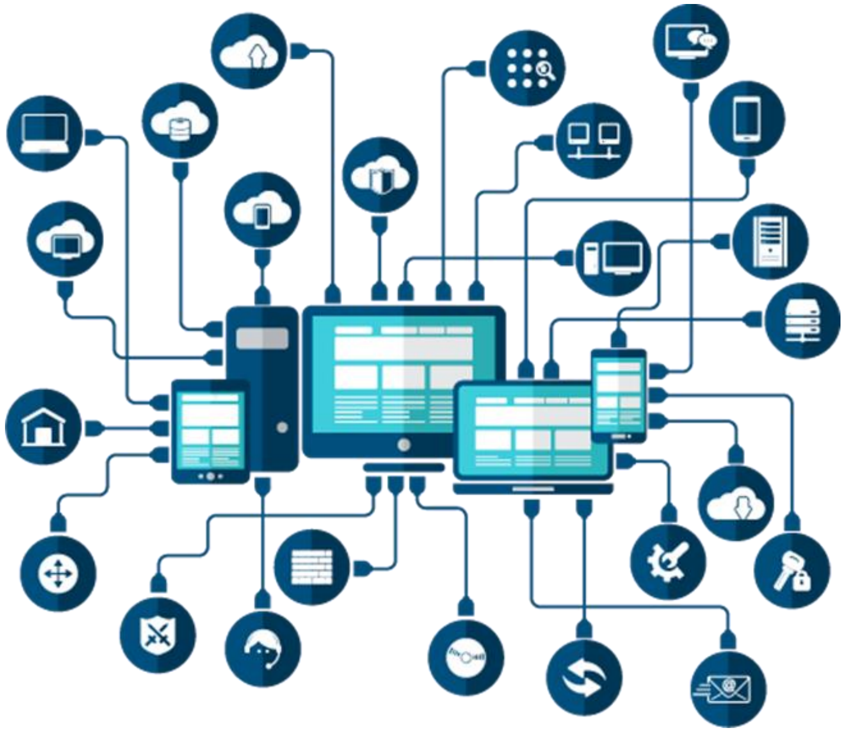


COMPUTER NETWORKS 1

Stage Three

CHAPTER ONE

INTRODUCTION TO COMPUTER NETWORKS

Introduction

Data communications and networking have changed the way we do business and the way we live. Business decisions must be made ever more quickly, and the decision-makers require immediate access to accurate information. Why wait a week for that report to arrive by mail when it could appear almost instantaneously through computer networks? Businesses today rely on computer networks and internetworks.
Data communication and networking have found their way not only through business and personal communication but also through many applications in political and social issues. People have found how to communicate with other people in the world to express their social and political opinions and problems. Communities in the world are not isolated anymore.
But before we ask how quickly we can get hooked up; we need to know how networks operate.

.

Data Communication

When we communicate, we share **information**. This sharing can be **local** or **remote**. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term **telecommunications**, which includes telephony, telegraphy, and television, means communication at a **distance**.

The **data** refers to facts, concepts, and instructions presented in whatever form is agreed upon by the parties creating and using the data. In the context of computer information systems, data is represented by binary information units produced and consumed in the form of **0**s and **1**s.

Data communication is the transfer of data between a source and a receiver. The source transmits the data and the receiver receives it. The actual generation of the information is not part of data communications nor is the resulting action of the information at the receiver. Data Communication is interested in the **transfer of data**, the **transfer method**, and the **preservation of the data** during the transfer process.

Data Communication aims to provide the **rules** and **regulations** that allow computers with different operating systems, languages, cabling, and locations to share resources. The rules and regulations are called **protocols** and **standards** in Data Communications.

For data communication to occur, the communicating devices must be part of a communication system made up of a combination of hardware and software. The effectiveness of a data communication system depends on the following fundamental **characteristics**:

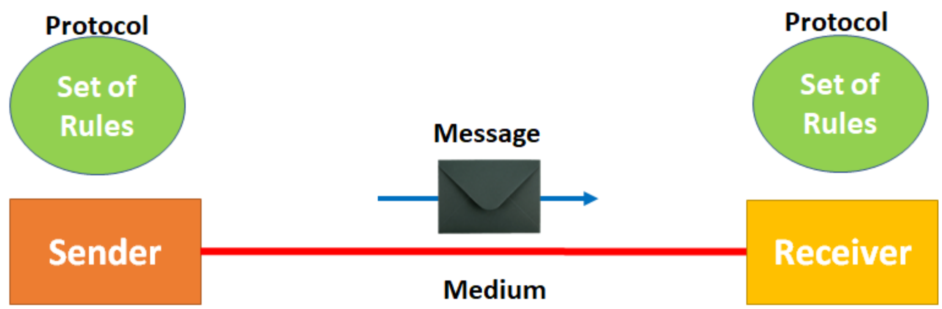
1. **Delivery**: The System must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy**: The system must deliver data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. **Timeliness**: The system must deliver data in a timely manner. Data delivered late are useless. In the case of video, audio, and voice data, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. this kind of delivery is called real-time transmission.

4. Jitter: Jitter is the variation in time delay between when a signal is transmitted and when it's received over a network connection, measuring the variability in ping. This time delay is often caused by network congestion, poor hardware performance or not implementing packet prioritization.

The longer the delay, the more likelihood of choppy audio calls, bad quality video, an inability to upload or download files and other issues that can highjack your network and lead to unwanted downtime.

Data Communication Components

The following are the basic requirements for working on a communication system.



1. **Message**: This is a most useful asset of a data communication system. The message simply refers to data which is to be communicated. A message could be in any form, it may be in form of a text file, an audio file, a video file, etc.

2. **Sender**: To transfer messages from source to destination, someone must be there who will play the role of a source. The sender plays the part of a source in a data communication system. It is simply a device that sends data messages. The device could be in form of a computer, mobile, telephone, laptop, video camera, workstation, etc.

3. **Receiver**: It is a destination where finally message sent by the source has arrived. It is a device that receives messages. Same as the sender, the receiver can also be in form of a computer, telephone mobile, workstation, etc.

4. **Transmission Medium** In the entire process of data communication, there must be something that could act as a bridge between sender and receiver, transmission medium plays that part. It is the physical path by which data or message travels from sender to receiver. Transmission medium could be guided (with wires) or unguided (without wires), for example, twisted pair cable, fiber optic cable, radio waves, microwaves, etc.

5. **Protocol**: To govern data communications, various sets of rules had been already designed by the designers of the communication systems, which represent a kind of agreement between communicating devices. These are defined as protocols. In simple terms, the protocol is a set of rules that govern data communication. If two different devices are connected but there is no protocol among them, there would not be any kind of communication between those two devices. Thus, the protocol is necessary for data communication to take place.

Data Flow in Communication

Data Flow in Communication means how data transfers between devices. Communication means the transfer or exchange of data between two different devices. In the Communication process whenever data transfers it depends on the condition or depends on devices through which type of data will transfer.

Data Flow in communication has the following **types**:

1. Simplex

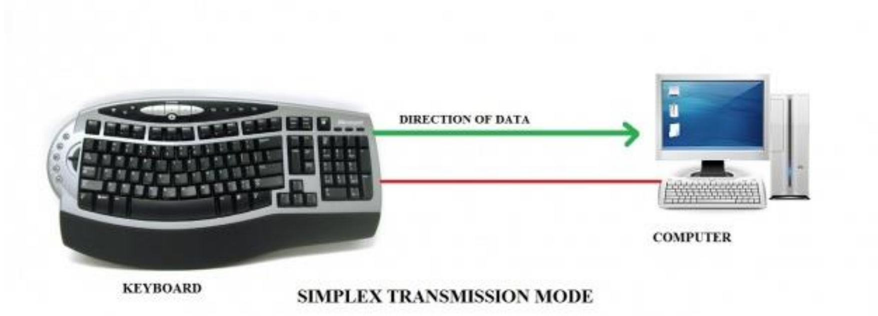
2. Half duplex

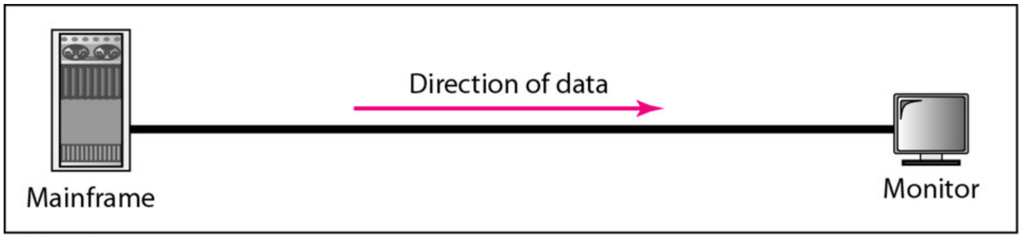
3. Full duplex

1. Simplex

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive which can be represented in the following figure. Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction. In this type, the channel will use all of its capacity only in sending data.

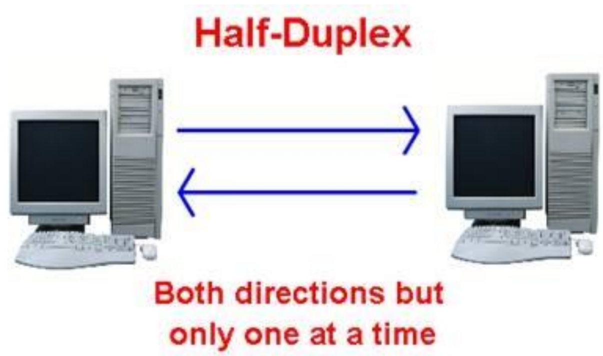
.





2. Half duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa which will represent in the following figure.



The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. In half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkie's radio is half-duplex systems.

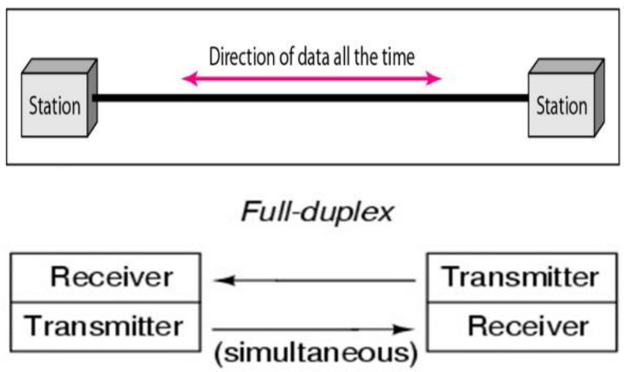
The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

.

3. Full Duplex

In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously as shown in the following figure. The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the

.



other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between the signals traveling in both directions.

One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

.

.

Data Representation

Data today comes in different forms such as text, numbers, images, audio, and Video.

a. **Text**: Text is represented as a bit pattern, a sequence of bits (0s or 1s). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding.

b. **Numbers**: Numbers are also represented by bit patterns. The number is directly converted to a binary number to simplify mathematical operations.

c. **Images**: Images are also represented by bit patterns. An image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution.

d. **Audio**: Audio refers to the recording or broadcasting of sound or music. It is continuous, not discrete.

e. **Video**: Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

Computer Networks

The term '**Network**' means a group, chain, or a collection of something that comes together for the purpose of communication. In the computer's reference, the exact definition holds value but there is a slight change.

A **computer network** is a set of devices (often referred to as **nodes**) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. It is connected together for the purpose of sharing information between two or more computing devices, the connection between two or more computers can be done via cabling or via wirelessly. Connected computers can share resources like access to the internet, printers, file servers, and others.

.

