fleet tracking
Social networking	Consumers, volunteer organizations

Businesses benefit from the availability of high-quality teleconferencing systems like Cisco's TelePresence because they enable meetings to take place without incurring travel costs. Reducing travel expenditures significantly decreases costs in many firms. Applications for social networking, including Facebook, Second Life, and YouTube, are remarkable because they have forged new social ties between groups of individuals who only know one another online. According to sociologists, these apps will make it easier for individuals to form small social groups and connect with others who share their interests.

Users of the Internet have access to a wide range of services, such as video teleconferences, email, and online surfing. Unexpectedly, none of the services are a part of the fundamental communications infrastructure. Instead, all services are built on the general purpose communication infrastructure provided by the Internet, and individual services are provided by application software that runs on computers connected to the Internet. In fact, whole new services may be developed without altering the Internet. Two fundamental ideas that clarify Internet application. The begins by describing the conceptual framework that programmes use when they communicate with one another via the Internet. This also goes into depth on the socket Application Programming Interface (socket API), which is a standard tool for Internet applications.

By mastering a few fundamental ideas, a programmer may create apps that communicate over the Internet, proving that one need not be an expert in data transfer or network protocols to create creative applications. Examining advanced Internet applications like email in the continuation of the debate. Despite the fact that anybody can learn to programme and that it is feasible to construct Internet apps without having any prior knowledge of how networks function, understanding network protocols and technologies helps a programmer to produce dependable and efficient code that enables programmes that can run on several locations. Subsequent sections of the book detail data communications and the protocols that make up the Internet in order to supply the essential information.

Two Foundational Internet Communication Models

The stream paradigm and the message paradigm are the two fundamental communication paradigms that the Internet offers. The distinctions are summarised in Table 3.3.

Table 3.3: The two paradigms used by Internet applications

Stream Paradigm	Message Paradigm
Connection-oriented	Connectionless
1-to-1 communication	Many-to-many communication
Sequence of individual bytes	Sequence of individual messages

Arbitrary length transfer	Each message limited to 64 Kbytes
Used by most applications	Used for multimedia applications
Built on TCP protocol	Built on UDP protocol

Internet Stream Transport

The word "stream" refers to an application programming paradigm in which a series of bytes is sent from one programme to another. In actuality, the Internet's method sets up two streams—one going in each direction—between a pair of interacting programmes. In order to connect with a web server, for instance, a browser may utilise the stream service. The browser would issue a request, and the web server would answer by transmitting the page. Both applications may enter data, which the network then transmits to the other application. The stream technique moves a series of bytes without giving them any context or adding any boundaries. In particular, a transmitting programme has the option of generating either blocks of bytes or one byte at a time. The amount of bytes to deliver at any given moment is decided by the network. That is, the network may decide to split a big block into smaller blocks or merge smaller blocks into a single large block.

Internet Message Transport

A message paradigm is used by the alternative Internet communication method, in which the network receives and distributes messages. The network never sends partial messages or combines numerous messages; each message that is sent to a receiver matches to a message that was sent by a sender. Hence, if a sender inserts precisely n bytes in an outgoing message, the receiver will find exactly n bytes in the in- coming message. Delivery through broadcast, multicast, or unicast is possible with the message paradigm. That example, a message may be broadcast to all computers on a network or multicast to a subset of computers on a network. A message can also be transmitted directly from an application on one computer to an application on another. Moreover, a particular programme may receive notifications from applications running on several machines. As a result, the message paradigm might provide communication on a one-to-one, one-to-many, or many-to-one basis. However, the messaging service makes no promises about the sequence of messages transmitted or whether a certain message will arrive. The service per- mits messages to be:

1. Lost
2. Duplicated
3. Delivered inadvertently

While using the message paradigm, a programmer must ensure that the application continues to function properly even if packets are lost or rearranged. Programmers often employ the stream service since the majority of applications want delivery assurances, with the exception of specific cases like video when multicast is required and the application has support for handling packet loss and reordering. Hence, we'll concentrate on the stream paradigm.

Connection-oriented Communication

Since the Internet stream service is connection-oriented, it functions similarly to a phone conversation in that two apps must first seek a connection in order to interact. The connection enables the programmes to transfer data in either way after it has been established. The programmes ask for the connection to be stopped after they have finished communicating.

The Client-Server Interaction Model:

The client-server paradigm of interaction holds the key to the solution. One programme, referred to as a server, launches initially and waits for communication. The connection is started by a second programme, referred to as a client. The interaction is summarized in Table 3.4.

Table 3.4: Summary of the client-server paradigm

Server Application	Client Application
Starts first	Starts second
Does not need to know which client will contact it	Must know which server tocontact
Waits passively and arbitrarily long for contact from a client	nitiates a contact whenever communication is needed
Communicates with a client by bothsending and receiving data	Communicates with a server by sending and receiving data
Stays running after servicing oneclient, and waits for another	May terminate after interactingwith a server

The usage of the client-server paradigm by certain services is covered in the sections that follow. For now, it is sufficient to understand:

Client and Server Personalities

While small differences occur, most instances of client-server interaction share the same core features. Typically, client software is a generic application programme that, when remote access is required, temporarily transforms into a client while continuing to do other computations is directly called by a user and only runs for one session operates locally on a user's laptop actively starts a conversation with a server. Can access numerous services as required, but typically only makes one request at a time to a remote server not very demanding on computer hardware Server software, on the other hand: is a privileged, special-purpose application designed to manage several distant clients simultaneously with one service is automatically launched at system startup and continues to run across several sessions runs on a strong, big computer passively awaits communication from any distant clients accepts inquiries from anybody wants to contact them, but only provides one service needs strong hardware and an advanced operating system.

Server Software and Machines Fit For a Server

Sometimes, the phrase "server" causes confusion. Technically, the word does not relate to the computer on which the application is running, but rather to a software that waits passively for communication. Nonetheless, a computer itself may be referred to as a server when it is used only to execute one or more server programmes. Hardware suppliers add to the confusion by labelling PCs with strong operating systems, fast Processors, and enormous amounts of memory as servers. The definitions are shown in Figure 3.3.

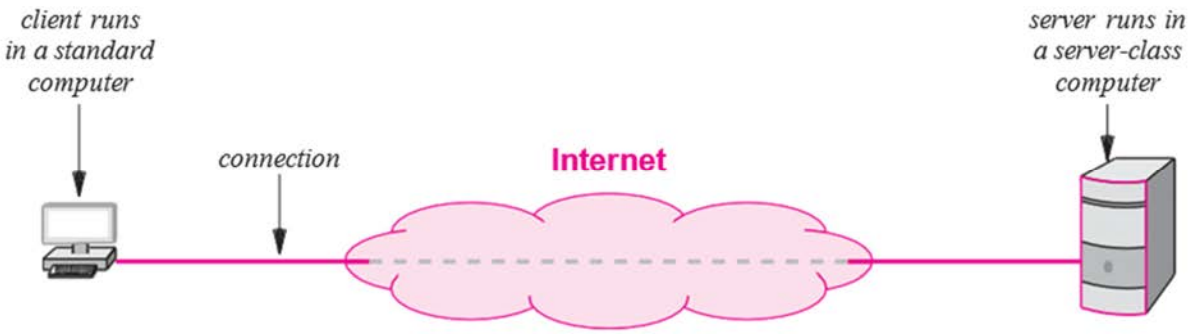


Figure 3.3: Illustration of a client and server

Requests, Reactions, and Data Flow Direction

Which side begins interaction gives birth to the phrases client and server. After making contact, two-way communication is feasible (i.e., data can flow from a client to a server or from a server to a client). In most cases, a client makes a request to a server, and the server responds with a response. Sometimes a client may submit several requests, and the server will respond with multiple replies (e.g., a database client might allow a user to look up more than one item at a time). The idea may be summed up as follows:

Using Many Clients and Servers

An application software is what makes up a client or server, and a computer may execute several apps at once. As a result, a computer may execute:

A solitary customer a solitary server

Several instances of a client making contact with the same server several clients that each make connect with a certain server several servers, each dedicated to a different service. Enabling a computer to handle numerous clients is advantageous since services may be accessed concurrently. An individual may, for instance, have three windows open at once, each running a different application: one for retrieving and displaying email, another for connecting to a chat service, and a third for a web browser. Each programme acts as a client that independently of the others, contacts one server. In actuality, the technology enables a user to run two instances of the same programme simultaneously, each of which contacts a server (e.g., two copies of a web browser).

Enabling a particular computer to run several servers is advantageous since the hardware may be shared. Also, compared to several computer systems, a single computer has less administrative overhead. Even more significant, experience has shown us that demand for servers is often erratic, and they might sit inactive for extended periods of time. While awaiting a request, an idle server does not utilise its CPU. As a result, if there is little demand for services, combining servers into a single computer may dramatically save costs without impairing performance.

Server recognition and demultiplexing

What distinguishes a client from a server? Identification is divided into two parts by the Internet protocols: a way to identify the machine that a server is running on an identification number for a certain computer service

Identifying a Computer. Each machine on the Internet is allocated a unique 32-bit identifier known as an Internet Protocol address (IP address). A client must provide the server's IP address when contacting it. Each computer is given a name in order to make server identification simple for users, and the Domain Name System is used to convert names into addresses.

Choosing A Service: The protocol port number, a 16-bit identification that is exclusive to each service offered over the Internet, is issued to each service (often abbreviated port number). For instance, port 25 is allocated to email, whereas port 80 is assigned to the web. A server registers with its local system when it starts up by stating the port number for the service it provides. A port number is included in the request when a client makes contact with a distant server to request services. It's a good idea to have a backup plan in case anything goes wrong. By outlining the fundamental steps a client and server take to interact, Figure 3.4 summarises the subject.

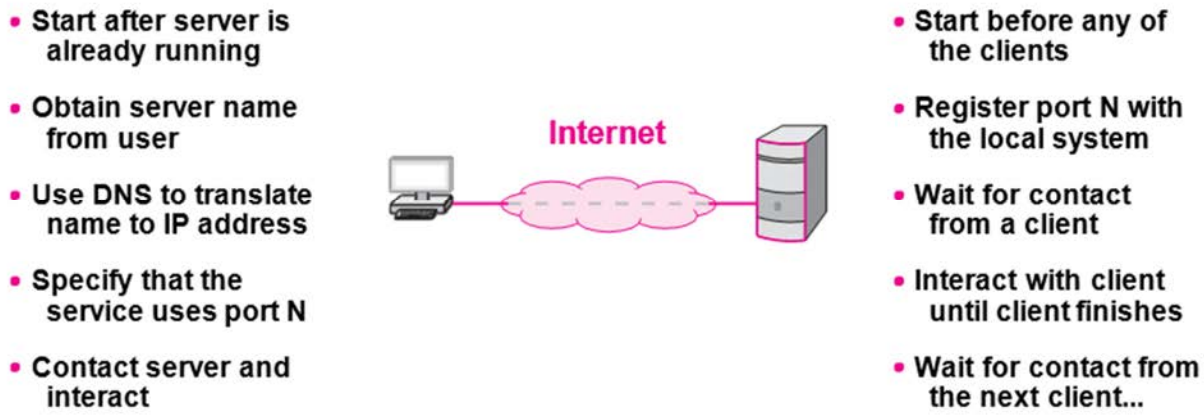


Figure 3.4: The conceptual steps a client and server take to interact

Concurrent Servers

According to the methods in Figure 3.4, a server only deals with one client at once. While a serial technique may be used in a few simple situations, concurrent servers are more common. In other words, a server manages several clients at once by using multiple threads of control. Think about what occurs when a client downloads a video from a server to comprehend the significance of simultaneous service. All clients are forced to wait while the server sends the video if a server only processes one request at a time. A concurrent server, on the other hand, does not make a client wait. As a result, if a second client comes online and makes a quick download request (such as for a single song), the second request will begin right away and can end before the movie transfer is finished.

Concurrent server code is split into two parts: a main programme (thread) and a handler. The specifics of concurrent execution depend on the operating system being utilised. The primary thread does little more than acknowledge a client's interaction and establish a control thread for the client. Each control thread communicates with a single client and executes the handler code. The thread ends after it has finished serving one client. After starting a thread to process a request, the main thread waits for another request to come in order to maintain server life.

It should be noted that if N clients are using a concurrent server at the same time, N+1 threads will be active: the main thread is waiting for new requests, and N threads are each communicating with one client.

Circular Server Dependencies

Technically, a client is any programme that initiates interaction with another, while a server is any programme that receives contact from another. When a server for one service might also function as a client for another, the lines between the two become fuzzier in reality. For instance, a web server might need to sign up as a database client before it can fill out a web page. A server might use a security service as a client as well (e.g., to verify that a client is allowed to access the service). Naturally, programmers must take care to prevent server circular dependencies. Think about what may occur, for instance, if a server for service X1 becomes a client of service X2, which then becomes a client of service X3, which then becomes a client of X1. There is no limit to how many requests may be made before all three servers run out of resources. As no one programmer has complete control over all servers, the possibility for circularity is particularly great when services are implemented in a dependent manner.

Interactions between Peers

When a service is offered by a single server, the network connection to the Internet may get congested. The architecture is shown in Figure 3.5.

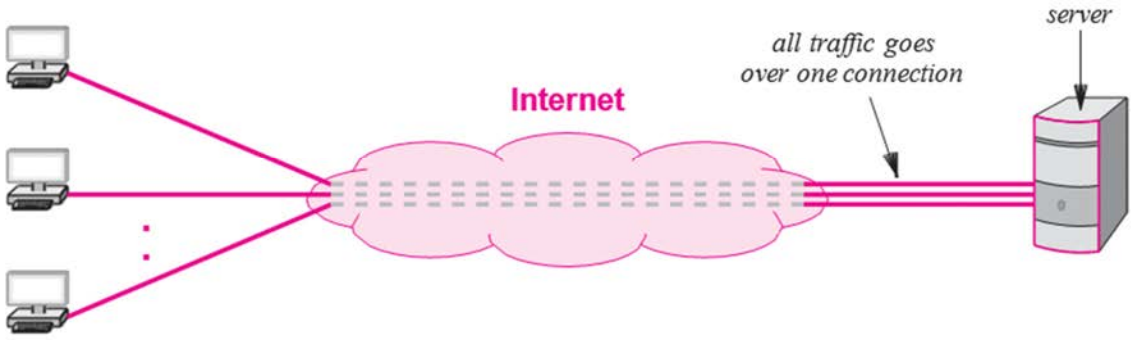


Figure 3.5 shows the single server design's traffic constraint.

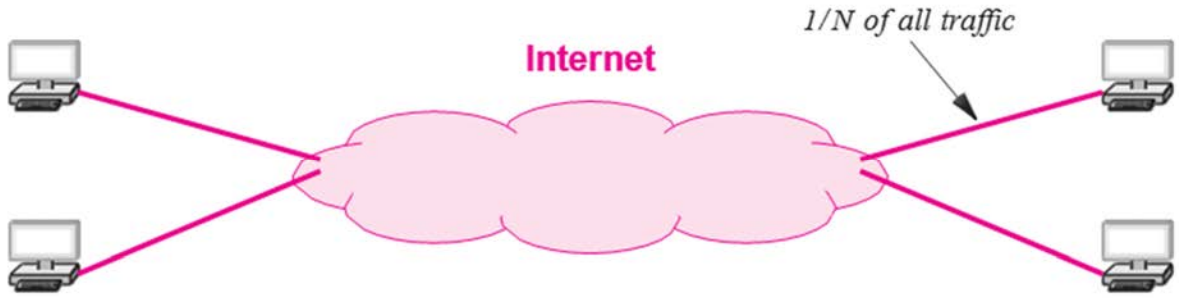


Figure 3.6 Interaction in a peer-to-peer system.

Can Internet services be delivered without resulting in a central bottleneck? File sharing programmes are based on a method to prevent bottlenecks. The system, sometimes referred to as a peer-to-peer (p2p) architecture, avoids storing data on a centralised server. Each client

request is transmitted to the proper server, and conceptually, data is spread evenly across a group of N servers. The quantity of traffic between a server and the Internet is 1/ N times as much as in the single-server design since a particular server only supplies 1/ N of the data. As a result, server software may be executed on computers that also act as clients. Figure 3.6 depicts the structure.

CHAPTER 4

INTERNET APPLICATIONS AND NETWORK PROGRAMMING

Merin Thomas, Associate Professor,
Department of Computer Science and Engineering, Jain (Deemed to be University)
Bangalore, India
Email Id- merin.thomas@jainuniversity.ac.in

An application programme interface (API) is the name for the interface that an application uses to describe communication. One particular API has become the de facto standard for software that interacts via the Internet, even if the specifics of an API vary depending on the operating system. The socket API, sometimes known as sockets, is accessible on a variety of operating systems, including Linux and several UNIX systems as well as Microsoft's Windows systems.

Network I/O, Descriptors, And Sockets

The socket API is intertwined with I/O due to its history as a UNIX operating system component. In particular, the operating system provides a brief integer descriptor that identifies the socket when an application establishes one for Internet communication. The programme then uses functions to carry out an action on the socket and sends the descriptor as an argument (e.g., to transfer data across the network or to receive incoming data). Socket descriptors are often used with other I/O descriptors in operating systems. As a consequence, a programme may utilise file or socket I/O for read and write activities. To sum it up:

The Socket API and Parameters

In contrast to traditional I/O, socket programming requires that an application declare a number of specifics, including the address of a distant computer, the protocol port number, and whether the application will function as a client or a server (i.e., whether to initiate a connection). The socket API's creators decided to create multiple functions rather than one socket function with many arguments. In essence, a socket is created by an application, which then calls functions to provide specifics. The benefit of the socket technique is that most functions only have three arguments or less; the drawback is that while utilising sockets, a programmer must remember to call many functions. The socket API's main functionalities are outlined in Table 4.1.

Table 4.1: presents an overview of the socket API's key features.

Name	Used By	Meaning
accept	server	Accept an incoming connection
bind	server	Specify IP address and protocol port
close	either	Terminate communication
connect	client	Connect to a remote application
getpeername	server	Obtain client’s IP address
getsockopt	server	Obtain current options for a socket
listen	server	Prepare socket for use by a server
recv	either	Receive incoming data or message

recvmsg	either	Receive data (message paradigm)
recvfrom	either	Receive a message and sender's addr.
send (write)	either	Send outgoing data or message
sendmsg	either	Send an outgoing message
sendto	either	Send a message (variant of sendmsg)
setsockopt	either	Change socket options
shutdown	either	Terminate a connection
socket	either	Create a socket for use by above

Socket Calls in a Client and Server

The series of socket calls performed by a typical client and server while using a stream connection are shown in Figure 4.1. In the illustration, the client transmits data first while the server waits to receive data. Some programmes, in reality, arrange for the server to transmit first (i.e., send and recv are called in the reverse order).

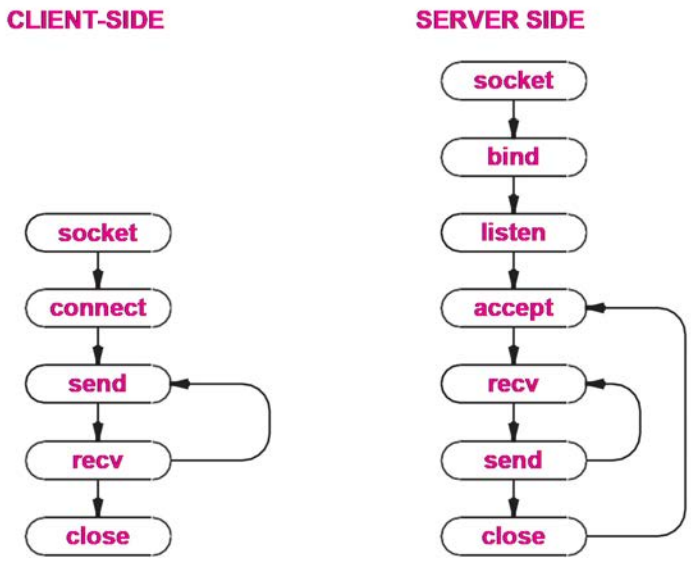


Figure 4.1: Using the stream paradigm, a client and server invoke a series of socket methods.

Client and Server Usage of Socket Functions

The Socket Function

A socket is created via the socket function, which also returns an integer descriptor:

descriptor = socket(protofamily, type, protocol)

The protocol family to be used with the socket is specified by the argument protofamily. The TCP/IP protocol suite used on the Internet is identified by the identifier PF INET. The argument type indicates the kind of communication that will take place through the socket: SOCK

STREAM provides stream transfer, while SOCK DGRAM specifies connectionless message transmission.

A specific transport protocol that is utilised with the socket is specified by the argument protocol. A single protocol suite may have two or more protocols that provide the same service when there is a protocol argument in addition to a type argument. Depending on the protocol family, several values may be used with the protocol argument.

The Send Function

The send function is used to communicate data between clients and servers. A client typically submits a request, and a server typically responds. Sent has four justifications:

send(socket, data, length, flags)

Argument data is the location in memory of the data to transmit, Argument length is an integer that indicates the amount of bytes of data, and Argument flags includes bits that request extra settings. Argument socket is the descriptor of a socket to use.

The Recv Function

Recv is used by both a client and a server to retrieve data that has been sent by the other the form of the function is:

recv(socket, buffer, length, flags) (socket, buffer, length, flags)

The descriptor for a socket from which data is to be received is argument socket. Argument length and argument buffer both provide the size of the buffer as well as the location in memory where the receiving message should be stored. Last but not least, an argument allows the caller to customise the details (e.g., to allow an application to extract a copy of an in- coming message without removing the message from the socket). Recv waits for data to arrive, then inserts as many bytes as necessary into the buffer (the return value from the function call specifies the number of bytes that were extracted).

Use Sockets to Read and Write

The operating system functions read and write may be used in place of the recv and send commands on certain operating systems, such as Linux. Both read and write need three arguments, with read taking the same three arguments as recv's first three arguments and write taking the same three arguments as send's first three arguments. It is possible to design an application programme that transmits data to or from a descriptor without knowing whether the descriptor corresponds to a file or a socket thanks to the read and write commands' universality. Hence, before trying to connect via a network, a programmer may test a client or server using a file on a local drive. The main drawback of read and write is that a programme may need to be modified in order to run on another system.

The Close Option:

The close command instructs the operating system to stop using a socket. It takes the shape of

close(socket)

where socket is a term used to describe a socket that is closed. Close ends a connection if it is already active (i.e., informs the other side). The descriptor is released when a socket is closed, halting usage instantly and prevents the programme from sending or receiving data again.

A Client-Only Function Used For Connections

To connect to a particular server, clients use the connect command. The format is:

connect(socket, saddress, saddresslen)

The descriptor of a socket to be used for the connection is argument socket. Parameter saddress defines the server's address and protocol port number via a sockaddr structure, and argument saddresslen specifies the server address length in bytes. Connect starts a transport-level connection to the chosen server for a socket that employs the stream paradigm. It must be that the server is awaiting a connection (see the accept function described below).

Socket Functions That a Server Uses Only

The Bind Function:

A socket is generated without knowledge of the local or distant address or protocol port number. In order to provide a protocol port number at which to listen for incoming connections, a server makes a call to bind. Bind accepts three inputs:

bind(socket, localaddr, addrlen)

The description of a socket to utilise is argument socket. Parameter addrlen is an integer that indicates the length of the address, and argument localaddr is a structure that provides the local address to be allocated to the socket.

The format of an address depends on the protocol being used since a socket may be used with any protocol. Each protocol family must then explain how their protocol addresses utilise the generic form, which is defined by the socket API as a general form for representing addresses. The sockaddr structure is the standard manner for displaying an address. Despite several releases, most systems describe a sockaddr structure as having three fields:

```
struct sockaddr {
      u_char  sa_len;        /* total length of the address */
      u_char  sa_family;     /* family of the address       */
       char   sa_data[14];   /* the address itself          */
};
```

The length of the address is specified by the single byte that makes up the field sa len. The family to which an address belongs is specified by the field sa family (Internet addresses utilise the symbolic constant AF INET). The address is lastly included in field sa data. The precise format of addresses used with the sa data field of a sockaddr structure is specified by each protocol family. As an example, Internet protocols employ the sockaddr in structure to specify an address:

```
struct sockaddr_in {
       u_char  sin_len;   /* total length of the address */u_char
       sin_family;  /* family of the address   */ u_short sin_port;
       /* protocol port number     */struct  in_addr sin_addr;/* IP
       address of computer   */char  sin_zero[8]; /* not used (set
       to zero)  */
};
```

Structure sockaddr in's first two fields match the first two fields of the generic sockaddr structure perfectly. The last three fields provide an Internet address's precise format. There are

two things to keep in mind. Each address first identifies a computer as well as a protocol port on that machine. The computer's IP address is shown in the field's sin addr and sin port, respectively, along with the protocol port number. Second, the generic sockaddr structure reserves fourteen bytes even though a full address only requires six bytes to be stored. In order to pad the structure to the same size as sockaddr, the last field in the sockaddr in structure specifies an 8-byte field of zeros.

As previously stated, a server will use bind to indicate the protocol port number at which it will accept incoming connections. Structure sockaddr in, however, also has a field for an address in addition to a field for the protocol port number. While a server has the option to fill in a particular address, doing so presents issues when a computer is multihomed, meaning it has numerous network connections. This is because the machine has many addresses. The socket API offers a unique symbolic constant, INADDR ANY that enables a server to specify a port number while permitting interaction at any of the computer's addresses. This lets a server to run on a multi-homed host.

The Listen Function

After defining a protocol port using bind, a server uses listen to put the socket in passive mode and ready to receive connections from clients. Listen to these two defences:

listen(socket, queuesize) (socket, queuesize)

Parameter queuesize determines the length of the socket's request queue, whereas argument socket is a descriptor for a socket. For every socket, an operating system creates a unique request queue. The line is empty at first. Each client request that comes in is added to the queue. The system pulls the following request from the queue when the server requests to retrieve an incoming request from the socket. Queue length is crucial because the system rejects requests that come when the queue is full.

The Accept Function

To connect with a client, a server invokes accept. If there is a request in the queue, accept it and it will return right away; if none have come, the server will be blocked until a client makes a request. The server communicates with a client via the connection once it has been accepted. The server cuts off the connection when it has finished communicating.

The form of the accept function is:

Accept newsock (socket, caddress, caddresslen)

The descriptor for a socket that the server has generated and assigned to a particular protocol port is called an argument socket. The arguments caddress and caddresslen each represent an address of a structure of the type sockaddr. Accept sets caddresslen to the length of the argument and fills in the argument fields with the client's address that established the connection. Lastly, accept establishes a new socket for the connection, and provides the descriptor of the new socket to the caller. After communicating with the client via the new connection, the server shuts the socket. The server's original socket is unaffected by this, and after it has finished communicating with one client, it utilises the original socket to accept connections from other clients. Hence, communication solely takes place through the new socket established by accept, with the previous socket merely being utilised to receive requests.

The Message Paradigm and Socket Functions

Since there are more parameters available, the socket functions used to transmit and receive messages are more complex than those used with the stream paradigm. For instance, a sender may decide whether to supply the recipient's address each time a message is delivered or to mention the recipient's address once and send data instead. A sender may also supply the address and message as distinct arguments in one function while putting the address and message in a structure and passing the structure's address as an argument in another.

Sendto and Sendmsg Socket Functions

Functions Using an unattached socket is possible via sendto and sendmsg, which both require the caller to select a destination.

sendto(socket, data, length, flags, destaddress, addresslen)

The last two define the destination address and its length, whereas the first four parameters match the send function's first four arguments. A sockaddr structure, especially sockaddr in, corresponds to the argument dest- address. Similar to the sendto function, the sendmsg function condenses the parameters by establishing a structure. Programs that utilise sendmsg may be simpler to comprehend thanks to the condensed parameter list:

sendmsg(socket, msgstruct, flags) (socket, msgstruct, flags)

Argument msgstruct is a structure that includes details about the recipient address, the length of the address, the message that will be delivered, and the message's length:

```
struct  msgstruct {               /* structure used by sendmsg */
        struct sockaddr *m_saddr;  /* ptr to destination address */
        struct datavec  *m_dvec;  /* ptr to message (vector)   */int
        m_dvlength;    /* num. of items in vector    */struct access
        *m_rights; /* ptr to access rights list  */int m_alength; /*
        num. of items in list  */
};
```

The specifics of the message structure are irrelevant; rather, it should be seen as a means of incorporating several arguments into a unified framework. Just the first three elements, which identify a destination protocol address, a list of the data items that make up the message, and the number of items in the list, are often used by applications.

Functions for Recvfrom and Recvmsg

An arbitrary number of clients may send messages to a disconnected socket. When this occurs, the system sends the sender's address back with each incoming message (the receiver uses the address to send a reply). The inputs to the function recvfrom define a location for the following incoming message and the sender's address:

recvfrom(socket, buffer, length, flags, sndraddr, saddrlen)

The first four parameters match those of recv, whereas the last two arguments, sndraddr and saddrlen, are used to save the sender's Internet address. Arguments sndraddr and saddrlen are pointers to sockaddr structures and integers, respectively that the system uses to store the sender's address and address length information, respectively. It should be noted that recvfrom saves the sender's address in precisely the format that sendto anticipates, making it simple to send a reply.

The function recvmsg, which is sendmsg's opposite, functions similarly to recvfrom but needs less parameters. It has the structure:

recvmsg(socket, msgstruct, flags)

Argument where msgstruct provides the location of a structure that stores the address for an incoming message as well as the Internet address of the sender. Recvmsg records messages in a format that is identical to the structure used by sendmsg, making it simple to respond.

Extra Socket Features

Many support methods are included in the socket API. To find out the address of the distant client that requested the connection, for instance, a server may use the getpeername function after accepting an inbound connection request. Gethostname is a command that a client or server may use to learn more about the machine that it is currently executing on. To control socket settings, two all-purpose routines are utilised. Functions getsockopt retrieves the current option values, whereas functions setsockopt puts values in a socket's options. Options are mostly used to manage unique scenarios (e.g., to increase the internal buffer size). Internet addresses and machine names may be converted using two functions. The gethostbyname function retrieves an Internet address for a computer given the name of the machine. To convert a user-entered name into a matching IP address, clients often execute gethostbyname. Given an IP address for a computer, the function gethostbyaddr offers an inverse map-ping and returns the name of the machine. In order to convert an address into a name that a user can comprehend, clients and servers may use gethostbyaddr. With several active servers, the socket API performs effectively. While specifics vary depending on the underlying operating system, the socket API implementations follow the following inheritance principle:

Each socket is managed by the socket implementation using a reference count method. The system initially sets the reference count of a socket to 1, and the socket survives as long as the reference count is positive. Each open socket that a programme owns receives a pointer when a new thread is created, and the system increases each socket's reference count by 1 as well. When a thread calls close, the system decreases the socket's reference count; if it reaches zero, the socket is deleted.

In regard to a concurrent server, the main thread is the owner of the socket that receives incoming connections. The main thread generates a new thread to handle the connection when a connection request comes in, and the system opens a new socket for the new connection. Both the initial socket and the newly generated socket are immediately accessible by a thread, and each socket has a reference count of two. The reference count of each socket is decreased to 1 when the service thread and main thread both call close on the new and original sockets, respectively. Finally, the service thread calls close on the new socket after it has finished communicating with a client, bringing the reference count to zero and resulting in the socket's deletion. Hence, a concurrent server's socket lifespan may be summed up.

CHAPTER 5

INTERNET APPLICATIONS TRADITIONALLY

Sindhu Madhuri G, Assistant Professor,
Department of Computer Science and Engineering, Jain (Deemed to be University)
Bangalore, India
Email Id- g.sindhumadhuri@jainuniversity.ac.in

Internet applications and network programming are subjects that are introduced in the preceding. This describes the client-server approach that application programmes use to communicate and discusses how Internet services are defined by application programmes. The study of Internet applications is continued. This defines the term "transfer protocol" and describes how transfer protocols are implemented by applications then discusses common Internet apps and explains the transmission protocol that each one employs.

Application-Layer Protocols

Every time a programmer constructs two apps that interact with one another across a network, they provide information like: the language that messages may be exchanged in both syntax and semantics for further information, see the website. Steps to take if a mistake is made. How the parties decide when to cut off contact. A programmer constructs an application-layer protocol to describe the specifics of communication. Application-layer protocols may be divided into two categories based on their intended uses:

Confidential conversation

A pair of Internet-based applications is created by a programmer with the goal that they only be used privately. Most of the time, there are no complicated interactions between the two programmes, therefore a programmer may decide to develop code without creating a formal protocol specification.

Uniformed service

The definition of an Internet service assumes that several programmers will develop client or server software to provide the service. In these situations, the application-layer protocol must be specified in detail and without ambiguity in order for all clients and servers to communicate with one other effectively.

The length of a protocol specification is determined by the service's complexity; one page of text may include the specification for a simple service. A defined application service called DAYTIME, for instance, is part of the Internet protocols and enables a client to discover the time and date where the server is located. The protocol is straightforward: a client opens a connection to a server, the server delivers an ASCII representation of the date and time, and the server closes the connection.

Transfer and Representation

Two components of interaction are specified by application-layer protocols: representation and transfer. The difference is explained.

Data Representation: Translation of numbers, characters, and files across computers; particular format used during transmission; data representation syntax of transferred data objects;

Data Exchange: Termination of contact, management of valid and incorrect exchange errors, message syntax and semantics, and client-server interaction.

A single protocol standard may define both parts of a simple service; more complex services need different protocol standards to define each component. For instance, the DAYTIME protocol, which was previously explained, employs a single standard to mandate that a date and time be represented as an ASCII string. During the transmission, a server sends the string before cutting off communication. The web employs several protocols to express web page syntax and web page transport, as explained in the following section. The difference is made explicit by protocol designers:

Web Protocols

One of the most popular Internet services is the World Wide Web. Due to the complexity of the Web, several protocol standards have been developed to explain its various facets and specifics. The three main standards are listed below.

Markup Language for Hypertext (HTML): a representational standard that outlines the structure and content of a web page

Locator for Uniform Resources (URL): A representation standard that governs the format and meaning of web page IDs

Protocol for Hypertext Transfer (HTTP): A transfer protocol that outlines the communication between a web server and a browser while transferring data

HTML Document Representation

The syntax for a web page is specified by the HyperText Markup Language (HTML) representation standard. The following qualities of HTML are typical:

1. Use language as a representation
2. Describes multimedia-containing pages

Uses a declarative paradigm rather than a procedural one the specification of markup rather than formatting Allows a hyperlink to be placed in an arbitrary object allows the addition of metadata to documents. While an HTML document consists of a text file, the language enables a pro- grammer to define an arbitrarily sophisticated web page that comprises pictures, audio and video, as well as text. In reality, because HTML permits any item, such as an image, to include a link to another web page, the designers need to have used hyper- media in the name instead of hypertext to be correct (sometimes called a hyperlink).

HTML is categorised as declarative since it simply allows for the specification of what has to be done, not how. HTML is categorised as a markup language as it does not provide specific formatting instructions but simply broad recommendations for presentation. HTML, for instance, does not mandate that the author describe the precise font, typeface, point size, or spacing for the heading, but it does let a page to express the priority level of a heading. In essence, a browser selects every aspect of presentation. Since it enables a browser to adjust the page to the underlying display technology, the usage of a markup language is crucial. A page, for instance, might be designed for a big screen, a tiny hand-held device like an iPhone or PDA, a high quality or low resolution display, or all three.

HTML employs tags that are embedded in the document to define markup. Tags, which are composed of a phrase surrounded by the less-than and greater-than symbols, provide the document structure and formatting cues. White space, which includes extra lines and blank characters, may be added anywhere in an HTML page without affecting how it is structured and shown by a browser. Tags govern all display. An HTML page, for instance, begins with the tag "HTML" and concludes with the tag "/HTML". The tags "HEAD" and "/HEAD" surround the head, and the tags. The body is enclosed by the tags BODY and /BODY. The content that makes up the document title is surrounded by the tags TITLE> and /TI- TLE> in the head.

```
<HTML>
  <HEAD>
     <TITLE>
           text that forms the document title
     </TITLE>
  </HEAD>
  <BODY>
    body of the document appears here
  </BODY>
</HTML>
```

The IMG element in HTML is used to encode a reference to an outside image. For instance, the IMG SRC="house icon.gif"> tag. says that the browser should put an image from the house icon.gif file into the page. The alignment of the figure with the surrounding text may be specified using additional parameters in an IMG tag. Figure 5.1, for instance, displays the results of the HTML that aligns the text with the figure's centre.

A home is shown in this symbol. IMG ALT="middle" SRC="house icon.gif">

The text is centred on the picture, and the image is vertically positioned by the browser.

A home is shown in this symbol.

Figure 5.1: Shows how to align a figure in HTML.

Standardized Resource Locators and Links

The Web utilises a syntactic form known as a Universal Resource Locator (URL) to define a web page. A URL's standard form is:

protocol: document name%parameters, computer name:port

Where protocol denotes the name of the protocol used to access the document, computer name denotes the computer's domain name, port denotes an optional protocol port number at which the server is listening, document name denotes the optional name of the document on the specified computer, and %parameters denote optional parameters for the page. Several of the components are missing from typical URLs that users input. For instance, the URL

www.netbook.cs.purdue.edu omits the parameters, document name, protocol (http is assumed), port (80 is assumed), and protocol (index.html) (none are assumed).

The data a browser needs to get a page is included in a URL. The URL is split into four parts by the browser using the separator letters colon, slash, and percent: a protocol, a machine name, a document name, and parameters. The browser uses the computer name and protocol port to make a connection to the server on which the page lives, then uses the document name and parameters to request a particular page. In HTML, an anchor element utilises URLs to offer a linking capability (i.e., the ability to link from one web document to another). The word Prentice Hall is surrounded by an anchor in the HTML source code in the example below:

```
This book is published by
<A HREF="http://www.prenhall.com">
Prentice Hall, </A> one of
the larger publishers of Computer Science textbooks.
```

The anchor makes a mention to the website prenhall.com. The output of the HTML input when shown on a screen is:

HTTP Web Document Transfer

The most common transmission protocol used by a browser to communicate with a web server is called HTTP. A browser is a client in the client-server architecture that gets a server name from a URL and connects the server. Most URLs explicitly mention the protocol as http:// or omit it altogether, in which case HTTP is presumed to be the case:

Use text-based command messages file transfers for binary data Can upload and download data; includes caching. An HTTP request is sent to the server by the browser after it has established a connection. The four main request kinds are given below:

3. **GET** A document is requested using GET, and the server replies by delivering status information and then a copy of the requested document.
4. **HEAD** asks the server for a status update; the server replies with a status update but not a copy of the document.
5. **POST** sends information to a server, which appends it to a particular item (e.g., a message is appended to a list).
6. **PUT:** sends information to a server, which utilises it to totally replace the requested item (i.e., overwrites the previous data).