Network Criteria

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

1. **Performance:**

   Performance can be measured in many ways, including transit time and response time. **Transit time** is the amount of time required for a message to travel from one device to another. **Response time** is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software. Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

2. **Reliability:**

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

3. **Security:**

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

.

Networks Advantages:

· **File Sharing**: The major advantage of a computer network is that is allows file sharing and remote file access.

· **Resource Sharing**: Files, modems, printers…

· **Increased Storage Capacity**: As there is more than one computer on a network which can easily share files, the issue of storage capacity gets resolved to a great extent.

· **Increased Cost Efficiency**: There are many software available in the market which are costly and take time for installation. Computer networks resolve this issue as the software can be stored or installed on a system or a server and can be used by the different workstations.

Networks Disadvantages:

· **Security Issues**: Physical access, computer hacker can get unauthorized access by using different tools.

· **Rapid Spread of Computer Viruses**: If any computer system in a network gets affected by computer virus, there is a possible threat of other systems getting affected too.

· **Expensive Set Up**: The initial set up cost of a computer network can be high depending on the number of computers to be connected. Costly devices like routers, switches, hubs, etc., can add up to the bills of a person trying to install a computer network. He will also have to buy NICs (Network Interface Cards) for each of the workstations, in case they are not inbuilt.

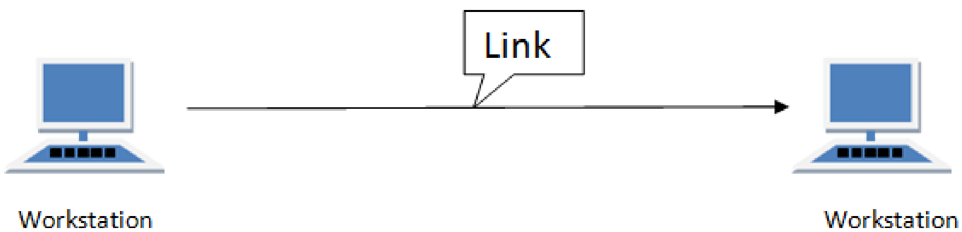
· **Dependency on the Main File Server**: In case the main File Server of a computer network breaks down, the system becomes useless. In case of big networks, the File Server should be a powerful computer, which often makes it expensive.

Physical Structures:

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: **point-to-point** and **multipoint**.

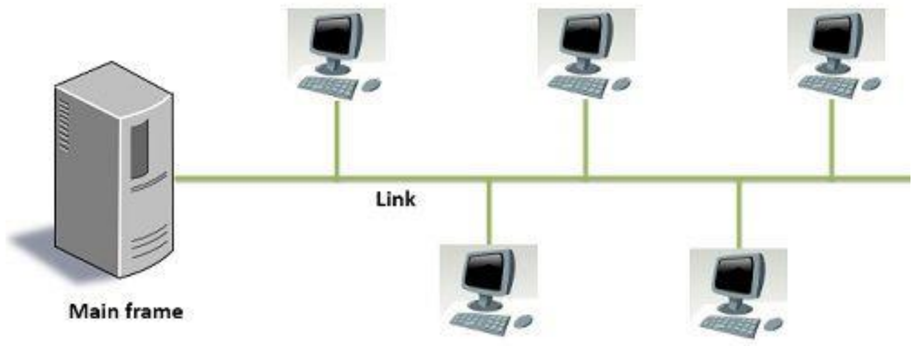
1. Point-to-Point

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



2. Multipoint

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



Multipoint Connection

Network Topologies

When building a computer network, you need to define which network topology you want to use. There are multiple types of network topologies used nowadays, each with its pros and cons(إيجابيات وسلبيات) . The topology you choose determines the optimal performance of your network, scalability options, ease of maintenance, and the costs of building the network. That’s why it is important to select the right network topology type.

What is Network Topology?

Network topology refers to how various nodes, devices, and connections on your network are physically or logically arranged in relation to each other. Think of your network as a city, and the topology as the road map. Just as there are many ways to arrange and maintain a city—such as making sure the avenues (الطرق) and boulevards (الشوارع) can facilitate passage between the parts of town getting the most traffic—there are several ways to arrange a network. Each has advantages and disadvantages and depending on the needs of your company, certain arrangements can give you a greater degree of connectivity and security.

The network topology or network configuration defines the structure of the network and how network components are connected. Network topology types are usually represented with network topology diagrams for convenience and clarity. There are two types of network topology: **physical** and **logical**.

Physical topology describes how network devices (called computers, stations, or nodes) are physically connected in a computer network. The geometric scheme, connections, interconnections, device location, the number of used network adapters, types of network adapters, the type of cable, cable connectors, and other network equipment are the aspects of the physical network topology.

Logical topology represents the data flow from one station to another, how the data is transmitted and received, the path of data in the network, and which protocols are used. The logical network topology explains how data is transferred over a physical topology. Cloud and virtual network resources are part of the logical topology.

Why Is Network Topology Important?

The layout of your network is important for several reasons. Above all, it plays an essential role in how and how well your network functions. Choosing the right topology for your company's operational model can increase performance while making it easier to locate faults, troubleshoot errors, and more effectively allocate resources across the network to ensure optimal network health. A streamlined and properly managed network topology can increase energy and data efficiency, which can in turn help to reduce operational and maintenance costs.

The design and structure of a network are usually shown and manipulated in a software-created network topology diagram. These diagrams are essential for a few reasons, but especially for how they can provide visual representations of both physical and logical layouts, allowing administrators to see the connections between devices when troubleshooting.

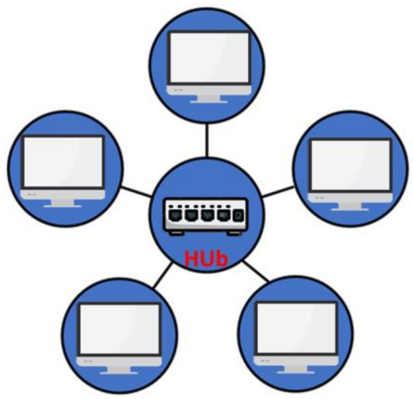
Effective network management and monitoring require a strong grasp of both the physical and logical topology of a network to ensure your network is efficient and healthy.

What's the Most Common Type of Network Topology?

1. Star Topology

A star topology, the most common network topology, is laid out so every node in the network is directly connected to one central hub via coaxial, twisted-pair, or fiber-optic cable. Acting as a server, this central node manages data transmission—as information sent from any node on the network has to pass through the central one to reach its destination—and functions as a repeater, which helps prevent data loss.

.



Advantages of Star Topology

Star topologies are common since they allow you to conveniently manage your entire network from a single location. Because each of the nodes is independently connected to the central hub, should one go down, the rest of the network will continue functioning unaffected, making the star topology a stable and secure network layout.

Additionally, devices can be added, removed, and modified without taking the entire network offline.

On the physical side of things, the structure of the star topology uses relatively little cabling to fully connect the network, which allows for both straightforward setup and management over time as the network expands or contracts. The simplicity of the network design makes life easier for administrators, too, because it's easy to identify where errors or performance issues are occurring.

Disadvantages of Star Topology

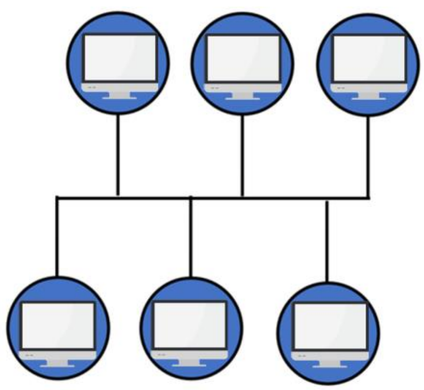
On the flip side, if the central hub goes down, the rest of the network can't function. But if the central hub is properly managed and kept in good health, administrators shouldn't have too many issues.

The overall bandwidth and performance of the network are also limited by the central node's configurations and technical specifications, making star topologies expensive to set up and operate.

2. Bus Topology

A bus topology orients all the devices on a network along a single cable running in a single direction from one end of the network to the other—which is why it's sometimes called a "line topology" or "backbone topology." Data flow on the network also follows the route of the cable, moving in one direction.

.



Advantages of Bus Topology

Bus topologies are a good, cost-effective choice for smaller networks because the layout is simple, allowing all devices to be connected via a single coaxial or RJ45 cable. If needed, more nodes can be easily added to the network by joining additional cables.

Disadvantages of Bus Topology

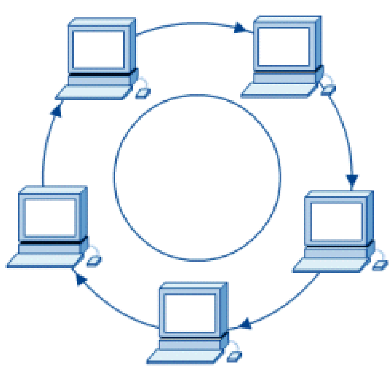
However, because bus topologies use a single cable to transmit data, they're somewhat vulnerable. If the cable experiences a failure, the whole network goes down, which can be time-consuming and expensive to restore, which can be less of an issue with smaller networks.

Bus topologies are best suited for small networks because there's only so much bandwidth, and every additional node will slow transmission speeds.

Furthermore, data is "half-duplex," which means it can't be sent in two opposite directions at the same time, so this layout is not the ideal choice for networks with huge amounts of traffic.

3. Ring Topology

Ring topology is where nodes are arranged in a circle (or ring). The data can travel through the ring network in one direction, with each device having exactly two neighbors.



Advantages of Ring Topology

Since each device is only connected to the ones on either side, when data is transmitted, the packets also travel along the circle, moving through each of the intermediate nodes until they arrive at their destination. If a large network is arranged in a ring topology, repeaters can be used to ensure packets arrive correctly and without data loss.

Only one station on the network is permitted to send data at a time, which greatly reduces the risk of packet collisions, making ring topologies efficient at transmitting data without errors.

By and large, ring topologies are cost-effective and inexpensive to install, and the intricate point-to-point connectivity of the nodes makes it relatively easy to identify issues or misconfigurations on the network.

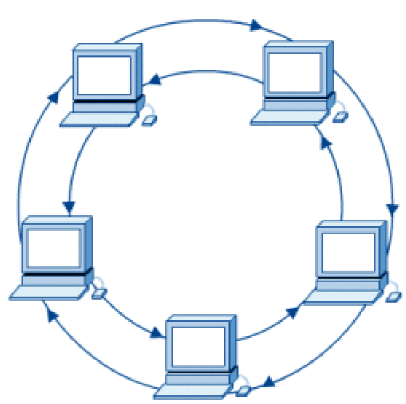
Disadvantages of Ring Topology

Even though it’s popular, a ring topology is still vulnerable to failure without proper network management. Since the flow of data transmission moves unidirectionally between nodes along each ring, if one node goes down, it can take the entire network with it. That’s why it’s imperative for each of the nodes to be monitored and kept in good health. Nevertheless, even if you’re vigilant and attentive to node performance, your network can still be taken down by a transmission line failure.

Additionally, the entire network must be taken offline to reconfigure, add, or remove nodes. And while that’s not the end of the world, scheduling downtime for the network can be inconvenient and costly.

4. Dual-Ring Topology

A network with ring topology is half-duplex, meaning data can only move in one direction at a time. Ring topologies can be made full-duplex by adding a second connection between network nodes, creating a dual ring topology.



Advantages of Dual-Ring Topology

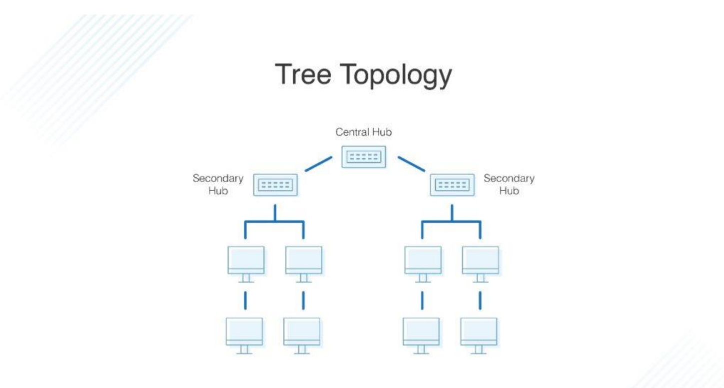
The primary advantage of dual ring topology is its efficiency: because each node has two connections on either side, information can be sent both clockwise and counterclockwise along the network. The secondary ring included in a dual-ring topology setup can act as a redundant layer and backup, which helps solve for many of the disadvantages of traditional ring topology. Dual ring topologies offer a little extra security, too: if one ring fails within a node, the other ring is still able to send data.

Disadvantages of Dual-Ring Topology

- Network issues from bad ports or malfunctioning Media Access Unit (MAU) cards.
- Negative network impact from any added, altered or damaged device.

5. Tree Topology

The tree topology structure gets its name from how the central node functions as a sort of trunk for the network, with nodes extending outward in a branch-like fashion. However, where each node in a star topology is directly connected to the central hub, a tree topology has a parent-child hierarchy to how the nodes are connected. Those connected to the central hub are connected linearly to other nodes, so two connected nodes only share one mutual connection. Because the tree topology structure is both extremely flexible and scalable, it's often used for wide-area networks to support many spread-out devices.



Advantages of Tree Topology

Combining elements of the star and bus topologies allows for the easy addition of nodes and network expansion. Troubleshooting errors on the network is also a straightforward process, as each of the branches can be individually assessed for performance issues.

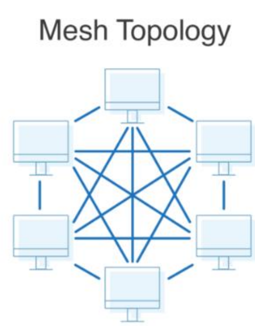
Disadvantages of Tree Topology

As with the star topology, the entire network depends on the health of the root node in a tree topology structure. Should the central hub fail, the various node branches will become disconnected, though connectivity within—but not between—branch systems will remain.

Because of the hierarchical complexity and linear structure of the network layout, adding more nodes to a tree topology can quickly make proper management an unwieldy, not to mention costly, experience. Tree topologies are expensive because of the sheer amount of cabling required to connect each device to the next within the hierarchical layout..

6. Mesh Topology

A mesh topology is an intricate and elaborate structure of point-to-point connections where the nodes are interconnected. Mesh networks can be full or partial mesh. Partial mesh topologies are mostly interconnected,



with a few nodes with only two or three connections, while full-mesh topologies are fully interconnected.

The web-like structure of mesh topologies offers two different methods of data transmission: routing and flooding. When data is routed, the nodes use logic to determine the shortest distance from the source to the destination, and when data is flooded, the information is sent to all nodes within the network without the need for routing logic.

Advantages of Mesh Topology

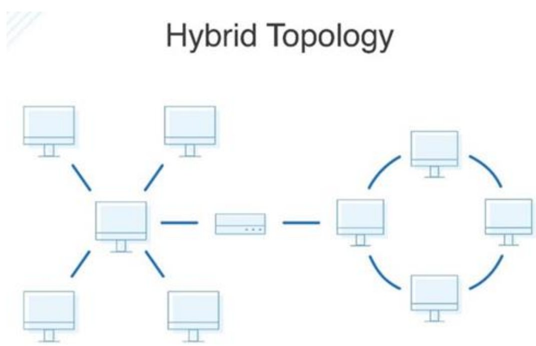
Mesh topologies are reliable and stable, and the complex degree of interconnectivity between nodes makes the network resistant to failure. For instance, no single device going down can bring the network offline.

Disadvantages of Mesh Topology

Mesh topologies are incredibly labor-intensive. Each interconnection between nodes requires a cable and configuration once deployed, so it can also be time-consuming to set up. As with other topology structures, the cost of cabling adds up fast, and to say mesh networks require a lot of cabling is an understatement.

7. Hybrid Topology

Hybrid topologies combine two or more different topology structures—the tree topology is a good example, integrating the bus and star layouts. Hybrid structures are most commonly found in larger companies where individual departments have personalized network topologies adapted to suit their needs and network usage.



Advantages of Hybrid Topology

The main advantage of hybrid structures is the degree of flexibility they provide, as there are a few limitations on the network structure itself that a hybrid setup can't accommodate.

Disadvantages of Hybrid Topology

However, each type of network topology comes with its own disadvantages, and as a network grows in complexity, so too does the experience and know-how required on the part of the admins to keep everything functioning optimally. There’s also the monetary cost to consider when creating a hybrid network topology.

Which Topology is Best for Your Network?

No network topology is perfect, or even inherently better than the others, so determining the right structure for your business will depend on the needs and size of your network. Here are the key elements to consider:

Cable Length

Generally, the more cable involved in network topology, the more work it’ll require to set up. The bus and star topologies are on the simpler side of things, both being fairly lightweight, while mesh networks are much more cable- and labor-intensive.

Cable Type

The second point to consider is the type of cable you’ll install. Coaxial and twisted-pair cables both uses insulated copper or copper-based wiring, while fiber-optic cables are made from thin and pliable plastic or glass tubes. Twisted-pair cables are cost-effective but have less bandwidth than coaxial cables. Fiber-optic cables are high performing and can transmit data far faster than twisted-pair or coaxial cables, but they also tend to be far more expensive to install, because they require additional components like optical receivers. So, as with your choice of network topology, the wiring you select depends on the needs of your network, including which applications you’ll be running, the transmission distance, and desired performance.

Cost

As I've mentioned, the installation cost is important to account for, as the more complex network topologies will require more time and funding to set up. This can be compounded if you're combining different elements, such as connecting a more complex network structure via more expensive cables (though using fiber-optic cables in a mesh network is overdoing it, if you ask me, because of how interconnected the topology is). Determining the right topology for your needs, then, is a matter of striking the right balance between installation and operating costs and the level of performance you require from the network.

Scalability

The last element to consider is scalability. If you anticipate your company and network expanding—or if you'd like it to be able to—it'll save you time and hassle down the line to use an easily modifiable network topology. Star topologies are so common because they allow you to add, remove, and alter nodes with minimal disruption to the rest of the network. Ring networks, on the other hand, have to be taken entirely offline for any changes to be made to any of the nodes.

How to Map Network Topology

When you're starting to design a network, topology diagrams come in handy. They allow you to see how the information will move across the network, which, in turn, allows you to predict potential choke points. Visual representation makes it easier to create a streamlined and efficient network design, while also acting as a good reference point if you find yourself needing to troubleshoot errors.

.

A topology diagram is also essential for having a comprehensive understanding of your network's functionality. In addition to assisting with the troubleshooting process, the bird's-eye view provided by a topology diagram can help you visually identify the pieces of the infrastructure your network is lacking, or which nodes need monitoring, upgrading, or replacing.

The good news is you don't have to do it manually: you can easily create a map of your network topology with tools.

What are the different types of networks?

A computer network can be divided into the following types, based on the geographical area that they cover, they are:

1. LAN (Local Area Network)
2. MAN (Metropolitan Area Network)
3. WAN (Wide Area Network)

LAN (Local Area Network)

A local area network is a network, which is designed to operate over a very small geographical or physical area such as an office, building, group of buildings, etc.

Generally, it is used to connect two or more personal computers through a communication medium such as coaxial, twisted-pair cables, etc. A LAN can use either a wired or wireless mode of communication. The LAN which entirely uses wireless media for communication can be termed a **WLAN (Wireless Local Area Network)**.

Local Area Networks came into existence around the 1970s. IEEE developed the specifications for LAN. The speed of this network varies from 10mbps (Ethernet network) to 1gbps (FDDI or Gigabit Ethernet).

In other words, a LAN connects a relatively small number of machines in a relatively close geographical area. Bus, Ring, and Star topology are generally used in a local area network. In LAN, one computer can become a server in a star topology, serving all other computers called clients. Two different buildings can be connected very easily in LAN using a 'Bridge'.

Ethernet LAN is the most commonly used LAN. The speed of a Local Area Network also depends on the topology used. ***For example,*** a LAN using bus topology has a speed of 10mbps to 100mbps, while in ring topology it is around 4mbps to 16mbps. LANs are generally privately owned networks.

Following are the functionalities of a Local Area Network:

1. **File Serving:** In LAN, a large storage disk acts as a central storage repository.
2. **Print Serving:** Printers can be shared very easily on a LAN by various computers.
3. **Academic Support:** A LAN can be used in the classroom, labs, etc. for educational purposes.
4. **Manufacturing Support:** LAN can support the manufacturing and industrial environment.
5. **High Reliability:** Individual workstations might survive the network in case of failures.

Following are the advantages of a LAN:

1. File transfer and file access
2. Resource or peripherals sharing
3. Personal computing
4. Document distribution
5. Easy to design and troubleshoot
6. Minimum propagation delay
7. High data rate transfer
8. Low error rate
9. Easily scalable (devices can be added or removed very easily)

Following are the disadvantages of a LAN:

1. Equipment and support may be costly
2. Some hardware devices may not inter-operate properly

MAN *(Metropolitan Area Network)*

A Metropolitan Area Network is a bigger version of LAN that uses similar technology as LAN. It spans a larger geographical area such as a town or an entire city.

It can be connected using an optical fiber cable as a communication medium. Two or more LANs can also be connected using routers to create a MAN. When this type of network is created for a specific campus, then it is termed CAN (Campus Area Network).

The MAN spans a geographical area of about 50km. The best example of MAN is the cable television network that spans the whole city.

A MAN can be either a public or privately owned network. Generally, a telephone exchange line is most commonly used as a communication medium in MAN. The protocols that are used in MAN are RS-232, Frame Relay, ISDN, etc.

Uses of MAN are as follows:

1. MAN can be used for connecting the various offices of the same organization, spread over the whole city.
2. It can be used for communication in various governmental departments.

Following are the advantages of using MAN:

1. Large geographical area covers as compared to LAN
2. High-speed data connectivity
3. The Propagation delay of MAN is moderate

Following are the disadvantages of MAN:

1. It is hard to design and maintain a MAN
2. MAN is less fault-tolerant
3. It is costlier to implement
4. Congestions are more in a MAN
5.

WAN *(Wide Area Network)*

A Wide Area Network is the largest spread network. It spans very large distances such as a country, continent, or even the whole globe. Two widely separated computers can be connected very easily using WAN. For Example, the Internet.

A WAN may include various Local and Metropolitan Area Network. The mode of communication in a WAN can either be wired or wireless. Telephone lines for wired and satellite links for wireless communication can be used in a wide area network.

In other words, WAN provides long-distance transmission of data, voice, image, and video, over a large geographical area. A WAN may span beyond the 100km range. It may be privately or publicly owned.

The protocols used in WAN are ISDN (Integrated Service Digital Network), SMDS (Switched Multi-Megabit Data Service), SONET (Synchronous Optical Network), HDLC (High Data Link Control), SDLC (Synchronous Data Link Control), etc.

The advantage of WAN is that it spans a very large geographical area, and connects a huge mass of people.