When a browser asks a server for a page, interactivity often starts there. The server answers to the browser's GET request by delivering a header, a blank line, and the requested content across the connection. A request and a header used in a response are both text-based elements in HTTP.

Version GET /item CRLF

Where item defines the URL of the requested item, version identifies the protocol version (often HTTP/1.0 or HTTP/1.1), and CRLF stands for the pair of ASCII letters known as carriage return and linefeed, which indicate the end of a line of text. Version information is crucial to HTTP since it enables changes to the protocol while maintaining backward compatibility. For instance, when a server using a higher version of the protocol communicates with a browser using version 1.0 of the protocol, the server falls back on the earlier version and responds appropriately.

A status code that informs the browser if the server processed the request is found in the first line of a response header. The status code identifies the issue, whether the request was created

improperly or the object was unavailable when it was re-queried. For instance, if a server cannot locate the requested item, it will return the well-known response code 404. A server provides status code 200 when it fulfils a request; subsequent lines of the header include details about the item, such as its length, the most recent modification date, and the content type. The overall layout of the lines in a fundamental response header.

`HTTP/1.0` ***status_code status_string CRLF***
`Server:` ***server_identification CRLF***
`Last-Modified:` ***date_document_was_changed CRLF***
`Content-Length:` ***datasize CRLF***
`Content-Type:` ***document_type CRLF***
CRLF

A status is indicated by the numeric value in the field status code, which is shown as a character string of decimal digits, and the human-readable status string. Examples of frequently used status codes and strings are shown in table 5.1. A human-readable description of the server is provided in the field server identification, which may also include the server's domain name. The size of the data item that follows, measured in bytes, is specified by the datasize field in the Content-Length header. A string in the document type field tells the browser what the document's contents are. The document type and its representation are the two elements in the string that are separated by a slash. For instance, a server may return a jpeg file with a document type of text/ html when it delivers an HTML document.

Table 5.1: Samples of HTTP status codes are shown

Status Code	Corresponding Status String
200	OK
400	Bad Request
404	Not Found

Sample output from an Apache web server. A text file with sixteen characters is the object being re- quested (i.e., the text This is a test. plus a NEWLINE character). The server uses HTTP version 1.1 even if the GET request calls for HTTP version 1.0. The contents of the file, a blank line, and nine lines of header are all returned by the server.

HTTP/1.1 200 OK
Date: Sat, 15 Mar 2008 07:35:25 GMT
Server: Apache/1.3.37 (Unix)
Last-Modified: Tue, 1 Jan 2008 12:03:37 GMT ETag:
"78595-81-3883bbe9"
Accept-Ranges: bytes Content-
Length: 16 Connection: close
Content-Type: text/plain

This is a test.

Browser Caching

Since consumers often visit the same websites, caching plays a significant role in online access optimization. Large pictures that adhere to the Joint Picture Encoding Group (JPEG) or

Graphics Image Format (GIF) standards make up a significant portion of a particular website's content. These pictures typically have stationary backdrops or banners.

The issue of what happens if the web server's document changes after a browser keeps a copy there emerges. In other words, how can a browser detect whether the copy it has cached is outdated? One hint may be found in the Last-Modified header of the response in Figure 4.8. The header indicates when a document was last modified whenever a browser downloads one from a web server. A browser keeps the Last-Modified date information along with the cached copy. A browser sends a HEAD request to the server and checks the Last-Modified dates of the server's copy and the cached copy before using a page that is stored locally. The browser downloads the fresh version if the cached version is outdated.

The algorithm leaves out a number of little facts. HTTP, for instance, enables a website to specify a No-cache header, which indicates that a particular item should not be cached. Also, since downloading a tiny item with a GET request takes about the same amount of time as making a HEAD request, and because keeping a lot of small things in a cache might slow down cache search speeds, browsers do not store small objects.

Architecture of Browsers

A browser is complicated since it supports a graphical user interface and offers generic functions. Of course, a browser has to comprehend HTTP, but it also supports additional protocols. A browser must have client code for each of the protocols used since a URL might specify a protocol. The browser must understand how to communicate with servers and how to decipher their answers in order to use each service. For instance, a browser needs to understand how to use the FTP service that is covered in the next section. Figure 5.2 displays components that a browser comprises.

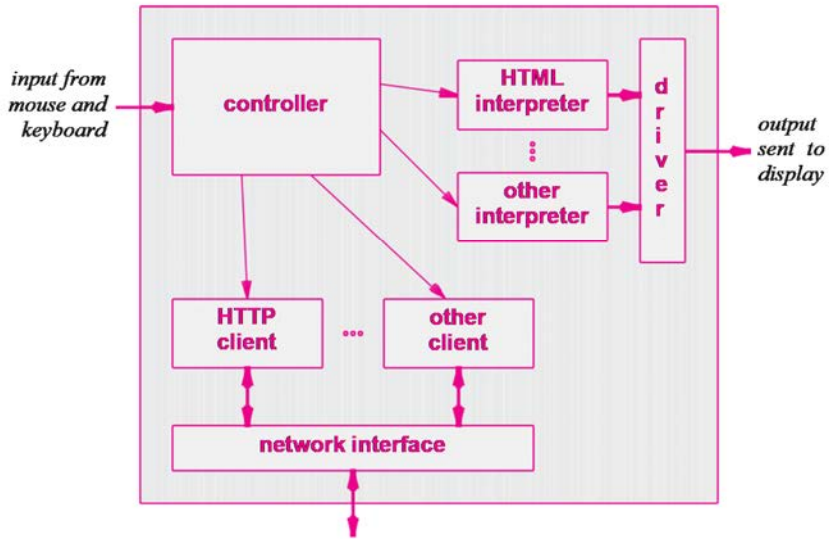


Figure 5.2: A browser's architecture that may access many service

File Transfer Protocol

The most basic storage abstraction is a file. A facility that transfers a copy of a file from one computer to another offers a strong mechanism for the exchange of data since a file may store

any item (for example, a document, spreadsheet, computer programme, graphic picture, or data). For this kind of service, we use the phrase file transfer.

File transmission via the Internet is hard because computers are heterogeneous, which means that each computer system determines file formats, type information, naming, and file access procedures.

A JPEG picture may have either the.jpg or.jpeg extension depending on the computer system some systems, each line in a text file is concluded by a single LINEFEED character, but other systems need CARRIAGE RETURN followed by LINEFEED. Some systems separate file names with a slash (/), whereas others use a backslash (). Moreover, an operating system may specify a group of user accounts, each of which is granted permission to view certain files. The user X on one computer is not the same as the user X on another, however, since the account information varies across machines.

The File Transfer Protocol is used by the most extensively used file transfer service on the Internet (FTP). FTP is best described as:

Arbitrary File Contents. Every sort of material, including documents, photos, music, and recorded videos, may be sent through FTP a two-way transfer. FTP may be used to upload files as well as download them (from server to client) (transfer from server to client). Support for Ownership and Authentication. Each file may have ownership and access limitations, and these constraints are respected by FTP to be able to browse folders. A client may access a directory's contents via FTP (i.e., a folder).

Control messages sent by text. The control messages delivered between an FTP client and server are sent as ASCII text, much like many other Internet application services. Accommodates Heterogeneity. FTP may move a copy of a file between any two computers and conceals the specifics of each computer's operating system. FTP applications are seldom started by users, hence the protocol is often undetectable. Yet, when a user requests a file download, a browser immediately invokes FTP.

Framework for FTP Communication

The interaction between a client and server is one of the most fascinating features of FTP. The method seems to be simple in general: a client connects to an FTP server and makes a series of requests, to which the server replies.

An FTP server does not deliver replies over the same connection that a client uses to submit requests, in contrast to HTTP. Instead, orders are only sent through the first connection the client makes, known as a control connection. The server creates a new connection each time it wants to download or upload a file. The connections used to transport files are known as data connections in order to separate them from the control connection.

Unexpectedly, the client-server relationship for data connections is reversed via FTP. In other words, while establishing a data connection, the client behaves as a server (i.e., waits for the data connection) and the server behaves as a client (i.e., initiates the data connection). The data connection is shut off after one transmission has been made using it. A new data connection is established by the server whenever the client makes another request (Figure 5.3).

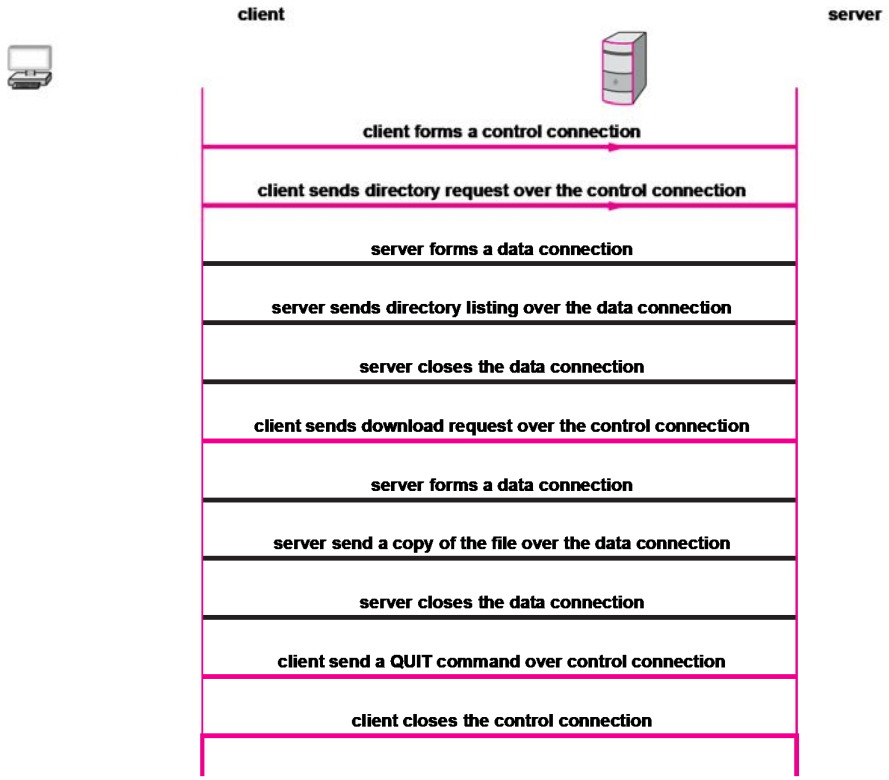


Figure 5.3: FTP connections seen during a typical session

The figure omits a number of crucial facts. For instance, a client has to log into the server after establishing the control connection. Using FTP, the client may send the USER command to offer a login name and the PASS command to supply a password. Through the control channel, the server delivers a numeric status response to inform the client as to the success or failure of the login. A client may only provide more commands after a login has been completed.

The protocol port number to be utilised for a data connection is another crucial component. When connecting to a client, what protocol port number should the server use? An intriguing solution is offered by the FTP protocol. A client selects a protocol port on their local operating system and communicates the port number to the server before sending a request to the server. In order to tell the server what port is being used, the client first binds to the port to wait for a connection. Next, the client sends a PORT command over the control connection. While the exchange of port information between two programmes may seem unimportant, it is not, and the method is not always effective. In particular, if one of the two endpoints is hidden behind a Network Address Translation (NAT) device, such a wireless router used in a home or small business, transmission of a protocol port number would fail. To enable FTP, a NAT device identifies an FTP control connection, examines the contents of the connection.

Internet mail

Email still ranks among the most popular Internet apps, despite the rise of instant messaging services. Email was created to enable a user on one computer to send a message straight to a user on another computer since it was built before personal computers and handheld PDAs were accessible (Figure 5.4).

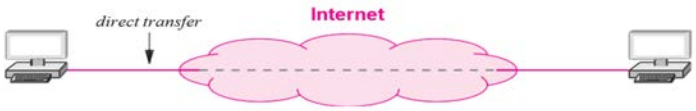


Figure 5.4: First email setup with a direct transfer from the computer of the sender to the computer of the receiver.

Even early email software was split into two conceptually distinct parts, as the algorithm suggests:

Software for sending mail: The email interface programme is directly accessed by a user. The user may create and update outgoing messages as well as view and handle incoming email using the interface's built-in tools. It's a good idea to have a backup plan in place, especially if you're going to be travelling. Instead, the interface programme receives emails from the user's mailbox, which is a file on their computer, and places outgoing emails in an outgoing mail queue, which is normally a folder on their disc. A mail server and a mail transfer application are independent programmes that manage the transfer. The mail server on the destination computer receives incoming messages and deposits each one in the mailbox of the relevant user; the mail transfer application operates as a client to deliver messages to the mail server on the destination computer.

Description Transfer: A procedure for transferring a duplicate of an email message from one computer to another

Access: a protocol that enables users to see or send email messages, access their inbox, and more

Representation: a standard that spells out how email messages should be formatted before being saved to disc

Simple Mail Transmission Protocol:

A mail transfer application sends an email message to a server over the Internet using the Simple Mail Transfer Protocol (SMTP), a common protocol. SMTP may be summed up as: adheres to the stream paradigm use text-based command messages only texts are transferred. Enables a sender to verify and define the names of each recipient one copy of the specified message is sent. The limitation of SMTP to textual information is its most surprising feature. The MIME standard, which is explained in a later section, permits email to contain attachments like graphic pictures or binary files, although the underlying SMTP method is limited to text only.

The capacity of SMTP to transmit a single message to many recipients on a single machine is the subject of its second feature. The protocol enables a client to send a single message to the whole list of users after listing each user one at a time. That is, a client sends a message "I have a mail message for user A," and the server either answers "OK" or "No such user here". In reality, each SMTP server message begins with a number code; hence answers are of the kind "250 OK" or "550 No such user here". When a mail message is transmitted from user John Q Smith on computer example.edu to two users on machine somewhere.com, an example SMTP session.

CHAPTER 6

ABOUT DATA COMMUNICATIONS

Sunanda Das, Associate Professor,
Department of Computer Science and Engineering, Jain (Deemed to be University)
Bangalore, India
Email Id- sunanda.das@jainuniversity.ac.in

The text's introduction analyses Internet applications and talks about network programming. The socket programming covers the application programming interface (API) that operating systems provide to application software and demonstrates how a programmer may develop Internet-using programmes without being familiar with the underlying technologies. The rest of the book will teach us about the intricate technologies and protocols that enable communication, and we'll see how knowing about the complexity may aid programmers in producing better code.

This section of the book investigates information transmission across physical mediums, including cables, optical fibres, and radio waves. We'll see that although the specifics may differ, the fundamental principles of knowledge and communication hold true regardless of the method of transmission. We will comprehend how data communications offers analytical and conceptual tools that give a comprehensive description of how communication systems function. Most importantly, data communications reveals the theoretically potential transfers as well as the realistic transmission systems' physical limitations. This gives a general overview of data communications and shows how the conceptual components come together to create a functioning communication system (Figure 6.1). One topic is thoroughly explained in each that follows.

Data Communications' Fundamental Principles

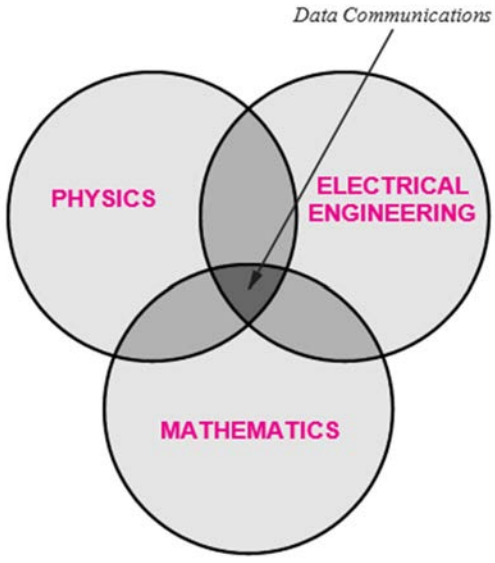


Figure 6.1: The field of data transmission is a nexus of Physics, Mathematics, and Electrical Engineering.

Data communications impacts on physics since it includes the transfer of information via physical means. Electric current, light, and other types of electromagnetic radiation are concepts that are included into the topic. Data communications employ mathematics and include several types of analysis since information is digitised and delivered as digital data. Ultimately, data communications focuses on creating methods that electrical engineers can utilise since the end objective is to provide useful ways to design and construct transmission networks (Figure 6.1).

The motivation for data communications is mostly based on three basic concepts, which also assist to define its scope. The information sources may be of any sort. A physical system is used for transmission.

The underlying medium may be shared by many sources of information. The first point that information is not limited to bits that have been saved in a computer—is particularly pertinent in light of the popularity of multimedia applications. However, data may also be gleaned from the real world, including audio and video. So, it's crucial to comprehend the many informational sources and formats, as well as how one form might be changed into another.

The second argument makes the case that we must convey information via natural processes like electricity and electromagnetic waves. Understanding the many media types and their individual characteristics is crucial.

Additionally, we need to comprehend the connection between data communications and the underlying transmission as well as how physical phenomena might be exploited to communicate information through each channel. Lastly, we need to comprehend the boundaries of physical systems, potential issues with transmission, and methods for identifying or resolving such issues.

The final argument makes the fundamentality of sharing clear. In fact, we'll discover that sharing is essential to the majority of computer networks.

In other words, a network often enables several communication pairs to interact over a single physical media. Consequently, it is crucial to understand the numerous ways underlying facilities might be shared, the benefits and drawbacks of each, and the ensuing modes of communication.

The Components of A Communication System Conceptually

For further information, please visit the website. It can appear straightforward to communicate in such a system. Each source requires a method for gathering data, preparing it for transmission, and transmitting it over the common physical media. Similar to that, a technique is required to extract and transmit the information for the destination. Figure 6.2 depicts the oversimplified perspective.

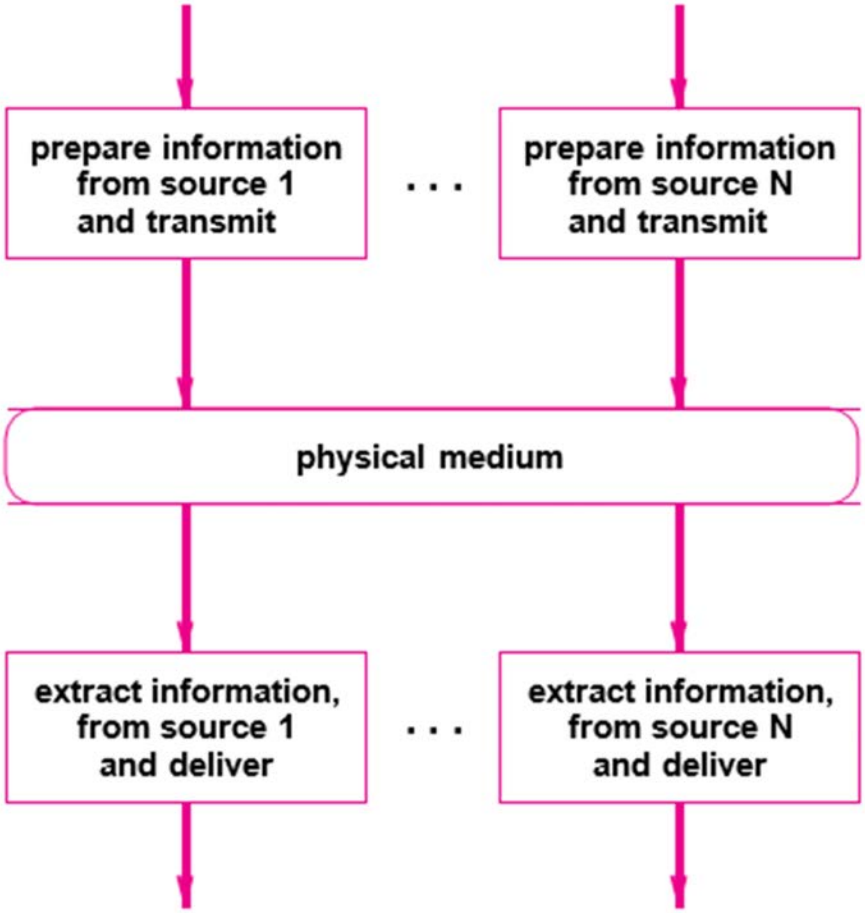


Figure 6.2 shows a simplified representation of data communications using a common channel for transmitting data from a number of sources to a number of destinations.

Data transmission is far more complicated in reality than the overly-simplistic diagram in Figure 6.2 would have you believe. The methods used to manage sources differ according to the variety of sources from which information may be obtained. Information must be digitised and additional data must be included to prevent against mistakes before it can be transferred. The data may need to be encrypted if privacy is an issue. The data from each source must be recognised and blended together for transmission in order to convey numerous streams of information through a common communication method. Hence, a system is required to distinguish between each source and ensure that data from one source is not accidentally mixed up with data from another.

To illustrate the key components of data communications, engineers have constructed a conceptual framework that explains how each subtopic fits into a communication system. The theory behind the framework is that each component may be studied alone, and that when all parts have been looked at, the whole topic would be comprehended. The framework is shown in Figure 6.3, which also demonstrates how the conceptual components fit into the broader structure of a communication system.

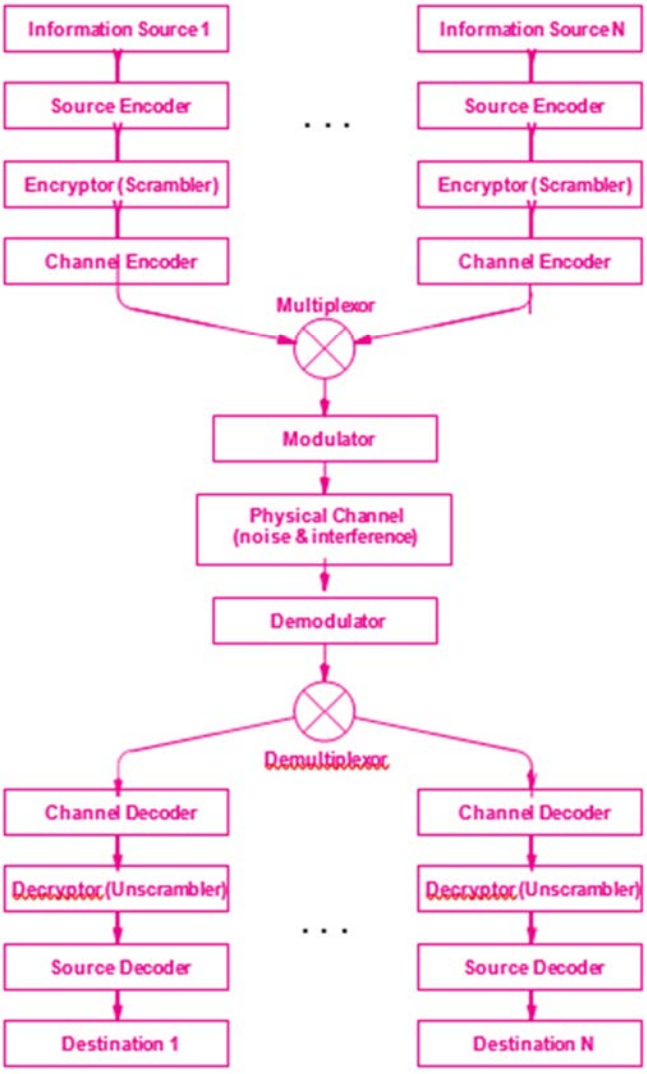


Figure 6.3: a system for data communications conceptually. Many sources provide information to several destinations across a physical channel.

Sources of information

Digital or analogue sources of information are both acceptable. Signal properties including amplitude, frequency, and phase, as well as categorization as either periodic or aperiodic, are crucial ideas. The translation of information between analogue and digital forms is another aspect of this subtopic.

Encoder and Decoder for Source

Digital representations may be altered and modified after information has been digitally represented. Data compression and the effects on communications are crucial ideas.

A decryptor and an encryptor

Information may be encrypted (i.e., scrambled) before transmission and decoded after receipt to safeguard it and keep it secret. Cryptographic methods and algorithms are important ideas.

Encoder and decoder for channels

In order to identify and fix transmission faults, channel coding is utilised. Techniques used in computer networks, such as parity checking, checksums, and cyclic redundancy codes, are useful tools for detecting and limiting faults.

Both a demultiplexor and a multiplexor: Multiplexing is the process of combining information from several sources for transmission via a common media. Techniques for simultaneous sharing and approaches that enable sources to use the media alternately are both crucial topics.

Both a modulator and a demodulator: Electromagnetic radiation is utilised to transfer information in a process known as modulation. Both analogue and digital modulation systems, as well as modems—devices that carry out the modulation and demodulation—are concepts.

Transmission via a physical channel: Transmission medium and transmission modes are covered under this subject. The terms "bandwidth," "electrical noise and interference," "channel capacity," and "serial and parallel transmission modes" are all crucial.

Sources of Information and Signals

A more thorough investigation of data communications. The themes of information sources and the properties of information-carrying signals are both covered. The examination of data communications is continued in later by introducing new concepts.

Information Sources

Remember that a communication system receives information from one or more sources and transmits it from one source to another to a designated destination. A pair of application programmes that create and consume data serve as the source and destination of information for a network like the worldwide Internet.

Data communications theory, on the other hand, focuses on low-level communications systems and is applicable to any kind of information source. For instance, information sources may include microphones, sensors, and measurement tools like thermometers and scales in addition to more traditional computer peripherals like keyboards and mouse. In a similar vein, places may include equipment that produce light, such as LEDs, as well as audio output devices like earphones and loudspeakers.

Digital and Analog Signals

Analog and digital information are the two kinds that data communications works with. A continuous mathematical function is what defines an analogue signal; as the input changes from one value to the next, it does so by traversing all conceivable intermediate values. An instantaneous transition from one valid level to another characterises each change in a digital signal, which has a finite set of valid levels.

Figure 6.4 provides examples of how the signals from analogue and digital sources change over time to help explain the idea. If one measured the output of a computer keyboard instead of a microphone, the analogue signal in the image may be produced, and vice versa for the digital signal.

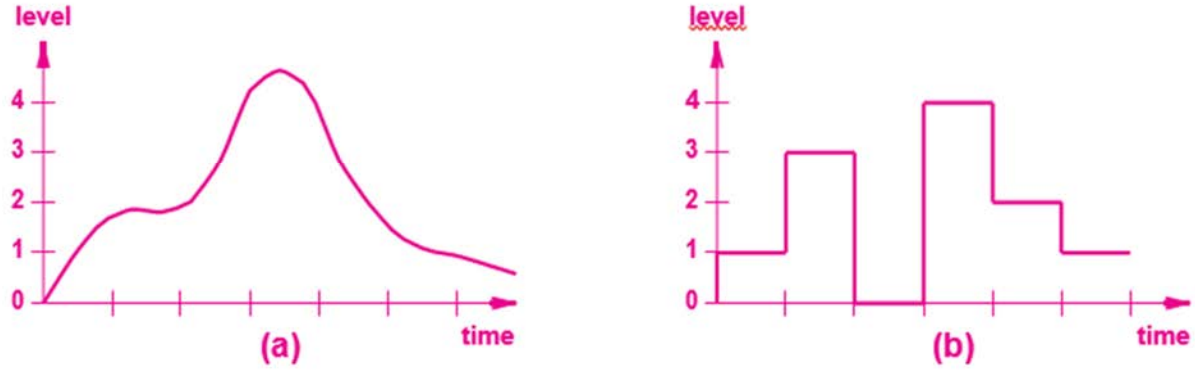


Figure 6.4 shows an example of both an analogue and a digital signal.

Periodic and aperiodic signals:

Depending on whether they recur, signals are widely categorised as periodic or aperiodic (also known as non-periodic). As the analogue signal in Figure 6.1a does not recur, it is aperiodic across the shown time frame. Figure 6.5 shows an example of a periodic signal (i.e., repeating).

Figure 6.5 Repetition of a periodic signal.

Signal Characteristics and Sine Waves

We'll discover that a lot of data communications analysis uses trigonometric sine functions, particularly sine, which is sometimes abbreviated as sin. As sine waves are produced by natural occurrences, they have a specific role in information sources. For instance, a sine wave is produced when a microphone detects an audible tone. Similar to this, a sine wave may be used to describe electromagnetic radiation. We are particularly interested in sine waves that correlate to a time-varying signal, such as the wave shown in Figure 6.5.

There are four crucial sine wave-related features of signals:

The number of oscillations per unit time is known as frequency (usually seconds) the difference between the greatest and smallest signal heights is known as amplitude. Phase: the amount by which the sine wave's beginning is offset from a reference time. The length of a wave when a signal travels through a medium.

Wavelength is governed by how quickly a signal spreads (i.e., is a function of the underlying medium). Mathematical expressions exist for the other three attributes. The simplest concept to grasp is amplitude. Remember that sin(t) has an amplitude of 1 and may generate values between -1 and +1. So, if the value is multiplied by A, the resultant wave's amplitude is A. The sine wave is shifted to the right or left along the x-axis by the phase, which is a mathematical offset added to t. As a result, sin(t+) has a phase of. A signal's frequency is expressed in Hertz, or the number of sine wave cycles per second. Two radians are required for a full sine wave. Hence, sin(t) has a frequency of 1 Hertz if t is a time in seconds and = 2. The three mathematical properties are shown in Figure 6.6.

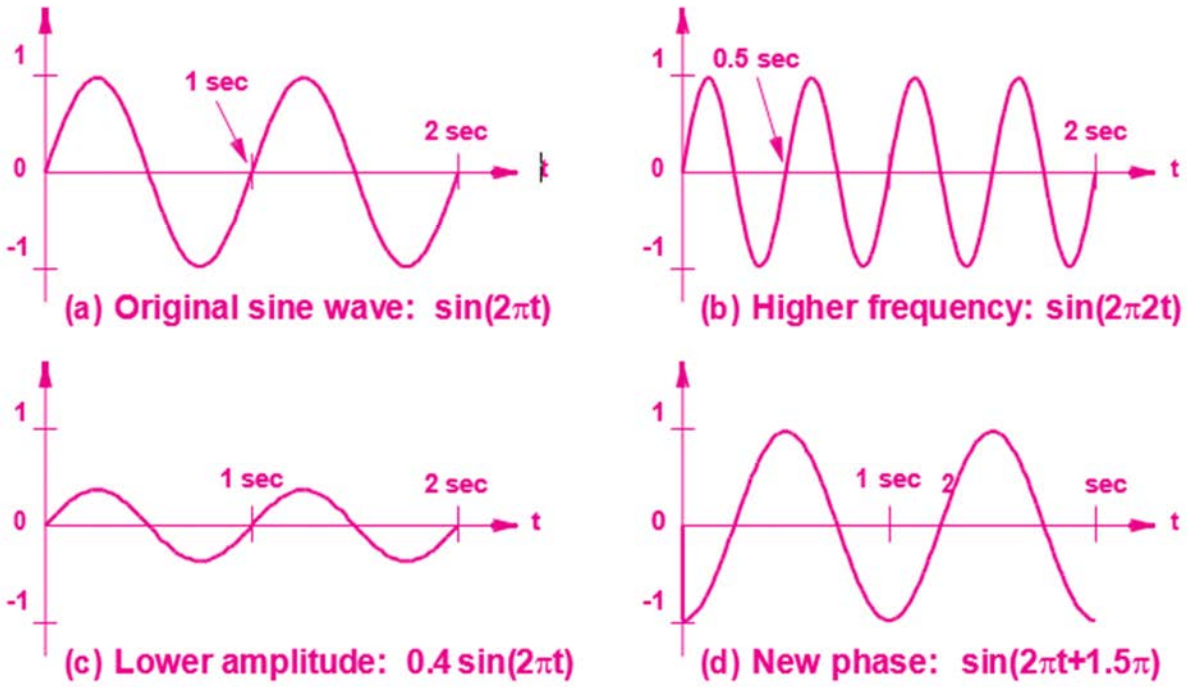


Figure 6.6: Frequency, amplitude, and phase characteristics.

The period, sometimes referred to as the frequency, may be computed as the inverse of the amount of time needed for one cycle. The sample sine wave in Figure 6.6a has a frequency of 1 / T, or 1 Hertz, with a period of T = 1 seconds. The example in Figure 6.6b has a frequency of 2 Hertz and a period of T = 0.5 seconds, both of which are regarded as very low frequencies. Often measured in millions of cycles per second, high frequencies are used in typical communication systems. Engineers use fractions of a second to indicate time and megahertz to express frequency to better understand high frequencies. Time scales and frequently used prefixes are shown in Table 6.1.

Table 6.1: Units of time and frequency prefixes and acronyms

Time Unit	Value	Frequency Unit	Value
Seconds (s)	10^0 seconds	Hertz (Hz)	10^0 Hz
Milliseconds (ms)	10^{-3} seconds	Kilohertz (KHz)	10^3 Hz

Microseconds (□s)	10^{-6} seconds	Megahertz (MHz)	10^{6} Hz
Nanoseconds (ns)	10^{-9} seconds	Gigahertz (GHz)	10^{9} Hz
Picoseconds (ps)	10^{-12} seconds	Terahertz (THz)	10^{12} Hz

Composite Signals (Simple signals are those that consist of a single sine wave that cannot be further subdivided, such as those seen in Figure 6.6. In reality, the majority of signals are categorised as composite because they can be broken down into a collection of straightforward sine waves. Figure 6.7, for instance, shows a composite signal created by combining two straightforward sine waves.

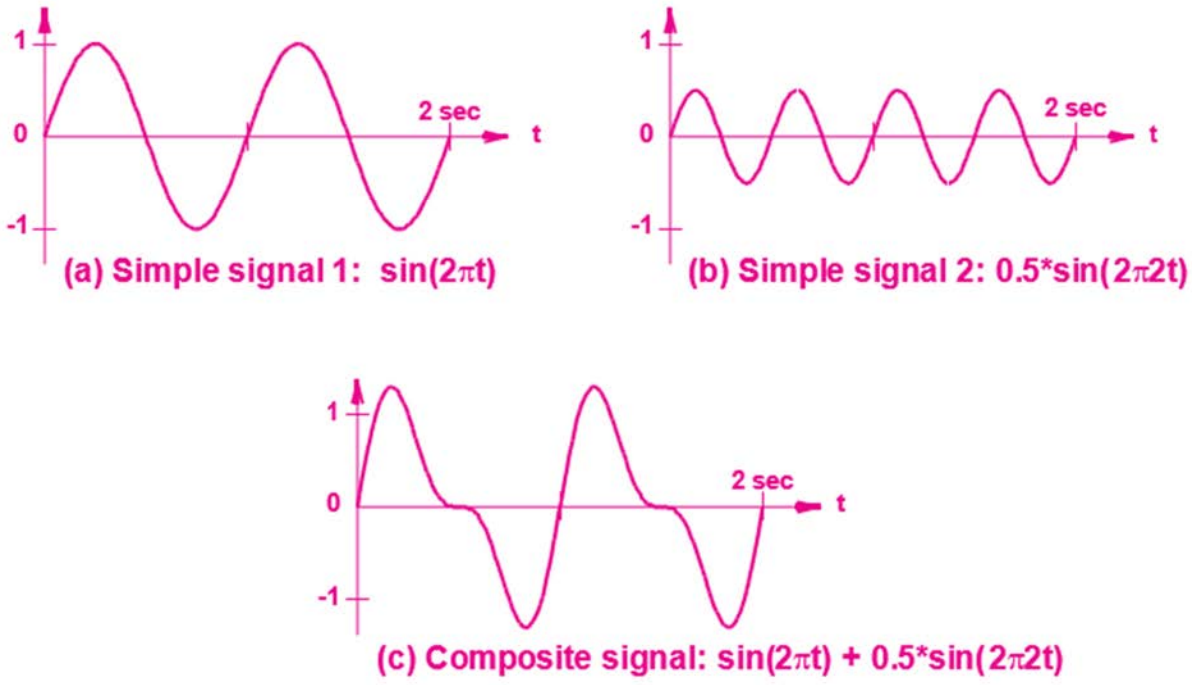


Figure 6.7: A composite signal created from two basic signals.

Composite signals and sine functions are important

Why do sine functions and composite signals appear to be the focus of data communications? We shall comprehend one of the main causes when we study modulation and demodulation: modulated signals are often composite signals. Just the motive must be understood for the time being. Typically, modulation creates a composite signal. A composite signal may be broken down into a collection of sine functions, each having a frequency, amplitude, and phase, according to Fourier, a mathematician.

According to Fourier's analysis, the constituent components will also be periodic if the composite signal is. As a result, we shall find that the majority of data communications systems employ composite signals to transmit information: at the sending end, a composite signal is

formed, and at the receiving end, the signal is broken down into its original simple components. The key is:

Representations in the Time and Frequency Domains

Composite signals have undergone substantial research due to their importance, and several ways have been developed to represent them. A graph of a signal as a function of time is one form that we have previously seen in earlier figures. According to engineers, a graph like this depicts the signal in the temporal domain. A frequency domain representation is the major substitute for a time domain representation. A series of straightforward sine waves that make up a composite function are represented by a frequency domain graph. The frequency is shown on the x-axis, while the amplitude is shown on the y-axis. Hence, a single line of height A that is positioned at x=t represents the function A sin(2t). For instance, Figure 6.8s frequency domain graph is a composite of Figure 6.8.

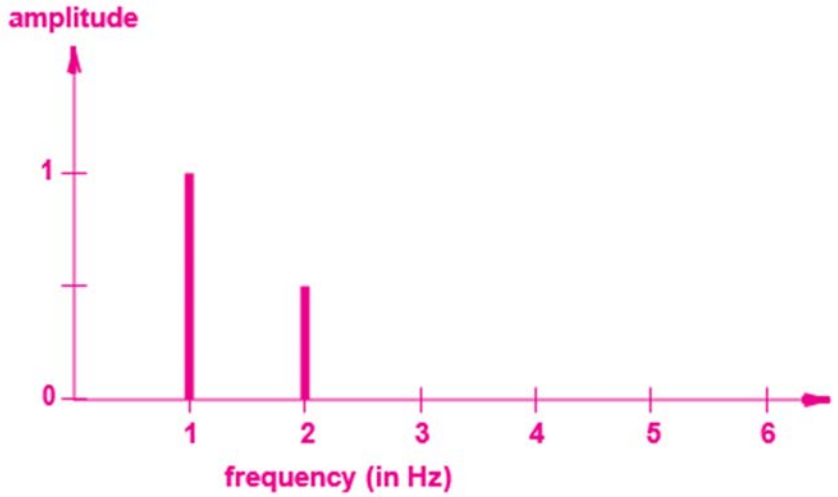


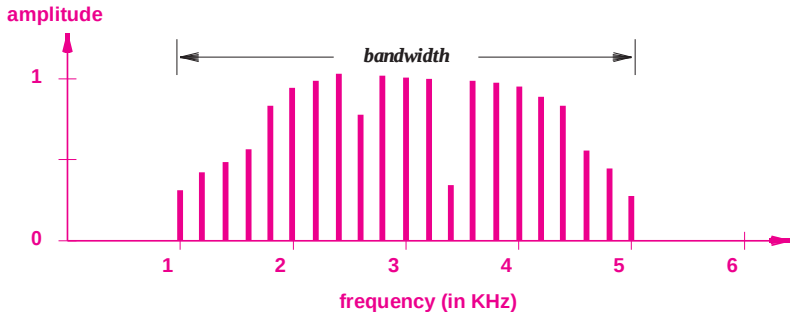
Figure 6.8: Frequency domain representation of sin(2t) and 0.5sin(2t2).

A group of basic periodic signals are shown in the illustration. Nonperiodic signals may also be represented in the frequency domain, however aperiodic representation is not necessary to comprehend the topic. The compactness of the frequency domain representation is one of its benefits. Since each sine wave takes up a single point along the x-axis, a frequency domain representation is both tiny and simple to read compared to a time domain representation. When a composite signal consists of several simple signals, the benefit is obvious.

Bandwidth of An Analog Signal

Virtually everyone is familiar with the term "network bandwidth" and is aware of the benefits of having a large network. The definition of network bandwidth will be covered later. We shall focus on analogue bandwidth for the time being as a related idea. The difference between the highest and lowest frequencies of the component elements is how we define an analogue signal's bandwidth (i.e., the highest and lowest fre- quencies obtained by Fourier analysis). As shown in the simple example of Figure 6.5c, the bandwidth is the difference, or 1 Hertz, between the signals produced by Fourier analysis at 1 and 2 Hertz. For computing bandwidth, a frequency domain plot has the benefit of making the highest and lowest frequencies evident. For instance, it is obvious from the Figure 6.6 that the bandwidth is 1.

A frequency domain plot with frequencies measured in Kilohertz is shown in Figure 6.9. (KHz). These frequencies are within the range of human ear audibility. The bandwidth of the image is equal to the difference between the highest and lowest frequency (5 KHz - 1 KHz = 4 KHz).



6.9: bauds per second and bits

How much information may be delivered at one time? Two components of the communication system will determine the solution. As we've seen, the amount of signal levels affects the speed at which data may be delivered. The time the system spends at one level before going on to the next is a further element that is crucial. For example, in Figure 6.8a depicts time along the x-axis, and the time is split into eight segments, with one bit being transferred during each segment. Two times as many bits will be transferred in the same amount of time if the communication system is adjusted to utilise half as much time for a specific bit.

In a real system, the hardware establishes restrictions on how short the time may be. If the signal does not stay at a specific level for a long enough period of time, the receiving hardware will not be able to detect it. It's interesting to note that the standard measurement of a communication system doesn't include a time limit. Instead, engineers count the baud, which is defined as the number of times the signal may change each second. We say a system works at 1000 baud, for instance, if the signal must maintain at a certain level for.001 seconds. The main point is that the bit rate is determined by both baud and the quantity of signal levels. A system with two signal levels can transmit precisely 1000 bits per second if it runs at 1000 baud. Yet, a system that runs at 1000 baud may transmit 2000 bits per second if it has four signal levels (because four signal levels can represent two bits). The connection between baud, signal levels, and bit rate is expressed in equation 6.1.

$$\textit{bits per second} = \textit{baud} \times \left\lfloor \log_2(\textit{levels}) \right\rfloor \qquad (6.1)$$

Analog to Digital Signal Conversion

How can a digital signal be transformed into its analogue equivalent? Remember that a sine wave composite with each sine wave in the set having a distinct amplitude, frequency, and phase may be used to describe an arbitrary curve according to Fourier's theory. Fourier's theorem is true for any curve, hence it also holds true for digital signals. From a technical standpoint, Fourier's solution is problematic for digital signals since ac- curate representation of a digital signal needs an endless collection of sine waves.

Engineers reach a compromise: approximate conversion of a signal from digital to analogue. In other words, engineers create machinery to produce analogue waves that are very similar to the digital signal. Approximation requires creating a composite signal from just a few sine waves. It is possible to employ as few as three sine waves by picking ones that are the right multiples of the frequency of the digital signal. Figure 6.10 illustrates the approximation by

displaying (a) a digital signal and approximations with (b) a single sine wave, (c) a composite of the original sine wave plus a sine wave of 3 times the frequency, and (d) a composite of the wave in (c) plus one more sine wave at 5 times the original frequency. The exact details are outside the scope of this text.

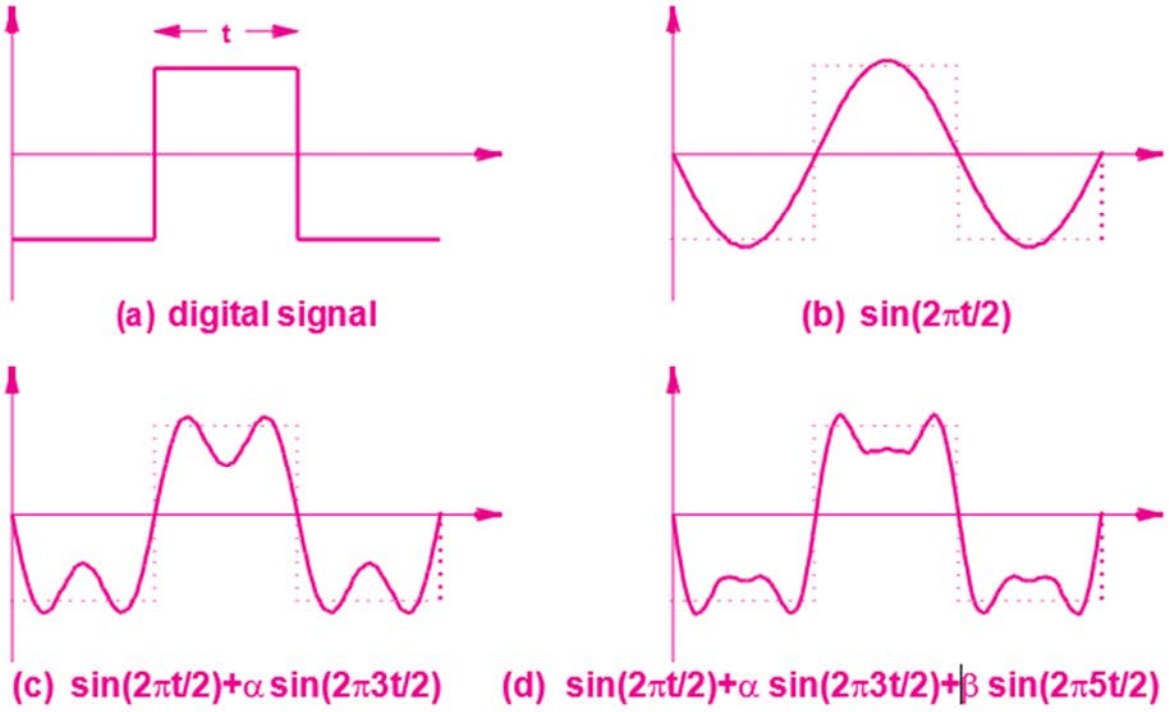


Figure 6.10 Approximation of a digital signal with sine waves.

CHAPTER 7

TECHNOLOGIES FOR NETWORK LAN

Chandramma R, Assistant Professor,
Department of Computer Science and Engineering, Jain (Deemed to be University)
Bangalore, India
Email Id- chandramma.cse@gmail.com

An extensively used LAN technology is Ethernet. In the year 1970, Bob Metcalfe and D.R. Boggs developed this technology. In 1980, it was specified in IEEE 802.3. Ethernet distributes data. A shared media network has a significant likelihood of data collision. Carrier Sense Multi Access/Collision Detection (CSMA/CD) technology is used by Ethernet to identify collisions. When a collision occurs in Ethernet, all of the hosts roll back, wait a predetermined period of time, and then retransmit the data. A network interface card with an Ethernet connection has a 48-bit MAC address. This facilitates the identification and communication of distant Ethernet devices by other Ethernet devices. Specifications for 10BASE-T are used in conventional Ethernet. The letters 10 stand for 10 Mbps, BASE for baseband, and T for thick ethernet. 10BASE-T Ethernet employs coaxial cable or Cat-5 twisted pair cable with an RJ-5 connection and offers transmission speeds of up to 10MBPS. Ethernet segments may be up to 100 metres long and use the Star topology. All devices are linked to a hub/switch in a star configuration.

Fast-Ethernet

Ethernet expands into Fast-Ethernet in order to meet the demands of rapidly developing software and hardware innovations. It can function wirelessly, via UTP, and through optical fibre. It offers speeds of up to 100MBPS. This standard uses Cat-5 twisted pair cable and is known as 100BASE-T in IEEE 803.2. It employs the CSMA/CD method for wired media sharing between Ethernet hosts and the CSMA/CA (Collider Avoidance) method for wireless Ethernet LAN. According to the 100BASE-FX standard, fast Ethernet over fibre offers speeds of up to 100MBPS. Ethernet over fibre may be extended over multimode fibres up to 2000 metres in full-duplex mode and up to 100 metres in half-duplex mode.

Giga-Ethernet

Fast-Ethernet, which debuted in 1995, barely maintained its high speed designation for three years until Giga-Ethernet did. The maximum speed offered by giga-Ethernet is 1000 mbits/second. Giga-Ethernet over UTP utilising Cat-5, Cat5e, and Cat-6 cables is standardised by IEEE802.3ab. Giga-Ethernet over Fiber is defined by IEEE802.3ah. In Ethernet, shared media only creates one Broadcast domain and one Collision domain. When switches were added to Ethernet, the problem with a single collision domain has been resolved, and each device connected to a switch now operates in a distinct collision domain. Even switches, however, are unable to partition a network into distinct broadcast domains. To split a single broadcast domain into many broadcast domains, use virtual local area networks (LANs). There is no communication between hosts in different VLANs. Every host joins the same VLAN by default (Figure 7.1).

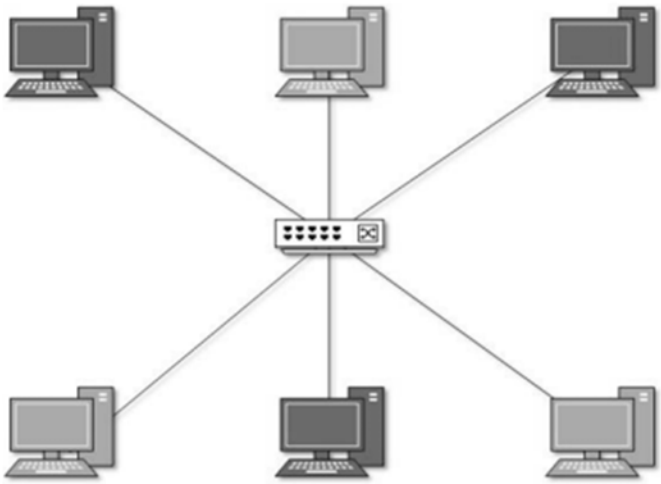


Figure 7.1: Represent the VLAN

Several VLANs are shown in this diagram using various colour schemes. Even when connected to the same switch, hosts in one VLAN are unable to observe or communicate with hosts in other VLANs. Layer-2 technology called VLAN tightly integrates with Ethernet. A Layer-3 device, such as a router, is needed to transport packets between two separate VLANs. The configuration of how computer systems or network devices are linked to one another is known as a topology. Topologies may specify a network's logical and physical aspects. A network may have the same or distinct logical and physical topologies.

Point-to-Point

A single piece of cabling connects precisely two hosts, such as computers, switches, routers, or servers, in a point-to-point network. The transmitting end of one host is often linked to the receiving end of another, and vice versa (Figure 7.2).

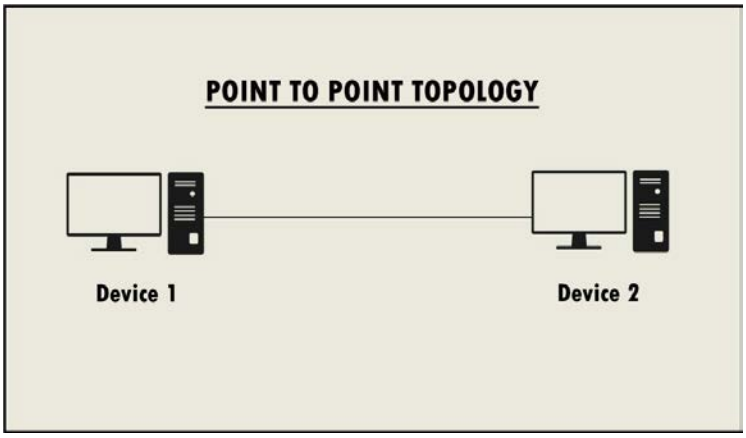


Figure 7.2: Point-to-Point

If the hosts are logically linked point-to-point, then there could be many intermediary devices. Yet, the end hosts see one another as if they are directly linked and are not aware of the underlying network.

Bus Topography

All devices in a bus topology share a single communication line or cable. Bus topology may have difficulties with numerous hosts providing data at the same time. Consequently, to address the problem, Bus topology either employs CSMA/CD technology or designates one host as Bus Master. It is one of the straightforward networking models where a device's failure has no impact on the other devices. But, if the common communication channel fails, all other devices might become inoperable. All of the stations are linked by a single cable known as a backbone cable thanks to the bus topology's design. Either a drop cable or a direct connection to the backbone cable connects each node to it. A node puts a message across the network whenever it wishes to transmit a message. Regardless of whether it has been handled, the message will reach every station in the network. Most 802.3 (ethernet) and 802.4 standard networks employ the bus topology. As comparison to other topologies, the setup of a bus topology is rather straightforward. The backbone cable is referred to as a "single channel" via which all of the stations get the same message. Among bus topologies, CSMA is the most used access technique (Carrier Sense Multiple Access).

CSMA is a media access control used to manage data flow and ensure data integrity, or the prevention of packet loss. When two nodes deliver the messages concurrently, there are two different solutions to the issues that arise.

CSMA CD: A collision detection access technique, CSMA CD is used to find collisions. The sender will cease sending data once the collision has been identified. It focuses on "recovery after the accident" as a result.

CSMA CA: CSMA CA (Collision Avoidance) is an access technique used to prevent collisions by determining whether or not the transmission medium is in use. If the medium is busy, the sender waits until it is free of activity. This method successfully lowers the likelihood of a collision. "Recovery after the collision" is not possible.

Benefits of the bus topology

Affordable cable: With a bus architecture, nodes connect to the cable directly rather than through a hub. As a result, installation has a minimal initial cost.

Moderate data speeds: Bus-based networks that offer up to 10 Mbps typically employ coaxial or twisted pair wires.

Technology that is well-known: Bus topology is a well-known technology since hardware components are readily accessible and installation and troubleshooting methods are well-known. One node's failure will only have a limited impact on the other nodes.

Drawbacks of Bus topology:

Heavy wiring: A bus architecture is very easier, but yet it needs a lot of cabling. Troubleshooting is challenging because identifying cable issues needs sophisticated test equipment. All of the nodes' communication would be hampered if a cable failure occurred.

Signal interference: If two nodes transmit messages at the same time, their signals will interfere with one another.

Configuration challenging: Adding more devices to the network would make it slower.

Attenuation: Loss of signal caused by attenuation makes communication difficult. The signal is renewed using repeaters.

Topologies of Computer Networks

The shared channel has line terminators at both ends. The data is only delivered in one way, and the terminator cuts the line off when the data reaches the very end.

Star Topology

With a star topology, every host is linked through a point-to-point link to a central component called the hub device. In other words, the hosts and hub are connected point to point. Any of the following may serve as the hub device (Figure 7.3):

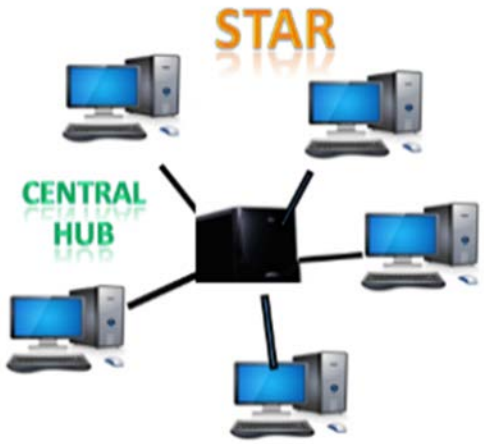


Figure 7.3: Star Topology

1. Layer-1 device, such as a repeater or hub
2. Devices at Layer 2 like switches and bridges
3. Layer-3 gadget, such a router or gateway
4. Networking and Data Communication

As in Bus topology, hub functions as single point of failure. If the hub fails, none of the hosts are able to connect to any other hosts. The hub is the sole channel via which hosts may communicate with one another. The cost of using a star topology is low since just one cable is needed to connect an additional host, and setup is straightforward. A network configuration known as a "star topology" connects each node to a central hub, switch, or computer. The peripheral devices connected to the main computer are referred to as clients, while the server is referred to as the computing device. Computer connections are made via coaxial or RJ-45 wires. The most often used topology for network implementation is the star topology.

Positive aspects of star topology

Effective problem-solving As compared to bus topology, troubleshooting in a star topology is far more effective. The manager must examine the kilometres of cable in a bus topology. All of the stations are linked to the central network in a star topology. As a result, the network administrator must visit the single station to investigate the issue. Network management: The star topology makes it simple to add intricate network control functions. Any modifications to the star topology are immediately taken into account.

Restricted failure: Since each station has its own connection connecting it to the central hub, a cable failure won't take down the whole network. Star topology is a well-known technique since its tools are affordable.

It is readily scalable since additional stations may be connected to the hub's open ports. Star topology networks are economical because they make use of coaxial cable, which is cheap.

High data rates: It can handle around 100 Mbps of bandwidth. One of the most often used Star topology networks is Ethernet 100BaseT.

Cons of the Star topology

A single point of failure: All linked nodes will be unable to interact with one another if the main hub or switch fails.

Cable: When a substantial volume of cable routing is necessary, it may sometimes become challenging.

Topology of rings

Each host computer in a ring topology links to precisely two more hosts, resulting in a circular network structure. Data passes via all intermediate hosts if one host attempts to interact with or send a message to another host that is not nearby. The administrator may just only one more cable to connect a second host to the current setup (Figure 7.4).

Figure 7.4: Ring Topology

Similar to a bus topology, but having linked ends, is the ring topology. The node will retransmit to the next node after receiving the message from the prior computer. Data is unidirectional, meaning that it only goes in one way. An infinite loop is a continuous flow of data in a single loop. It has no terminated ends, meaning that every node is linked to every other node and lacks a point of termination. With a ring topology, the flow of data is clockwise.

Token passing is the ring topology's most used access technique. A network access mechanism called token passing involves passing a token from one node to another. A frame that travels across the network is a token. Passing of Tokens at Work. Until it reaches its destination, a token travels via the network and is transmitted from computer to computer. By including the address with the contents, the sender alters the token. Until the destination address matches, the data is transmitted from one device to another. The acknowledgement is sent to the sender after the target device has received the token. A carrier is a token in a ring architecture.

The benefits of ring topology

Network administration: It is possible to remove problematic devices from the network without disrupting it.

Product availability: Numerous hardware and software solutions for network operation and monitoring are available.

Twisted pair cabling is affordable and widely accessible. As a result, installation is quite inexpensive. Since the communication mechanism is not reliant on a single host computer, the network is more dependable.

Drawbacks of Ring topology:

Challenging troubleshooting: To identify the cable defects, specialist test equipment is needed. All of the nodes' communication would be hampered if a cable failure occurred.

Failure: The network as a whole fails when one station malfunctions.

Configuration challenging: Adding more devices to the network would make it slower.

Delay: The number of nodes directly affects the communication latency. The amount of time between devices becomes longer as more are added.

Hybrid Topology:

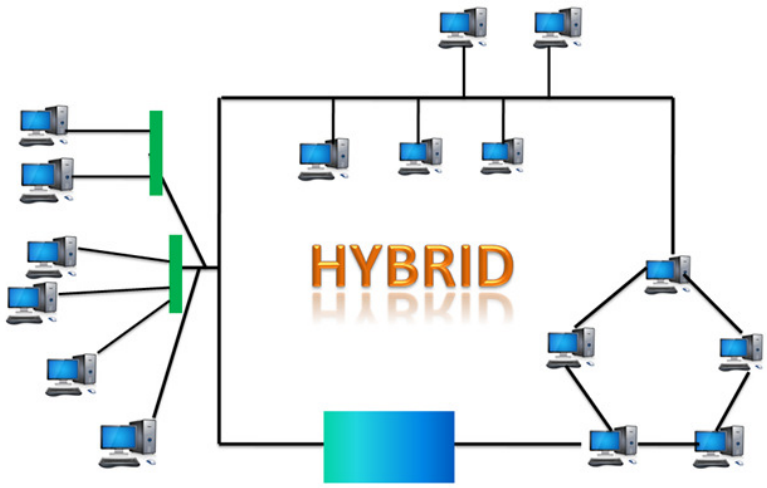


Figure 7.5: Hybrid topology

Hybrid topology is the fusion of many distinct topologies. A hybrid topology connects several connections and nodes in order to transport data. Hybrid topology is defined as the combination of two or more distinct topologies; comparable topologies linked to one another do not produce hybrid topology. For instance, if ICICI Bank has a bus topology in one branch and a ring topology in another branch, linking the two will provide a hybrid topology (Figure 7.5).

Hybrid Topology's benefits

Reliable: It's important to note that this is a placeholder page and does not constitute a formal announcement of our services.

Scalable: By adding more devices, the network's size may be simply increased without harming its operation.

Flexible: Its topology may be tailored to meet the needs of the company, making it particularly adaptable.

Effectiveness: Hybrid topology may be built to optimise a network's strengths and reduce its weaknesses, making it extremely effective.

Issues with hybrid topology

The Hybrid network's architecture is the main flaw in the Hybrid topology. The hybrid network's architecture is highly challenging to design.

Costly Hub: Since they vary from the typical hubs used in other topologies, the hubs utilised in the hybrid topology are quite pricey. Infrastructure is quite expensive since a hybrid network needs a lot of cabling, network equipment, etc.

Tree Topology:

Figure 7.6: Tree topology

The traits of both bus topology and star topology are combined in tree topology. A sort of structure called a "tree topology" connects all the computers in a hierarchical manner. All other nodes in a tree topology are descendants of the root node, which is the topmost node. For the data transfer between two nodes, there is only one route. A parent-child hierarchy is created as a result (Figure 7.6).

Tree topology's advantages

Broadband transmission assistance: Broadband transmission, or the ability to send signals across great distances without attenuation, is the principal use of tree topology.

Expandable without difficulty: We may connect the new device to the current network. Thus, we may assert that tree topology is amenable to expansion.

Easy to handle: Star networks, which are simple to operate and maintain, are used to segment the whole network in tree topology.

Error detection: A tree topology makes it extremely simple to find errors and rectify them.

One station's failure has a limited impact on the network as a whole. It contains point-to-point wiring for each of the separate segments.

Tree topology's drawbacks

Tough troubleshooting: Whenever a node defect arises, it is difficult to find the source of the issue.

High cost: Broadband transmission requires a lot of expensive equipment.

Failure: A main bus wire is the major source of failure for a tree architecture, harming the whole network.

Conversion challenges: It gets challenging to modify when additional devices are introduced.

CHAPTER 8

MEDIA FOR TRANSMISSION

Sonal Sharma, Associate Professor,
Department of Computer Science and Engineering, Jain (Deemed to be University)
Bangalore, India
Email Id- s.sonal@jainuniversity.ac.in

The study of data communications is continued in this by looking at several types of transmission medium, such as cable, wireless, and optical media. This covers fundamental ideas of electromagnetic transmission, provides a taxonomy of media kinds, and describes how shielding may lessen or stop interference and noise. This concludes by explaining the idea of capacity. The study of data communications is continued in subsequent.

Guided and unguided transmission

Depending on the sort of route, communication may either follow a precise course, like a wire, or it might have no clear path at all, like a radio broadcast. According to energy type, cables employ electrical energy, wireless uses radio transmission, and optical fibre uses light. To differentiate between radio transmissions that flow in all directions via free space and physical media that give a specified route, such as copper wire or optical fibres, we use the words guided and unguided transmission. Engineers jokingly refer to wired and wireless. Notice that the informality may be somewhat misleading because one is likely to hear the phrase wired even when the actual media is an optical fibre.

A Taxonomy of Energy Types

The classification of physical media based on the kind of energy utilised to transfer data is shown in Figure 8.1. Each of the media kinds is described in a series of parts.

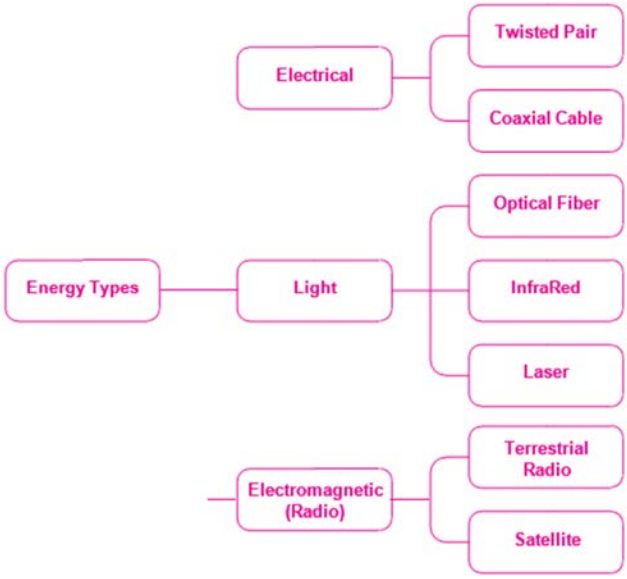


Figure 8.1: A classification of media kinds based on the type of energy utilised.

The categories are not flawless, like with most taxonomies, and there are some outliers. A space station in orbit around the planet, for instance, may use non-satellite non-terrestrial communication. Yet, the majority of communications are covered by our taxonomy.

Radiation Background and Electrical Noise

Remember from elementary physics that an electrical current travels the whole length of a circuit. A wire to the receiver and a wire back to the sender are thus required for all electrical energy transfers in order to complete the circuit. A cable with two copper wires within it makes up the most basic kind of wiring. Each wire is covered in a plastic covering that acts as an electrical insulator. In order to make it simpler for people to connect equipment, the outside coating of the cable keeps similar wires together. Wiring in computer networks is done differently. Three facts are necessary to comprehend why.

- Noise, or erratic electromagnetic radiation, pervades the environment. In actuality, electrical noise is a byproduct of regular functioning for communication equipment.
- Electromagnetic radiation produces a little signal when it strikes metal, which implies that random noise may obstruct communication signals.
- Metal serves as a barrier because it absorbs radiation. Hence, it is possible to prevent noise from interfering with transmission by putting enough metal between a source of noise and a communication channel.

The first two facts highlight a basic issue with electrical or radio-powered communication medium. The issue is more acute near a source that releases random radiation. For instance, electric motors that are very strong like those used to run elevators, air conditioners, and refrigerators also generate radiation. It's surprising to learn that even little gadgets like paper shredders or electric power tools may produce enough radiation to obstruct communication.

Twisted copper wiring in pairs

The wiring utilised with communication systems is described in the third fact in the preceding section. There are three types of wiring that assist in lowering electrical noise interference. Twisted pair wire, also known as unshielded twisted pair wiring, is the first kind and is widely used in communications. Twisted pair wiring consists of two wires that are twisted together, as the name suggests. Of course, there is a plastic coating on each wire that serves to insulate the two wires and block the passage of electrical current. Unexpectedly, twisting two wires reduces their sensitivity to electrical noise compared to keeping them parallel. Figure 8.2 explains.

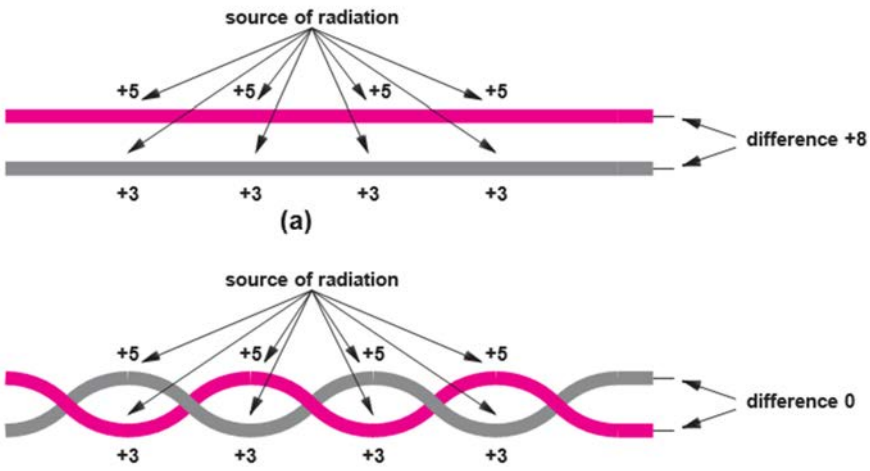


Figure 8.2 Effects of unwanted electromagnetic radiation on twisted pair wiring and two parallel wires, respectively.

As the image demonstrates, there is a strong likelihood that one of two parallel lines is located nearer to the electromagnetic radiation source than the other. One wire in particular often serves as a shield, absorbing some of the electromagnetic radiation. The second wire gets less energy as a result of being buried beneath the first wire. Each of the two examples receives a total of 32 units of radiation in the illustration. Why is equal absorption significant? The answer is that if interference produces ex- actly the same amount of electrical energy in each wire, no additional current will flow.

Coaxial cable and shielded twisted pair are examples of shielding.

Twisted pair wiring does not provide a complete solution, while being resistant to the majority of ambient radiation. Twisted pair often has issues with:

Very loud electrical noise

Physically close proximity to the noise source high-frequency communication uses. Even twisted pair may not be enough if the intensity is high (for example, in a facility where electric arc welding equipment is used) or communication cables are located near to the source of electrical noise. As a consequence, interference may occur if a twisted pair crosses a fluorescent light bulb in an office building and runs above the ceiling. Additionally, it is difficult to create equipment that can discriminate between legitimate high frequency signals and noise, which means that when using high frequencies, even a tiny quantity of noise may produce interference. Twisted pair wire may be used in cases when it is inadequate, but there are other wiring types that contain additional metal shielding. The wiring for cable television is the most well-known kind. The wiring is referred to as coaxial cable (coax), and it features a thick metal shield made of braided wires that fully encircles a core wire that transmits signals. The idea is shown in Figure 8.3.

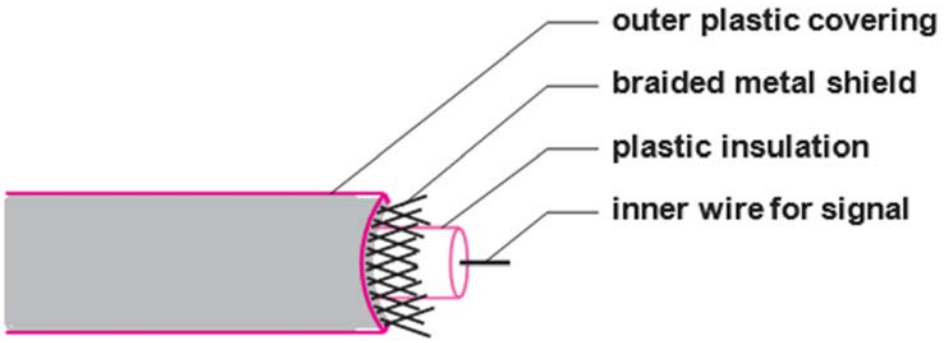


Figure 8.3 shows a coaxial cable with the signal wire encased in a shield.

A coaxial cable's shield encloses the inner wire in a flexible cylinder that acts as a shield against electromagnetic radiation coming from any angle. The obstacle also stops electromagnetic radiation from being radiated by signals on the inner wire that could affect adjacent cables. Hence, a coaxial cable may be utilised for high frequencies and positioned close to electrical noise sources and other wires. Coaxial cable is kept flexible by the use of braided wire rather than a solid metal shield, however the hefty shield does make coaxial cable less flexible than twisted pair cabling. Shielding variations have been developed that provide a compromise: the

cable is more flexible but has a modest reduction in its resistance to electrical noise. Shielded twisted pair is one common variant (STP). One or more twisted pairs of wires are surrounded by a metal shield that is thinner and more flexible on the cable. The shield in most STP cable models is made of metal foil, much to the aluminium foil used in cooking. Compared to coaxial cable, STP cable offers the benefits of being more flexible and less prone to electrical interference (UTP).

Types of Twisted Pair Cable

Twisted pair wiring used in the telephone network was first subject to standards set by the telephone companies. Twisted pair cables are utilised in computer networks, and more recently, three standards groups collaborated to develop standards for these cables. It's been a while since I've been here.

Light-based and optical fiber-based media

Three types of media are classified under the taxonomy in Figure 8.4 as using light energy to transmit information:

Laser fibres transmission via infrared directional lasers

The most significant kind of light-based medium is an optical fibre. A thin glass or translucent plastic strand enclosed in a plastic sheath makes up each fibre. One end of a conventional optical fibre is connected to a laser or LED that transmits light, while the other end is connected to a photosensitive device that detects incoming light. This configuration is used for communication in a single direction. Two fibres are utilised, one for information transmission in each direction, to offer two-way communication. A cable contains at least two fibres, and a cable used between big locations with many network devices may have several fibres. Optical fibres are often grouped into cables by wrapping a plastic cover over them.

An optical fibre is flexible enough to create a circle with a diameter less than two inches without breaking, despite the fact that it cannot be bent at a straight angle. The reason why light circumnavigates a fibre bend is a mystery. Physics provides the solution, explaining that when light hits a border between two substances, its behaviour is influenced by the densities of the two materials as well as the angle at which the light is incident on the boundary. There is a critical angle,, measured with respect to a line perpendicular to the boundary, for a particular pair of substances. Light goes along the border if the angle of incidence is exactly equal to the critical angle. Light passes the border and is refracted when the angle is less than degrees, and when the angle is larger than degrees, light is reflected as if the barrier were a mirror. The idea is shown in Figure 8.4.

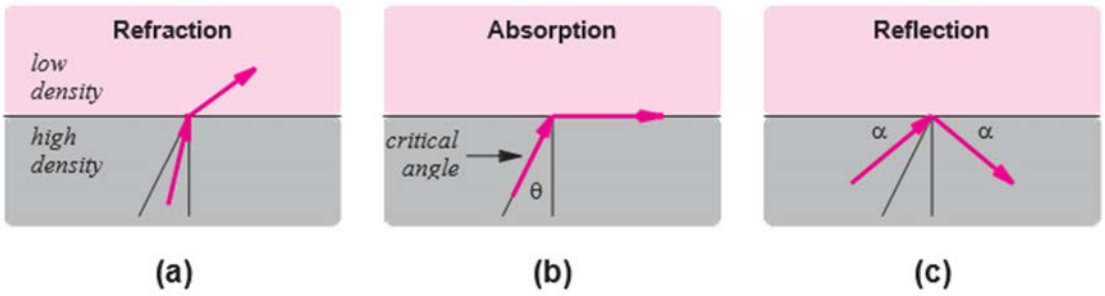
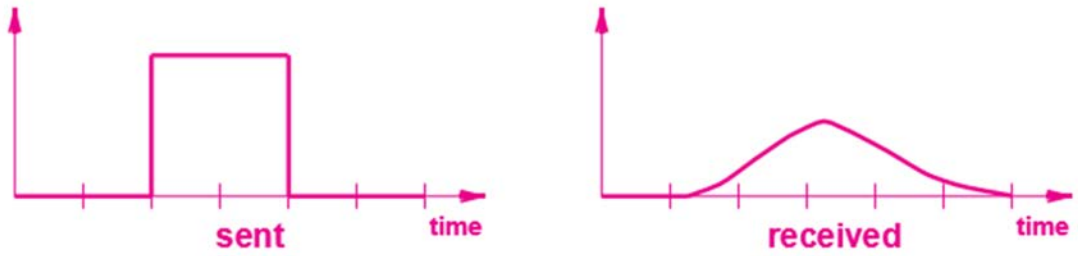


Figure 8.4: shows the behaviour of light at a density boundary for angles of incidence that are (a) less than, (b) equal to, and (c) larger than the critical angle.

The reason why light remains within an optical fibre is seen in Figure 8.4c. A material called cladding is glued to the fibre to create a barrier. Light is reflected from the barrier as it moves along.

Sadly, there are certain imperfections in optical fibre reflection. A little quantity of energy is absorbed through reflection. Also, a photon that travels in a zigzag pattern and encounters several reflections off the fiber's walls will cover a little more ground than one that follows a straight route. As a consequence, as shown in Figure 8.5, a pulse of light transmitted at one end of a fibre emerges with reduced energy and is scattered (or stretched) over time.



Graph 8.5: An optical fibre transmits and receives a light pulse.

Dispersion doesn't provide a difficulty for optical fibres used to link a computer to a local device, but it poses a significant issue for long optical fibres, such as those used to connect two cities or run under the Atlantic Ocean. In order to balance performance and cost, three types of optical fibres have been developed:

The cheapest fibre is multimode, Step Index fibre, which is utilised when performance is not a concern. Because of the abrupt transition between the fibre and the cladding, light reflects often. Dispersion is high as a result. Step index fibre is somewhat less costly than multimode, graded index fibre. Yet, it has the benefit of having the den- sity of the fibre grow at the edge, which decreases reflection and lowers dispersion. The fiber's reduced diameter and other features contribute to a reduction in reflection. Long distances and greater data rates need single mode.

Varieties of Fiber and Light Transmission

Light is focused by single mode fibre and the hardware employed at either end. A pulse of light may thus cover distances of thousands of kilometres without dispersing. Since a pulse corresponding to one bit does not spread into the pulse corresponding to an additional bit, minimal dispersion helps enhance the pace at which bits may be delivered. The fiber's compatibility with the transmission equipment is crucial. The options for mechanisms are:

Transmission: Injection laser diode or a light-emitting diode (LED) (ILD).

Reception: a photodiode or a photosensitive cell. In general, single mode fibre is utilised across long distances with high data rates, necessitating ILDs and photodiodes. Multimode fibre is often used for short distances and slower bit rates.

Copper Wiring Vs Optical Fiber

Optical fibre is preferable than copper cable due to a number of factors. Electrical signals flowing via copper do not attenuate as much as those going across optical fibre, which also has a larger bandwidth and is resistant to electrical noise. Copper wiring is less costly, however.

Copper wire installation does not need the same specialised tools or knowledge as optical fibre installation since optical fibre ends must be polished before they can be utilised. Copper wires are also less prone to break if tugged or bent accidently due to their strength.