Following are the disadvantages of WAN:

1. The propagation delay is more in a WAN
2. The data rate is low
3. The error rate is high
4. It is very complex to design a WAN

These are the types of networks according to a geographical area.

Following are the types of networks, based on functionality:

- **Client-Server Network:** Client-Server network is a network in which a client runs the program and accesses data that are stored on the server. In this kind of network, one computer becomes the server, serving all other computers called clients.
- **Peer-to-Peer Network:** Peer-to-Peer network facilitates the flow of information from one peer to another without any central server. In other words, each node on a server act as both client and server.

Following are the types of networks, based on Ownership:

- **Private Network:** A private network is a network in which various restrictions are imposed to secure the network, to restrict unauthorized access. This type of network is privately owned by a single or group of people for their personal use. A Local Area Network (LAN) can be used as a private network.
- **Public Network:** A public network is a network that has the least or no restrictions on it. It can be freely accessed by anyone, without any restrictions. This type of network is publicly owned by the government or NGOs. Metropolitan Area Network (MAN) and Wide Area Network (WAN) can be used as public networks.

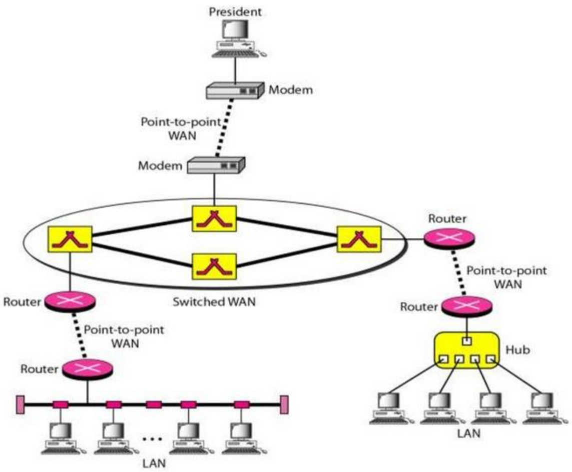
Following are the types of networks, based on Transmission Media:

- **Bound/Guided Media Network:** Bounded/Guided media can also be referred to as wired media. This kind of network provides a physical link between two nodes connected in a network. The physical links are directed in a particular direction in the network. Co-axial, twisted pair, optical fiber cable, etc. can be used in such networks for connectivity. Local Area Network (LAN) and Metropolitan Area Network (MAN) can be used as a Bound/Guided media network.
- **Unbound/Unguided Media Network:** Unbounded/Unguided media can also be referred to as wireless media. This kind of network does not need any physical link for electromagnetic transmission. Radio waves, Microwaves, Infrared, etc. can be used in such networks for connectivity. Metropolitan Area Network (MAN) and Wide Area Network (WAN) can be used as an Unbound/Unguided media network.

Interconnection of Networks: Internetworking

Today, it is very rare to see a **LAN**, a **MAN** (metropolitan area network), or a LAN in isolation; they are connected to one another. When two or more networks are connected, they become internetwork or internet.

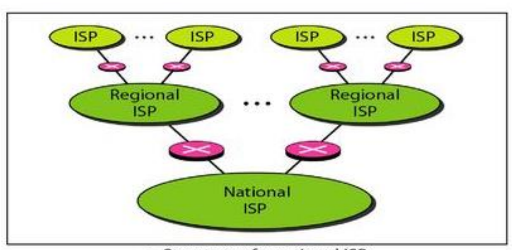
As an example, assume that an organization has two offices, one on the east coast and the other on the west coast. The established office on the west coast has a bus topology LAN; the newly opened office on the east coast has a star topology LAN. The president of the company lives somewhere in the middle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



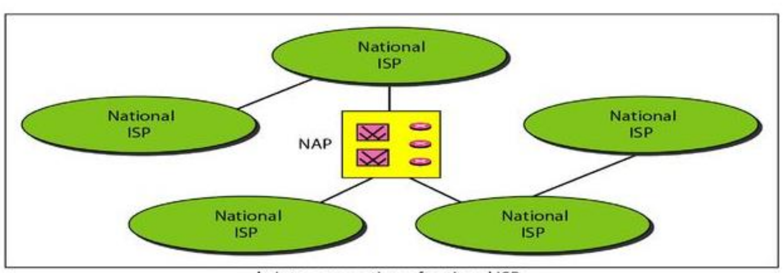
A heterogeneous network made of four WANs and two LANs

THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. Count the ways you've used the Internet recently. Perhaps you've sent an electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule all by using the Internet. Or maybe you researched a medical topic, booked a hotel reservation, chatted with a fellow, or comparison-shopped for a car. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.



a. Structure of a national ISP



b. Interconnection of national ISPs

PROTOCOLS AND STANDARDS

In this section, we define two widely used terms: protocols and standards. First, we define a protocol, which is synonymous with the rule. Then we discuss standards, which are agreed-upon rules.

Protocols

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules
that govern data communications. A protocol defines what is communicated, how k is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

❖ **Syntax.** The term syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

❖ **Semantics.** The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?

❖ **Timing.** The term timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

Standards

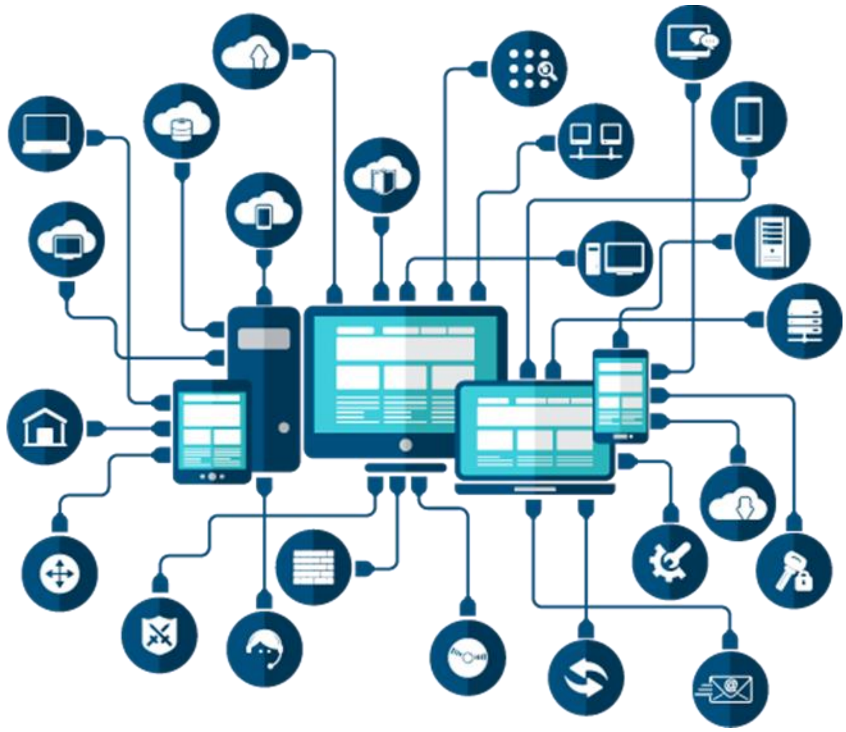
Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes. Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

Standards Organizations

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

Regulatory Agencies

All communications technology is subject to regulation by government agencies such as the Federal Communications Commission (FCC) in the United States. The purpose of these agencies is to protect the public interest by regulating radio, television, and wire /cable communications. The FCC has authority over interstate and international commerce as it relates to communications.



COMPUTER NETWORKS 1

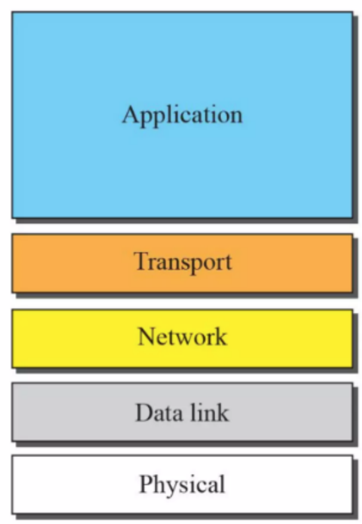
Stage Three

CHAPTER TWO

TCP/IP Protocol Suite , OSI Model and Addressing

TCP/IP Protocol Suite

The TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application. The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model (see Figure down below). The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer.



TCP/IP Protocol Suite

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

2. Network Layer At the network layer (or the internetwork layer), TCP/IP supports the Internetworking Protocol (IP). IP uses four supporting protocols: ARP, RARP, ICMP, and IGMP as described in the following:

The **Internetworking Protocol (IP)** is the transmission mechanism used by the TCP/IP protocols. IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated.

The **Address Resolution Protocol (ARP)** is used to associate a logical address with a physical address. ARP is used to find the physical address of the node when its Internet address is known.

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

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

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

3. Transport Layer

The main protocols in transport layer are the TCP and UDP. IP protocol in network layer is a source-to-destination protocol, meaning that it can deliver a packet from one physical device to another. Whereas, UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process (process-to-process protocols).

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

The **Transmission Control Protocol (TCP)** is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.

At the sending end of each transmission, TCP divides a stream of data into smaller units called **segments**. Each segment includes a sequence number for reordering after receipt. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

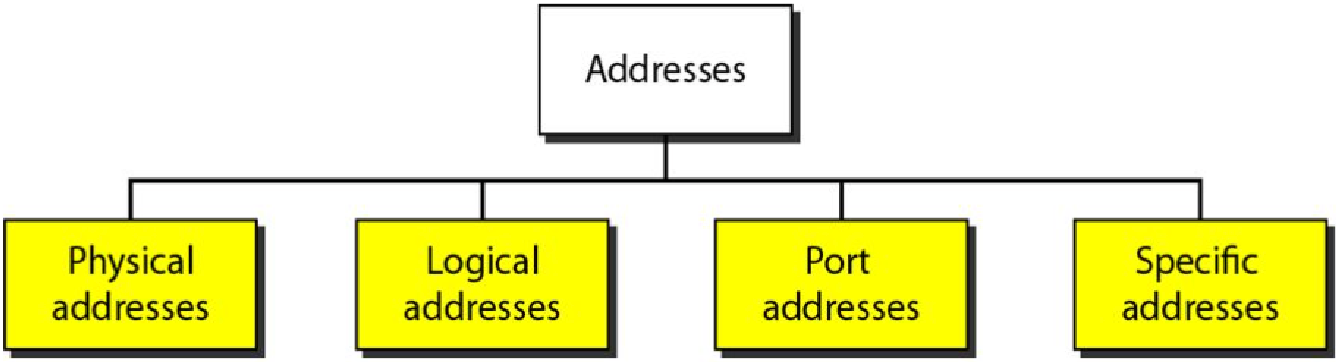
The **Stream Control Transmission Protocol (SCTP)** provides support for newer applications such as voice over the Internet.