Technologies for Infrared Communication

Similar to how a conventional television remote control emits energy, infrared (IR) communication technologies employ electromagnetic radiation that looks like visible light but is invisible to the human eye. Frared dissipates fast, much like visible light. A smooth, hard surface may reflect infrared signals, but an opaque material as thin as a sheet of paper or atmospheric moisture can block the signal.

The most often used infrared technology is meant to link a computer to a nearby peripheral, such as a printer. Both the computer's interface and the printer's interface transmit infrared signals that span an arc of about 30 degrees. Each gadget can pick up the signal of the other as long as they are aligned. With laptop computers, infrared's wireless aspect is particularly appealing since it allows users to walk about a room while still having access to a printer. The three most often used infrared technologies are listed in Figure 8.8, together with the data rates that each one allows.

Point-to-point laser communication

The infrared methods mentioned above may be categorised as delivering point-to-point communication since they link two devices with a beam that follows the line of sight. Several point-to-point communication technologies exist in addition to infrared. One method of point-to-point communication makes use of a laser-produced coherent light beam. Similar to infrared, laser communication relies on a clean, unobstructed channel between the communicating locations and follows line-of-sight. A laser beam does not, however, cover a large region as an infrared transmitter does. Instead, there are just a few beams.

Broad by centimetres: In order to ensure that the sender's beam reaches the sensor in the receiver's equipment, the sending and receiving equipment must be exactly aligned. Two-way communication is required in a typical communication system. As a result, both transmitters and receivers are required on either side, and they must be carefully aligned. As alignment is so important, point-to-point laser equipment is often permanently placed.

In comparison to infrared, laser beams have the benefit of being acceptable for outdoor usage and having a wider range. As a consequence, cities may communicate from one building to another via laser technology. Consider a large firm that has offices in two nearby structures. A company is not allowed to run cables between buildings over roadways. However, a firm may acquire laser communication equipment and permanently put the equipment, either on the sides of the two buildings or on the roofs. The operational expenses are generally modest after the equipment has been bought and installed.

Radio and Electromagnetic Communication

Remember that the word "unguided" refers to communication techniques that allow energy to spread without the need for a carrier like a wire or optical fibre. Wireless networking systems that use electromagnetic energy in the Radio Frequency (RF) band make up the most prevalent kind of unguided communication mechanisms. As RF radiation can travel great distances and penetrate solid items like building walls, it has a unique advantage over light transmission.

The frequency affects the precise characteristics of electromagnetic radiation. The range of potential frequencies is referred to as the "spectrum," and governments all around the globe

assign certain frequencies to different uses. The Federal Communications Commission in the United States establishes guidelines for frequency distribution and sets restrictions on the maximum power that communication equipment may produce at each frequency. The total electromagnetic spectrum and the fundamental properties of each component are shown in Figure 8.6. One portion of the spectrum, as seen in the image, corresponds to the previously mentioned infrared light. The spectrum utilised for RF communications comprises frequencies designated for radio and television broadcast, satellite, and microwave communications, and ranges in frequency from around 3 KHz to 300 GHz.

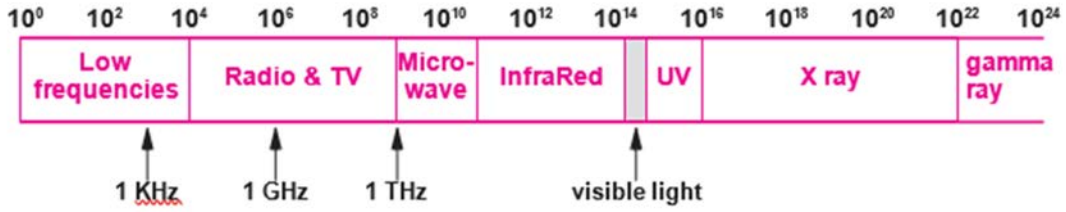


Figure 8.6: shows the main frequencies of the electromagnetic spectrum on a log scale.

Signal Propagation

The frequency of an electromagnetic wave determines how much information it can carry. An electromagnetic wave's frequency affects its propagation as well. As the lowest frequencies of electromagnetic radiation follow the earth's surface, it should be able to locate a receiver from a transmitter beyond the horizon if the terrain is relatively flat. A transmitter and receiver may be farther apart when using medium frequencies since the signal can bounce off the ionosphere on its way between them. The signal travels in a straight line from the transmitter to the receiver at the highest frequencies of radio transmission, therefore the route has to be clear of obstacles.

Following are two major categories into which wireless technologies are divided: Terrestrial. a few s. swiping the swiping the swiping the swiping swiping s sp. sp. The summits of hills, man-made towers, and large buildings are typical places for antennas or other equipment. Nonterrestrial. Outside of the earth's atmosphere, some communication equipment is utilised. Various wireless technologies are presented together with descriptions of their individual features. For now, it is sufficient to know that properties such as whether the signal may pass through solid objects depend on the frequency and power employed, as well as the speed at which data can be delivered, the greatest distance over which communication is possible, and other factors.

Satellite Types

The velocity of an object that circles the earth is governed by the rules of physics, notably Kepler's Law. In particular, the period (i.e., time necessary for a full orbit) depends on the distance from the earth. In light of this, communication satellites are divided into three major groups according to how far they are from the planet.

GEO communication satellites:

The fundamental trade-off in communication satellites is between height and period. The main benefit of a satellite in geostationary earth orbit (GEO) is that the orbital period coincides perfectly with the speed of earth rotation. A GEO satellite, when placed above the equator, is always at the same spot above the surface of the globe. If a satellite is immobile, it never needs

to move after a ground station has positioned itself in front of it. The principle is shown in Figure 8.7.

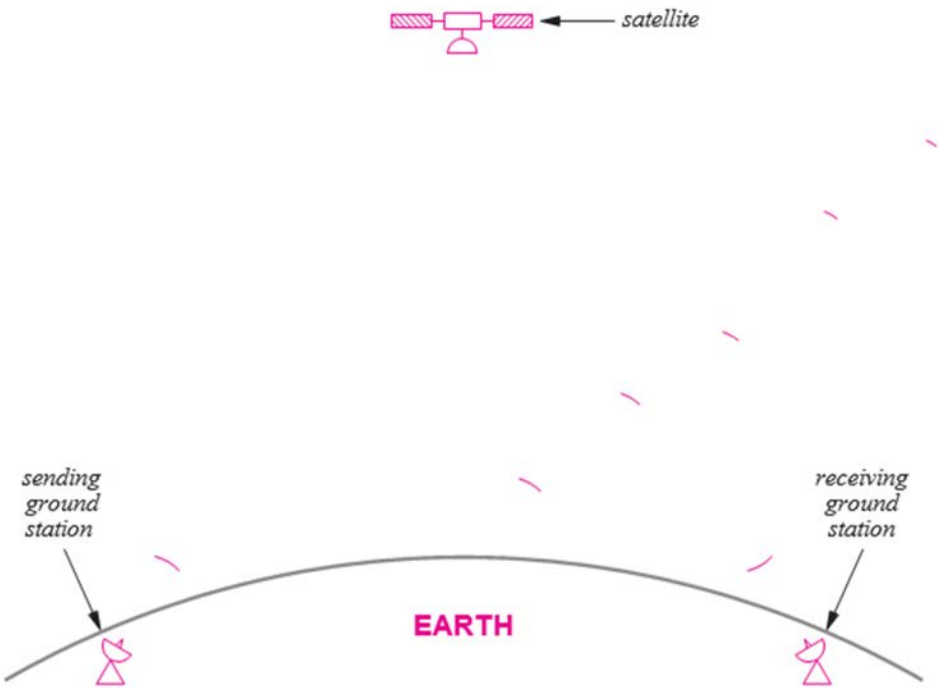


Figure 8.7: A GEO satellite and ground stations are permanently aligned.

Sadly, a geostationary orbit requires a distance of 35,785 kilometers or 22,236 miles, which is about one-tenth the distance to the moon. Consider a radio signal going to a GEO satellite and back to see what such a distance implies for communication. The distance travelled in 0.238 seconds at the speed of light, or 3 108 metres per second.

Even while it may not seem like much, certain apps might benefit from a delay of around 0.2 seconds. A human may detect a 0.2 second delay during a phone conversation or visual teleconference. Delaying an offer by 0.2 seconds might represent the difference between a successful and failed offer for electronic transactions like a stock exchange issuing a certain set of bonds.

Covering Of the Planet:

The maximum number of GEO communication satellites is how many? The geosynchronous orbit above the equator has a finite quantity of "space" because communication satellites must be spaced apart from one another in order to prevent interference. The angular separation may need to be between 4 and 8 degrees, depending on the wattage of the transmitters. So, without more advancements, only 45 to 90 satellites can be placed in the complete 360-degree circle over the equator. How many satellites would be required to completely cover the planet? Three. See Figure 8.8, which shows the globe with three GEO satellites orbiting it at a distance of 120 degrees, to understand why. The diagram shows how the three satellites' transmissions reach the whole globe. The size of the planet and the separation between the satellites are shown in the image at scale.

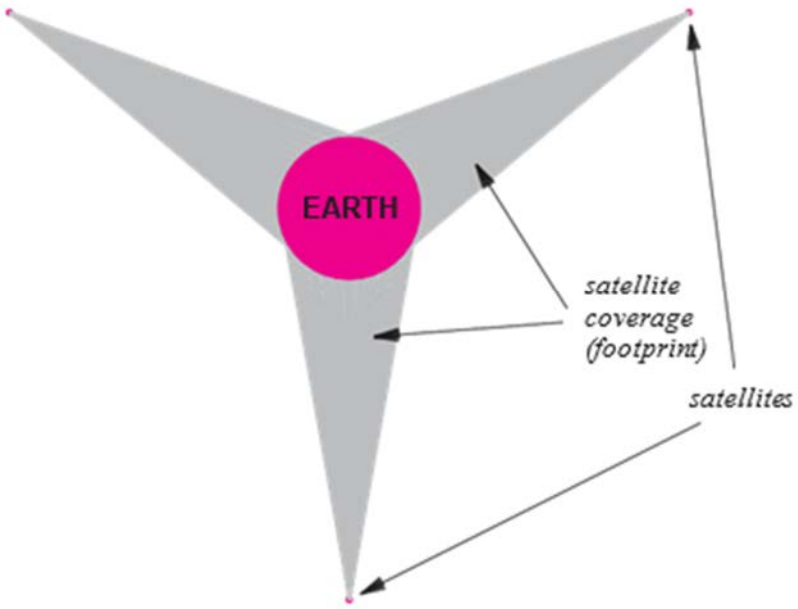


Figure 8.8: The world may be covered by the transmissions from three GEO satellites.

Satellites in Low Earth Orbit (LEO) and Complexes

Low Earth Orbit (LEO), which is defined at heights up to 2000 Kilometers, is the main alternative to GEO for communication. Practically speaking, a satellite must be positioned above the atmosphere's edge to prevent the drag caused by coming into contact with gases. LEO satellites are so often positioned at 500 Kilometres or higher in height. Short delays (usually 1 to 4 milliseconds) are a benefit of LEO, but there is a drawback—a satellite's orbit does not revolve around the planet. An LEO satellite seems to move across the sky from an observer on the earth, therefore a ground station needs an antenna that can rotate to monitor the satellite. Given how quickly satellites move, tracking is challenging. The earth is orbited by the lowest LEO satellites in around 90 minutes, whereas the highest LEO spacecraft take several hours.

Clustering or array deployment is the basic method utilised with LEO satellites. LEO satellite constellations are made to cooperate in vast numbers. A satellite in the group may interact with other satellites in the group in addition to terrestrial stations. The group members maintain contact and agree to forward communications as necessary. Think about what occurs, for instance, when a person in Europe sends a message to a user in North America. The message is sent to the satellite currently in orbit from a base station in Europe. The satellites in the group communicate to send the message to the one that is presently passing over a ground station in North America. The message is then sent to a ground station by the satellite that is presently above North America.

Tradeoffs across Different Media Varieties

The selection of a media is difficult and requires careful consideration of many different aspects. The following items must be taken into account: Cost: supplies, installation, operation, and upkeep Data rate: the maximum bit rate that may be sent Delay: the amount of time needed for signal processing or propagation Attenuation and distortion are effects on the signal. Environment: Exposure to electrical noise and interference Security: Eavesdropping vulnerability

Measurement of Transmission Medium:

A signal's propagation delay is the amount of time it takes to go across a medium. The maximum data rate that the medium can support is known as channel capacity. A scientist by the name of Nyquist identified a fundamental connection between a transmission system's bandwidth and its ability to move data in the 1920s. The connection, sometimes referred to as the Nyquist Theorem, offers a theoretical upper limit on the rate at which data may be sent while taking noise into account.

CHAPTER 9

MODES OF TRANSMISSION

Jagdish Chandra Patni, Professor,
Department of Computer Science and Engineering, Jain (Deemed to be University)
Bangalore, India
Email Id- jagdish.cp@jainuniversity.ac.in

The basic ideas that underpin data communications are covered in this section of the work. By concentrating on the methods of data transmission, this continues the debate. This defines common terms, covers the key ideas of synchronous and asynchronous communication, and describes the benefits and drawbacks of parallelism. Subsequent demonstrate how these concepts are used in networks throughout the Internet.

A Classification of Transmission Methods

The method by which data is sent across the underlying media is referred to as the transmission mode. Transmission modes may be categorised into two basic groups: One bit is transmitted at a time in serial. Several bits are delivered simultaneously in parallel. We will show that the time of transmissions further categorises serial transmission. A general taxonomy of the transmission modalities discussed in this and shown in Figure 9.1.

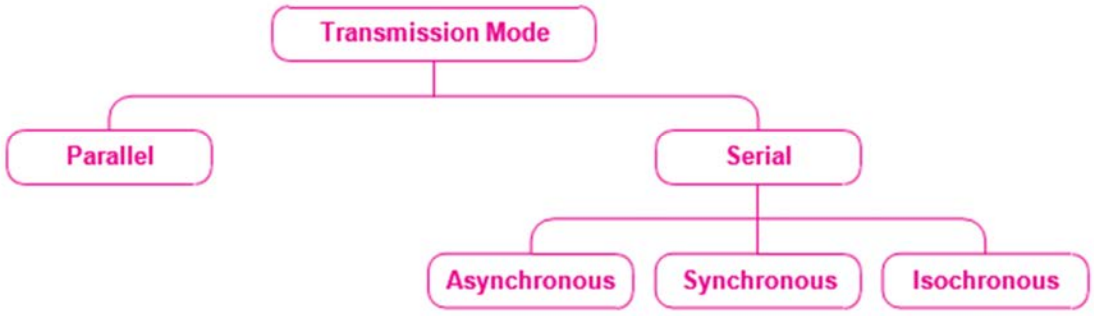


Figure 9.1: Taxonomy of transmission modalities.

A transmission method that sends several data bits simultaneously through various mediums is referred to as parallel transmission. In general, a wired media that employs several, separate wires is employed with parallel transmission. Also, each bit crosses each cable at the exact same moment thanks to the synchronisation of all the signals on all the wires. Figure 9.2 demonstrates the idea and explains why engineers refer to the wire as parallel. Every wire operates concurrently and carries the signal for one bit.

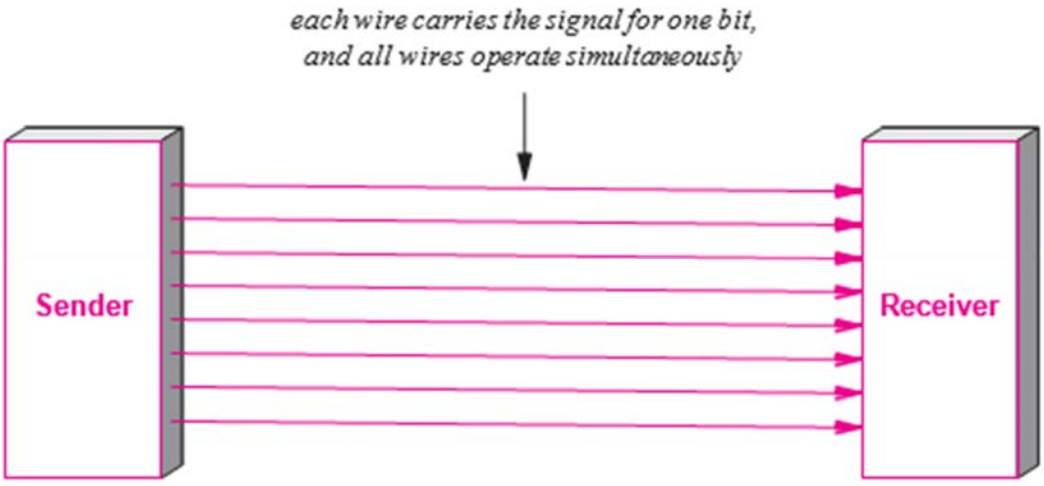


Figure 9.2 shows an example of parallel transmission using 8 lines to deliver 8 bits simultaneously.

Two crucial facts are missing from the figure. Secondly, a parallel interface often includes additional wires that enable the sender and receiver to cooperate in addition to the parallel wires that individually convey data. Second, the wires for a parallel transmission system are contained in a single physical cable to facilitate installation and troubleshooting. Hence, instead of a collection of separate physical wires, one anticipates seeing a single, substantial connection linking a sender and receiver.

Two key benefits of a parallel method of transmission are:

A parallel interface may work N times quicker than an identical serial interface because it can communicate N bits at once align with the underlying hardware. Hardware for computers and communications employs parallel circuitry inside. Hence, a parallel interface works well with the internal hardware.

Serial Communication

Serial transmission, which is an alternative to parallel transmission, transfers data one bit at a time. It may appear that anybody developing a data communications system would choose for parallel transmission given the focus on speed. Nonetheless, serial mode is the preferred communication method. There are mostly two causes. Secondly, since fewer physical cables are required and intermediary electrical components are less costly, serial networks may be extended over large distances at a significantly lower cost. Second, since there is only one physical wire utilised, there is never a timing issue brought on by one wire being a little bit longer than the other a difference of millimetres can be significant in a high speed communication system.

The transmitter and receiver must both include a tiny piece of hardware that transforms data from the parallel form used within the device to the serial form used on the wire in order to perform serial transmission. The setup is shown in Figure 9.3.

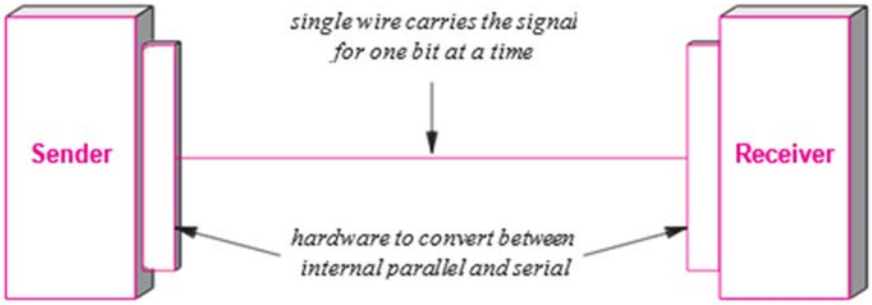


Figure 9.3. An example of a serial transmission mode

Depending on the kind of serial communication method used, the hardware required to convert data between an internal parallel form and a serial form might be simple or complicated. The conversion is carried out in the simplest scenario by a single Universal Asynchronous Receiver and Transmitter (UART) chip. The conversion for synchronous networks is handled by a comparable device called the Universal Synchronous-Asynchronous Receiver and Transmitter (USART).

Bits and Bytes in Transmission Order

Engineers refer to systems that transmit the LSB first as little-endian systems, and those that send the MSB first as big-endian systems. Either form may be used, but both parties must agree. It's interesting to note that the question of transmission order is not entirely answered by the order in which bits are transferred. Bytes are used to store data in computers, and each byte is further broken into bits (typically 8 bits per byte). As a result, selecting a bit order and byte order separately is conceivable. For instance, Ethernet technology mandates that data be sent in bit and byte big-endian formats. The sequence in which Ethernet transfers bits from a 32-bit amount is shown in Figure 9.4.

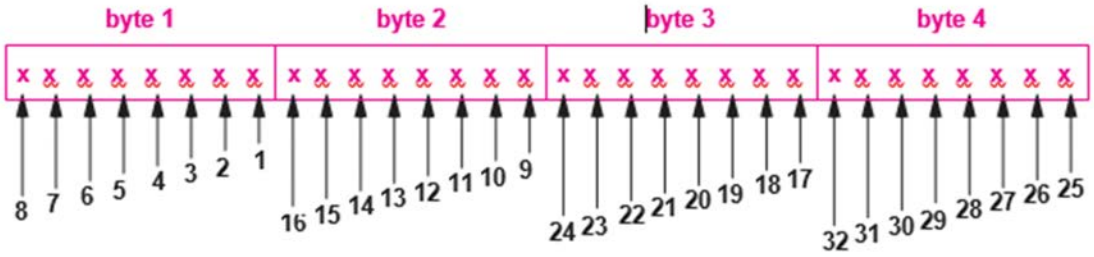


Figure 9.4: The least-significant bit of the most significant byte is delivered first, as seen in Figures illustration of byte big-endian, bit little-endian order.

Serial transmission timing

Depending on how transmissions are spread in time, serial transmission systems may be categorised into one of three basic categories:

A random delay may exist between the transmissions of two data items in asynchronous transmission, which can happen at any moment. There is no pause between the transfers of two data items while synchronised transmission is active. A predetermined pause separates each

transmission of two data items during isochronous transmission, which happens at regular intervals.

Transmission of Asynchronous Data

When a transmission system permits the physical medium to sit idle for any amount of time in between transmissions, it is referred to as being asynchronous a user typing on a keyboard or a user that clicks on a link to obtain a web page, reads for awhile, and then clicks on a link to obtain another page. A receiver cannot predict how long the medium will be idle until fresh data arrives while the medium is inactive due to a lack of coordination between the sender and receiver.

A few additional bits are often sent by the sender before each data item in asynchronous technologies to signal to the receiver that a data transfer is about to begin. The additional bits enable synchronisation of the receiver's circuitry with the incoming signal. The additional bits are referred to as start bits in certain asynchronous systems and preambles in others.

Asynchronous Character Transfer via RS-232

Consider the transmission of characters across copper wires between a computer and a device like a keyboard as an example of asynchronous communication. For character communication, the Electronic Industries Alliance (EIA) standard asynchronous communication technique has gained the greatest traction. The EIA standard, referred to as RS-232-C and sometimes shortened as RS-232, includes the physical connection (for instance, the connection must be fewer than 50 feet long), electrical details (for instance, the voltage ranges from -15 volts to +15 volts), and line coding (e.g., negative voltage corresponds to logical 1 and positive voltage corresponds to logical 0).

The RS-232 standard stipulates that each data item represents one character since it is intended for use with equipment like keyboards.

The circuitry may be set up to transmit seven-bit or eight-bit characters and to adjust the precise amount of bits per second. While a sender may wait for as long they like before transmitting a character, once transmission has started, a sender sends all of the character's bits consecutively and without pause. As soon as a character has finished transmitting, the transmitter leaves the wire with a negative voltage (equivalent to logical 1) until a new character is prepared for transmission.

How can a receiver determine the beginning of a new character? Before sending the bits that make up a character, RS-232 requires that a sender transmit an additional 0 bit, known as a start bit. Moreover, RS-232 mandates that a sender must leave the line unattended between characters.

At least as long as it takes to transmit one bit. So, one may imagine each character having a phantom 1 bit added to it. The phantom bit is referred to as a stop bit in RS-232 nomenclature. Figure 9.5 shows the voltage changes that occur when a start bit, eight character-specific bits, and a stop bit are communicated.

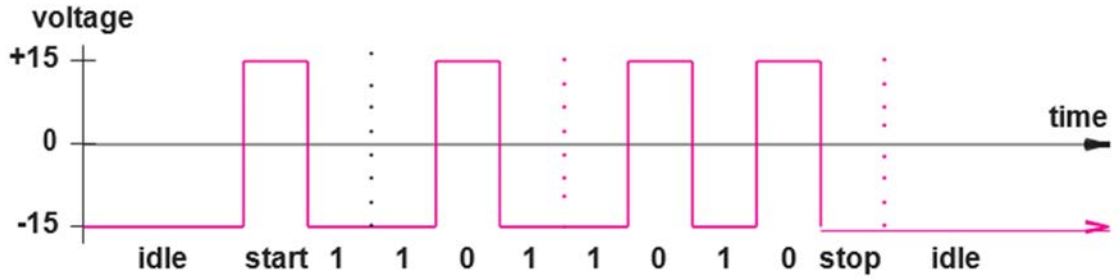


Figure 9.5 shows a voltage illustration during RS-232 transmission of an 8-bit character.

Synchronous transmission:

With the advent of the internet, the world has become a global village. A synchronous system sends data bits continuously, with no pauses in transmission, at the most fundamental level. In other words, the sender transmits a bit from the next data byte after broadcasting the last bit of the previous byte. The fundamental benefit of a synchronous mechanism is that there is minimal synchronisation overhead since the transmitter and receiver are always in sync. Compare the transmission of 8-bit letters on an asynchronous system, as shown in Figure 9.5, with a synchronous transmission system, as shown in Figure 9.6, to comprehend the overhead. Even if no idle time is introduced, each character delivered via RS-232 needs an additional start bit and stop bit, making each 8-bit character require at least 10 bit times. Each character is conveyed on a synchronous system without any start or stop bits.

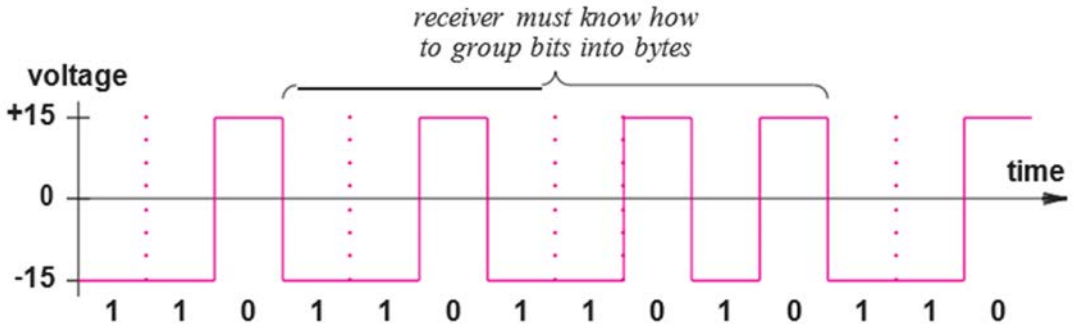


Figure 9.6: The initial bit of a byte immediately follows the final bit of the preceding byte in synchronous transmission.

Frames, Bytes, and Blocks

What happens if a sender does not always have data ready to transmit if the underlying synchronous mechanism requires constant bit sending? The solution may be found in a framing technique, which involves adding an interface to a synchronous mechanism that takes and delivers a frame, or block of data. A frame begins with a specific set of bits that ensures the sender and receiver remain in sync. A unique idle sequence (sometimes known as an idle byte) is also included in the majority of synchronous systems and is sent whenever the sender has no data to deliver. The idea is shown in Figure 9.7.

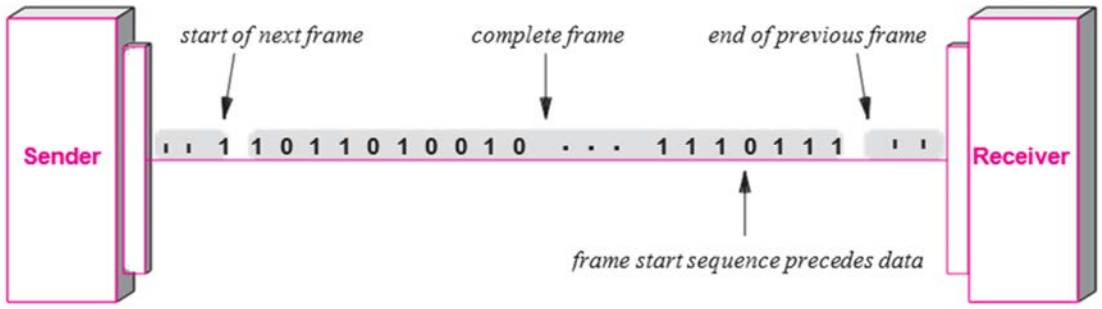


Figure 9.7: Framing on a synchronous transmission system

The effect of framing may be summed up as follows:

Synchronous Transfer

A new underlying mechanism is not offered by the third kind of serial transmission technology. It may be thought of as a significant application of synchronous transmission. The technology, often referred to as isochronous transmission, is intended to provide constant bit flow for multimedia applications that include speech or video. It is crucial to provide this data at a constant pace since jitter, or fluctuations in latency, might interfere with receipt (i.e., cause pops or clicks in audio or make video freeze for a short time).

An isochronous network is made to receive and transmit data at a predetermined rate, R, as opposed to leveraging the presence of data to drive transmission. In actuality, the network's interface requires that data be provided to it for transmission at precisely R bits per second. For instance, a voice-transfer isochronous mechanism runs at a rate of 64,000 bits per second. A receiver must be able to accept and play the stream, and a transmitter must continually produce digital audio.

An underlying network has the option to employ framing and decide to send additional information along with data. Yet in order for a system to be isochronous, it must be built such that both the transmitter and the receiver view a continuous stream of data, without any additional delays at the beginning of a frame. As a result, an isochronous network that offers a data rate of R bits per second often includes an underlying synchronous mechanism that runs at a bit rate that is a little bit higher than R bits per second.

Transmission in Simplex, Half-Duplex, and Full-Duplex

Depending on the direction of transmission, a communication channel might be one of three types:

Full-Duplex Simplex Half-Duplex

Simplex. The best of the best, the best of the best. A simplex mechanism can only transport data in one way, as the name suggests. Since it includes a transmitting device (such as an LED or laser) at one end and a receiving device (such as a photosensitve receptor) at the other, a single optical fibre, for instance, functions as a simplex transmission mechanism. Simplex transmission is equivalent to broadcast radio or television. Simplex communication is shown in Figure 9.8a.

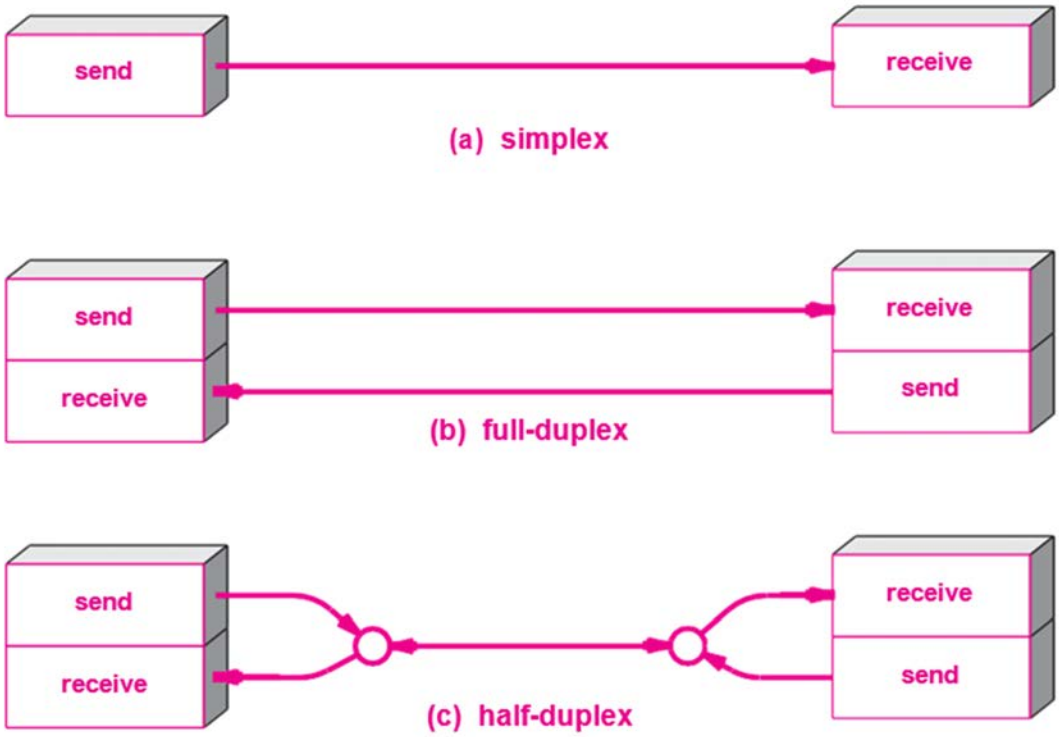


Figure 9.8: Three operating modes

Full-Duplex. A full-duplex method is also simple since the underlying system permits simultaneous transmission in both directions. As shown in Figure 9.8b, a full-duplex mechanism typically consists of two simplex mechanisms, one of which carries information in each direction. For instance, by running two optical fibres in parallel and setting up data transmission in the opposite directions, a pair of them may be employed to provide full-duplex communication. Full duplex communication may be compared to a spoken telephone discussion in which one party can talk while the other can hear background music.

Half-Duplex. A shared communication channel is necessary for a half-duplex mechanism. It is possible to communicate in both directions via the shared media, but it is not possible to do so at the same time. Using walkie-talkies where only one side may broadcast at once is an analogy for half-duplex communication. In order to ensure that only one side communicates at any one moment during a half-duplex transmission, an extra mechanism is required at either end.

DCE and DTE Hardware

In order to differentiate between the terminal equipment owned by a subscriber and the communications equipment held by the phone company, AT&T first coined the phrases Data Communications Equipment (DCE) and Data Terminal Equipment (DTE). The terms are still used: if a company rents a data circuit from a phone company, the phone company will install DCE equipment at the firm and the company will buy DTE equipment that connects to the phone company's equipment. From a scholarly perspective, equipment ownership is not the key idea behind the DCE-DTE distinction. Instead, it resides in the capacity to create a temporary user interface. For instance, the DCE equipment may provide a synchronous or isochronous interface to the user's equipment depending on whether the underlying network supports synchronous transmission. Figure 9.9 provides an illustration of the conceptual structure.

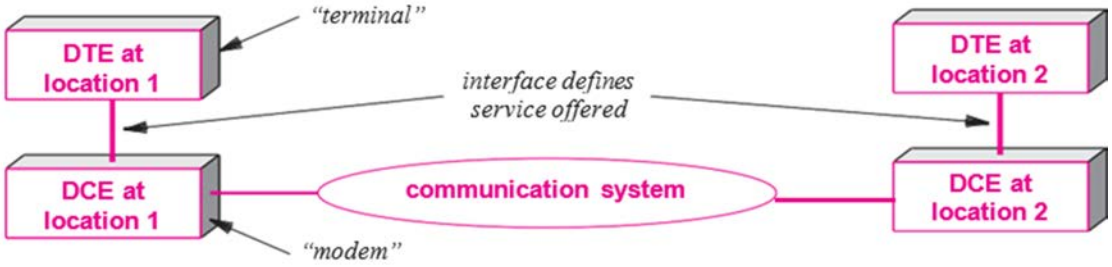


Figure 9.9: A communication service between two sites is shown in Figure by data communications equipment and data terminal equipment.

There are several standards that outline a potential interface between DCE and DTE. For instance, it is possible to utilize both the RS-232 standard discussed in this and the RS-449 standard suggested as a successor. A standard called X.21 is furthermore available.

CHAPTER 10

MODULATION AND MODEMS

Gaurav Londhe, Associate Professor,
Department of Computer Science and Engineering, Jain (Deemed to be University)
Bangalore, India
Email Id- gaurav.londhe@jainuniversity.ac.in

A different facet of data transfers. Information sources, how a signal might represent information, and types of energy employed with different transmission mediums are all covered in this section.

Propagation, Frequency, and Carriers

A carrier is an electromagnetic wave that continually oscillates and is used in many long-distance communication systems. Little adjustments are made to the carrier by the system to reflect the transmission of information. Understanding that electromagnetic energy's frequency affects how the energy propagates will help you to appreciate the significance of carriers. The aim to choose a frequency that would propagate successfully, regardless of the pace at which data is transferred, is one reason for the usage of carriers.

Methods for analogue modulation

We refer to modifications made to a carrier in accordance with the information being delivered as modulation. In theory, modulation produces a modulated carrier as an output from two inputs—a carrier and a signal. Essentially, a sender must alter a basic property of the wave. As a result, there are three main ways to modulate an electromagnetic carrier in accordance with a signal:

Modulation of amplitude Modulation of frequency Modulation via phase shift. The first two modulation techniques are the most well-known and have been used often. They were developed and utilised for broadcast radio and are still used for broadcast television, thus they did not start out as computer networks.

Intensity Modulation

Amplitude modulation is a method that modifies a carrier's amplitude in relation to the data being sent (i.e., according to a signal). The wave's amplitude fluctuates as the carrier oscillates at a constant frequency an analogue information stream, an unmodulated carrier wave, and the resultant amplitude modulated carrier. Since just the sine wave's amplitude (or magnitude) is altered, amplitude modulation is simple to grasp. Additionally, the signal's form may be seen in the time-domain graph of a modulated carrier. For instance, if one visualises an envelope as a curve connecting the sine wave's peaks, the resultant curve will resemble the signal. Frequency modulation is an alternative to amplitude modulation. When frequency modulation is used, the carrier's amplitude stays constant, but the carrier frequency varies depending on the strength of the signal: when the signal is greater, it rises slightly, and when the signal is weaker, it lowers slightly a carrier wave that has been modulated according to the signal's frequency.

As the illustration demonstrates, frequency modulation is harder to picture since minute variations in frequency are less obvious. When the modulation signal is stronger, one may see that the modulated wave has greater frequencies.

Modulation using phase shifts

A sine wave's phase, or the offset from a reference time at which it starts, is its third characteristic. Changes in phase may be used to represent a signal. To describe these shifts, we use the phrase phase shift.

While theoretically viable, modulating phase is seldom used to analogue signals. To see why, consider the fact that the following sine wave will begin a little bit later than when cycle k ends if there are any phase shifts after cycle k. A little delay seems like a frequency shift. Phase shift modulation may thus be seen as a particular kind of frequency modulation for analogue input. Yet, phase shifts will be crucial when a digital signal is used to modulate a carrier, as we will see. The variation in amplitude between a maximum and virtually zero. Although while it is simple to comprehend, the is a little deceptive since, in reality, modulation very minimally alters a carrier's amplitude dependent on a constant called the modulation index.

Consider Shannon's Theorem to comprehend why real-world systems do not permit a modulated signal to approach zero. The signal-to-noise ratio will decrease as the signal gets closer to zero, assuming the quantity of noise remains constant. In order to maintain the highest possible signal-to-noise ratio and enable the transmission of more bits per second, the carrier wave should be kept close to its maximum value.

Shift Keying, Digital Input, And Modulation

As was mentioned before, modulation is the process of modifying a carrier using an analogue information stream. It is necessary to consider "how digital input may be employed." Simple adjustments to the modulation schemes mentioned above provide the solution: digital systems utilise discrete values rather than modulation that is proportional to a continuous signal. Moreover, we refer to shift keying rather than modulation to differentiate between analogue and digital modulation. Shift keying basically works the same way analogue modulation does. Digital shift keying has a defined set of values rather than an infinite range of potential values. For instance, amplitude modulation enables a carrier's amplitude to fluctuate in response to changes in the signal being utilised by arbitrary tiny amounts. Amplitude shift keying, in contrast, employs a predetermined range of amplitudes. In the most straightforward scenario, a full amplitude may be equivalent to a logical 1 and a much lesser amplitude can be equivalent to a logical 0. Frequency shift keying typically employs two fundamental frequencies. Waveforms for Amplitude Shift Keying (ASK) and Frequency Shift Keying are produced using a carrier wave, a digital input signal, and these elements (FSK).

Keying in Phase Shift

While amplitude and frequency variations are effective for transmitting audio, unless a specific encoding method is utilised, both need at least one carrier wave cycle to transmit a single bit (e.g., unless positive and negative parts of the signal are changed independently). The Nyquist Theorem stated that if the encoding strategy allows several bits to be encoded in a single carrier cycle, the number of bits delivered per unit time may be increased. As a result, techniques that can convey more bits are often used in data communications systems. Phase shift keying, in particular, suddenly alters the carrier wave's phase to encode data. Phase shifts are used to describe each such transition. When a sine wave experiences a phase shift, the carrier keeps oscillating but quickly moves to a new spot in the sine wave cycle.

A constellation diagram with phase shift

How can phase shifts be used to encrypt data? In the simplest scenario, a sender and receiver may agree on the number of bits per second, and they can use a logical 1 in the absence of phase shift and a logical 0 in the presence of phase shift. A system may use a 180 phase shift,

for instance. To represent the precise assignment of data bits to certain phase changes, a constellation diagram is utilized.

Hardware is capable of more than just detecting phase shifts; a receiver can quantify how much a carrier moved during a phase change. As a result, it is conceivable to develop a communication system that can identify a number of phase shifts and utilise each one to represent a distinct amount of data. Systems are often built to employ a power of two shifts, allowing a sender to choose one of the shifts using bits of data.

There are several types of phase shift keying. Binary Phase Shift Keying (BPSK) is a kind of phase shift mechanism that, for instance, allows a sender to communicate one bit at a time. The two potential values are indicated by the notation 2- PSK. The version is sometimes referred to as a 4-PSK mechanism. The range of phase changes may theoretically be expanded to boost data flow. As a result, a 16-PSK mechanism has a bit rate that is twice as fast as a 4-PSK mechanism. Hardware's capacity to discriminate between slight variations in phase shifts is, however, constrained in practise by noise and distortion.

Quasi-Amplified Modulation

How can the data rate be raised if the hardware is unable to recognise arbitrary phase changes? The solution is found in a mixture of modulation methods that simultaneously alter two carrier properties. The most advanced technology combines phase shift keying and amplitude modulation. The method, sometimes referred to as quadrature amplitude modulation (QAM), represents values by varying both phase and amplitude. We utilise amplitude as a function of distance from the origin to depict QAM on a constellation diagram. As in the constellation diagram for the 16QAM variation, where the amplitudes are shown by dark grey regions.

Modulation and demodulation hardware for modems

A hardware device known as a modulator receives a series of data bits and modifies a carrier wave in accordance with the bits; a demodulator accepts a modulated carrier wave and reconstructs the sequence of data bits that modulated the carrier. As a result, a modulator and a demodulator are needed at each end of the transmission channel for data transfer. The majority of communication systems in use today are full duplex, which means each site need both a modulator and a demodulator in order to transmit and receive data. Modulation and demodulation methods are combined into a single device known as a modem by manufacturers to keep costs down and make the pair of devices simple to install and use (modulator and demodulator). Modems are created to enable communication across great distances. A 4-wire circuit that connects two modems may span a whole building, several buildings on a corporate campus, or even multiple cities.

Radio Frequency and Optical Modems

Modems may be utilised with RF transmission, optical fibres, and other media in addition to dedicated lines. A pair of Radio Frequency (RF) modems, for instance, may be used to transmit data through radio waves, while a pair of optical modems can transmit data over two optical fibres. The idea is the same, even though these modems work over completely different medium than modems that utilise dedicated wires: at the sending end, a modem modulates a carrier; at the receiving end, data is retrieved from the modulated carrier.

DSL modems

Voice telephone systems are a fascinating additional use for modems. A dialup modem employs an audio tone as the carrier rather than an electrical signal. The carrier is modulated at the transmitting end and demodulated at the receiving end, much as in traditional modems. The

main difference between dialup and traditional modems, apart from the capacity to make and receive phone calls, therefore comes from the reduced bandwidth of audible tones.

When dialup modems were originally developed, the strategy made perfect sense: because the telephone system carried analogue signals, a dialup modem turned data into a modulated analogue carrier. Paradoxically, a contemporary telephone system has a digital inside. As a result, a dialup modem modulates an audible carrier on the sending side before transmitting it to the phone system. The phone system transfers the audio input into a digital form, digitises it, and then delivers the digitally transformed audio as analogue audio. The receiving modem obtains the original digital data by demodulating the analogue carrier. Dialup modems' satirical mix of analogue and digital transmissions. A dialup modem is often built inside a computer. We refer to an embedded device as an internal modem and a separate physical device as an external modem.

To increase the pace at which data may be delivered, dialup modems can also employ QAM, or quadrature amplitude modulation. It demonstrates the bandwidth available on a dialup connection, in order to comprehend why. The majority of telephone connections, as shown in the illustration, transfer frequencies between 300 and 3000 Hz, however a particular connection may not be able to handle the extremes. Dialup modems employ frequencies between 600 and 3000 Hz, which implies the usable bandwidth is 2400 Hz, to provide better reproduction and reduced noise. The data rate may be considerably raised using a QAM method. A V.32bis modem employs 128 different phase shift and amplitude shift combinations to provide a 14,400 bps data rate in each direction. This constitution. To identify the minute variation between a point in the constellation and a nearby point, sophisticated signal processing is required.

The Multiplexing Concept

We refer to combining information streams from several sources for transmission across a common means as multiplexing, and we refer to the device that makes this combination happen as a multiplexor. Similar to this, we refer to the process of splitting up a combination of information into individual information streams as demultiplexing, and we refer to the device that does the splitting as a demultiplexor. The concept of combining and splitting communication provides a basic base utilised in many aspects of computer networking. Multiplexing and demultiplexing are not limited to hardware or to individual bit streams. 11.1 The theory.

Each sender and recipient interact with only one another in the. Although each pair relies on autonomous communication, they all use the same transmission means. In order for the demultiplexor to separate the information for the receivers, the multiplexor mixes information from the senders for transmission.

The Primary Multiplexing Types

There are four fundamental methods for multiplexing, and each has a range of modifications and applications. Multiplexing by division multiplexing by wavelength multiplexing with time division:

Multiplexing with code division

There is a lot of application for time and frequency division multiplexing. A kind of frequency division multiplexing used with optical fibre is called wavelength division multi-plexing. Cell phone systems employ code division multiplexing, a mathematical technique. Since it serves as the foundation for broadcast radio, Frequency Division Multiplexing (FDM) is simple to comprehend. The fundamental idea comes from transmission physics: several radio stations may send electromagnetic signals concurrently without interfering with one another as long as

they each utilise a different channel (i.e., carrier frequency). The same approach is used by data communications systems when delivering several carrier waves over a single copper wire or when utilising wavelength division multiplexing to transfer different light frequencies over an optical fibre. A demultiplexor is used at the receiving end to apply a series of filters that successively extract a narrow band of frequencies close to one of the carrier frequencies. the organisation.

The filters used in FDM only look at frequencies is a crucial concept. The FDM mechanism will distinguish a certain carrier frequency from others without changing the signal if a transmitter and receiver pair is given that frequency. The simultaneous use of a transmission channel by several pairs of communicating entities is the main benefit of FDM. As though each pair had a unique physical transmission channel, we see FDM giving each pair a distinct transmission way. Of course, the range of frequencies that may be employed as channels is limited in any real FDM system. Interference may happen if the frequencies of two channels are too close together. Demultiplexing gear that receives a combined signal also has to be able to split it into individual carriers. The Federal Communications Commission (FCC) oversees broadcast radio stations in the US to ensure that carrier frequencies are spaced apart enough. The same strategy is used by designers of data communications systems, who choose a group of carrier frequencies with a guard band—a space—between them.

Consider the channel assignment in which each of the six channels is given 200 KHz with a guard band of 20 KHz in between as an example.

Why are blocks of frequencies allocated in the example if a carrier only utilises a single frequency? Consider the following common FDM features to comprehend the motivation:

Long-lived. Modern data communications precede FDM since early radio experiments gave rise to the notion of segmenting the electromagnetic spectrum into channels.

A lot of usage. The AMPS cellular telephone system, cable television, and broadcast radio and television all employ FDM.

Analog. Hardware for FDM multiplexing and demultiplexing receives and transmits analogue signals. FDM hardware considers a carrier as an analogue wave even though it has been modified to carry digital data.

Versatile. FDM is adaptable since it filters on frequency bands without analysing other facets of signals.

The versatility offered by the analogue feature outweighs the downside of making frequency division multiplexing subject to noise and distortion. Most FDM systems, in particular, provide each transmitter and receiver pair a selection of frequencies and the freedom to decide how to utilise them. Systems primarily use a variety of frequencies in two ways.

Increasing the data rate

A sender splits the channel's frequency range into K carriers and delivers 1/K of the data across each carrier to enhance the total data rate. A sender essentially uses frequency division multiplexing inside the allotted channel. In certain systems, the subdivision is referred to as subchannel allocation. Spread spectrum is a method used by a transmitter to enhance immunity to interference. Many versions of spread spectrum may be employed, but the main principle is to split the range of the channel into K carriers, broadcast the same data across numerous channels, and enable a receiver to accept a copy of the data that arrives with fewest mistakes. When noise is anticipated to interfere with certain frequencies at a particular moment, the technique performs very well.

A pyramidal FDM

Hardware's ability to change frequencies accounts for some of FDM's versatility. Multiplexing hardware may leave the first stage alone, map the second onto the range of 4 KHz to 8 KHz, map the third onto the range of 8 KHz to 12 KHz, and so on if a group of incoming signals all fall within the frequency range of 0 to 4 KHz. The method serves as the foundation for an FDM multiplexor hierarchy that maps each input to a wider, continuous range of frequencies.

Similarly with the, a group of twelve analogue telephone signals that range in frequency from 0 to 4 KHz make up the fundamental input. The signals are multiplexed at the first stage into a single signal known as a group that operates in the 0–48 KHz frequency range. The next step involves multiplexing five groups into a single supergroup that operates between frequencies 0 and 240 KHz, and so forth. 3600 telephone transmissions have been multiplexed into one signal at the very end.

Multiplexing by wavelength (WDM)

Frequency division multiplexing on optical fibre is referred to as Wavelength Division Multiplexing (WDM). The inputs and outputs of this kind of multiplication are light wavelengths, which are also known as colours and are represented by the Greek letter. Remember from elementary physics that the colours of the spectrum are dispersed when white light goes through a prism to get an understanding of how multiplexing and demultiplexing may function with light.

A prism may also function in the other direction; if a series of coloured light beams are all directed into it at the proper angle, the prism will combine the beams to create a single white light beam. Lastly, keep in mind that what we experience as colour is really a spectrum of light wavelengths.

The foundation of optical multiplexing and demultiplexing is prisms. A prism is used by a multiplexor to combine light beams of different wavelengths into a single beam, and by a demultiplexor to separate the wavelengths.

Multiplexing with time division (TDM)

The main FDM substitute is called Time Division Multiplexing (TDM). TDM is less esoteric than FDM and does not depend on unique electromag- netic energy characteristics. Instead, multiplexing in time merely refers to the transmission of data from one source, followed by data from a second source, and so on.

TDM synchronised

The term "time division multiplexing" refers to a broad idea that may take many different forms and is often used online. Hence, it just a conceptual viewpoint, and the specifics may change. As an example, the displays objects being delivered in a round-robin manner (i.e., an item from sender 1 followed by an item from sender 2, etc). While some TDM systems do, others do not employ round-robin order.

A second point is that not all TDMs fit this description. The displays a little space between the objects. If a communication system employs synchronous transmission, there is never a pause between bits. No gap between items happens in synchronous networks when TDM is used. Synchronous Time Division Multiplexing is the end outcome. Round-robin order is used in synchronous TDM systems to choose items. For a system with four senders, synchronised TDM functions.

Framing in the TDM version for telephone systems

To multiplex digital streams from many phone conversations across a single media, telephone systems employ synchronous TDM. In reality, the particular kind of TDM used to multiplex digital phone conversations is referred to as TDM by telephone providers.

An intriguing method to ensure that a demultiplexor maintains synchronisation with the multiplexor is included in the phone system specifications for TDM. See how a synchronous TDM system delivers slots one after another without indicating the output at which each slot occurs to comprehend the necessity for synchronisation. A little variation in the clocks used to time the bits may lead a demultiplexor to read the bit stream incorrectly since it is impossible for it to determine where a slot starts.

The TDM version used in the phone system has an additional input framing channel to avoid misunderstandings. Framing just inserts one bit into the stream every round as opposed to taking up a whole slot. A demultiplexor pulls data from the framing channel and examines other channels for alternating 0 and 1 bits. According to the theory, it is quite probable that the framing check will identify an error and let the transmission to resume if a mistake causes a demultiplexor to lose a bit using frame pieces.

Structured TDM

TDM may be organised in a hierarchy, much as FDM. A TDM hierarchy utilises N times the bit rate for each subsequent step, but an FDM hierarchy uses N times the frequencies for each successive level. Extra framing bits are added to the data, which implies that the bit rate of each subsequent tier of hierarchy is somewhat larger than the aggregate voice traffic. Compare the example FDM example to the example TDM hierarchy.

Synchronous TDM's Drawback Unoccupied Slots

If each source generates data at a consistent, fixed rate equal to 1/ N of the capacity of the common media, synchronised TDM performs well. For instance, data will come at a constant rate of 64 Kbps if the source is a digital phone call. Nevertheless, many sources provide data in bursts with periods of inactivity in between, which interferes with a synchronous TDM system. Think about the example to see why.

The sources on the left of the create data points at random in the. As a result, if the matching source has not generated an item by the time the slot needs to be delivered, the synchro- nous multiplexor leaves the slot empty. In reality, a slot can never be vacant since the underlying system must always be sending data. In order to signal that the value is invalid, an additional bit is set after the slot is as-signed with a value (such as zero).

TDM statistics

How can a multiplexing system use a shared media more effectively? Statistical time division multiplexing, sometimes referred to as statistical multiplexing, is one method to boost the total data rate. While the language is odd, the approach is simple: choose things for transmission in a round-robin way, but skip any sources that do not have data available, rather than leaving an empty slot. Statistical TDM requires less time to convey the same amount of data since unwanted slots are eliminated.

Statistical multiplexing incurs additional expense even if it doesn't leave open slots. Consider demultiplexing to see why. A demultiplexor in a synchronous TDM system is aware that each nth slot belongs to a specific receiver. The data in a specific slot in a statistical multiplexing system may relate to any receiver. Each slot must thus include information identifying the recipient to whom the data is being transferred in addition to the data itself.

Multiplexing in reverse

When various transmission mediums are the sole means of connecting two sites, but none of them has an adequate bit rate, multiplexing takes on an intriguing new twist. Service providers, for instance, need greater bit rates than are accessible at the Internet's core. Multiplexing is employed in reverse to address the issue: split a high-speed digital input over a number of lower-speed circuits for transmission, then combine the outcomes at the receiving end.

In actuality, one cannot simply link the components of a typical multiplexor backward to create an inverse multiplexor. Hardware should instead be created so that sender and receiver may agree on how data coming from the input will be distributed across slower connections. More importantly, the system must be designed to manage situations when one or more of the slower connections have higher delay than others in order to guarantee that all data is sent in the same order as it came. Inverse multiplexing is often used on the Internet despite being complicated.

Multiplexing with code division

Code Division Multiplexing is a last kind of multiplexing that is utilised for certain satellite communications as well as a portion of the cellular telephone network (CDM). Code Division Multi-Access is the name of the particular version of CDM utilised in mobile devices (CDMA).

CDM does not depend on physical characteristics like frequency or time, unlike FDM and TDM. Instead, CDM is based on an intriguing mathematical principle that enables interference-free addition and subtraction of values from orthogonal vector spaces. The most straightforward version is that utilised in the telephone network. The unique binary code Ci that serves as each sender's signature is referred to as a chip sequence. Chip sequences that are orthogonal vectors are chosen (i.e., the dot product of any two chip sequences is zero). Each sender has a value to communicate, Vi, at any given moment. Each sender multiplies Ci by Vi and sends the results. In essence, the values are added up as the senders broadcast simultaneously. A receiver multiplies the total by Ci to get value Vi.

Consider an example to help the idea become clearer. We will use a chip sequence that is just two bits long and data values that are four bits long in order to make the example simple to understand. The chip sequence is seen as a vector. The result of multiplying the chip sequence by the vector is treated as a sequence by the receiver, which transforms it to binary by reading positive values as binary 1 and negative values as binary 0. Receiver number 1 then calculates:

Keep in mind that V1 should have a value of 1010. Receiver 2 will take V2 from the same broadcast in the meanwhile. It would seem that CDM provides few genuine advantages over TDM. In fact, even if just a few senders transmit over a given time, CDM is fairly inefficient since a lengthy chip sequence is necessary. Hence, statistical TDM performs better than CDM when usage is low.

The benefits of CDM come from its capacity to scale and from the fact that it provides less latency in a network that is heavily used. Consider a statistically tuned TDM system to see the significance of low delay. A TDM multiplexor gives the initial sender another opportunity after N-1 additional senders have had a chance to broadcast. The possible latency between subsequent broadcasts from a particular sender may thus be significant if all senders are active. Yet in a CDM system, a sender may communicate concurrently with other senders, which reduces the latency. As a telephone service must transmit high-quality speech, a minimal transmission latency makes CDM particularly appealing.

A key idea in data transmission is multiplexing. Pairs of senders and receivers may communicate across a common medium thanks to a multiplexing technique. A demultiplexor

separates and distributes the inputs that a multiplexor has multiple senders transmit via a common channel.

The four fundamental methods of multiplexing are code division, wavelength division, time division, and frequency division. Division by Frequency With the use of many channels, each of which corresponds to a different frequency of electromagnetic radiation, multiplexing (FDM) allows for simultaneous communication. A kind of frequency division multiplexing called wavelength division multiplexing (WDM) delivers different light frequencies via an optical cable.

One item is sent across the shared medium at a time using Time Division Multiplexing (TDM). A Synchronous TDM system often uses round-robin selection to send information without any idle time in between. A statistical TDM system skips any sender that does not have an item prepared to transmit during its turn in order to prevent empty spaces.

In order to allow several senders to communicate simultaneously and without interference, code division multiplexing (CDM) employs a mathematical combination of codes. The capacity to grow with little delay accounts for the majority of CDM's benefits.

CHAPTER 11

TECHNOLOGY FOR ACCESS AND CONNECTIVITY

Ramesh S, Professor,
Department of Computer Science and Engineering, Jain (Deemed to be University)
Bangalore, India
Email Id- ramesh.s@jainuniversity.ac.in

The provides instances of circuits that common carriers provide to companies and Internet service providers, as well as expanding on the concept of the telephone system multiplexing hierarchy. By taking multiplexing and data rates into account, the discussion concentrates on the technologies' data communications features.

Technologies for Internet Access: Upstream and Downstream

An Internet subscriber (usually a private home or business) is connected to an Internet Service Provider (ISP), such as a telephone company or cable provider, using a data communications network known as Internet access technology. The majority of Internet users follow an asymmetric pattern, which is important to grasp in order to comprehend how access technology is created. An average household customer uses the Internet to receive more data than they provide. For instance, a browser transmits a URL, which is made up of a few bytes, to visit a web page. A web server replies with content, which may be hundreds of bytes of text or tens of thousands of bytes of an image. A company that operates a web server can see the reverse traffic pattern, where more data is sent than is received.

Data that is sent via the Internet from a service provider to a subscriber is referred to as downstream in the networking business, and data that is transferred from a subscriber to a service provider as upstream.

Technology for Narrowband and Broadband Access

Access to the Internet is made possible by several different technologies. Based on the data rate they provide, they may be split into two major groups:

Narrowband Broadband

While clarifies the distinction between a transmission medium's bandwidth and its data rate, the nomenclature used for access networks does not do so. Conversely, the networking sector often refers to data rate as network bandwidth. The designations narrowband and broadband, then, correspond to industrial practise.

Technology for Narrowband

In general, systems that transmit data at up to 128 Kbps are referred to as narrowband. For instance, 56 Kbps is the highest data rate that can be obtained through a dialup connection using the most advanced modem technology and the least raucous phone lines. Dialup is thus categorised as a narrowband technology. Similar to narrowband, slower-speed digital lines, analogue modem circuits, and some of the data services provided by telecommunications providers (like ISDN) are all narrowband.

Internet Technologies

Broadband, as a generic phrase, refers to technologies that provide high data speeds, albeit the precise line separating it from narrowband is hazy. Numerous experts claim that broadband technology can produce speeds more than 1 Mbps. Yet, providers such as telephone companies use the term broadband when they market a service that provides a greater rate than dialup. As a result, telephone companies sometimes claim that ISDN service, which offers 128 Kbps, is broadband.

The primary methods of broadband Internet access.

Regional Loop also ISDN

The physical link between a subscriber's location and a telephone company Central Office (CO) is referred to as a local subscriber line or local loop. It's crucial to conceive of a local loop as independent from the rest of the phone system in order to comprehend how it might be utilised. The local loop section of the phone system is made of twisted pair and often has a substantially larger bandwidth, even though the whole phone system is designed to provide each dialup call 4 KHz of bandwidth. In instance, a subscriber near a CO may have a local loop that may support frequencies higher than 1 MHz.

Telephone companies investigated methods to leverage the local loop to enable faster data connection as data networking grew more crucial. The Integrated Services Digital Network is one of the earliest initiatives by a phone operator to provide users extensive digital services (ISDN). From the perspective of a subscriber, ISDN provides three distinct digital channels, labelled B, B, and D (often written 2B + D). The D channel, which runs at 16 Kbps, serves as a control channel. The two B channels, each of which works at a speed of 64 Kbps, are intended to convey digitised speech, data, or compressed video. The D channel is often used by subscribers to request services, which are subsequently provided across the B channels (e.g., a phone call that uses digital voice). A single channel with an effective data rate of 128 Kbps may be created by bonding or combining both of the B channels. 128 Kbps appeared significantly quicker than dialup modems when ISDN was initially being discussed. ISDN is now only used in a few limited circumstances since newer local loop technologies provide better data speeds at cheaper costs.

Technology for Digital Subscriber Lines (DSL)

One of the key methods for offering high-speed data communication services over a local loop is digital subscriber line (DSL). The DSL variants. The abbreviation xDSL is used to refer to the set as a whole since the names only vary in the first word.

Technology for Digital Subscriber Lines (DSL) 203

The majority of residential customers utilise ADSL, which is the version that has been introduced the most broadly. Frequency division multiplexing is used by ADSL to split the local loop's bandwidth into three areas. Two zones provide data connectivity, while one region corresponds to conventional analogue phone service, sometimes referred to as Plain Old Telephone Service (POTS) in the business. The key is:

Properties and Adaptation of Local Loops

Since no two local loops have the same electrical properties, ADSL technology is complicated. Instead, the length of the cable, its diameter, and the quantity of electrical interference all affect how well a signal can travel. Consider two subscribers who reside in different areas of the same town. A commercial radio station's broadcast will produce interference at the frequency the station utilises if the telephone line going to the first subscriber passes close by. The frequency

that the radio station uses could be suitable for data on that subscriber's line if the second subscriber doesn't reside close to the same radio station. The second subscriber, however, can encounter interference on a different frequency. As a result, the ADSL designers were unable to choose a specific combination of carrier frequencies or modulation methods that would be effective in every local loop.

ADSL is adaptable to account for variations in local loop characteristics. In other words, when a pair of ADSL modems is switched on, they agree to communicate using methods that are best for the connection after probing the line to determine its features. In specifically, ADSL makes use of a method called Discrete Multi-Tone Modulation (DMT), which combines inverse multiplexing and frequency division multiplexing methods.

In order to perform frequency division multiplexing in DMT, the bandwidth is split into 286 distinct frequencies, or subchannels, with 31 subchannels designated for upstream data transmission and 255 subchannels designated for downstream data transfer. For control information, two upstream channels are set aside. Theoretically, each subchannel is operating a distinct "modem" with its own modulated carrier. The carriers are separated by 4.1325 KHz intervals to prevent signal interference. Moreover, ADSL avoids utilising the bandwidth below 26 KHz to ensure that its transmissions do not interfere with analogue phone signals. As ADSL begins, both ends investigate the available frequencies to see which ones are clear of interference and which ones encounter it. Together with choosing frequencies, the two ends evaluate the signal quality at each frequency and choose a modulation technique based on the quality. ADSL chooses a modulation strategy that encodes many bits per baud when the signal-to-noise ratio on a given frequency is good; it chooses a modulation method that encodes fewer bits per baud when the quality on a given frequency is poor.

The ADSL Data Rate

How quickly can ADSL function? On short local loops, ADSL may reach downstream speeds of 8.448 Mbps and upstream speeds of 640 Kbps. The effective upstream rate for user data is 576 Kbps since the network control channel, which is required, needs 64 Kbps. Under ideal circumstances, ADSL2 can download at rates of around 20 Mbps.

From the perspective of the user, adaptability has an intriguing characteristic: ADSL does not promise a data rate. Instead, ADSL can only promise to perform as well as the line conditions let its methods to accomplish. Lower data rates are experienced by subscribers whose local loop passes close to sources of interference or whose local office is located further away from them than customers whose local office is located close to the central office and whose local loop does not. As a result, the upstream rate ranges from 32 to 640 Kbps and the downstream rate from 32 to 8.448 Mbps.

The ADSL data rate only applies to the local loop connection between a subscriber and the telephone Central Office, which is an essential distinction to be aware of. The total data rates that a user encounters are influenced by a variety of different variables. For instance, the access method used to link the server's site to the Internet or the inter-mediate networks between the user's CO and the provider that manages the server may all have an impact on the effective data rate when a user accesses a web server.

Splitters and Installation for ADSL

Lifting a receiver may cause noise that interferes with DSL signals even though conventional analogue phones operate at frequencies below 4 KHz. ADSL employs a splitter, an FDM device, to divide the bandwidth by sending low frequencies to one output and high frequencies to another in order to ensure total isolation. An interesting fact about splitters is that they run without electricity since they are passive. A splitter is often installed when the local loop enters

a building or place of business. The splitter has two connections: one side goes into the POTS wire, the other into an ADSL modem.

An intriguing ADSL wiring variant has gained popularity. The alternate method, often known as DSL light, does not need a splitter to be put on the incoming phone line. Alternatively, DSL utilises the existing wire in the home, and a splitter has to be put between each telephone and the wiring in the house. The benefit of the alter-native method is that a subscriber may install DSL by inserting a telephone and a splitter into a wall socket.

Technology for Cable Modems

Telephone local loop wiring has intrinsic restrictions, despite the fact that technologies like ADSL provide data speeds that are far greater than were once considered practical. The electrical properties of twisted pair wire are the main issue. The wire is vulnerable to interference since it is not shielded, which significantly lowers performance for certain subscribers. Alternative wiring schemes have become increasingly significant as demand for higher bit rates has grown. For application in the local loop, several wireless and wired technologies have been developed.

Using the existing cable television infrastructure is one of the most alluring alternative access technologies. The media utilised in cable systems is coaxial cable, which has a large bandwidth and is less vulnerable to electromagnetic interference than twisted pair. In addition, frequency division multiplexing (FDM) is used by cable television networks to broadcast a number of entertainment channels at once.

With so many channels accessible, one may imagine that a cable operator could use each subscriber's own channel to send digital information. In other words, multiplex a channel (i.e., carrier frequency) onto the cable together with television signals by using a pair of cable modems, one in the CATV centre and the other at a subscriber's site.

Although though CATV systems have a lot of bandwidth, there isn't enough of it to support a frequency division multiplexing technique that extends a channel to every customer. To see why, consider the fact that a single cable provider may have millions of customers in a large urban area. Thus, using a different channel for each subscriber is not scaleable.

Cable systems combine FDM and statistical multiplexing to address the issue by allocating a digital communication channel to a group of subscribers (usually, everyone in a neighbourhood) (typically, every- one in a neighborhood). The address to whom a message has been sent is included in every message transmitted over the channel, which is given to each subscriber in turn. The modem of a subscriber listens to the allotted frequency, but before accepting a message, the modem confirms that the message's address corresponds to the address given to the subscriber.

The Cable Modem Data Rate

How quickly can a cable modem function? 52 Mbps downstream and 512 Kbps upstream are theoretical data rates that a cable network can sustain. In reality, the rate can be much lower. First off, a cable modem's data rate only applies to transmissions between the subscriber's location and the nearby cable office. Second, a set of N subscribers, whose size is determined by the cable provider, share the bandwidth. Because the effective data rate that each individual subscriber has access to changes over time, sharing the bandwidth with other subscribers may be disadvantageous from the perspective of the subscriber. In the worst situation, each subscriber will only have access to 1/N of the capacity if N users share a single frequency.

Installation of a cable modem

FDM-based cable systems make cable modem installation simple. In contrast to xDSL technologies, which use on splitters, cable modems connect directly to the ca- ble wiring. Data and entertainment channels won't interfere with one another thanks to the FDM hardware in cable modems and existing cable boxes.

Coax Fiber Hybrid

Hybrid Fiber Coax (HFC), a technology that offers high-speed data connections, is one of the most promising concepts (HFC). A hybrid fibre coax system, as its name suggests, combines coaxial cables and optical fibres, using coax for connections to individual subscribers and fibre for central facilities. An HFC system is fundamentally hierarchical. The network's most bandwidth-intensive sections employ fibre optics, while areas that can handle slower data rates use coax. A provider installs converters between optical and coaxial cable in each neighbourhood to execute such a system. Each device uses a coaxial cable to connect to nearby homes and an optical fibre to link back to the service provider.

The phrase feeder circuit is used in the cable industry to describe the connection to a single subscriber, whereas the term trunk is used to describe the high-capacity connections between the cable office and each neighbourhood area. Up to 15 kilometres can separate two trunk connections.

Access Methodologies Using Optical Fiber

Cable companies have put up a number of methods that either extend optical fibre all the way to each customer or use it in a hybrid system. (FTTC) Fiber to the Curb (FTTC). Given that it employs optical fibre for high capacity trunks, as the name suggests, FTTC is comparable to HFC. The plan is to run copper for the feeder circuits after running optical fibre near to the final subscriber. Because FTTC uses two media in each feeder circuit, it varies from HFC and enables the cable system to provide an extra service, like voice. Particularly in the United States and Canada, the technology is being used in select places.

FTTB (Fiber to the Building) (FTTB). The amount of bandwidth that enterprises will want and whether access technologies based on copper (even coaxial cable) will be adequate are two key issues. High upstream data speeds will be possible with FTTB thanks to the utilisation of optical fibre.

FTTH (Fiber to the Home) (FTTH). In contrast to FTTB, FTTH is an access technology that uses optical fibre to give home subscribers better downstream data speeds. Although FTTH offers faster upstream data rates as well, the focus is on a wide variety of entertainment and video channels.

FTTP, or fibre to the premises (FTTP). Both FTTB and FTTH are covered by the general term FTTP.

Terminology for Head-End and Tail-End Modems

A pair of modems are needed for an access technology, one at the subscriber's location and the other at the provider's location. The term "tail-end modem" refers to a modem used at the subscriber's location, whereas "head-end modem" refers to a modem used in the central office. Head-end modems are not standalone electronics. Instead, a sizable collection of modems is constructed as a single entity that can be managed, observed, and controlled. A cable provider's use of head-end modems is referred to as a cable modem termination system (CMTS) (CMTS). The Data over Cable System Interface Standards (DOCSIS) are a set of industry standards that

define both the data format that can be transferred and the messages that are used to request services (such as pay-per-view movies) (e.g., pay-per-view movies).

Access Technologies for Wireless

While technologies like ADSL or HFC can supply digital services to the majority of consumers, they are not capable of handling all situations. Rural areas are where the main issues are found. Consider a farm or a far-off village that is located kilometres from the closest city. The maximum distance for technologies like ADSL is exceeded by the twisted pair wiring used to supply telephone service to such places. Moreover, cable television service is less prevalent in rural locations.

Even in suburbs, the sort of connection that can be used by technologies like ADSL may be governed by technical limitations. For instance, it might not be viable to use high frequencies on telephone lines that have repeaters, bridge taps, or loading coils. Hence, even in locations where a local loop technology serves the majority of subscribers, it could not be compatible with all lines.

Broadband Connections at Internet Central

Access technologies, according to networking experts, take care of the last mile problem, which is defined as the link to a typical home subscriber or a small enterprise. The capacity of an access technology is adequate for a household subscriber or a small enterprise (industry uses the term Small Office Home Office or SOHO). More bandwidth is needed for connections to companies or connections between providers. Professionals use the word "core" to describe these connections in contrast to those found at the Internet's edge, and they refer to high-speed technologies as core technologies.

Consider a provider that serves 5,000 clients to gain an understanding of the data rates required for the core. Suppose the service provider employs access technology capable of delivering up to 2 Mbps per user. Think about what would occur if all subscribers attempted to download data simultaneously. 12.10 displays the total Internet traffic directed at the provider. What technology can a provider utilise to transmit data at a pace of 10 Gbps over large distances? A point-to-point digital circuit that was rented from a phone company holds the key to the problem. High-capacity digital circuits are accessible for a monthly fee, even though they were initially intended to be used internally in the phone system to carry data. A circuit can run between two buildings, across a city, or from one city to another because telephone companies are permitted to construct wiring that crosses municipal streets. The cost is determined by the circuit's data rate and the distance travelled.

DSU/CSU, Circuit Termination, and NIU

One must consent to abide by the terms of the telephone system, including the standards created for sending digitised voice, in order to use a leased digital circuit. It might seem that since computers are also digital, adhering to standards for digitised information would be simple. The standards for telephone system digital circuits are different from those used in the computer industry, though, as the telephone and computer industries originated independently. Thus, a unique piece of hardware is required to connect a computer to a digital circuit made available by a phone company. The device, also known as a Data Service Unit or Channel Service Unit (DSU/CSU), includes two functional components that are often assembled into a single chassis. Line termination and diagnostics are handled by the CSU component of the DSU/CSU device. For instance, the diagnostic circuitry in a CSU can check to see if the line has been disconnected. Moreover, a CSU has a loopback test function that enables it to send a copy of all data that passes through the circuit back to the sender without additional processing.

Computer engineers are surprised by a CSU's service, which forbids too many consecutive 1 bits. The usage of electrical signals necessitates the requirement to prevent excessive 1s. Engineers were particularly concerned that having too many continuous 1 bits would result in excessive current on the wire because the telephone company initially intended their digital circuits to function over copper lines. A CSU can either employ bit stuffing or an encoding that ensures balance, such as differential encoding, to prevent issues.

A DSU/DSU CSU's section manages the data. It converts data between the digital format required by the computer equipment of the customer and the digital format utilised on the carrier's circuit. The computer side's interface standard is based on how quickly the circuit runs. The computer can use RS-232 if the data rate is under 56 Kbps. The computer must have interface gear that can handle higher speeds for rates greater than 56 Kbps (e.g., hardware that uses the RS-449 or V.35 stan- dards).

A Net- work Interface Unit (NIU), which the phone company further provides, creates a barrier between the subscriber's equipment and the equipment held by the phone company. The boundary is referred to demark by the telephone company.

Standards for Digital Telephone Circuits

The digital transmission standards used by the phone company to carry digital phone calls are also used when a digital circuit is leased from that firm. The names of the standards for digital telephone circuits in the US start with the letter T and then a number. These are collectively referred to as the T-series standards by engineers. One of the most well-liked is called T1, and many small companies use a T1 circuit to transport data.

T-standards, regrettably, are not applicable everywhere. Japan used modified T-series standards, while Europe went with a somewhat different framework. The usage of the letter E helps to distinguish European standards. The telephone companies utilise a multiplexing hierarchy to combine many voice calls into a single digital channel, DS Terminology and Data Rates. As a result, the T standards' data rates have been selected so that they may each support a number of voice conversations. The capacity of circuits does not increase linearly with their number, which is an important point to keep in mind. For instance, the T3 standard specifies a circuit that has significantly higher capacity than three times that of T1. Finally, it should be remembered that phone companies do lease fractional T1 circuits, which are lines with lower capacity than those stated in the.

The T-standards, which define the underlying carrier system, must be distinguished from the standards that outline how to multiplex many phone calls onto a single connection in order to be technically accurate. The latter are referred to as DS standards, or Digital Signal Level standards. Similar to the T-standards, the names are written as the letters DS followed by a number. For instance, the terms DS1 and T1 refer to different services that can multiplex 24 phone calls onto a single circuit. Technically speaking, it is more accurate to refer to "a circuit running at DS1 speed" rather than "T1 speed" because DS1 sets the effective data rate. Few engineers actually try to differentiate between T1 and DS1 in practise. As a result, "T1-speed" is likely to be mentioned by someone.

Most powerful circuits (STS Standards)

Telephone companies have developed a number of standards for digital trunk circuits and use the term "trunk" to refer to a high-capacity channel. These standards, also referred to as Synchronous Transport Signal (STS) standards, define the specifics of high-speed connections. The data rates connected to different STS standards. As all data rates are listed in Mbps, it is simple to compare them. Data rates for STS-24 and higher are larger than 1 Gbps, it should be mentioned.

Specifications for Optical Carrier

The phone provider defines an equivalent set of optical carrier (OC) standards in addition to STS standards. The names of copper standards and optical standards. To be clear, there is a difference between the terms STS and OC: the STS standards refer to electrical signals utilised in the digital circuit interface (i.e., over copper), whereas the OC standards refer to optical signals that travel across fibre. Few professionals understand the difference, as is the case with other network terminologies. So, regardless of whether the circuit uses copper or optical fibre, one frequently sees networking specialists use the phrase "OC-3" to refer to a digital circuit that works at 155 Mbps.