4. Application Layer

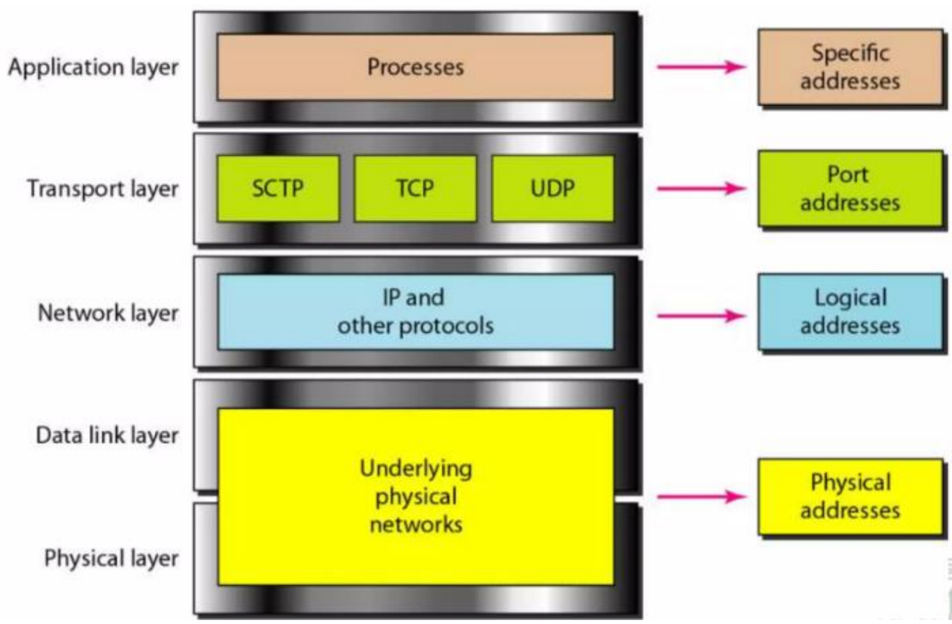
The application layer in TCP/IP is **equivalent** to the combined **session**, **presentation**, and **application** layers in the OSI model. Many protocols are defined at this layer.

Addressing

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical (link) addresses, logical (IP) addresses, port addresses, and specific addresses (see Figure down below).



Each address is re lated to a specific layer in the TCP/IP architecture, as shown in the Figure down below:



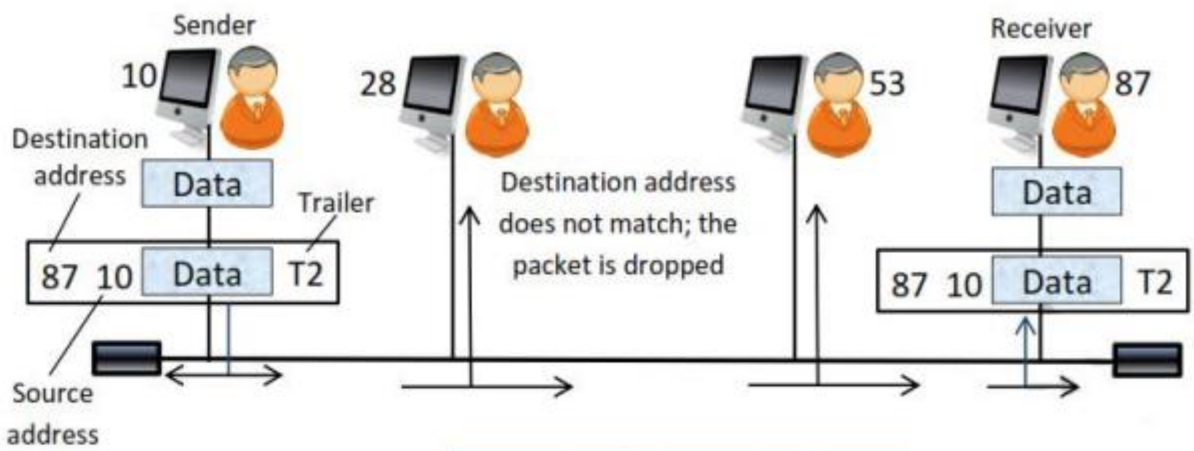
Relationship of layers and addresses in TCP/IP

Physical Addresses

The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address.

Example 1

In Figure down below, a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). At the data link layer, this frame contains physical (link) addresses in the header. These are the only addresses needed. The data link layer at the sender receives data from an upper layer. It encapsulates the data in a frame, adding a header and a trailer. **Encapsulation** means that a packet (header, data and maybe trailer) at a specific level is encapsulated in one whole packet.



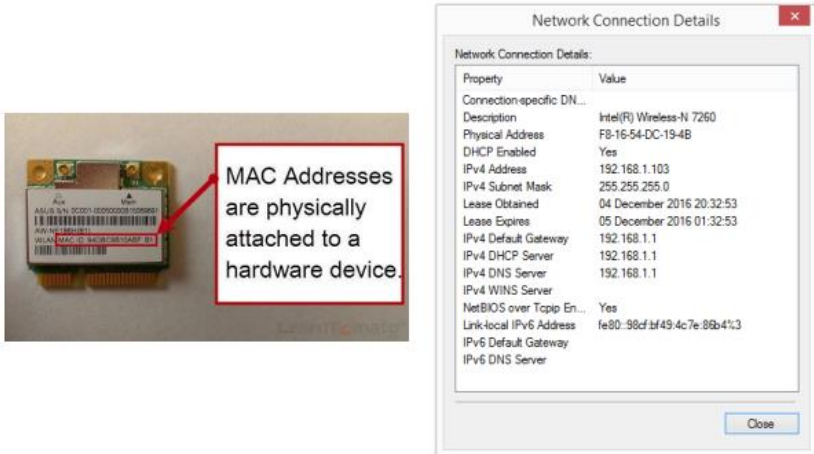
Example 2

Most local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address

The physical address is imprinted on the network interface card (NIC) as shown in the left picture and can be displayed on any computer as shown in the screenshot down below.



A screenshot that shows a physical address and other connection details

Logical Addresses

Physical addresses are not enough in an internetwork environment. A universal (or logical) addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network.

A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. No two publicly addressed hosts on the Internet can have the same IP address.

192.168.1.100

IP (or logical address), Version 4, Class C

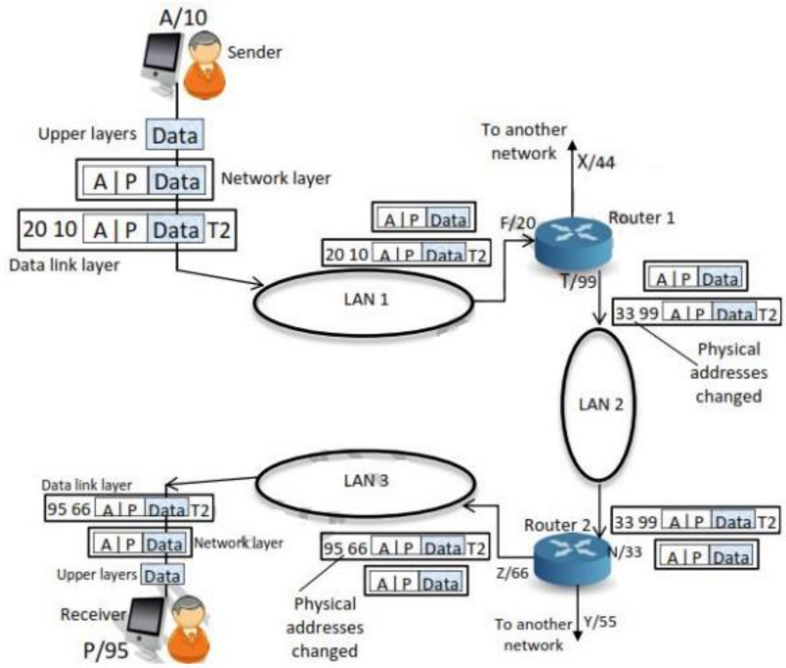
<u>Example 3</u>

The Figure down below shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical). The computer with **logical address A** and **physical address 10** needs to send a packet to the computer with **logical address P** and **physical address 95.**

The sender encapsulates its data in a packet at the network layer and adds two logical addresses (A and P). The network layer, however, needs to find the physical address of the next hop before the packet can be delivered. The network layer consults its **routing table** and finds the logical address of the next hop (router 1) to be F. The **ARP** finds the physical address of router 1 that corresponds to the logical address of 20. Now the network layer passes this address to the data link layer, which in turn encapsulates the packet with physical destination address 20 and physical source address 10.

Since the logical destination address does not match the router's logical address, the router 1 knows that the packet needs to be forwarded to router 2. When the frame reaches the destination, the packet is de-capsulated. The destination logical address P matches the logical address of the computer. The data are decapsulated from the packet and delivered to the upper layer.

<u>Note</u>: Although physical addresses will **change from hop to hop**, logical addresses **remain the same** from the source to destination (but there are some exceptions to this rule).



Example of logical (IP) addresses

Port Addresses

Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process. Therefore, we need a method to label the different processes. In the TCP/IP architecture, the label assigned to a process is called a **port address**. A port address in TCP/IP is 16 bits in length.

Example 4

The Figure down below shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses (a), (b), and (c). The receiving computer is running two processes at this time with port addresses (j) and (k). Process (a) in the sending computer needs to communicate with process (j) in the receiving computer. Note that although both computers are using the same application, FTP, for example, the port addresses are different because one is a **client program** and the other is a **server program.**

Note: Although **physical addresses** change from hop to hop, **logical and port addresses** remain the same from the source to destination (there are some exceptions to this rule).

Specific Addresses

Some applications have user-friendly addresses that are designed for that specific address, for example:

- The e-mail address (for example, someone@gmail.com) that defines the recipient of an e-mail.
- Universal Resource Locator (URL) (for example, www.google.com) that is used to find a document on the World Wide Web (WWW).

The e-mail and URL addresses **are changed** automatically to the **corresponding port** and **logical addresses** by the sending computer (**by using the DNS: *Domain Name System***).

For example, the Figure down below shows a screenshot of the command prompt window in which the 172.217.17.196 is the logical address of the URL address: www.google.com

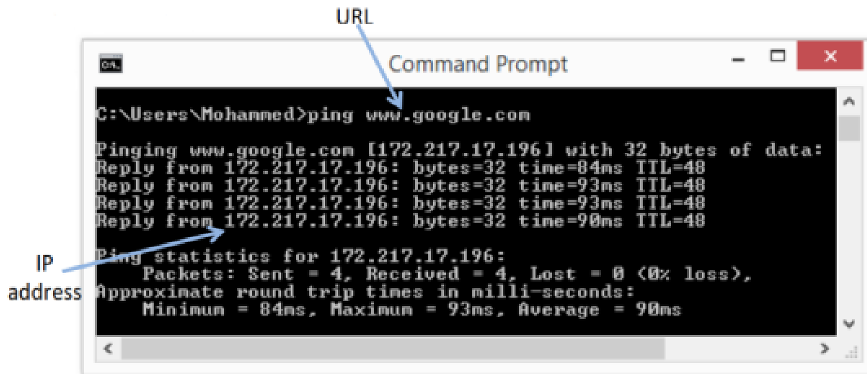
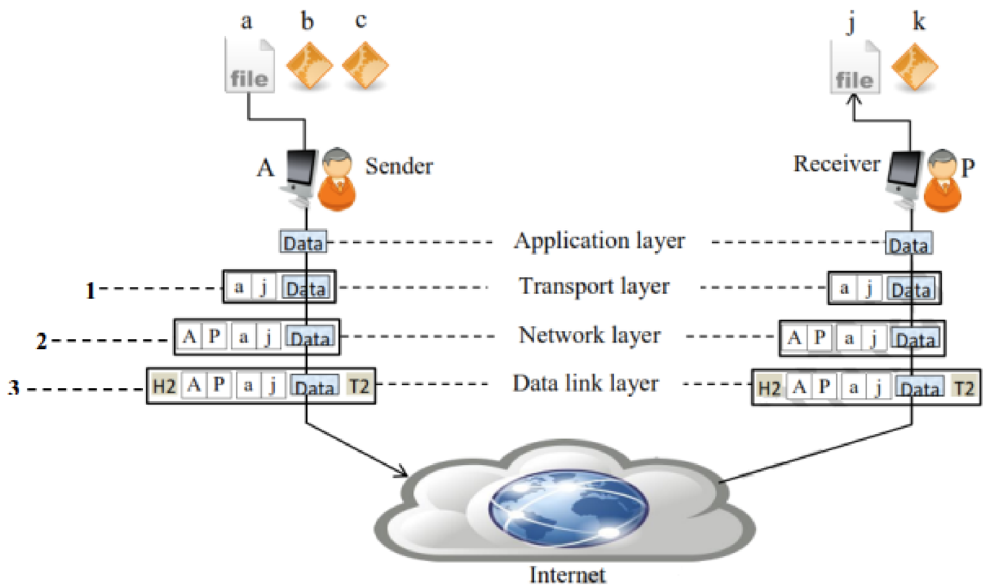


Figure 3.6 Using **ping** instruction to know the corresponding IP address of ww.google.com



According to the function of each layer, **the encapsulation operation** of the above figure is included the following:

1. The transport layer **encapsulates** data from the application layer in **a packet** and adds two port addresses (a) and (j), source and destination.

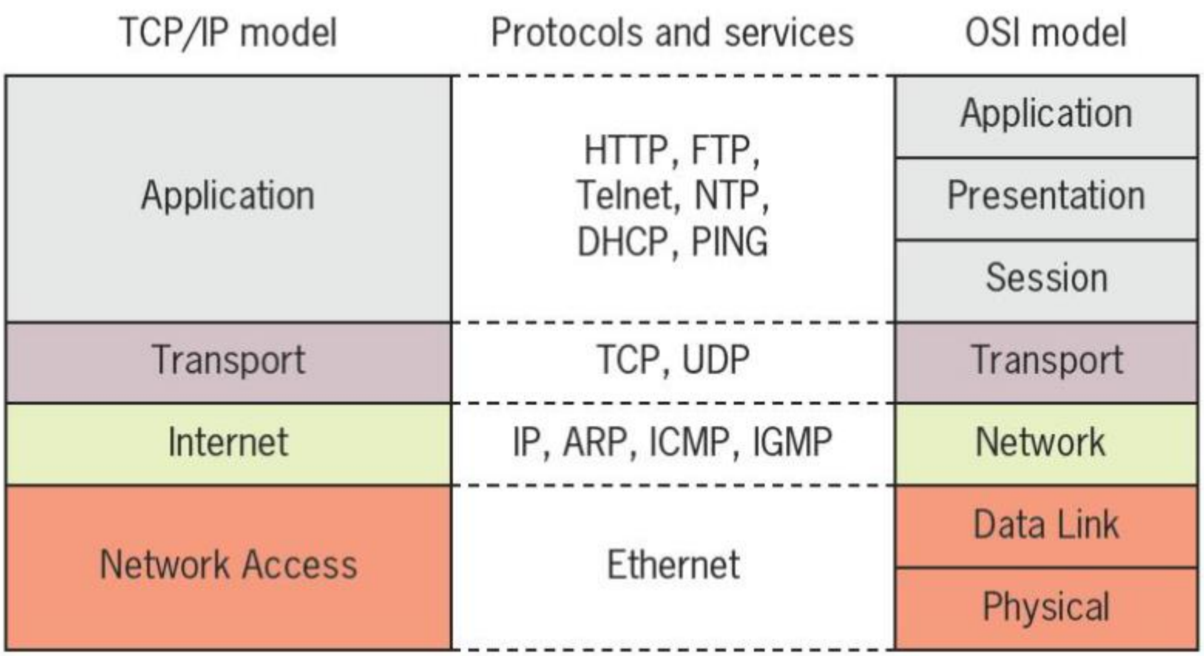
2. The packet from the transport layer is then **encapsulated** in another **packet** at the network layer with logical source and destination addresses (A and P).

3. Finally, the packet is **encapsulated** in **a frame** with the physical source and destination addresses of the next hop.

Network Models

The layered model that dominated data communications and networking literature before 1990 was the Open Systems Interconnection (OSI) model. Everyone believed that the OSI model would become the ultimate standard for data communications, but this did not happen. The TCP/IP protocol suite became the dominant commercial architecture because it was used and tested extensively in the Internet; the OSI model was never fully implemented.

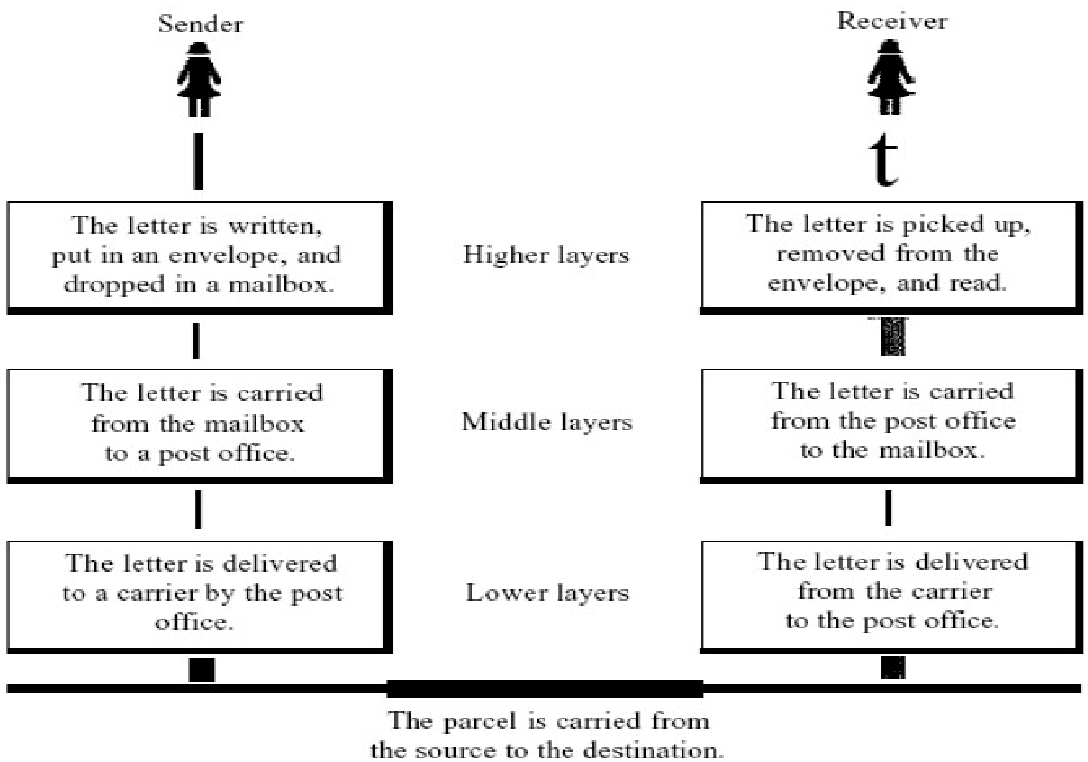
The Figure down below shows the layers included in the TCP/IP and OSI models and also the main protocols and services provided by each layer.



The TCP/IP and OSI models for data communications and networking

Layered Task

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office. Figure down below shows the steps in this task.



Tasks involved in sending a letter

Each layer at the sending site uses the services of the layer immediately below it. The sender at the higher layer uses the services of the middle layer. The middle layer uses the services of the lower layer. The lower layer uses the services of the carrier.

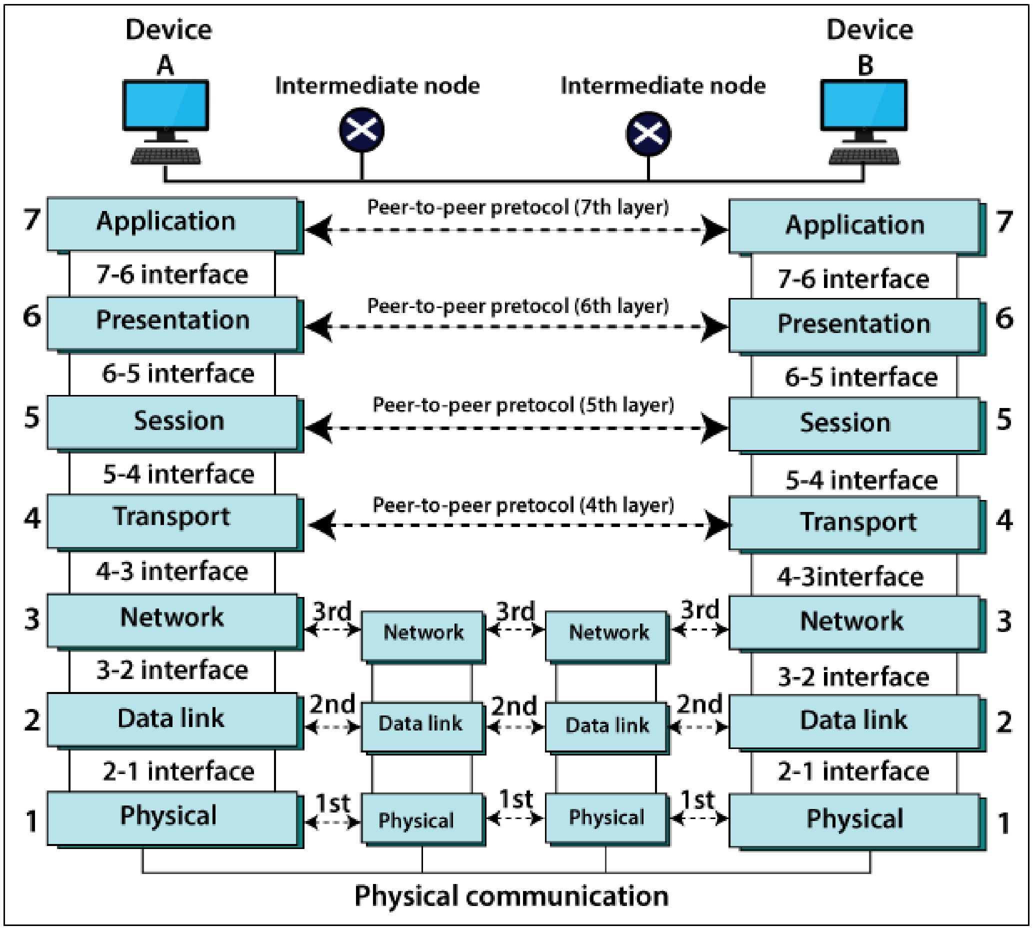
The OSI Model

The Open Systems Interconnection (OSI) model is introduced in the late 1970s by the International Standards Organization (ISO). (Note: ISO is the organization. OSI is the model.)

The OSI model is a layered model for the design and understands of network systems that allows communication between all types of computer systems.

OSI consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

Figure down below shows the layers involved when a message is sent for example from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes, called routers. These intermediate nodes usually involve only the first three layers of the OSI model.



The interaction between layers in the OSI model

Each layer defines a family of functions distinct from those of the other layers. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4.

The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

The **interfaces** between layers are to define the information and services that each layer must provide for the layer above it.