The prefix C

The nomenclature used for Synchronous Transport Signal and Optical Carrier has one more aspect not mentioned above: an optional suffix of the letter C, which stands for concatenated. The suffix indicates a circuit without inverse multiplexing when it is present. In other words, an OC-3 circuit can be made up of a single OC-3C (STS-3C) circuit that works at 155.520 Mbps or it can be made up of three OC-1 circuits that each operate at 51.840 Mbps.

Is a single circuit running at maximum speed preferable to numerous circuits running at reduced speeds? Depending on how the circuit is being used, the answer may vary. In general, more flexibility is offered and inverse multiplexing hardware is not required when a single circuit is working at full capacity. More specifically, data networks are distinct from voice networks. High-capacity circuits are used in voice systems to combine smaller voice streams. Yet, there is only one data stream present in a data network. As a result, given the option, the majority of network designers would choose an OC-3C circuit over an OC-3 circuit.

Network for Synchronous Optics (SONET)

The phone companies established a broad set of standards for digital transmission in addition to the STS and OC standards already mentioned. The standards are referred to as Synchronous Optical NETwork (SONET) in North America and Synchronous Digital Hierarchy in Europe (SDH). Data framing, multiplexing of lower-capacity circuits into a high-capacity circuit, and the transmission of synchronous clock information are only a few of the specifics that SONET lays down. Due to the widespread use of SONET by carriers, if someone rents an STS-1 circuit, the carrier is likely to insist that SONET encoding be used on the circuit. How is the SONET frame format utilised on an STS-1 circuit, for instance.

There are 810 octets in each frame. Octets in the frame are separated into 90 "columns" in each of 9 "rows," as described by SONET. It's interesting to note that a SONET frame's size is influenced by the underlying circuit's bit rate. Yet, when utilised on an STS-3 circuit, each SONET frame has a capacity of 2430 octets.

? Remember that 8,000 PCM samples are recorded every second during digital telephony, which translates to one sample being taken every 125 microseconds. This will help you grasp the difference. The time is used by SONET to choose frame size. A frame is made up of 810 8-bit octets when transmitted at the STS-1 transmission rate of 51.840 Mbps, which results in a bit transfer rate of precisely 6480 bits per second. Similar to this, 2430 octets can be transmitted in 125 seconds using the STS-3 rate. The main benefit of making the frame size dependent on the circuit's bit rate is that it simplifies synchronous multiplexing, making it simple to combine three STS-1 SONET streams into a single STS-3 SONET stream while maintaining synchronisation.

Although SONET is the encoding strategy used by the majority of data networks on a single point-to-point circuit, the standard offers other options. In particular, it is feasible to create a

high-capacity, single-point-failure-tolerant counter rotating ring network utilising SONET technology. An add/drop mux is a device used by each station on the ring. The add/drop mux can be configured to accept additional data from a local circuit and add it to frames travelling over the ring in addition to forwarding received data across the ring. It can also be configured to extract data and deliver it to a nearby computer. When the ring breaks, the hardware recognises the loss of frame data and reconnects using the counter rotating ring.

CHAPTER 12

LOCAL AREA NETWORKS: PACKETS, FRAMES

Rajesh A, Professor,
Department of Computer Science and Engineering, Jain (Deemed to be University)
Bangalore, India
Email Id- a.rajesh@jainuniversity.ac.in

A communication method that creates a path between a sender and receiver with assured isolation from paths used by other pairs of senders and receivers is referred to as circuit switching. Because a telephone system offers a dedicated connection between two telephones, circuit switching is frequently linked to telephone technology. In actuality, the phrase was first used in connection with early dial-up telephone networks that created a physical circuit using electromechanical switching devices. Circuits are currently established by electronic devices in circuit switching networks. Moreover, several circuits are multiplexed over shared media to create virtual circuits rather than having each circuit correspond to a physical channel. So, the difference between circuit switching and other networking techniques is not due to the existence of discrete physical pathways. A circuit switching paradigm is instead defined by three general characteristics:

Point-to-point dialogue

separate procedures for creating, using, and shutting down circuits equivalent to an isolated physical path in terms of performance The first characteristic ensures that a circuit is created between precisely two endpoints, while the second characteristic separates switched (i.e., temporary) from permanent circuits (i.e., always remain in place ready for use). The three-step procedure used by switched circuits is comparable to making a phone call. A circuit is created in the initial stage. In the second, the two parties communicate using the circuit; in the third, they stop using it.

A key distinction between circuit switched networks and other types is made by the third attribute. Circuit switching refers to the fact that even though all communication is multiplexed across a single medium, communication between two parties is unaffected in any manner by communication between other parties. For each pair of communicating entities, circuit switching must in particular give the impression of an independent path. Hence, multiplexing circuits over a common channel requires the adoption of methods like frequency division multiplexing or synchronous time division multiplexing.

Network switching

The foundation of the Internet is packet switching, the primary substitute for circuit switching. In a packet switching system, statistical multiplexing is used to compete for the use of shared media among communications from various sources. Because a packet switching system requires a sender to split each message into blocks of data known as packets, this is where packet switching differs most from other types of statistical multiplication. Each packet switching technology has a maximum packet size that varies depending on the size of the packet.

1. A packet switched paradigm is defined by three general characteristics:
2. Asynchronous, arbitrary communication
3. There is no setup necessary before communication starts.
4. Because to statistical multiplexing of packets, performance varies.

According to the first property, packet switching enables communication between a sender and one or more recipients, and it enables a recipient to receive messages from a single sender or from several different senders. Moreover, a sender can delay arbitrarily long between subsequent communications, and communication can happen at any moment. The second characteristic indicates that a packet switched system, as opposed to a circuit switched system, and is always prepared to deliver a packet to any destination. As a result, a sender is not required to initialise before communicating and is not required to inform the underlying system when communication ends.

The third characteristic indicates that multiplexing takes place between packets rather than between bits or bytes. To put it another way, a sender who has gained access to the underlying channel broadcasts a whole packet before allowing other senders to send a packet. A single sender can send repeatedly if no other senders are prepared to deliver a packet. But, if there are N senders and each of them has a packet to send, then each sender will send about 1/N of the packets. The cheaper cost that results from sharing is one of the main benefits of packet switching. A circuit-switched network must contain connections for each computer as well as at least N/2 independent channels in order to facilitate communication among N computers. With packet switching, a network only needs one shared path but still requires a connection for each computer.

Wide-Area and Local Packet Networks

According to the range of distances they cover, packet switching systems are frequently categorised. The most expensive networks span great distances, while the least expensive networks use technologies that span short distances (such as within a single building) (e.g., across several cities). summarises the vocabulary.

Network types that fall into three groups.

MAN networks have not been commercially successful, and few MAN technologies have been developed in practise. As a result, networking experts typically just use the phrases LAN and WAN and lump MAN technology into the WAN category.

Specifications for Packet Identification and Format

Each packet sent across such a network must carry the identity of the intended receiver because packet switching systems rely on sharing. Additionally, all senders must agree on the precise details of how to identify a recipient and where to place the identification in a packet in order to ensure that there are no ambiguities. Standards bodies provide protocol documents that contain all the specifics. The Institute for Electrical and Electronic Engineers developed the most popular set of LAN standards (IEEE).

To provide networking standards, IEEE established the Project 802 LAN/MAN Standards Committee in 1980. Understanding that the IEEE is made up of engineers who concentrate on the lower two tiers of the protocol stack is crucial to understanding IEEE standards. In fact, it may seem that all other aspects of networking are insignificant if one reads the IEEE documents. There are numerous standards bodies, though, and they all focus on different layers of the stack.

The IEEE MAC Sub-Layer:

In addition to discussing both static and dynamic channel allocation, the describes multi-access protocols. How is access to a shared medium coordinated amongst numerous independent computers? There are three general strategies that they can employ: a modified multiplexing technique, a distributed method for controlled access, or a random access tactic.

Allocation of Static and Dynamic Channels

A mapping between a specific communication and a channel in the underlying transmission system is what we refer to as channelization. Channelization and multiplexing techniques are related. Take a frequency division multiplexing (FDM) method, for instance. The majority of FDM systems designate a distinct carrier frequency for each pair of interacting entities. In other words, a distinct channel is given to each couple. Moreover, there is no change in the mapping between a pair of things and a carrier frequency. In such cases, we refer to the mapping as 1-to-1 and static between communicating entities and a channel.

Allocation of Static and Dynamic Channels

When the group of communication entities is fixed and known in advance, static channel allocation is effective. However, the number of entities utilizing a network frequently changes over time. Take cellular phones in a metropolis as an example. Mobile phone users can roam about and turn their devices on and off at any moment. As a result, the variety of mobile devices that are active within a given cell tower's coverage area changes regularly. A dynamic channel allocation mechanism is required in such circumstances; a mapping can be made when a new station (such as a mobile phone) arises, and the mapping can be erased when the station vanishes.

FDMA

Channelization techniques use frequency, time, and code division multiplexing, as shown in the shows. One technology that promotes frequency division multiplexing is Frequency Division Multiple Access (FDMA). The extension basically entails a mechanism that enables independent stations to select carrier frequencies that won't interfere with the carriers used by other stations. How are carriers assigned in FDMA? A central controller offers a dynamic assignment in some systems. A designated control channel is used by every new station to connect with the controller when it first appears. The controller receives a request from the station, selects an open frequency, and notifies the station. The station only communicates using the given channel (i.e., the as-signed carrier frequency) following the initial exchange. Similar to the extension for frequency division multiplexing is the Time Division Multi-Access addition to time division multiplexing. In the most straightforward scenario, each active participant is given a sequence number between 1 and N, and stations transmit in the following order: 1, 2, 3, etc. Similar to FDMA, some TDMA systems allow for dynamic allocation, whereby a station is given a time slot when it initially joins the network.

CDMA

By mathematically encoding each broadcast, code-division multiplexing allows numerous stations to communicate at the same time. The main use of code division multiplexing is known as Code Division Multi-Access (CDMA), as it is explained in.

Access Control Protocols

A centralised controller is used in networks that use polling to cycle between stations and give each one a chance to broadcast a packet. Algorithm

Token Exchange

Token passing is frequently associated with ring topologies and has been utilised in a number of LAN systems. Imagine a group of interconnected computers in a ring, and suppose that at any given time only one of the computers has received a unique control message known as a token. This will help you to grasp token passing. Each machine follows a set protocol to limit access.

When no station has any packets to send in a token passing system, the token constantly circulates among all stations. The ring in a ring topology determines the sequence of circulation. In other words, the next station indicated in the algorithm refers to the next actual station in clockwise order if a ring is configured to convey messages in a clockwise direction. When token passing is used with different topologies (such as a bus), each station is given a place in a logical sequence, and the token is passed in accordance with the allocated order.

Protocols for Random Access

A controlled access mechanism is not used by many networks, particularly LANs. Instead, a group of computers connected to a common medium make uncoordinated attempts to access it. Because access only happens when a specific station has a packet to broadcast and randomization is used to avoid simultaneous use of the media by all computers on a LAN, the term random is used to describe access. The explanations of although some older LANs used the token passing ring technology, token passing networks are becoming less common.

ALOHA

Random access was first introduced by the pioneering ALOHAnet network, a pioneering Hawaii-based network. Yet, the concepts have been expanded even though the network is no longer in operation. The network was made up of a single, strong transmitter in the middle of the country, surrounded by a number of stations, each of which represented a computer. Every station had a transmitter that could connect to the main transmitter (but not powerful enough to reach all the other stations). Two carrier frequencies were utilised by ALOHAnet: one at 413.475 MHz for broadcast traffic sent from the central transmitter to all stations, and one at 407.305 MHz for station-to-station communications.

The ALOHA protocol is simple: a station transmits a packet on the inbound frequency when it has one to send. The signal is repeated by the central transmitter on the outgoing frequency (which all stations can receive). An outbound channel is listened to by a sending station to ensure that transmission is successful. The sending station moves on to the next packet if a copy of its packet shows up; if not, it waits a brief while before trying again.

What could cause a shipment not not arrive? The solution is interference; if two stations try to transmit on the inbound frequency at the same time, the signals will clash and muddle each other's transmissions. When two transmitted packets clash in the media, we use the word collision. The protocol requires a sender to resend each lost packet in order to handle a collision. The concept is widespread and is used in numerous network protocols.

It is important to take care while deciding how long to wait before retransmission. Otherwise, two stations will interfere with one another once more and wait exactly the same length of time before resending. Therefore, the likelihood of interference is greatly reduced if randomization is applied (i.e., each station choose a random delay). Research reveals that numerous crashes happened when ALOHAnet was busy. Collisions reduced successful data transfer in ALOHAnet to around 18% of channel capacity (i.e., channel usage was 18%) even with randomization.

The CSMA/CD

A random access protocol was employed in 1973 by researchers at Xerox PARC to develop a network technology that was incredibly successful. A standard was developed in 1978 by Digital Equipment Corporation, Intel, and Xerox and is colloquially known as the DIX standard. The original Ethernet technology, also known as Ethernet, was made up of a solitary, lengthy wire to which computers connected. Instead of broadcasting radio frequency broadcasts across the environment, Ethernet conveyed signals down a cable, serving as a shared

medium. Additionally, Ethernet enables all communication to happen across the common cable rather than needing two frequencies and a central transmitter. Despite their differences, Ethernet and ALOHAnet had to address the same fundamental issue: collisions happen when two stations try to transmit at the same time.

Three improvements to the way collisions are handled were made possible by Ethernet:

1. Sensei Carrier detection of collisions
2. Backoff in binary exponential

Company Sense. Ethernet mandates that each station watch the cable to determine whether another transmission is already in progress. This is different from other protocols that enable a station to broadcast anytime a packet is ready. The carrier sense approach greatly increases network utilisation while preventing the most visible collision issues.

Detection of collisions. Despite the fact that carrier sense is employed, a collision can still happen if two stations wait for a transmission to end, discover the cable is empty, and then both begin transmitting. Even at the speed of light, a signal needs time to travel down the cable, which contributes to a small portion of the issue. Hence, a station at one end of the cable cannot quickly detect the start of transmission from a station at the other end.

Each station keeps an eye on the cable during transmission to prevent collisions. A collision has happened if the signal being sent by the station and the signal being received on the cable are different. The process is called collision detection. The sending station stops transmitting when a collision is found.

Ethernet transmission is complicated by numerous factors. For instance, after a collision, transmission continues until enough bits are provided to ensure that the colliding signals are received by all stations. In order to ensure that every station detects an idle network and has a chance to send, stations must wait for an interpacket gap (9.6 seconds for a 10 Mbps Ethernet) after a transmission. Such specifics demonstrate how meticulously the technology was created.

Backoff with a binary exponential. Ethernet not only detects collisions, but also bounces back from them. A computer must wait for the cable to become idle once more once a collision occurs before transmitting another frame. Randomization is employed, like in ALOHAnet, to prevent simultaneous transmission from many stations while the cable is idle. In other words, the standard establishes a maximum delay, d, and demands that each station select a random delay that is less than d following a collision. When two stations choose a random value, in most instances the station with the least delay will send the packet first, and the network will resume regular operation.

If two or more computers choose delays that are roughly the same, they will start transmitting almost simultaneously and cause a second collision. Ethernet mandates that each computer twice the range from which a delay is selected after each collision in order to prevent a series of collisions. After each collision, a computer chooses a random delay ranging from 0 to d, 0 to 2d after the next, 0 to 4d after the third, and so on. The range from which a random value is selected grows after a few collisions. In order to avoid a collision, some computers will choose a random delay that is shorter than the others.

Binary exponential backoff is the process of increasing the random delay after each collision by two times. As each computer agrees to wait longer periods of time between requests when the cable becomes busy, exponential backoff essentially means that an Ethernet can recover swiftly after a collision. Exponential backoff ensures that contention for the connection will decrease after a few collisions, even in the unlikely scenario when two or more computers choose delays that are roughly identical.

Carrier Sensing Multi-Access with Collision Detection (CSMA/CD) is the name given to the combination of the aforementioned approaches.

Because to the constrained range of a wireless LAN transmitter, SMA/CD does not perform as well in wireless LANs. In other words, a receiver farther than will not be able to detect a carrier and will not be able to receive a signal from the transmitter.

Computer 1 in the is able to interact with Computer 2, but it is unable to receive the signal from Computer 3. As a result, if computer 1 transmits a packet to computer 2, carrier sense mechanism on computer 1 won't notice the transfer. Similar to this, only computer 2 will notice a collision if computers 1 and 3 broadcast at the same time. The issue is occasionally referred to as the "hidden station problem" since some stations are concealed from some users.

Wireless LANs use a modified access protocol known as Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA) to make sure that all stations correctly share the transmission media. The CSMA/CA protocol used with wireless LANs initiates a brief communication from the intended receiver before transmitting a packet, as opposed to relying on all other computers to receive all messages. Any computers in range of either will be aware that a packet transmission is starting if both the sender and recipient emit a message.

In the, computer 3 sends a brief message to computer 2 indicating that it is prepared to send the latter a packet, and computer 2 replies by sending a brief message indicating that it is prepared to receive the former. The original announcement is sent to all computers within range of computer 3, and the reaction is sent to all computers within range of computer 2. As a result, computer 1 is aware that a packet transmission is happening even if it cannot perceive a carrier or receive the signal.

By utilising CSMA/CA, control message collisions are possible but manageable. For instance, if computers 1 and 3 try to send a packet to computer 2 at the exact same time through the network, their control messages will clash. When Computer 2 notices the collision, it will not respond. The sending stations use random backoff once a collision occurs before resending the control messages. Control messages are substantially shorter than packets, hence there is a little chance of a second collision. One of the two control messages eventually arrives intact, at which point computer 2 transmits a reply.

The protocols that regulate access to a shared medium are found in the IEEE MAC layer. Frequency, Time, and Code Division Multi-Access are extensions to time, frequency, and code division multiplexing that make up channelization protocols. Channel allocation might be static or dynamic.

Independent stations are able to do statistical multiplexing thanks to controlled access protocols. A central controller is used in polling to repeatedly determine if stations are prepared to send a packet. With a reservation system, which is frequently used with satellites, stations must indicate if they are prepared for the upcoming transmission. A control message is passed between stations using token passing, which is frequently employed with a ring topology. When a station receives the token, it is then able to broadcast a packet.

Stations are able to compete for access using random access protocols. The original ALOHA system used two frequencies—one for inbound and one for outbound transmissions—and required stations to retransmit their packets if they did not get a copy. To control access to a shared connection, Ethernet uses Carrier Sense Multi-Access with Collision Detection (CSMA/CD). The protocol uses binary exponential backoff to prevent collisions in addition to preventing a station from transmitting while another transmission is in progress.

Wireless LANs use Carrier Sense Multi-Access with Collision Avoidance (CSMA / CA) since some stations are hidden from others. Each of the two computers sends a brief control message before transmitting a packet to the other, letting all other computers in its range know that a transmission is about to take place.

CHAPTER 13

WIRED LAN TECHNOLOGY (ETHERNET AND 802.3)

Shashikala H.K, Assistant Professor,
Department of Computer Science and Engineering, Jain (Deemed to be University)
Bangalore, India
Email Id- shashi.hk85@gmail.com

The venerable Ethernet was created at Xerox PARC and then standardised by Digital Equipment Company, Intel, and Xerox. After thirty years, Ethernet is still in use. Several foundations are consistent even when the gear, cabling, and media used with Ethernet have evolved significantly. The fact that newer versions of Ethernet maintain backward compatibility is one of the most intriguing features of their progression; a new version may detect an older form and automatically adjust to support the older technology.

Frame Format for Ethernet

The phrase "frame format" describes how a packet is structured, including specifics like the size and significance of each field. The frame format, which hasn't changed since the DIX standard was established in the 1970s, is mostly to blame for earlier versions of Ethernet continuing to work with newer ones. A fixed-length header, a variable-length payload, and a fixed-length Cyclic Redundancy Check make up an Ethernet frame, as shown in the diagram. Three fields make up the header: a 16-bit type field, a 48-bit source address field, and a 48-bit destination address field. The destination address field includes the address of the intended receiver.

Type Field and Demultiplexing for Ethernet

A given machine may have numerous protocols running at once thanks to the multiplexing and demultiplexing capabilities of the type field in an Ethernet packet. Explain afterwards how the Internet's protocols convey IP datagrams and ARP messages across Ethernet as an example. Each is given a special Ethernet type (hexade- cimal 0800 for IP datagrams and hexadecimal 0806 for ARP messages). The sender assigns a type of 0800 to a datagram before sending it in an Ethernet frame. The receiver looks at the type field of a frame when it reaches its destination and uses the value to decide which software module should handle the packet. The desmultifying. An Ethernet frame may be preceded by a 64-bit preamble of alternating 1s and 0s when it is sent across a network. Bits are encoded using the Manchester encoding mentioned.

IEEE's Ethernet Protocol

It's interesting to note that IEEE sought to reinvent the Ethernet frame format in 1983 by developing a standard for Ethernet. Professionals often refer to the IEEE standard as 802.3 Ethernet in order to differentiate it from other standards since it was created by an IEEE working group with the same name. The interpretation of the type field leads to the main distinction between 802.3 Ethernet and traditional Ethernet. The 802.3 standard adds an additional 8-byte header with the packet type and interprets the old type field as a packet length. Logical Link Control / Sub-Network Attachment Point (LLC / SNAP) header is the name of the additional header; most experts just refer to it as a SNAP header.

Network interface cards and LAN connections

A LAN seems to be an I/O device in terms of computer architecture and connects to the computer similarly to a disc or a visual device. This is accomplished by connecting a Network Interface Card (NIC) to the computer's bus. A NIC should be able to recognise addresses, calculate CRCs, and recognise frames (e.g., a NIC checks the destina- tion address on a frame, and ignores frames not destined for the computer). A NIC also establishes a connection to a network and manages data transfer details (i.e., sending and receiving frames). A NIC is physically made up of a circuit board with a connector on one side that takes a plug specific to a certain LAN and a plug that matches the computer's bus on the other. The majority of PCs already have a NIC installed. The NIC, however, is separate from the rest of the computer and may be changed on its own without affecting other components.

Thicknet wiring and Ethernet Evolution

Since its introduction in the 1970s, Ethernet has experienced a number of important alterations, with media and wiring seeing the most significant changes. Since the communication channel was a thick coaxial cable, the first Ethernet wiring scheme was colloquially known as thick wire Ethernet or Thicknet; the official name for the wiring is 10Base5. Thicknet hardware was split into two main categories. A transceiver, a separate electrical device linked to the Ethernet connection, handled carrier detection, the conversion of bits into the proper voltages for transmission, and the conversion of incoming signals into bits. A NIC handled the digital portions of communication.

A transceiver was attached to a NIC in a computer via a physical connection known as an Attachment Unit Interface (AUI). Typically, a transceiver was placed far away from a computer. Transceivers, for instance, might connect to an Ethernet in a corridor ceiling of an office building. An AUI cable was used in the initial Thicknet cabling to link a computer to a transceiver.

Wiring for Thinnet Ethernet

A thinner, coaxial cable that is more flexible than Thicknet is used in a second generation of Ethernet cabling. The wiring method, officially designated as 10Base2 and often known as Thinwire Ethernet or Thinnet, was quite different from Thicknet. Thinnet incorporates a transceiver directly on the Network Interface Card and connects computers using coaxial cables instead of utilising AUI connections between computers and transceivers.

Both benefits and drawbacks applied to thinnet. The main benefits were decreased total cost and simplicity of installation. There was no need for external transceivers, and Thinnet cable could be deployed in a practical location (e.g., across a tabletop between computers, under the floor, or in a conduit). The main drawback was that the whole network was exposed; if a user disconnected a section of the network to move cables or a computer, the entire network would cease to function.

Hubs and Twisted Pair Ethernet Wiring

Third-generation Ethernet wire had two significant changes. The third generation ditches coaxial cable in favour of a central electronic device that is independent of the network-connected PCs. The third generation makes use of twisted pair cable rather than bulky, insulated cabling. The third-generation technology, sometimes referred to as twisted pair Ethernet, has supplanted earlier iterations since it does not use coaxial wire. Consequently, twisted pair Ethernet is now meant when the term "Ethernet" is used.

The electrical gadget that functioned as the main interconnection for twisted pair Ethernet was referred to as a hub. Hubs were offered in a range of sizes, with the price increasing

proportionally with size. Four or eight ports on a tiny hub linked to a computer or other device at a time (e.g., a printer). Many connections might fit in larger hubs. The hub's electronic components simulate a physical wire so that the system functions like a standard Ethernet. A computer connected to a hub, for instance, accesses the network via CSMA/CD, gets a copy of every frame, and decides whether to execute or ignore a frame based on its address. Twisted pair Ethernet also uses the same frame format as its predecessors. The network interface on a computer handles the specifics and masks any variances, so software on a computer cannot tell the difference between thick Ethernet, thin Ethernet, and twisted pair Ethernet. The key is:

Ethernet, both physical and logical Topology

Remember that LANs are categorised based on their topology (i.e., overall shape). What is the topology of Ethernet, one could ask. Unexpectedly, the solution is intricate. It is obvious that the first Thicknet implementation of Ethernet used a bus architecture. In fact, the original Ethernet is often used as a prime illustration of bus topology. Twisted pair Ethernet could seem to follow a star topology. In actuality, the word "hub" was used to describe a major connectivity point. The system seems to operate as if PCs are connected to a cable, however, since a hub simulates a real wire. In fact, experts laughed that a hub really offered a "bus in a box."

We must differentiate between logical and physical topologies in order to comprehend Ethernet topology. Twisted pair Ethernet logically uses a bus architecture. Twisted pair Ethernet, however, has a star-shaped topology on a physical level. The key is:

Wiring inside a workplace

In a machine room or lab, the types of LAN wire utilised don't really matter. Nevertheless, when utilised in an office building, the kind of wiring has a significant impact on the kind and quantity of wires required, the distance to be covered, and the cost. Take notice in the twisted pair Ethernet needs several separate wires to connect offices to a hub, or wiring closet. Twisted pair Ethernet hence need meticulous cable labelling. Significant advancements have been achieved in the quality and insulation of twisted pair cables since the invention of twisted pair Ethernet. Twisted pair Ethernet now uses a higher data rate as a consequence.

The initial iteration of twisted pair Ethernet was officially given the name 10BaseT, where the number 10 denotes a 10 Mbps speed. Later versions that operated at 100 Mbps were called 100BaseT and were released under the term Fast Ethernet. One Gbps is the speed of Gigabit Ethernet, the third variation (i.e., 1000 Mbps). Higher-speed Ethernet technologies employ a switch rather than a hub, which is why experts sometimes shorten the moniker as Gig-E. Moreover, specifications for the higher-speed versions mandate that interfaces should automatically detect the maximum speed at which a connection can function and slow down to accommodate older devices in order to maintain backward compatibility. As a result, the new device will automatically detect the disparity and slow down to 10 Mbps if an Ethernet connection is plugged between an old device that uses 10BaseT and a new device that utilises 1000BaseT.

Twisted pair cables and connectors

RJ45 connections, which are bigger versions of the RJ11 connectors used to connect telephones, are used for twisted pair Ethernet. An RJ45 connection has a physical component that keeps it in place and can only be inserted into a socket in one direction. As a result, connections cannot be plugged in improperly and, once installed, do not dislodge. Most users do not need to design a cable since they may buy cables in a variety of lengths with an RJ45 connection attached on either end. Yet, there are two types of cables: straight and crossing, which causes confusion. A crossover cable joins two switches together by connecting one switch's pin to the second switch's pin using a different pin on each end. Each pin of the RJ45

linked to one end of the cable is directly connected to the matching pin on the RJ45 at the other end when a straight cable is used to connect a computer and a switch. Pin 1 thus connects to pin1, and so on. The majority of interface hardware will not work properly if a crossing connection is used when a straight cable is needed, even if the most sophisticated interface devices can detect an improper cable and adapt.

Since its introduction in the 1970s, Ethernet has grown to be accepted as the industry standard for wired Local Area Networks. A 14-byte header that comprises a 48-bit destination address, an 8-bit source address, and a 16-bit type field is the first 14 bytes of an Ethernet frame. Despite the fact that the IEEE version of standard 802.3 sought to create a new frame format with an extra 8-byte header, it is seldom utilised.

When a frame reaches its destination, DE multiplexing is performed using the Ethernet type field. A sender provides the type when producing a frame; the receiver uses the type to decide which module should handle the frame. The wiring architecture and Ethernet cables have undergone significant alteration, even though the Ethernet frame structure has not changed since the initial standard. Ethernet wire has existed in three main iterations. Thicknet used a large coaxial cable with labels that identified each pin's intended use—transmit, receive, or be used for bidirectional communication—along each of the four potential data pathways. Transceiver-equipped cable kept apart from PCs. The network interface in each computer had a transceiver, and Thinnet connected computers through a flexible coaxial cable. Twisted Pair Ethernet employs twisted pair cabling to connect a computer to a hub instead of a coaxial cable and an electrical device known as a hub or switch. The system that results has both a logical bus topology and a physical star topology.

The initial Twisted Pair technology, known as 10BaseT, ran at 10 Mbps, much like previous iterations of Ethernet. Fast Ethernet is the brand name for a variant of 100BaseT that works at 100 Mbps. A third kind is known as Gigabit Ethernet, or Gig-E, and it runs at 1000 Mbps, or 1 Gbps. When a low-speed device is attached, higher-speed Ethernet hardware automatically detects this and lowers the speed.

Wireless Networking Technologies:

There have been several wireless technologies developed, wireless communication is employed across a broad variety of distances, and there are numerous commercial systems available. As a result, wireless networking seems to have a number of technologies, many of which have comparable properties, as opposed to the situation with wired networking where one technology predominates.

A Wireless Networks Taxonomy

Broadly speaking, wireless communication is applicable to all sizes and kinds of networks. Government laws that make some portions of the electromagnetic spectrum accessible for communication are one reason for the variability. Certain portions of the spectrum need a licence to use transmission equipment, whereas other portions of the spectrum are unlicensed. There are many different wireless technologies, and more are always being developed. According to the taxonomy, wireless technologies may be generally categorised by network type.

Person-to-Person Networks (PANs)

Wireless networking comprises Personal Area Networks in addition to the three network types (LANs, MANs, and WANs) that were previously mentioned (PANs). PAN technology enables communication across short distances and is designed to be used with single-user owned and operated devices. For instance, a PAN may enable communication between a mobile phone and

a wireless headphone. Between a computer and a nearby wireless mouse or keyboard, PAN technologies are also used. Three major categories may be used to classify PAN technology.

LANs and PANs Utilize ISM Wireless Bands

Three regions of the electromagnetic spectrum have been set aside by governments for usage by business, science, and health organisations. The frequencies, referred to as ISM wireless, are utilised for LANs and PANs and are widely accessible for goods. They are not licenced to particular carriers.

Wi-Fi and Wireless LAN Technology

There are several wireless LAN systems that use different frequencies, modulation methods, and data speeds. The majority of the standards are produced by IEEE and fall within the IEEE 802.11 category. The Wi-Fi Alliance is a nonprofit organisation that tests and certifies wireless equipment utilising the 802.11 standards. It was founded in 1999 by a collection of manufacturers of wireless equipment. Due to the alliance's strong marketing, the majority of customers now refer to wireless LANs as Wi-Fi.

Broadcasting techniques

The phrase spread spectrum describes how data is sent using several frequencies during spread spectrum transmission. In other words, data is scattered over many frequencies by the transmitter, and the receiver then mixes the data it receives from those various frequencies to recreate the original data. Spread spectrum may generally be utilised to accomplish one of the following two objectives:

The main multiplexing methods for WiFi.

Each method has benefits. The most flexibility is provided via OFDM. DSSS performs well, while FHSS improves a transmission's noise immunity. As a result, after defining a wireless technology, the designers choose an acceptable multiplexing technique. To accommodate DSSS and FHSS, the original 802.11 standard, for instance, was split into two variants. To sum it up:

Guidelines for Other Wireless LANs

Several wireless networking standards that support different forms of communication have been developed by IEEE. Each standard outlines the frequency range, multiplication and modulation to be utilised, as well as the data rate. A short explanation of each of the key standards that have been developed or proposed is provided.

Architecture for Wireless LAN

The three components that make up a wireless LAN are a collection of wireless hosts, also known as wireless nodes or wireless stations, a switch or router that connects access points, and access points, also known as base stations or wireless nodes. Two different kinds of wireless LANs are theoretically possible:

1. Without the need of a base station, ad hoc wireless hosts exchange data.
2. Infrastructure: A wireless host can only interact with an access point, which relays every packet.

There aren't many ad hoc networks in use nowadays. Instead, a company or service provider sets up a collection of access points, and every wireless host connects to one of them to communicate. For instance, a private business or institution could install access points all throughout its structures.

Twisted pair Ethernet often makes up the wired links that connect to access points. A Basic Service Set (BSS) is the collection of computers that fall inside the coverage area of a certain access point. Three Basic Service Sets, one for each access point, are included in the.

To put it simply:

The territory that a particular access point may reach is often referred to as a cell, much like the cellular telephone system. The 802.11 frame format, association, and overlap.

An infrastructure architecture is actually made more difficult by many details. On the one hand, a dead zone will occur between two access points if they are too far away (i.e., a physical location with no wireless connectivity). On the other hand, if two access points are placed too near to one another, a wireless host will be able to connect to both of them. The majority of wireless LANs also include an Internet connection. As a result, the interconnect mechanism often features a second wired connection to a router for the Internet.

802.11 networks need a wireless host to connect with a single access point in order to manage overlap. In other words, when a wireless host delivers frames to a certain access point, the access point then broadcasts the frames across the network.

Collaboration between Access Points

The topic of how much coordination between access points is necessary is an intriguing one. Early entry point designs were often intricate. The access points worked together to provide seamless mobility, much like a mobile phone network. In order to provide a seamless handoff when a wireless computer moved from the area of one access point to the area of another, the access points interacted with one another. When the signal strength at the new access point was stronger than the signal strength at the previous access point, for instance, some designs monitored signal strength and tried to relocate the wireless node to the new access point.

Several suppliers started providing less expensive, simpler access points that do not coordinate as an alternative. The manufacturers contend that signal strength is not a reliable indicator of mobility, mobile computers can switch between access points, and the wired network linking access points has enough capacity to support more centralised coordination. When a single access point is present in an installation, a simpler access point design is more suitable.

Contention and Access Devoid Of Contention

For channel access, the original 802.11 standard specified two main strategies.

They fit the following descriptions:

1. Contention-free service using the Point Coordinated Function (PCF) DCF (Distributed Coordinated Function) for service with congestion
2. A point-coordinated service prevents transmissions from interfering with one another by controlling stations in the Basic Service Set (BSS). For instance, an access point may designate a unique frequency for each station. PCF is never really utilised.

Every station in a BSS is set up to execute a random access protocol thanks to the distributed coordinated function. Remember that hidden station problems, where two stations may interact but a third station can only receive the signal from one of them, can occur in wireless networks. Additionally keep in mind that 802.11 networks use CSMA/CA, which requires a pair to exchange Ready to Send (RTS) and Clear to Send (CTS) signals before sending a packet, to address the issue. As an example, the standard specifies the following three timing parameters:

1. Short Inter-Frame Space (SIFS): 10 ms
2. Distributed Inter-Frame Space (DIFS): 50 ms Time Slot of 20 sec

The DIFS parameter, which is equal to SIFS plus two Slot Times, specifies how long a channel must remain idle before a station may try transmission. Intuitively, the SIFS parameter specifies how long a receiving station waits before providing an ACK or other response. How a packet transport uses the parameters.

It is challenging to distinguish between weak signals, interference, and collisions due to station separation and electrical noise. As a result, collision detection is not used in Wi-Fi networks. In other words, the hardware doesn't try to detect interference while a transmission is in progress. Instead, a sender waits for the ACK message, or acknowledgment, message. The sender uses a backoff approach similar to that used for wired Ethernet if no ACK is received, assuming that the transmission was lost. Retransmission is often only necessary in 802.11 networks with few users and no electrical interference. Other 802.11 networks, on the other hand, often incur packet loss and rely on retransmission.

Wireless WiMax and MAN Technologies

MAN innovations haven't generally had much commercial success. One wire-less MAN technology in particular stands out as having promise. The IEEE has standardised the technology under category 802.16. WiMAX, which stands for "Worldwide Interoperability for Microwave Access," was first used by a consortium of businesses, who also established the WiMAX Forum to encourage the use of the technology.

There are two primary WiMAX versions being developed, and they take different general approaches. The two are often called:

Mobile WiMAX Fixed WiMAX

Fixed WiMAX describes systems created in accordance with IEEE standard 802.16-2004, sometimes known as 802.16d. Since the system does not provide handoff between access points, the word "fixed" is used. As a result, rather of connecting a service provider and a mobile phone, it is intended to link a provider and a fixed place, such a home or office building.

Systems created in accordance with specification 802.16e-2005, also known as 802.16e, are referred to as mobile WiMAX. As the technology allows for handoff between access points, as the word "mobile" indicates, portable devices like laptop computers or cell phones may be utilised with a mobile WiMAX system. Many applications for WiMAX's broadband communication are available. WiMAX is one Internet connection technology that some service providers want to employ for the final mile. Others believe WiMAX has the ability to provide a general-purpose interconnection across physical places, particularly in cities. Backhaul is a different kind of interconnection that connects a service provider's main network facility to far-off places like cell towers.

Possible applications for WiMAX technology.

WiMAX backhaul installations often employ frequencies that need a clear Line-Of-Sight (LOS) between two connecting entities and provide the maximum data speeds. LOS stations are often installed on towers or the tops of structures. WiMAX installations for Internet connectivity may be fixed or mobile, but they typically employ frequencies that don't need line-of-sight. They are categorised as non-line-of-sight as a result (NLOS).

The following succinct list of WiMAX's primary characteristics:

Licensed spectrum is used (i.e., offered by carriers) each cell has a 3–10 km (or miles) radius. Scalable orthogonal FDM is used. Ensures high standards of service (for voice or video) can send and receive data at 70 Mbps over short distance offers 10 Mbps over a long (10 km) Zigbee range. The aim to unify wireless remote control technology, particularly for industrial

equipment, gave rise to the Zigbee standard (802.15.4). High data rates are not necessary since remote control devices simply transmit brief instructions. The main attributes of Zigbee are:

not data, but a wireless protocol for remote control Industry as well as residential automation are the targets.

utilised three frequency bands (868 MHz, 915 MHz, and 2.4 GHz) 20, 40, or 250 Kbps of data per second, depending on the frequency band little power usage. Defining three tiers of security two further wireless technologies that are often not combined with wireless PANs provide communication over short distances. RFID and InfraRED technologies work with sensors to give control and slow data transfers.