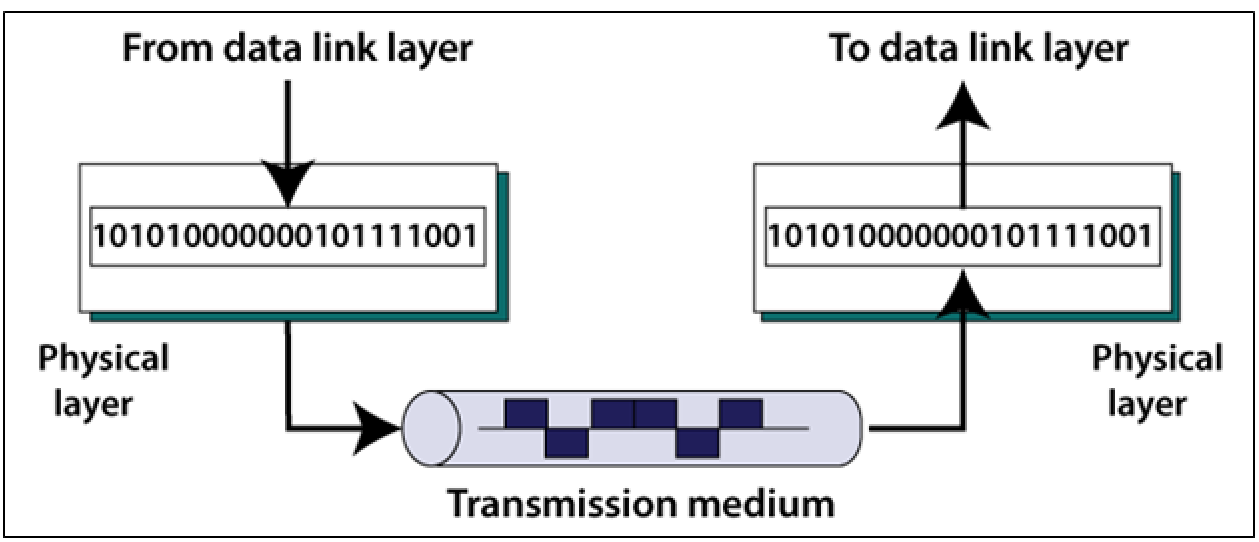
The seven layers are belonging to three subgroups. Layers 1, 2, and 3 are the network support layers; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, and physical addressing). Layers 5, 6, and 7 are the user support layers; they allow interoperability among unrelated software systems. Layer 4, the transport layer, links the two subgroups.

Layers in the OSI Model

In the following we describe the functions of each layer in the OSI model.

1. Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium (see Figure down below)



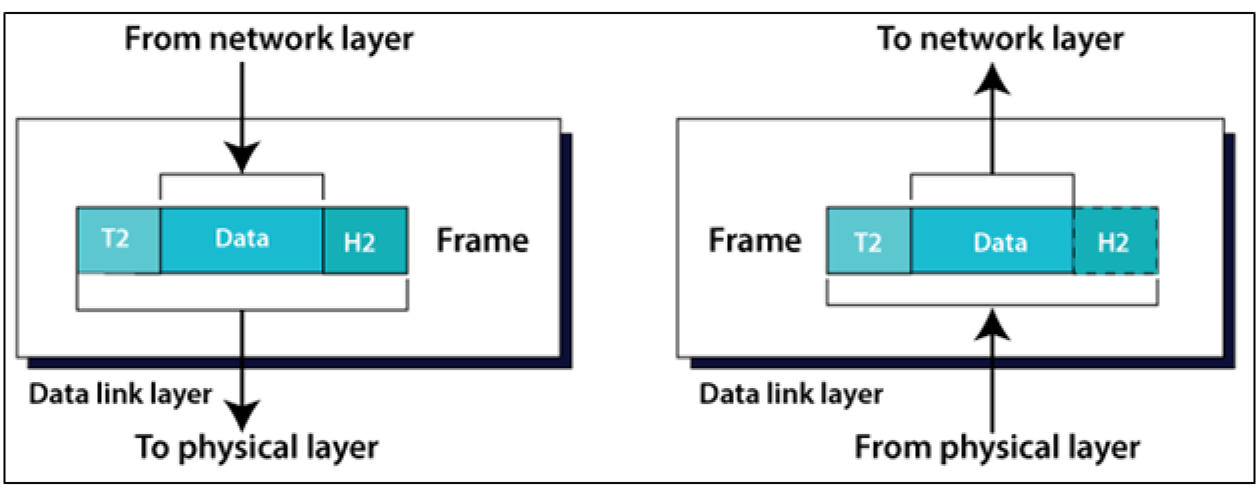
The physical layer is concerned with the following:

- Physical characteristics of interfaces and medium.
- Representation of bits (sequence of 0s or 1s) with defining the type of encoding (how 0s and 1s are changed to signals).
- Data rate or the transmission rate (the number of bits sent each second).
- Synchronization of bits. The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level.
- Line configuration (point-to-point or multipoint configuration).
- Physical topology (mesh, star, bus, etc.).
- Transmission mode (simplex, half-duplex, or full-duplex).

2. Data Link Layer

The data link layer makes the physical layer appear error-free to the upper layer (network layer).

The Figure down below shows the relationship of the data link layer to the network and physical layers.



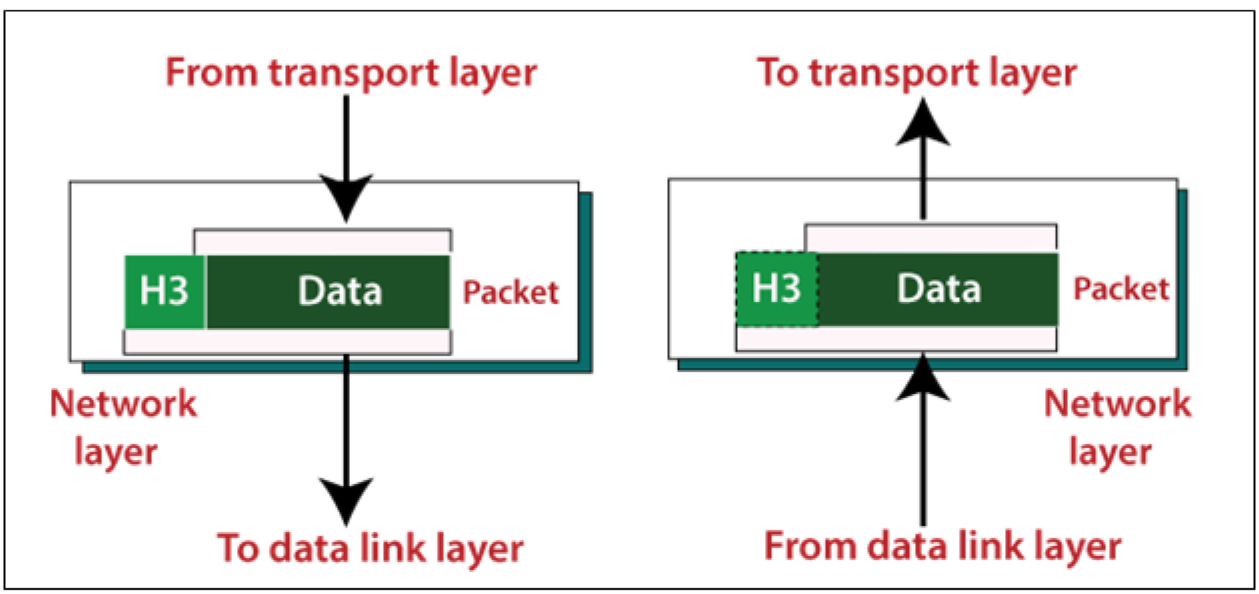
The data link layer is responsible for moving frames from one hop (node) to the next. Other responsibilities of the data link layer include the following:

- **Framing**. The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- **Physical addressing.** The data link layer adds a header to the frame to define the sender and/or receiver devices of the frame. The devises are defined by the physical address (or MAC address).
- **Flow control.** The data link layer ensures the rate at which data are produced in the sender and arrived in the receiver.
- **Error control**. The data link layer adds mechanisms to detect and retransmit damaged or lost frames. Error control is normally achieved through a trailer added to the end of the frame
- **Access control.** The data link layer controls the access to the link when two or more devices are connected to the same link.

3. Network Layer

The network layer is responsible for the source-to-destination delivery of a packet (see Figure down below), possibly across multiple networks (links).

Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links).

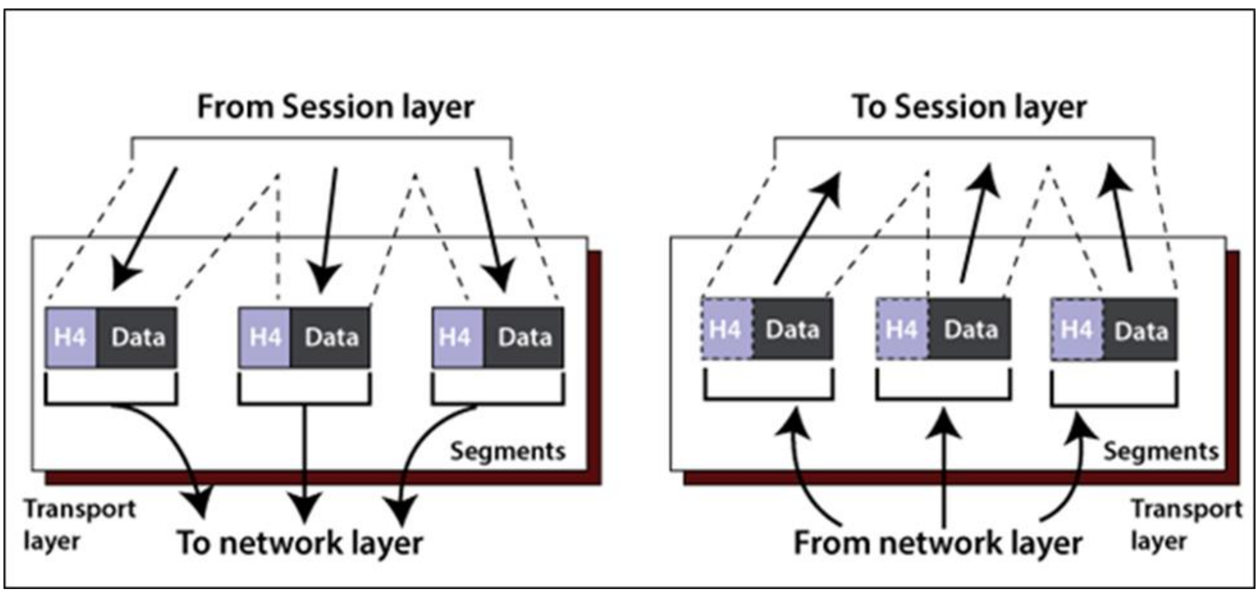


Other responsibilities of the network layer include the following:

- **Logical addressing**. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses (IP address) of the sender and receiver. We discuss logical addresses in a next lecture.
- **Routing**. When independent networks or links are connected to create internetworks, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

4. Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets.



Other responsibilities of the transport layer include the following:

- **Service-point addressing.** Computers often run several programs at the same time. The transport layer header includes a type of address called a servicepoint address (or port address) in order to deliver the entire message to the correct process on that computer.
- **Segmentation and reassembly.** A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly at the destination (see Figure down below)
- **Flow control.** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- **Error control.** Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process - to process rather than across a single link.