InfraRED. InfraRED technology is often seen in remote controllers and might take the role of cables in certain situations (e.g., for a wireless mouse). A collection of widely used standards was created by the Infrared Data Association (IrDA). The IrDA technology's main characteristics are:

A set of standards covering a range of speeds and uses Systems that are practical have a range of one to several metres. Data transfer speeds range from 2.4 Kbps (control) to 16 Mbps (data) typically low power use with very low power versions Surfaces may reflect signals, but solid objects cannot be penetrated by them. Identification Using Radio Frequency (RFID). An intriguing method of wireless communication is used by RFID technology to build a mechanism wherein a receiver may "extract" identifying data from a tiny tag that is attached to a small object.

There are more than 140 RFID standards available for a range of uses. RFIDs that are passive use the reader's signal to generate power. A battery is included in active RFIDs, and it might last up to 10 years. Limited range, despite active RFIDs' greater range than passive may use frequencies between 100 MHz and 868-954 MHz. Used for applications such as passports, sensors, and inventory management

Systems for Cellular Communication

The initial purpose of cellular networks was to provide voice services to mobile customers. In order to link cells to the public phone network, the system was created. Cellular networks are increasingly being utilised to provide data services and Internet connection. Each cell has a tower, and a cluster of cells (often adjacent cells) is linked to a mobile switching centre. The centre coordinates handoff while a mobile user moves between cells while being tracked by the centre. The Mobile Switching Center manages changes when a user switches between two cells that are connected to it. Two Mobile Switching Centers are engaged in the handoff when a user moves from one geo- spatial area to another. As the cells may be organised in a honeycomb, it is theoretically possible to achieve complete cellular coverage if each cell forms a hexagon. Cellular coverage is not flawless in reality. Omnidirectional antennas, which broadcast in a circular manner, are often used by cell towers. A signal, however, might be weakened or result in an erratic pattern due to impediments and electrical interference. As a consequence, cells sometimes overlap, and occasionally there are holes without any covering.

The diversity in cell density gives cellular technology another useful feature. Cell size is high in rural locations where there is a low predicted density of mobile phones; one tower may cover a sizable area. Yet, in an urban situation, a large number of mobile phones are gathered in one location. Take a city block in a large metropolis as an illustration. Such a location may include numerous occupied office or apartment buildings in addition to walkers and motorists. Designers divide an area into several cells in order to support more mobile phones. In contrast

to the 16.15a idealised structure, which has a single cell size, a real deployment employs cells of varied sizes, with smaller cells covering urban areas. The key is:

A fundamental tenet of cellular communication is:

Cellular planners use a cluster technique, in which a tiny pattern of cells is reproduced, to put the idea into practise.

Each of the forms in the may be used to tile a plane, geometrically speaking. In other words, it is feasible to completely fill a space without any gaps simply duplicating the same form. Also, if each cell in a certain form is given a different frequency, the repeating pattern won't give any neighbouring cells the same frequency. Each letter in the alphabet has a certain frequency, and each cell within a cluster is given a frequency.

Cellular Technology Generations

Cellular technologies are divided into four generations by the telecoms industry, which are referred to as 1G, 2G, 3G, and 4G, with intermediate versions known as 2.5G and 3.5G. The following characteristics apply to the generations: 1G. The early 1970s through the early 1980s marked the beginning of the first generation. Analog signals were utilised by the systems, which were first known as cellular mobile radio telephones, to convey voice. 2G and 2.5G. Early in the 1990s, the second generation got started, and it's still in use now. The primary difference between 1G and 2G is brought about by the usage of digital speech signals in 2G. Systems that add certain 3G functionalities to a 2G system are referred to as 2.5G systems. 3G and 3.5G. The third generation, which started in the 2000s, is characterised by the advent of faster data services. A 3G system is designed to enable applications like web surfing and picture sharing with download speeds ranging from 400 Kbps to 2 Mbps. A single phone may wander across Europe, Japan, and North America thanks to 3G technology.

The fourth generation, which started to emerge about 2008, focuses on real-time multimedia support, including streaming high-definition video. Moreover, 4G phones come with many connection options, including Wi-Fi and satellite, and at any given moment, the phone will automatically choose the best connection option available. Cellular standards and technologies come in a broad range. When 2G first appeared, many organisations each made an effort to decide on a strategy and establish a standard. The Global System for Mobile Communications (GSM), a TDMA technology, was selected by the European Conference of Postal and Telecommunications Administrators to build a system that was meant to serve as an international standard. Each carrier developed a network in the US using its own technologies. IDEN is a TDMA system created by Motorola. A CDMA strategy that was standardised as IS-95A was used by the majority of US and Asian operators. The PDC TDMA technology was developed in Japan. A number of additional technologies, not included in the, played a supporting role. Key 2G standards and parts of the 2.5G standards also developed.

Several services can function across the fundamental communication channels offered by the standards described in each. For instance, customers with GSM or IS-136 access may use the General Packet Radio Service (GPRS). A user has the option to access GPRS-based services after subscribing to it. Text messaging is done via the Short Message Service (SMS), web browsing is done through the Multimedia Messaging Service (MMS), and Internet access is done through the Wireless Application Service (WAP). With GPRS service, service providers often charge an additional fee, with the cost being charged per unit of data transmitted (e.g., per megabyte). After GPRS, advanced modulation and multiplexing methods have been developed in digital technologies to boost data speeds. Enchanced GPRS, also known as Improved Data rate for GSM Evolution (EDGE), provides a transmission rate of up to 473.6 Kbps. A successor called EDGE Evolution offers a 1 Mbps peak data rate.

It was clear that users desired mobile phone service that functioned internationally by the time service providers started to consider third generation technology. Providers pushed for technology interoperability as a consequence, and the sector streamlined many of the 2G techniques into a select few critical standards. The development of UMTS, a Wideband CDMA technology, was affected by the specifications of IS-136, PDC, IS-95A, and EDGE (WCDMA). In the meanwhile, CDMA 2000 was created by extending IS-95B.

Third-generation data services have given rise to a number of conflicting standards. About the same time, EVDV and EVDO both started to exist. To improve overall performance, each of the two uses a combination of CDMA and frequency division multiplexing methods. The most extensively used technology is EVDO, also known as Evolution Data Optimized or Evolution Data Only. There are two variants of EVDO, and they vary in the speed at which data is delivered: either 2.4 or 3.1 Mbps. High-Speed Downlink Packet Access (HSDPA), an alternative, provides download rates of 14 Mbps. For services that provide a larger data rate, carriers naturally charge more.

Satellite VSAT Technology

The three different kinds of communication satellites—LEO, MEO, and GEO—as well as channel access and reservation procedures are all employed to offer TDMA across satellites. Certain satellite technologies are described in this part to wrap up the debate. The dish-shaped parabolic antenna is the essential component of satellite communication. Because of its parabolic form, a satellite's electromagnetic radiation is reflected to a single focal point. A designer may ensure that a strong signal is received by pointing the dish towards a satellite and positioning a detector at the focal point. The design demonstrates how energy entering the system is reflected off the dish's surface and directed towards the receiver.

Early satellite communication employed ground stations with huge dish antennas larger than three metres in diameter to enhance the signal received. Consumers and small companies cannot install such ground stations on their land, even if they are suitable for circumstances like a transatlantic connection used by a telephone provider. Hence, the development of a technology known as a Very Tiny brought about a significant transformation. While it has been specified, the equivalent High-Speed Uplink Packet Access (HSUPA) protocol has attracted less attention than HSDPA. Aperture Terminal (VSAT) that makes use of dishes with a diameter under three metres. Less than one metre is the usual diameter of a VSAT antenna.

Numerous companies connect all of their shops using VSAT technology. For instance, pharmacies like Walgreens and CVS, fast-food restaurants like Pizza Hut and Taco Bell, and supermarkets like Wal Mart all use VSAT connectivity. Customers may also use VSAT services to access the Internet and for leisure. The three frequency bands that VSAT satellites employ vary in terms of the intensity of the signal they transmit, how sensitive they are to weather conditions like rain and other factors, and the footprints—or areas—of the globe they cover.

The Global Positioning System (GPS) satellites provide precise time and location data. Although not being a component of computer communication, location data is being utilised more often in mobile networking. Key characteristics include:

1. Between 20 and 2 metre precision (military versions have higher accuracy)
2. The planet is orbited by 24 satellites in total. Six orbital planes include satellites.
3. Allows for the time synchronisation that certain communication networks need.

In one sense, the method for obtaining position data is simple: because all GPS satellites orbit at well-known locations, a receiver can pinpoint a specific place on the surface of the planet by measuring the distance between three satellites. Examine the collection of points that separate satellite 1 and D1 to see why. A sphere is defined by the set. A different sphere is defined by

the collection of points that separate D2 from satellite 2. In the circle created by the intersection of the two spheres, there is a GPS system that is D1 from satellite 1 and D2 from satellite 2. A third sphere will intersect the circle at the GPS system's location if it is likewise at a distance of D3 from satellite 3, giving rise to two potential locations. It is simple to choose the right location since the satellites are positioned such that only one of the two points is on the surface of the Earth and the other is in space.

A GPS system uses the Newtonian physics formula, which states that distance equals rate times time, to calculate distance. The pace (the speed of light, 3 109 metres per second) is constant. Each GPS system is set up to calculate the local time, and each satellite is equipped with an accurate clock that is utilised to include a timestamp in the data being received. The time the information has been in transit may then be calculated by a receiver by deducting the timestamp from the local time.

The future of wireless technology, software radio

Each of the several wireless technologies listed in the uses specialised radio equipment. Using certain types of modulation and multiplexing, the antenna, transmitter, and receiver of a given device are made to function on specified frequencies. Three distinct radio systems are required for a mobile phone to be able to access the GSM, Wi-Fi, and CDMA networks, and the user must choose one of them.

1. Radios that use a programmable paradigm, in which functions are managed by software running on a CPU, are replacing conventional radios.
2. Features of a programmable radio that are managed by software.

Tunable analogue filters and multiple antenna management are the two main technologies that make software radios possible. Nowadays, analogue chips with tunable analogue filters are accessible. Thus, power and frequency selection are both feasible. Signal coding and modulation may be handled by digital signal processors (DSPs). The usage of many antennas is the most intriguing feature of software radios. A software radio may enable spatial multiplexing, a method that allows a signal to be delivered or received from a specific direction, by using numerous antennas at once rather than just one at a time. A system that uses several antennas for both transmission and reception is referred to as multiple-input multiple-output (MIMO) (i.e., can aim transmission or reception).

Software-programmable radios are now being used by the US military after emerging from the research lab. Moreover, GNU Radio and the Universal Software Radio Perimeter (USRP) are presently available for testing. Before programmable radios are used in commercial products, there are still a few details to be ironed out. The price is now too exorbitant ($1000 US), to start. Second, guidelines for the usage of the spectrum must be developed. Devices that transfer electromagnetic radiation, in particular, are approved to ensure that they do not obstruct communication. A user might unintentionally download a virus that could cause the radio to jam emergency channels if a software radio can be modified. As a result, methods are being developed to limit the amount of power a software radio may produce on certain frequencies.

Wireless LANs, PANs, MANs, and WANs may be built using a variety of wireless communication methods. Many LAN and MAN technologies have been standardised by IEEE. Wi-Fi adheres to the IEEE 802.11 standards, with several variations denoted by an abbreviation like 802.11b or 802.11g. The frame format for wireless LANs comprises a MAC address for an access point as well as a MAC address for a router that is beyond the access point. Wireless LANs may be ad hoc or employ an infrastructure design with access points. Wireless technologies are also employed for MANs and PANs in addition to LANs. WiMAX, the primary MAN technology, may be utilised for access or backhaul. PAN technologies come in

a number of forms, such as Bluetooth, Ultra Wideband, Zigbee, and IrDA. Another wireless communication method that is largely utilised for shipping and inventory management is RFID tags.

Cellular and satellite technologies are used in wireless WANs. There are several different cellular technologies, which are categorised as 1G (analogue), 2G (digital voice), 3G (digital voice plus data), and 4G (high-speed digital voice and data). Dish antennas are now feasible for both consumers and enterprises thanks to VSAT satellite technologies. New wireless systems use radios that can be programmed by software, giving software complete control over radio transmission. For military and specialised needs, programmable radios are now available but are pricey.

CHAPTER 14

FIBER MODEMS, REPEATERS, BRIDGES, AND SWITCHES FOR LAN EXTENSIONS

Mahesh T R, Associate Professor,
Department of Computer Science and Engineering, Jain (Deemed to be University)
Bangalore, India
Email Id- t.mahesh@jainuniversity.ac.in

LAN topologies and wiring strategies are covered in earlier. Although a standard LAN is designed to cover a few hundred metres, LAN technology is effective inside of a single building or a small campus. Two key ideas are covered: LAN switching and methods for extending a LAN across greater distances. In order to avoid forwarding loops, the presents repeaters, bridges, and the spanning tree technique.

Distance Restrictions and LAN Architecture

Distance restriction is an essential component of LAN designs. Engineers pick a mix of capacity, maximum latency, and distance that may be attained at a given cost when building a network technology. The fact that hardware is designed to emit a specific amount of energy places a limit on how far it can be used; if wire is stretched beyond these constraints, stations won't get a strong enough signal, and mistakes will result.

Extensions for Fiber Modems

To increase LAN connection, engineers have created a number of techniques. Often, extension devices do not only stretch wires or simply boost signal strength. Instead, the majority of extension methods include extra hardware that can relay signals across greater distances into the regular interface hardware. The simplest LAN extension method connects a PC to a distant Ethernet network using an optical fibre and two fibre modems. Figure 14.1 shows how the connections are related.

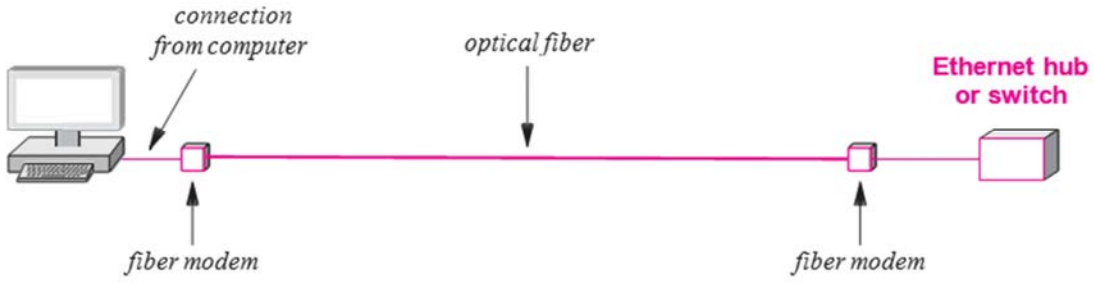


Figure 14.1: Fiber modems are shown in Figure as a link between a computer and a distant Network.

Both accepting packets over the Ethernet interface and sending them over the optical fibre, as well as accepting packets that come over the optical fibre and sending them over the Ethernet interface, are tasks that may be carried out by each fibre modem. Standard interfaces may be utilised on the computer and the LAN device if the modems have LAN interfaces on both ends. In actual implementations, simultaneous transmission in both directions is made possible by a pair of fibres.

Repeaters

An analogue device called a repeater is used to transmit LAN signals across great distances. Neither signal coding nor packets are understood by a repeater. Instead, it just amplifies the signal that is received and outputs that signal. Repeaters have been used with different LAN protocols and were widely employed with the original Ethernet. In order to enable a receiver to be placed at a greater distance from a computer, repeaters with infrared receivers have recently been created. Consider a scenario where the cable television controller's infrared receiver has to be in a separate room from the controller. A repeater may make the connection longer, as seen in Figure 14.2.

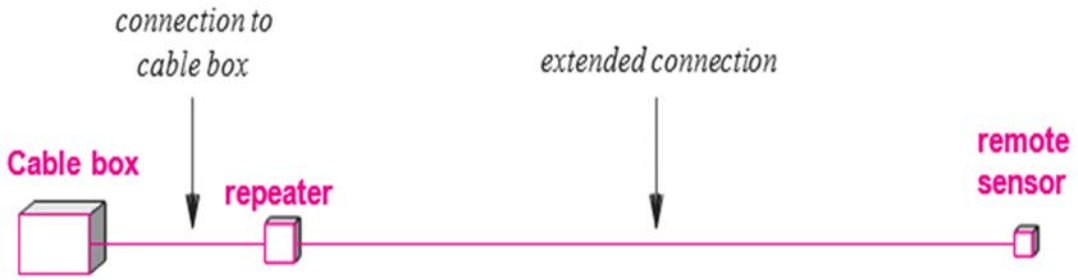


Figure 14.2.: A repeater-extended infrared sensor

Bridging and Bridges

A bridge is a device used to transmit packets between two Network segments (such as two hubs). The bridge listens on each segment in a promiscuous manner (i.e., receives all packets sent on the segment).

The bridge sends a duplicate of an intact frame it gets from one segment to the other section. A computer connected to either segment may transmit a frame to any other computer on the other segment, making two LAN segments joined by a bridge seem to function as a single LAN.

A broadcast frame is further sent to each machine on the two segments. Computers are thus unaware of whether they are linked to a bridged LAN or a single LAN segment.

Bridges were first offered for sale as separate hardware units with two network connections. Nowadays, bridge technology may be found in various gadgets like cable modems. Figure 14.3 provides an illustration of the conceptual design.

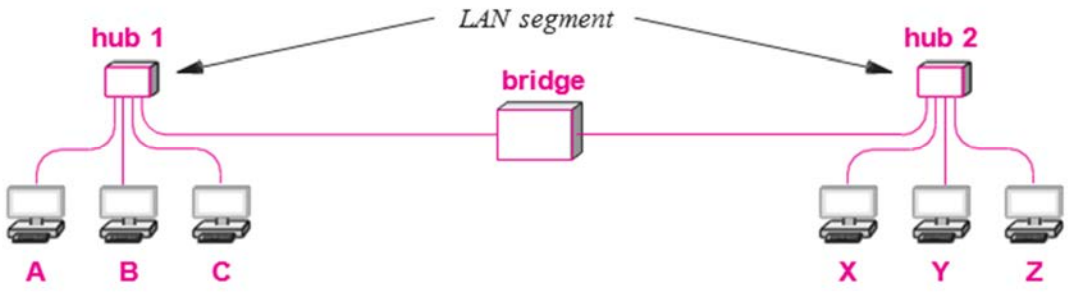


Figure 14.3 Illustration of six computers connected to a pair of bridged LAN segments.

Frame filtering and learning bridges

A copy of every frame is not automatically sent by bridges from one LAN to another. Instead, a bridge does filtering using MAC addresses. In other words, a bridge looks at the destination address in a frame before forwarding it to the other LAN segment unless it is absolutely essential. The bridge must naturally forward a copy of each broadcast or multicast frame if the LAN allows them in order for the bridged LAN to function as a single LAN. How does a bridge know which segments have which computers attached? The majority of bridges are referred to as adaptive or learning bridges since they automatically figure out where computers are. A bridge employs source addresses to do this. The bridge takes the source address from the header of each frame coming from a certain segment and adds it to a list of the computers connected to that segment. The bridge must then undoubtedly retrieve the MAC destination address from the frame and use it to decide whether or not to send the frame. So, as soon as a computer sends a frame, a bridge recognises that a computer is present on a segment.

The Benefits of Bridging

It's crucial to understand that a bridged network may perform better overall than a single LAN after it has learned the locations of every machine. Knowing that a bridge allows simultaneous transmission on each section will help you understand why. Computer A may transmit a packet to computer B in Figure 14.4 at the same time as computer X sends a packet to computer Y. The bridge will not forward either packet, even if it gets a copy of each one, since they were both delivered to destinations that were on the same segment as the source. The two frames are therefore just discarded by the bridge rather than being sent. Building a bridge connecting buildings on a campus is achievable because to the capacity to localise communication. The majority of communication is local (for instance, a computer will often speak with a printer inside the same building as opposed to a printer outside of it building). As a result, a bridge may facilitate communication between structures when necessary while minimising unnecessary packet sending. The idea of bridging is also used by DSL and cable modems; in these cases, the modem serves as a link between a subscriber's local network and a network at the ISP.

Distributed Spanning Tree

Have a look at Figure 14.4, which depicts four LAN segments linked by three bridges at the moment, with a fourth bridge going to be added. We presume that each of the hubs is also hooked into PCs, which are not shown in the picture.

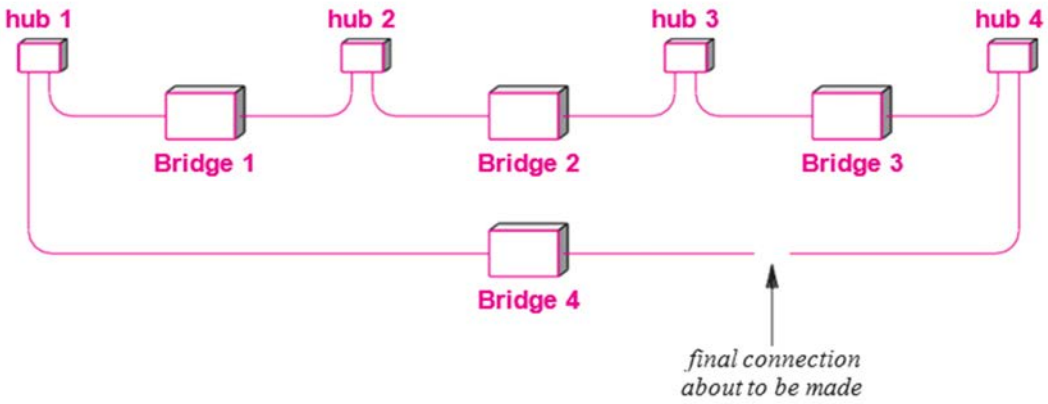


Figure 14.4: A network with three bridges is shown in and a fourth bridge is ready to be added.

The network functions as intended before the fourth bridge is added; any computer may transmit a unicast frame to another computer or a broadcast or multicast frame to every machine. Since a bridge always forwards a copy of a frame delivered to a broadcast or multicast address, broadcast and multicast both function. There will be an issue if a fourth bridge is added since there would be a loop. Copies of a broadcast frame will continue to circulate around the cycle indefinitely if at least one bridge is not prevented from forwarding broadcasts, with computers connected to hubs receiving an infinite number of copies.

Bridges use a technique that computes a Distributed Spanning Tree to stop a cycle from becoming an unending loop (DST). To put it another way, the algorithm treats bridges like nodes in a network and imposes a tree on the graph (a tree is a graph that does not contain cycles). The original method, known as the Spanning Tree Protocol, was created in 1985 at Digital Equipment Corporation for Ethernet networks (STP).

Selecting a root is the first step. Simple voting occurs when bridges multicast a packet containing their bridge IDs; the bridge with the shortest ID wins. A bridge ID is made up of a 48-bit MAC address and a 16-bit changeable priority number that allows a manager to govern the election. A bridge analyses the priority component of an ID first and breaks ties using the MAC address portion. By giving a bridge a priority that is lower than all other bridge priorities, a manager may ensure that a bridge becomes the root.

Calculating the shortest route is the second stage. The shortest route to the root bridge is calculated for each bridge. As a consequence, the spanning tree is made up of connections that are part of all bridges' shortest pathways.

Bridges start passing packets after computing a spanning tree. An interface connected to the shortest route is enabled for packet forwarding; an interface not on the shortest path is blocked, meaning no user packets may be transmitted through the interface.

Spanning tree has several intended and specified versions. IEEE developed the 802.1d standard, which underwent an upgrade in 1998. A physical medium is shared by a number of conceptually distinct networks that may operate in harmony without interfering with one another according to IEEE standard 802.1q. For usage on a VLAN switch, Cisco developed a proprietary form of spanning tree called Per-VLAN Span- ning Tree (PVST), and then

upgraded the protocol to PVST+ to make it compliant with 802.1q. The Rapid Spanning Tree Protocol was created in 1998 as part of IEEE standard 802.1w to speed up convergence after a topology change. STP has been replaced by Rapid Spanning Tree, which was introduced into 801.1d-2004. To support increasingly sophisticated VLAN switches, versions such as the Multiple Instance Spanning Tree Protocol (MISTP) and Multiple Spanning Tree Protocol (MSTP) were designed; MSTP was included in IEEE standard 802.1q-2003.

Layer 2 switches and switching

The idea of bridging clarifies switching, the fundamental component of contemporary Ethernets. An electronic hub-like device known as an Ethernet switch is sometimes referred to as a Layer 2 switch. A switch, like a hub, has several ports that each connect to a single computer. A switch also enables computers to transfer frames to one another. By convention, hexadecimal is used to represent Ethernet addresses, with colons between each set of two hex digits. Switching and VLAN switches are discussed in the following sections. A hub functions as an analogue device that transfers signals between computers, while a switch is a digital device that sends packets. This difference in operation is what distinguishes a hub from a switch. A switch may be thought of as replicating a bridged network with one computer per LAN segment, whereas a hub can be thought of as simulating a shared transmission channel. Bridges are conceptually used in a switch in Figure 14.5.

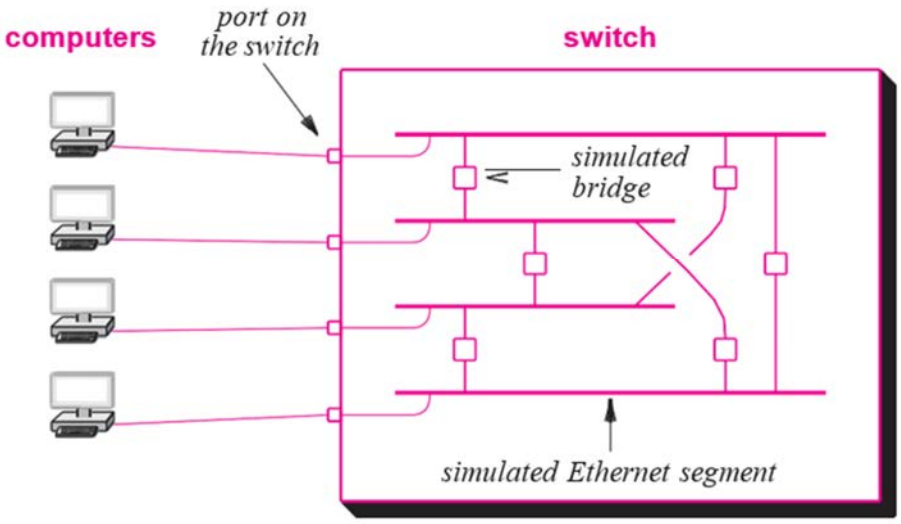


Figure 14.5: A switched Network is conceptually organized.

Despite the conceptual representation in the illustration, a switch does not have distinct bridges. Instead, a switch is made up of a core fabric that enables simultaneous transmission between pairs of interfaces and an intelligent interface coupled to each port. In order to receive an incoming packet, examine a forwarding table, and transfer the packet through the fabric to the appropriate output port, an interface must have a CPU, memory, and other hardware. Moreover, the interface receives packets from the fabric and sends them out the port. Most importantly, an interface may buffer incoming packets while an output port is busy because it has memory. As a result, if computers 1 and 2 simultaneously submit packets to computer 3, interfaces 1 or 2 will retain the packet while the other interface transmits. Figure 14.6 shows how the structure is laid up. Switches come in a wide variety of sizes on a physical level. The smallest consists of a cheap standalone device with four connections, enough to connect a computer, a printer,

and two other devices, such a scanner. To link tens of thousands of computers and other devices around the enterprise, businesses utilise the biggest switches.

Parallelism is the main benefit of a switched LAN over a hub. Whereas a hub can only handle one transmission at once, a switch allows for several transfers to take place simultaneously, provided that each transfer is independent (i.e., only one transfer is taking place at a time).

Layer 2 switches and switching

At any one moment, 301 packets are being transmitted to a certain port. Hence, N/ 2 transfers may happen simultaneously if a switch has N ports that are linked to N computers. The key is:

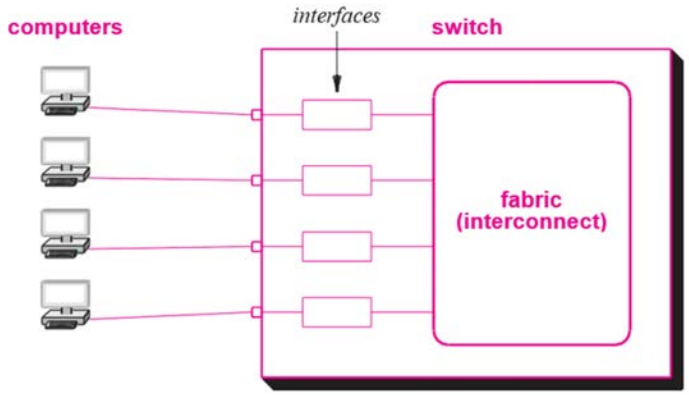


Figure 14.6: Example of a switch's construction

VLAN switches:

A switch that has been expanded via the addition of virtualization is referred to as a virtual local area network switch (VLAN switch). The idea is simple: use a manager to set up a single switch to mimic many independent switches. In other words, a manager identifies a set of switch ports to be part of virtual LAN 1, another set of ports to be part of virtual LAN 2, and so on. Only computers on the same virtual LAN as the broadcasting computer (computer on virtual LAN 2) receive the packet (i.e., once configured, a VLAN switch makes it appear that there are multiple switches).

It may not seem vital to divide computers into distinct broadcast domains until a major corporation or service provider is taken into account. In each situation, it can be crucial to ensure that a group of computers can interact without one another receiving their packets or outsiders sending them. A business could decide to install a firewall between the CEO's office PCs and other computers across the organisation, for instance. Installing a firewall is made possible by configuring a different VLAN for the CEO's computers.

Bridging With Additional Devices

While a bridge is described in our definition as a standalone device, bridging is a basic idea that has been used to other technologies. A DSL or cable modem, for instance, does bridging by setting up an Ethernet connection at the subscriber's home and transmitting Ethernet packets between that site and the provider's network. A sort of bridging is also used by certain wireless technologies to transmit frames from a mobile device to a service provider's network.

CHAPTER 15

DYNAMIC ROUTING AND WAN TECHNOLOGY

Vanitha K, Assistant Professor,
Department of Computer Science and Engineering, Jain (Deemed to be University)
Bangalore, India
Email Id- k.vanitha@jainuniversity.ac.in

This section of the work includes that cover various wired and wireless packet switching methods. LAN extensions were discussed in the preceding. This examines the design of a network that can cover any size region. The teaches the fundamental idea of routing as well as the basic building blocks required to create a packet switching system. The outlines the benefits of each of the two fundamental routing algorithms. A following introduces routing protocols that make use of the algorithms discussed here and expands the study of routing to the Internet.

Wide Area Networks with Long Spans

According to the distance covered, networking technologies may be categorized, as follows:

PAN — covers an area close to a person LAN — covers a structure or campus a sizable metropolitan region is covered by MAN. WAN — connects many cities or nations. Think about a business that links the LANs at two different locations via a satellite bridge. Should the network be considered an expanded LAN or a WAN? Does the answer alter if each location of the business simply has a PC and a printer? That does, really. The main difference between WAN and LAN technologies is scalability. A WAN must be able to expand as necessary to link several locations spread over vast distances, each with numerous computers. A WAN, for instance, ought to be able to link all the computers in a large company that has facilities scattered across thousands of square miles in dozens of sites, including offices and factories. A technology is also not considered a WAN unless it can provide enough performance for a big network. This means that a WAN must have enough bandwidth to allow communication amongst all computers, rather than just connecting to numerous computers at various places. Thus, a satellite bridge that links two PCs and printers is just an extended LAN.

Modern WAN Architecture

Conventional WAN technologies were created prior to the emergence of local area networks, the availability of personal computers, and the creation of the Internet. Therefore, classic WAN designs were created to link a collection of locations, where each location had a small number of massive computers. As LAN technologies were not yet accessible, WAN designers made the decision to develop a specialised hardware device that could be installed at each location. The equipment, sometimes referred to as a packet switch, offers connections for data circuits that link to other locations as well as local connections for computers at the location. Packet switch is theoretically made up of a compact computer system comprising a processor, memory, and I/O devices for sending and receiving packets. Early packet switches were built using standard computers, but the fastest WAN packet switches need specialised hardware. Figure 15.1 shows how the internal architecture is constructed.

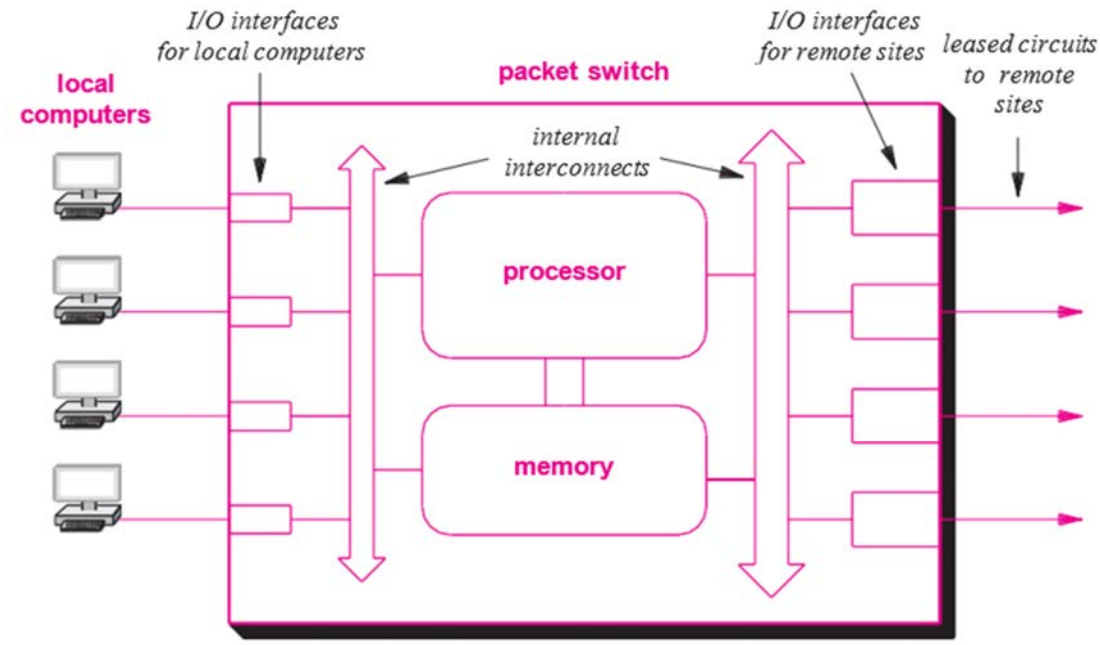


Figure 15.1: Example of a conventional packet switch design

A packet switch comprises two different kinds of I/O devices, as shown in the image. The switch is linked to a digital circuit by the first, a fast-operating one, which then connects to another packet switch. The switch's connection to a specific computer is made using the second kind of I/O device, which runs slower.

With the invention of LAN technology, the majority of wide area networks (WANs) divide a packet switch into two components: a Layer 2 switch for connecting nearby computers and a router for connecting to distant locations. It is necessary to know that transmission via a WAN and communication with local computers may be separated for the time being to appreciate how the principles taught here relate to the Internet in Part 4 of the book. Figure 15.2 shows how the separation is done.

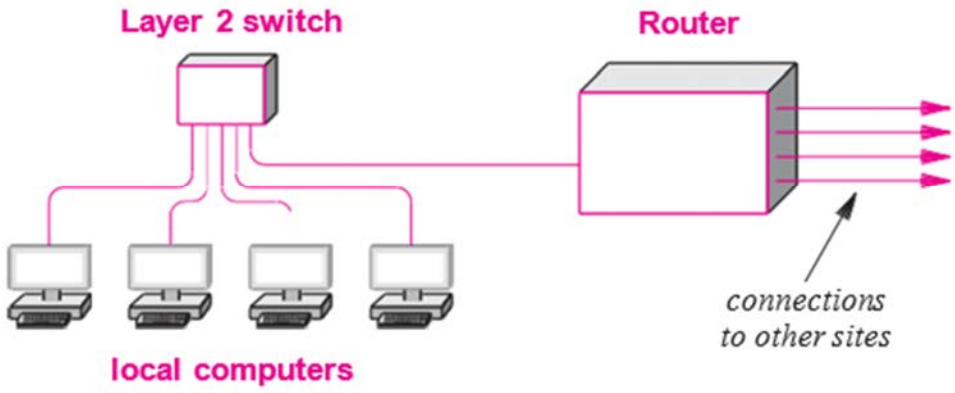


Figure 15.2 shows an example of a contemporary WAN site with a separate LAN managing local communication.

Creating A WAN:

In theory, a WAN may be created by linking a number of locations. The required data rate, the distance to be covered, and the acceptable latency all affect the specifics of the interconnections. Leased data lines are used by several WANs (e.g., a T3 circuit or an OC-12 circuit). Nonetheless, there are still more formats, including satellite and microwave channels. A designer must choose a topology in addition to the technology for a connection. There are several topologies that might exist for a certain collection of sites. Figure 15.3, for instance, shows one conceivable method of interconnecting eight computers and four conventional packet switches.

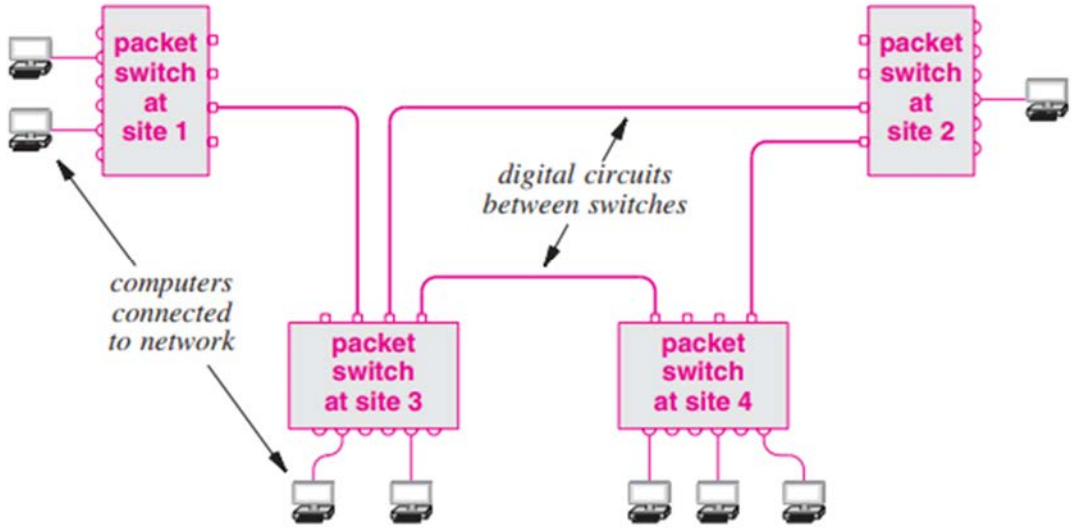


Figure 15.3: Shows a WAN made up of connected packet switches as an example.

The connections between packet switches and the capacity of each link may be selected to accommodate the anticipated traffic and offer redundancy in the event of failure, as shown in the figure. A WAN does not necessarily need to be symmetric. According to the illustration, the packet switch at site 1 has only one external connection, but the packet switches at the other sites all have at least two.

Store-and-Forward Model

Having as many computers deliver packets concurrently as feasible is the aim of a WAN. Store and forward is the underlying paradigm that allows for simultaneous transmission. A packet switch buffers packets in memory for store and forward processing. When a packet arrives, the store operation takes performed, and the packet switch's I/O hardware stores a copy of the packet in memory. After a packet has arrived and is waiting in memory, the forward action takes place. The processor looks through the packet, finds its destination, and then transmits it via the I/O interface leading there.

A system that employs the store and forward paradigm may maximise performance by maintaining data connection activity. More importantly, the packet switch may accept and keep packets in memory until the output device is ready if many packets are supplied to the same output device. Take packet transfer on the network shown in Figure 15.3 as an example. Let's say that at around the same moment, each of the two computers at site 1 creates a packet that is headed for a computer at site 3. Both computers may simultaneously transmit a packet to the

packet switch. Each time a packet comes in, the packet switch's I/O hardware stores it in memory and notifies the CPU. The processor looks at each packet's destination and decides that site 3 should receive the packets. When a packet arrives and the output interface that connects to site 3 is not in use, transmission begins right away. The CPU adds the outgoing packet to a queue for the output device if it is in use. The device extracts and transmits the next packet in the queue as soon as it has finished delivering a packet.

Addressing in a WAN

An associated computer's perspective of a standard WAN network is similar to that of a LAN. The precise frame format that a computer uses to transmit and receive data is defined by each WAN technology. Every machine linked to a WAN is also given an address. The sender must provide the destination address when transmitting a frame to another machine. While specifics vary, WAN addresses adhere to a fundamental Internet principle called hierarchical addressing. Hierarchical addressing separates each advertisement into two components conceptually:

In reality, each packet switch is given a unique number rather than a site-specific identifier, thus the first half of an address really identifies a packet switch and the second part identifies a particular computer. Figure 15.4 illustrates two-part hierarchical addresses for machines linked to two packet switches as an example.

Figure 15.4: A packet switch and any computers connected to the switch are identified by their respective addresses in Figure example address hierarchy.

Each address is shown in the picture as a pair of decimal numbers. A computer connecting to port 6 on packet switch 2 is given the address, for instance. In actuality, an address is encoded as a single binary value, with certain bits used to denote a packet switch and others to signify a machine. We shall see that the Internet employs the same system in Part 4 of the book. Each Internet address is made up of a binary number, where a prefix of the bits designates a particular Internet network and the remaining bits specify a machine that is connected to that network.

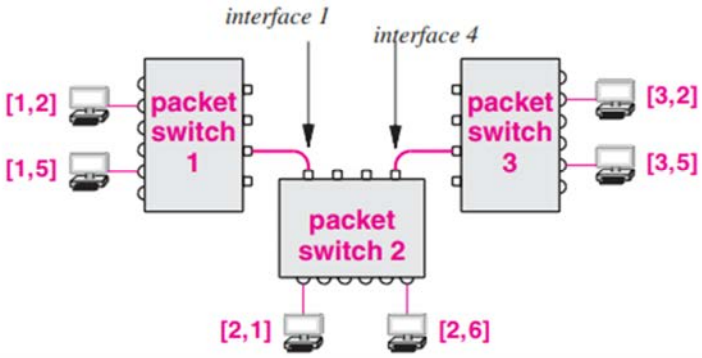
Next-Hop Forwarding:

When one examines packet processing, the value of hierarchical addressing is evident. A packet switch must decide which outgoing route to send a packet through when it arrives. The switch transfers a packet straight to the computer if it is meant for a nearby machine. If not, one of the connections leading to another switch must be used to forward the packet. A packet switch checks the destination address in the packet and extracts the packet switch number before making a decision. The packet is meant for a computer on the local packet switch if the destination address' number matches that device's own ID. If not, the packet is meant for a machine connected to a different packet switch. The key point is that a switch does not have to calculate the whole path a packet will take across the network or have comprehensive knowledge of how to reach all potential computers. Instead, a switch bases forwarding on

packet switch IDs, necessitating just knowledge of the appropriate outgoing link to connect to a specific switch.

We state that a switch merely needs to determine a packet's next hop. The procedure, known as "next-hop forwarding," is comparable to how airlines advertise trips. Let's say a traveller on a journey from San Francisco to Miami discovers there are only three flights that can be booked: one from San Francisco to Dallas, one from Dallas to Atlanta, and one from Atlanta to Miami. Miami stays the final destination throughout the journey, however the next hop varies at each airport. The next stop after the traveller departs San Francisco is Dallas. Miami is the next stop after Dallas for the passenger, while Atlanta is the stop after Atlanta for the passenger.

Table lookup is a technique used by packet switches to speed up calculation. To put it another way, each packet switch has a forwarding table that identifies all potential packet switches and specifies a next hop for each. Figure 15.5 provides a simple example to show next-hop forwarding.



to reach	send to
switch 1	interface 1
switch 2	local delivery
switch 3	interface 4

Figure 15.5 shows a network with three packet switches and the second switch's next-hop forwarding table.

The packet switch component of the destination address is used by the switch as an index in the forwarding table when using a forwarding table. Take the table in Figure 15.5, for instance. The switch extracts 3, reads the table, and transmits a packet to interface 4 that connects to switch 3 if it is intended for.

There are two practical repercussions when a packet is sent using just one element of a two-part hierarchical address. The forwarding table may be set up as an array that employs indexing rather than searching, which reduces the calculation time needed to send a packet. Second, rather of having one entry for each destination computer, the forwarding table now has one record for each packet switch. With several computers connected to each packet switch in a wide WAN, the decrease in table size may be significant.

In essence, until the packet reaches the final switch, a two-part hierarchical addressing system permits packet switches to utilise just the first part of the destination address (i.e., the switch to which the destination computer is attached). When the packet reaches the last switch, the switch selects a particular computer using the second half of the address.

Source Independence

It should be noted that next-hop forwarding is independent of both the packet's original source and the route it took to get to a specific packet switch. Instead, only the packet's destination determines which hop it will go to next.

The forwarding mechanism in a computer network may be efficient and small due to source independence. There is only need for one table since every packet takes the same route. The only part of a packet that has to be removed is the destination address since forwarding does not require source information. Also, a single mechanism manages packet forwarding consistently; both packets coming from other packet switches and those coming from directly linked computers utilise the same method.

WAN Dynamic Routing Updates

Each switch needs a forwarding table and must pass packets for a WAN to function properly. Moreover, the forwarding table's values must ensure the following:

Communication on a global scale. Every conceivable destination address must have a valid next-hop route in the forwarding table of each switch. The best routes. The next-hop value in a switch's forwarding table for a particular destination must link to the shortest route there. Forwarding is further complicated by network issues. For instance, forwarding should be altered to avoid the unavailable route if there are two pathways leading to a given destination and one of the paths becomes inaccessible due to hardware failure (for instance, a circuit gets unplugged). Hence, a manager cannot simply set a forwarding table's static values to include constant values. Instead, software running on the packet switches checks for errors continuously and updates the forwarding tables on its own. Software that automatically modifies forwarding tables is referred to as routing software.

The simplest approach to conceptualise route computation in a WAN is to picture a network-modeling graph, and then picture computer software that uses the graph to determine the shortest path to every potential destination. Each node in the graph represents a network packet switch (individual computers are not part of the graph). A graph has an edge or link between the respective nodes if the network has a direct connection between a pair of packet switches. Figure 15.6, for instance, displays a sample WAN and the related graph. Due of the close connection between graph theory and computer networking, terms like "link" and "network node" are often used to describe data circuits connecting two locations.

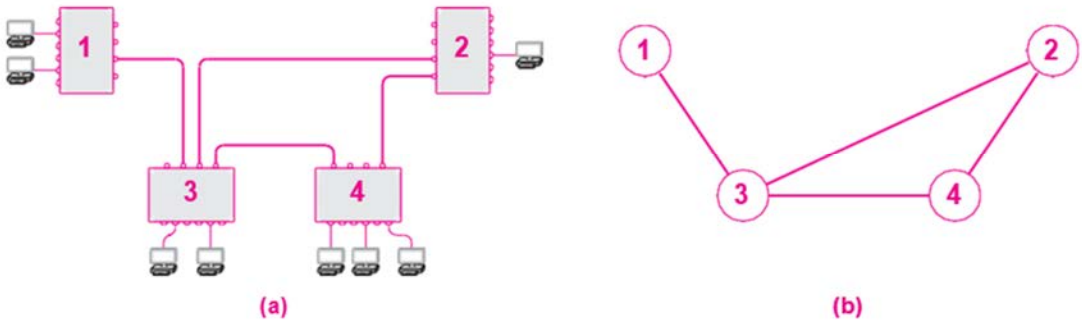


Figure 15.6: A WAN is seen in Figure along with the associated graph.

Nodes in the graph are given labels that match to the numbers supplied to the associated packet switches, as shown in the image. Since graph theory has been explored and effective algorithms have been created, a graph representation is particularly helpful in calculating next-hop forwarding. Also, a graph abstracts away the details so that routing software may focus on the core of the issue. A routing method must identify a connection in order to calculate next-hop forwarding for a graph. In our examples, a connection from node k to node j will be shown by

the notation (k, j). As a result, when a routing algorithm is applied to the graph in Figure 15.6b, the output is as shown in Figure 15.7.

to reach	next hop
1	–
2	(1,3)
3	(1,3)
4	(1,3)

node 1

to reach	next hop
1	(2,3)
2	–
3	(2,3)
4	(2,4)

node 2

to reach	next hop
1	(3,1)
2	(3,2)
3	–
4	(3,4)

node 3

to reach	next hop
1	(4,3)
2	(4,2)
3	(4,3)
4	–

node 4

Figure 15.7 each node in the graph shown in Figure 15.6b has its own forwarding table.

Standard Routes

A forwarding table may have many entries that link to the same next hop, as shown by the forwarding table for node 1 in Figure 15.7. The packet switch has only one connection to the network, which explains why all distant entries have the same next hop when the WAN in. The same connection must be used to send all traffic. So, every item in node 1's forwarding table has a next hop that links to the connection from node 1 to node 3, except from the entry that belongs to the node itself.

In our flimsy example, there aren't many duplicate forwarding table entries. A huge WAN, however, can have hundreds of duplicate entries. The majority of WAN systems provide a technique that may be used to remove duplicate entries, which is a frequent occurrence. The approach, known as a default route, enables a single item in a forwarding table to take the place of a lengthy sequence of entries with the same next-hop value. In a forwarding table, only one defect entry is permitted, and it has lower priority than the other entries. The default is used if the forwarding mechanism cannot discover an explicit entry for a specified destination. The forwarding tables from Figure 15.8 are updated in Figure 15.8 to utilise a default route.

to reach	next hop
1	–
*	(1,3)

node 1

to reach	next hop
2	–
4	(2,4)
*	(2,3)

node 2

to reach	next hop
1	(3,1)
2	(3,2)
3	–
4	(3,4)

node 3

to reach	next hop
2	(4,2)
4	–
*	(4,3)

node 4

Figure 15.8: The forwarding tables from Figure, with an asterisk next to the default routes.

Routing by default is optional; a default item only appears when many destinations have the same next-hop value. Since each item has a different next hop, the forwarding table for node 3 does not, for instance, have a default route. Yet, since every distant target has the identical next hop, the forwarding table for node 1 benefits from a default route.

Static rerouting. When a packet switch boots, a software computes and installs routes; the routes do not change route that changes. As a packet switch boots, a software creates an initial forwarding table, which it then modifies when network circumstances change. There are benefits and drawbacks to each strategy. Static routing's main benefits are simplicity and minimal overhead. The main drawback is rigidity; when connectivity is interrupted, static routes cannot be modified. Most WANs employ a kind of dynamic routing since big networks are built with redundant connections to manage sporadic hardware failures.

Distributed Route Computation

When network-related data is graph-encoded, a forwarding table may be generated using algorithm. WANs must really compute dispersed routes in reality. This means that each packet switch must locally calculate its own forwarding table rather than relying on a centralised software to determine all shortest pathways. Distributed route calculation must include all packet switches. There are two types in general: Distance-Vector Routing (DVR), which employs a different strategy, utilises Link-State Routing (LSR), which employs Dijkstra's algorithm. Each of the two strategies is described in the following sections. Each method's application to controlling Internet routes.

Link-State Routing

Shortest Path First, or SPF routing, is the abbreviation for what is officially known as link-state routing or link-status routing. The language is a result of Dijkstra's usage of it to describe how the algorithm works. Nonetheless, it is a little deceptive since all routing algorithms seek discover the shortest pathways. Packet switches regularly transmit messages across the network with the status of a connection between two packet switches in order to employ LSR routing. The connection between packet switches 5 and 9 is up, for instance, according to a measurement made by the switches. All switches get each status message that is transmitted. Every switch is equipped with software that gathers incoming status information and utilises them to create a network diagram.

Hardware faults may be accommodated via an LSR algorithm. A failure in a connection between packet switches will be detected by the associated packet switches, who will then broadcast a status message indicating that the link is down. After receiving the broadcast, all packet switches update their copies of the graph to reflect the modified connection state and recalculate the shortest pathways. Similar to when a connection is restored to availability, the packet switches attached to the link recognise that it is operational and begin providing status signals that signal the availability of the link.

Distance Vector Routing

The Distance-Vector Routing (DVR) approach is the main LSR substitute. The distance to a destination between two packet switches is defined as the total of the weights along the route between the two, much as with LSR, where each link in the network is given a weight. Distance-vector routing provides for packet switches to communicate on a regular basis, similar to LSR. A distance-vector system, in contrast to LSR, allows a packet switch to communicate

a comprehensive list of destinations together with the current cost of reaching each. A packet switch essentially delivers a string of distinct statements in the form of a DVR message when it sends one. "Destination X is within my grasp, and its present distance from me is Y."

Not aired are DVR messages. Instead, every packet switch sends a DVR message to its neighbours on a regular basis. Each message includes two of (destination, distance). Each packet switch must thus maintain a list of potential destinations, the distance to the destination as of the present time, and the next hop to utilise. The forwarding table contains a list of destinations together with the next hop for each. We may consider DVR software to be a forwarding table extension that keeps track of the distances to each destination.

When a message from neighbour N reaches a packet switch, that switch examines each item in the message and modifies its forwarding table if the neighbour has a shorter route than the one presently in use to a particular destination. The existing next hop for D will be replaced by neighbour N, and the cost to reach D will be five plus the cost to reach N, for instance, if neighbour N advertises a route to destination D as having cost five while the present trip via neighbour K has cost one hundred. Routes are modified while utilising the distance-vector technique.

Distributed Route Calculation

Algorithm

Provided are a local forwarding table, a distance to each neighbor's location, and an incoming DV message from a neighbour.

Create a new forwarding table. Method:

Each forwarding table item should continue to include a distance field; Create a single item in the forwarding table to serve as the table's initial entry, with the destination set to the local packet switch, the next hop left empty, and the distance set to 0; Wait for a routing message from a neighbour to come through the network; make the sender switch N; for each item in the message, make V the destination, and make D the distance; repeat indefinitely; Add the weight associated with the connection where the message arrived to D to get C; Check and make changes to the regional routing table: If (no route exists to V), add an entry for destination V with next-hop N and distance C to the local routing table; Instead, if (a route exists with next-hop N), replace the existing route's distance with C; Change the next-hop to N and distance to C if (a route exists with a distance larger than C);

Graph Shortest Path Calculation

Software employs Dijkstra's Algorithm to determine the shortest route from a source node to each of the other nodes in the graph after creating a graph that corresponds to a network; a next-hop forwarding table is formed during the calculation of shortest paths. Every node in the network must have one iteration of the method. That is, the node that corresponds to packet switch P is chosen as the source node, and the method is executed to calculate the forwarding table for packet switch P.

The versatility of Dijkstra's algorithm makes it useful for a variety of shortest route definitions. The method, in particular, does not demand that graph edges indicate geographic distance. Instead, the approach enables the assignment of a nonnegative value known as a "weight" to each edge and defines the distance between two nodes as the sum of the weights along a route between the nodes. The following is crucial: A sample graph with an integer weight given to

each edge and a least-weight route connecting two nodes is shown in Figure 15.9 to help explain the idea of weights.

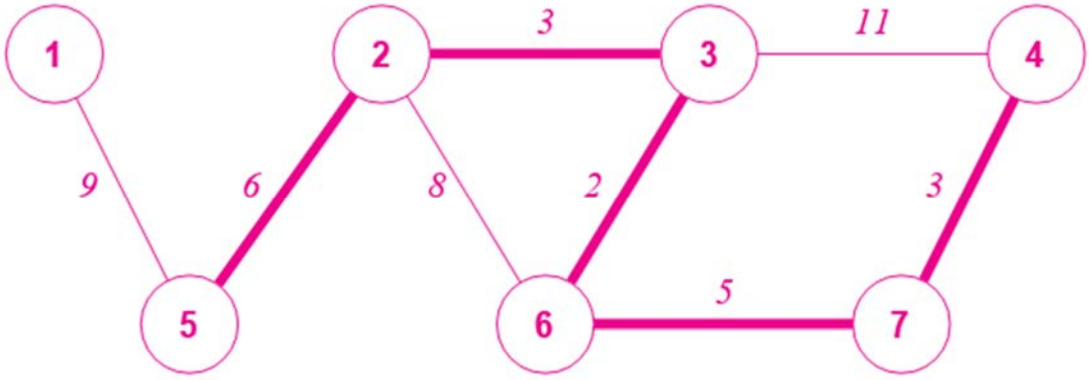


Figure 15.9 an illustration of a graph with weights given to each edge and a darkened shortest route between nodes 4 and 5.

A collection of nodes, S, is kept in the Dijkstra algorithm for which the minimal distance and subsequent hop have not yet been determined. All nodes in the set—aside from the source—are initialised. After then, the procedure repeats until set S is empty. The algorithm eliminates a node from S on each iteration that is closest to the source. The method checks the current distance from the source to each of node u's remaining neighbours as it removes node u. If a route leads through you to the nearby area. The method changes the distance to the neighbour when bor has less weight than the present route. The method will have determined the minimal distance to each node and a proper next-hop forwarding table for all feasible pathways after all nodes have been eliminated from S.

The Dijkstra algorithm is simple to put into practise. The current distance to each node, the subsequent hop for the shortest route, and data about the remaining set of nodes are three data structures that Dijkstra's method requires in addition to the data structure used to store information about the graph. As shown in Figure 15.9, nodes may have a number between 1 and n. This enables efficient implementation since a node number can be used as an index into a data structure. The approach may specifically make use of two arrays, D and R, which are both indexed by the node number. A current value for the shortest distance between the source and node I is kept in the ith item of array D. The next hop along the route being calculated is stored in the ith item of array R. A doubly linked list of node numbers may be used to maintain the set S, making it easier to search the whole set or remove an element.

How to determine the shortest routes in a graph is described in Algorithm 15.2. Weight (i,j) is a function that the algorithm employs to return the weight of the edge from node I to node j. If there is no edge from node I to node j, it is expected that function weight will return the reserved value infinite. In reality, any number may be used to symbolise infinity as long as it is more than the total of the weights along each route in the graph. The total of all weights on all edges may be increased by one to get a value of infinity.

One approach may be used to various distance measurements by allowing variable weights to be provided to graph edges. For instance, some WAN systems calculate the number of packet shifts along a route to determine the distance. The algorithm for such technologies assigns a

weight of 1 to each edge in the graph. The capacity of the underlying connections is reflected in the weights given in other WAN technologies. One option is for a manager to give links weights in order to manage routing. Consider a scenario in which there are two distinct pathways between a pair of packet switches, one of which is labelled as the main path and the other as a backup path. A manager may give the main connection a low weight and the other link a high weight to enforce such a policy. Unless the route is unavailable, in which case routing software will use the alternate way, routing software will arrange forwarding tables to utilise the low weight path.

Router Issues

The shortest pathways will be determined using either LSR or DVR routing, in principle. Also, each strategy will ultimately converge, which means that all packet switches' forwarding tables will be in agreement. Nonetheless, issues do arise. Two packet switches, for instance, may argue on the shortest route if LSR messages are missed. A link loss might lead two or more packet switches to form a routing loop where each packet switch believes the next packet switch in the set is the quickest way to a certain destination, making DVR issues more severe. A packet may thus continue to travel across packet switches forever.

Backwash is one of the main causes of issues with DVR systems (i.e., a packet switch receives information that it sent). Consider the following scenario: A switch informs its neighbours that it may reach destination D1 at a cost of 3. The switch will delete the entry for destination D1 from its forwarding table if the connection leading there fails (or mark the entry invalid). But, the switch has informed the nearby residents of the path. Imagine that a neighbour sends a DVR message saying specifically, "I can reach destination D1 at cost 4" just after the connection breaks. Sadly, the message will be taken at face value, leading to a routing loop.

The majority of useful routing algorithms include restrictions and heuristics to avoid issues like routing loops. For instance, split horizon is a technique used in DVR systems to ensure that switches do not broadcast information back to their source. In addition, the majority of realistic routing systems contain hysteresis, which inhibits the programme from undergoing a lot of changes quickly. Yet, routing issues might arise in a big network when several connections periodically fail and recover.

CHAPTER 16

NETWORKING TECHNOLOGIES

C R Manjunath, Associate Professor,
Department of Computer Science and Engineering, Jain (Deemed to be University)
Bangalore, India
Email Id- cr.manjunath@jainuniversity.ac.in

For each fundamental kind, several networking technologies have been established throughout the years. Some that were once of great significance have vanished into oblivion, while others still fulfil a specific need. This succinct summarises some of the key technologies and details their key traits and features. These are only a few instances that illustrate the wide range of technologies that have been developed and how swiftly they evolve.

Access and Connectivity Technologies

Other technologies have been developed, including wireless access mechanisms and one that transmits data through power lines. The group of technologies may be distilled into the following:

Synchronous optical network (SONET) or digital hierarchy

Originally intended to transport digital voice calls, SONET and the related TDM hierarchy were created. For the digital circuits used on the Internet, the technology has emerged as the norm. In order to provide redundancy, SONET supports the construction of physical rings. Data can still pass through even if a portion of the ring is destroyed since the technology can automatically identify and fix issues. A site is connected to a SONET ring using an Add-Drop Multiplexor. The Add-Drop Multiplexor inserts or terminates a group of data circuits, each of which connects to another Add-Drop Multiplexor on the ring, thus giving origin to the word. Time-division multiplexing is used by SONET to multiplex the circuits onto the supporting fibre. For circuits that may be built over a SONET ring, such a T3 circuit, SDH offers the well-known standards.

Optical carrier

The signalling used on an optical fibre SONET ring is defined by the OC standards. Compared to the T-series standards offered by SDH, OC standards provide faster data rates. A private business may decide to rent an OC circuit to link two of its locations. Circuits of OC-192 (10 Mbps) and OC-768 (40 Mbps) are used by Tier 1 ISPs in the Internet backbone.

Cable and Digital Subscriber Line (DSL) Modems

These two technologies have become the main methods for giving private houses and small enterprises access to the wide-band Internet. Both DSL and cable modem technologies leverage pre-existing telephone landlines and cable television infrastructure, respectively. Depending on the distance between a central office and a subscriber, DSL delivers data speeds of 1 to 6 Mbps; cable modems give up to 52 Mbps, however the capacity is shared among a number of users. Both systems are seen as transitory until optical fibre is accessible to the curb or to the residence.

WiMAX and Wi-Fi

Wi-Fi is a group of wireless technologies that have gained popularity for providing Internet access in public places including airports, hotels, cafés, and residences. The total data rates have grown across Wi-Fi technology generations. A MAN may be created using WiMAX, a new wireless technology. Both access and backhaul capabilities are offered by WiMAX, which has two specified versions to handle both stationary and mobile endpoints.

Extremely Small Aperture Satellite:

Internet connectivity through satellite is now accessible for individuals or small enterprises thanks to VSAT technology, which have dishes smaller than 3 metres. High data speeds are provided through VSAT, although there are significant delays.

Electricity line communication

PLC transmits data across power lines using high frequencies. The concept is to provide Internet access using existing infrastructure. Despite extensive development, the technique has not seen broad adoption.

LAN technologies

As LANs were developed, several organisations came up with designs or constructed test prototypes. Twenty years were spent developing new LANs, during which time a number of LAN technologies were well-liked and profitable. It's interesting to note that LAN technology has started to converge; new LANs are unanticipated.

IBM Fork Ring

Token passing as an access control technique was investigated in some of the first work on LANs. IBM made the decision to develop IBM Token Ring, a token-passing LAN system. As compared to its rival, Ethernet, which ran at 10 Mbps, the first iteration of IBM's Token Ring ran at 4 Mbps. Subsequently, IBM released a Token Ring variant that operates at 16 Mbps. While it had a low data rate and was expensive, IBM's Token Ring was well-liked by corporate IT departments and remained a significant LAN technology for many years. By the late 1980s, it was clear that the two main LAN technologies—Token IBM's Ring at 16 Mbps and Ethernet at 10 Mbps—were unable to keep up with the expanding demand. To raise LAN data speeds to 100 Mbps, the FDDI standard was developed. Designers proposed rewiring workplaces to provide fibre to the desktop at the time, arguing that increased data speeds necessitated using optical fibre rather than copper wire. Moreover, FDDI employed two counter-rotating rings to enhance redundancy; in the event that one of the rings failed, hardware would automatically loop the data line to divert traffic around the issue and maintain the ring operational. The last early LAN switch was introduced by FDDI, which allowed each computer to connect directly to the main FDDI mechanism. Hence, it was conceivable to have both a logical ring topology and a physical star topology.

FDDI gained popularity as a high-speed link among computers in a data centre because it provided the maximum attainable data rate and the potential for redundancy. Unfortunately, most businesses opted not to replace copper wire due to the high cost and specialised knowledge required for fibre installation. FDDI supporters developed a variant of FDDI called CDDI that operated over copper cable while development on Fast Ethernet continued. Finally, Ethernet was found to be more affordable, and FDDI technologies were abandoned.

Ethernet

In a certain sense, Ethernet has won the race and has taken over the LAN market totally. In fact, Ethernet LAN deployments outnumber those of every other LAN type. In a sense, new technology that is still referred to as Ethernet has entirely supplanted Ethernet. One might see, for instance, that there is essentially no similarity between the wiring and signalling used with gigabit Ethernet and the hefty coaxial cable and RF signalling used in early Ethernet. In addition to increases in data rate, hubs have taken the role of cables, Ethernet switches have taken the place of hubs, and switches have been replaced by VLAN switches.

WAN Technologies

Several technologies have been developed for Wide Area Networks testing and production usage. Some examples that highlight some of the diversity are provided in this section.

ARPANET

WANs with packet switching are just a few decades old. The U.S. Department of Defense requested funding for networking research in the late 1960s from the Advanced Research Projects Agency (ARPA). To ascertain if packet switching technology would be useful for the military, a significant ARPA research effort created a wide-area network. One of the earliest packet switched WANs was the network known as the ARPANET. Researchers from academia and industry were linked through the ARPANET. The ARPANET was sluggish by today's standards (leased serial data lines linking packet switches ran at just 56 Kbps), but it left behind ideas, techniques, and terminology that are still in use today.

The ARPANET served as the main network for communication and experimentation among academics when the Internet project first got underway. Everyone connecting to the ARPANET was mandated by ARPA to switch from the old protocols to the Internet protocols starting in January 1983. The ARPANET was the first Internet backbone as a result.

The International Telecommunications Union (ITU), which creates global telephony standards, created the first WAN standard that was widely adopted by public carriers. The standard is still referred to as the CCITT X.25 standard since the ITU at the time was known as the Consultative Committee for International Telephone and Telegraph (CCITT). In Europe as opposed to the US, X.25 networks were more widely used. An X.25 network consisted of two or more X.25 packet switches linked by leased lines, following the conventional WAN architecture. Direct connections between computers and packet switches. With X.25, data was sent using a connection-oriented paradigm similar to a phone call, which required a computer to first establish a connection.

While X.25 was developed prior to the widespread usage of personal computers, many early X.25 networks were designed to link ASCII terminals to distant timesharing systems. An X.25 network interface recorded keystrokes as a user typed data on a keyboard, packaged each one into an X.25 packet, and sent the packets across the network. Similar to this, when a programme on a distant computer produced output, the computer sent the output to the X.25 network interface, which then packaged the data in X.25 packets for transmission back to the user's screen. X.25 services were promoted by telephone companies, however the technology was pricey compared to the performance it provided and has since been superseded by newer WAN technologies.

Relay Frame

A number of wide area network technologies have been developed by long-distance carriers to carry data. One such service, Frame Relay, was intended to take and distribute blocks of data, where each block may hold up to 8K octets of data. The fact that the creators intended to utilise Frame Relay service to connect LAN segments is one of the driving forces for the huge data size (and the name). In order to transfer packets from a LAN segment at one site to a LAN segment at another, a company with offices in two cities might purchase a Frame Relay service for each location. The designers selected a connection-oriented paradigm that was suitable for multi-office companies. Frame Relay therefore had popularity prior to the development of less expensive alternatives. Frame Relay was intended to operate at rates between 4 and 100 Mbps since it was established to handle data from a LAN segment (the speed of LANs when Frame Relay was created). Nevertheless, in reality, many consumers opted for slower connections that ran at 1.5 Mbps or 56 Kbps due to Frame Relay service's exorbitant cost.

Switched Multi-Megabit Data Service

SMDS is a high-speed wide area data service provided by long-distance carriers, similar to Frame Relay. It is regarded as a precursor to ATM since it was based on IEEE standard 802.6DQDB. Data is intended to be carried by SMDS rather than voice traffic. Most importantly, SMDS is designed to function at the fastest possible rates. For instance, header information in packets may use a significant portion of the bandwidth. SMDS limits the amount of data that each packet may include to 9188 octets in order to minimise header overhead. A unique hardware interface used to link computers to a network was also specified by SMDS. Data may be sent as quickly as a computer can transport the data into memory thanks to the unique interface.

As their name suggests, SMDS networks often function at rates more than 1 Mbps (i.e., faster than a typical Frame Relay connection). The ways in which the two services may be applied were different. Due to its lack of a link, SMDS was flexible. Nevertheless, the majority of telephone companies preferred connection-oriented technologies, therefore SMDS was not widely used and was eventually superseded.

Asynchronous Transfer Mode

The telecoms sector developed ATM as a replacement for the Internet and made a big deal out of it. ATM had lofty objectives when it first came into being in the 1990s. According to its creators, it would eventually replace all WAN and LAN technologies and create a totally consistent global communication infrastructure. ATM was created to manage voice and traditional voice telephone traffic in addition to data transfer. Also, compared to previous packet switching technologies, ATM will grow to far greater data rates, according to its creators.

Label Switching is the main innovation used in ATMs. While ATM is a connection-oriented technology, packets do not often carry addresses. A packet instead contains a tiny ID called a label. Moreover, a label may be modified each time a packet traverses a switch. Each link in the route is given a special label during connection setup, and the labels are then added to tables in the switches. The switch checks the current label as a packet arrives and replaces it with a replacement label. Theoretically, label switching can be carried out in hardware more quickly than traditional forwarding.

Designers of ATMs included several features, including systems to give end-to-end service assurances, to meet all potential usage (e.g., guaranteed bandwidth and bounds on delay). As engineers started to implement ATM, they found that the hardware was complicated and expensive because to the abundance of functions. Also, the technique used to construct label switched pathways was unusable due to its complexity. ATMs were thus not accepted and essentially disappeared.

Multi-Protocol Label Switching

Even though MPLS is not a network technology, the ATM project is important because engineers modified label switching for use in Internet routers. MPLS may be added as a feature to existing software, as opposed to totally replacing the underlying hardware, like ATM intended to accomplish. An MPLS router takes Internet packets, encases each in a unique wrapper, transports the packet through an MPLS path using label switching, unwraps the packet, and then resumes standard forwarding. In the heart of the Internet, MPLS is heavily used; tier 1 ISPs employ MPLS to permit some packets to travel a particular channel (e.g., a large customer that pays more can have packets follow a shorter path that is not available to lower-paying customers).

Digital Network for Integrated Services (ISDN)

In order to provide network service at a faster data rate than could be accomplished with a dial-up modem, telephone companies developed ISDN. 128 Kbps appeared quick when it was initially suggested. When it became available, the technology appeared dated considering the cost. ISDN has mostly been superseded by DSL, cable modems, or 3G cellular technologies, all of which provide much faster data speeds, in most of the globe.

People Use the Internet for Work

Every network technology has been created to adhere to a certain set of limitations. LAN technologies, for instance, are created to provide high-speed communication over limited distances, while WAN technologies are created to offer communication across vast regions. Consequently, there is no perfect networking technology for every requirement. A big company with a variety of networking demands requires many physical networks. More importantly, the business will have a variety of networks if it selects the sort of network that is suitable for each purpose. For instance, a leased data line may be used to link a site in one city with a site in another, even if a LAN technology like Ethernet would be the best option for connecting computers at a particular location.

The Universal Service Idea

It should be clear why having several networks is problematic: only computers connected to the same network can interact with one another. Large corporations started to acquire several networks in the 1970s, which highlighted the issue. Throughout the organisation, every network served as an island. Each computer was connected to a single network in many early installations, and workers had to choose the best machine for the job. In other words, an employee had access to several displays and keyboards, and was compelled to switch between computers in order to transmit a message over the necessary network.

When each network requires its own computer, users are neither happy nor productive. As a result, the majority of contemporary computer communication systems provide communication between any two computers, just as a telephone system enables communication between any two telephones. The idea, sometimes known as universal service, is a cornerstone of networking. With universal service, every user may transmit messages or data to any other user

from any computer in any company. Moreover, because all information is accessible to all computers, a user need not switch computer systems while changing tasks. Users are thus more productive as a consequence. To sum it up:

Universal Service in a Diverse World

Is it feasible to provide universal service across different networks that use diverse technologies, or does it imply that everyone must choose a single network technology? Just connecting the cables across networks cannot create a huge network due to incompatibilities. Additionally, since each technology has its own packet format and addressing scheme, extension methods like bridging cannot be employed with heterogeneous network technologies. As a result, a frame created for one network technology cannot be sent across a network using another technology. The key idea is as follows:

Internetworking

Researchers have devised a plan that offers universal service across heterogeneous networks despite the incompatibilities between network technologies. The method, known as internetworking, makes use of both hardware and software. A number of physical networks are linked together using additional hardware systems. The associated PCs' software then offers universal service. The resultant network of physically linked systems is referred to as an internetwork or internet.

Working online is quite universal. A specific example of this is the fact that an internet is not limited in size; internets with just a few networks exist, while the global Internet has tens of thousands of networks. Similar to this, there may be a wide range in the number of computers connected to each network on an internet; some networks may have zero computers connected, while others may have hundreds.

Router-based physical network connection

A router is the fundamental piece of hardware that joins disparate networks together. A router is a piece of independent hardware that is used to link different networks. Similar to a bridge, a router has a CPU, memory, and unique I/O interfaces for each network it connects to. A connection to a router is handled by the network in the same way as a connection to any other computer. As router connections are not limited to a certain network technology, the graphic depicts each network as a cloud. Two LANs, a LAN plus a WAN, or two WANs may all be connected via a router. Additionally, two networks that belong to the same general category may be connected by a router without using the same technology. A router, for instance, may link an Ethernet to a Wi-Fi network. Each cloud, thus, stands for a different network technology.

Internet Architecture

Organizations may use routers to link all networks onto the internet and to enable them to choose the network technologies that are best suited for each need. Commercial routers may link more than two networks, even though the illustration only depicts each router with two connections. So, in the example, a single router may link all four networks. Even though it is possible, organizations seldom link all of their networks with a single router. Two of them are as follows:

The CPU in a particular router is unable to manage the traffic moving across an arbitrary number of networks since the router must forward every packet.

Internet dependability is increased via redundancy. Protocol software constantly checks internet connections to prevent a single point of failure and advises routers to move traffic along other routes when a network or router malfunctions.

As a result, while designing the internet, an organisation must choose an architecture that satisfies its requirements for capacity, dependability, and affordability. Particularly, the precise configuration of the internet topology often depends on the physical networks' capacity, the anticipated volume of traffic, the organization's needs for dependability, and the price and functionality of the router hardware that is readily accessible.

Developing Universal Service

Universal service over diverse networks is the aim of internetworking. Routers must concur to transmit data from a source on one network to a certain destination on another in order to offer universal service to all computers connected to the internet. Since the underlying networks' frame formats and addressing techniques might vary, the process is difficult. To provide universal service, protocol software is required on PCs and routers.

These demonstrate how Internet protocols work around variations in physical addresses and frame formats to enable communication across networks using various technologies. Understanding the impact an internet system has on connected computers is crucial before thinking about how Internet protocols function.

A virtual network

In general, Internet software gives the impression that multiple computers are connected to a single, seamless communication system. The system provides universal service, allowing any computer to transmit a packet to any other computer. Each machine is given an address. Internet protocol software also conceals the specifics of physical network connections, physical addresses, and routing data; neither consumers nor application programmes are aware of the underlying physical networks or the routers connecting them.

The communication system is an abstraction, which is why we refer to the internet as a virtual network system. That is, despite the appearance of a uniform network system caused by a mix of hardware and software, no such network really exists.

Internetworking Protocols

A number of protocols have been suggested for use with internets, but just one suite is the most popular. The set is officially named as the TCP/IP Internet Protocols, although most networking experts just call it TCP/IP. The worldwide Internet and TCP/IP were both created at the same time. The Internet architecture shown above was really suggested by the same academics that created TCP/IP. Development on TCP/IP proceeded until the early 1990s, when the Internet became commercially viable, at about the same time that Local Area Networks were being built.

Protocol Layers, Routers, and Host Computers

A computer that connects to the Internet and executes programmes is referred to as a host computer. A host may range in size from a smart phone to a mainframe. In addition, a host's memory may be big or little, its CPU can be sluggish or fast, and the network it connects to can run at high or low speed. Every pair of hosts may interact with one another using TCP/IP protocols, regardless of hardware differences.

TCP/IP protocol software is required for both hosts and routers. Nevertheless, not all layers' protocols are used by routers. In instance, because routers can not execute typical programmes, layer 5 protocols are not required for applications like file transfer. The next go into further depth into the TCP/IP protocol software and demonstrate how Internet layering works.