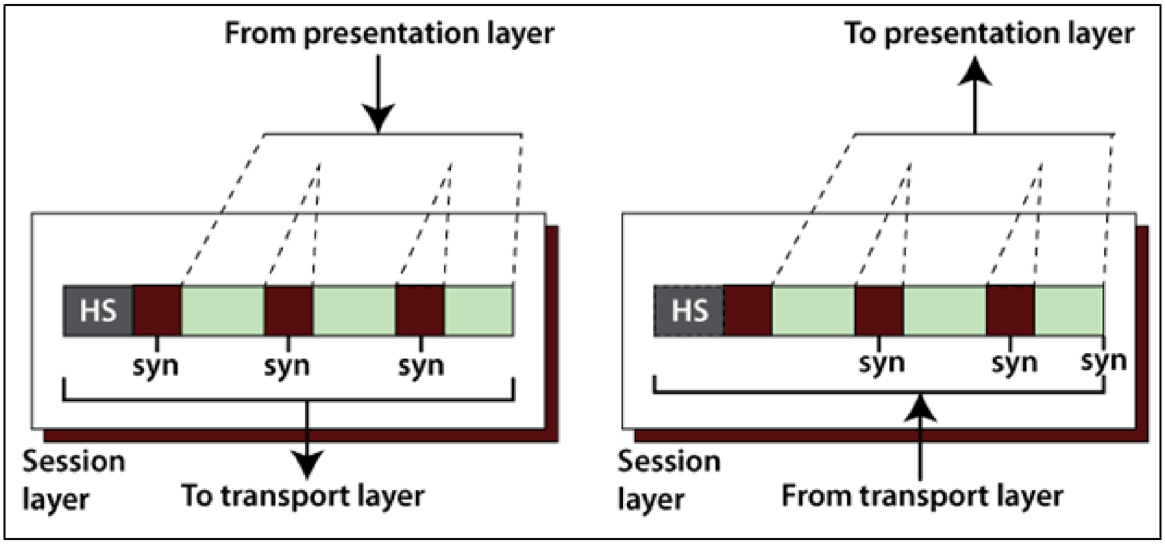
5. Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is responsible for dialog control and synchronization.

Specific responsibilities of the session layer include the following:

- **Dialog control.** The session layer allows the communication between two processes to take place in either half-duplex (one way at a time) or fullduplex (two ways at a time) mode.
- **Synchronization.** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data (see Figure down below).

  For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages.

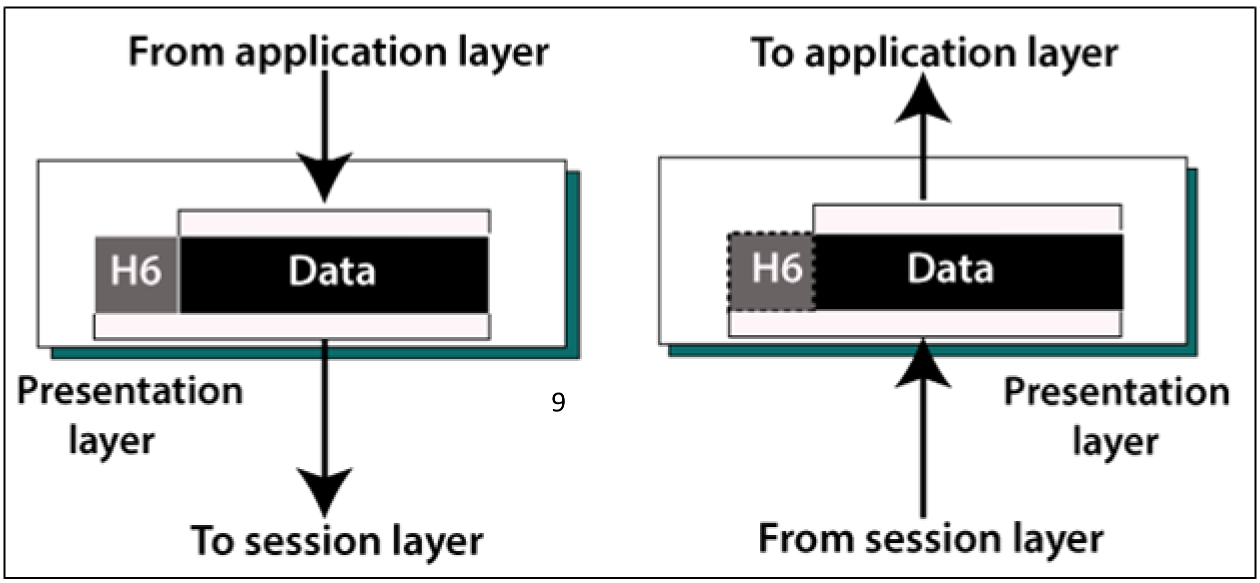


6. Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems (see Figure down below).

Specific responsibilities of the presentation layer include the following:

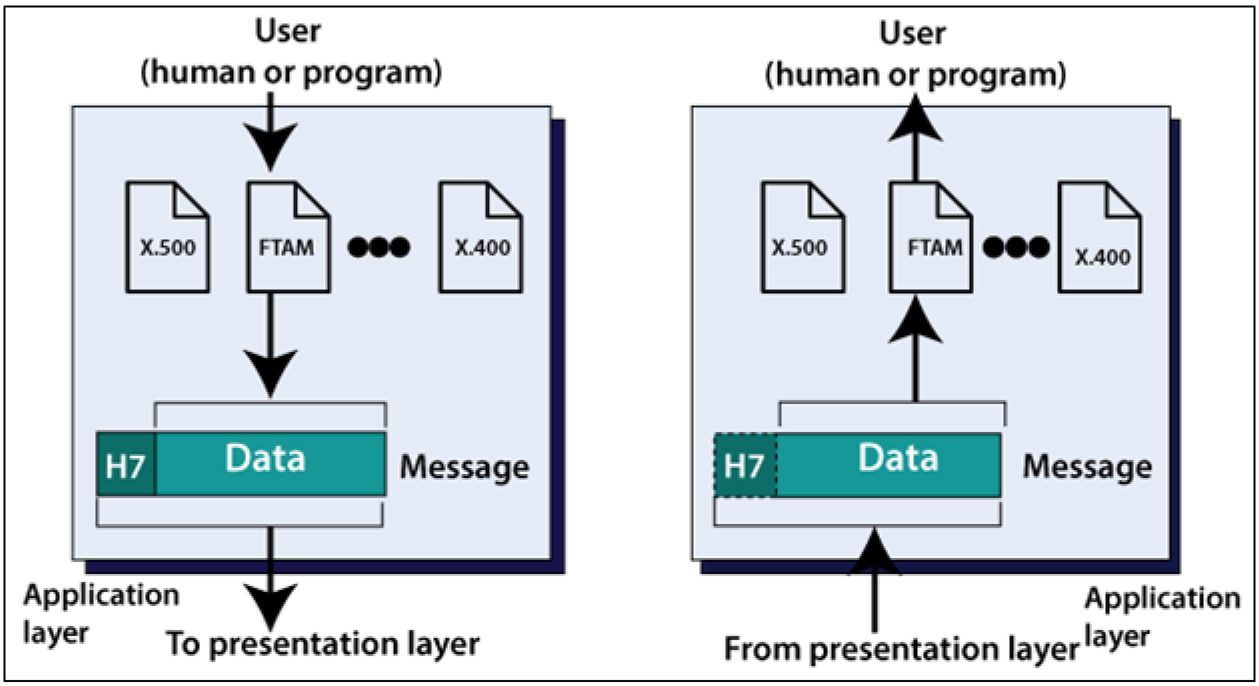
- **Translation.** Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.
- **Encryption**. To carry sensitive information, a system must be able to ensure privacy.
- **Compression**. Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the data transmission.

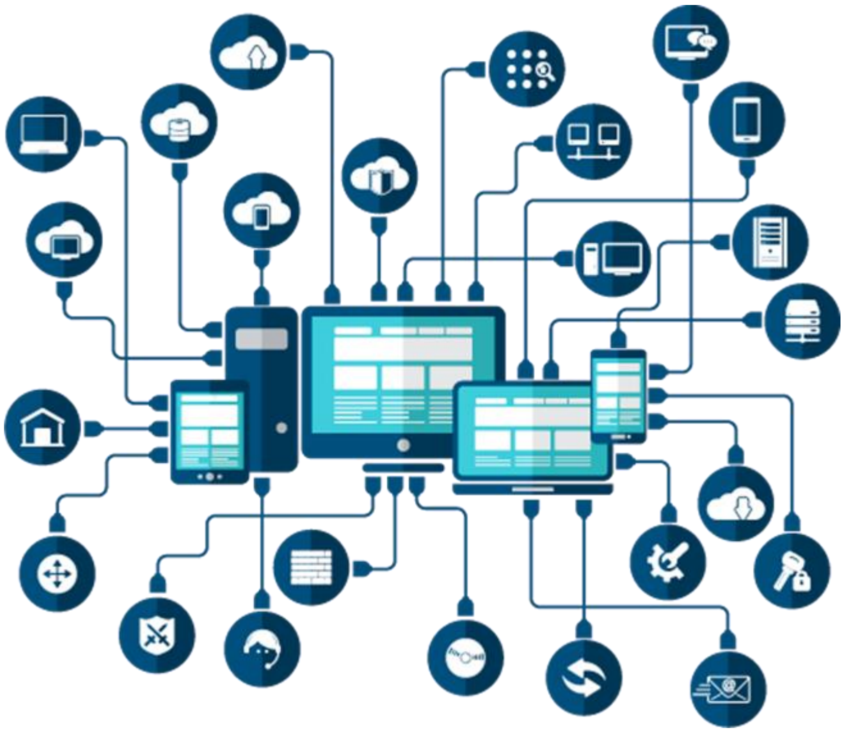


7. Application Layer

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

The Figure down below shows only three application services available on a user computer: XAOO (message-handling services), X.500 (directory services), and file transfer, access, and management (FTAM). The user in this example employs XAOO to send an e-mail message.





COMPUTER NETWORKS 1

Stage Three

CHAPTER THREE

Data and Analog Signals

Data and Signals

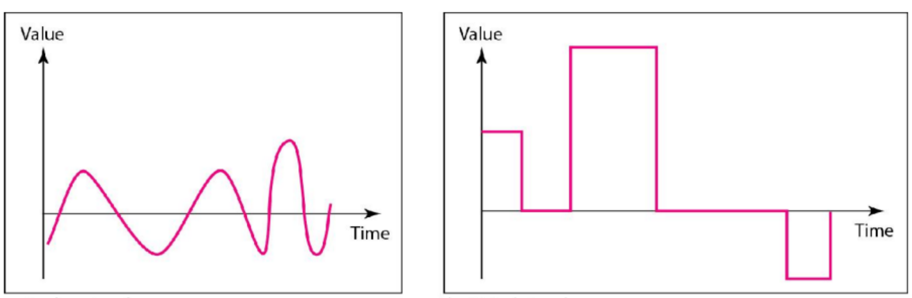
One of the major functions of the physical layer is to move data in the form of electromagnetic signals across a transmission medium. Generally, the data usable to a person or application are not in a form that can be transmitted over a network. For example, a photograph must first be changed to a form that transmission media can accept. Transmission media work by conducting energy along a physical path.

Analog and Digital Data

Data can be analog or digital. The term analog data refers to information that is continuous; digital data refers to information that has discrete states. **For example: the analog clock and the digital clock.**
Digital data take on discrete values. For example, data are stored in computer memory in the form of 0s and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.
Therefore, data can be analog or digital. **Analog data** are continuous and take continuous values.
Digital data have discrete states and take discrete values.

Analog and Digital Signals

Like the data they represent, signals can be either analog or digital. **An analog** signal has infinitely many levels of intensity over a period of time. A **digital signal**, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and 0.
Figure down below illustrates an analog signal and a digital signal. The vertical axis represents the value or strength of a signal. The horizontal axis represents time. Therefore, Signals can be analog or digital. Analog signals can have an **infinite number of values** in a range; digital signals can have only a **limited number of values.**



a. Analog signal b. Digital signal

Periodic and Non-periodic Signals

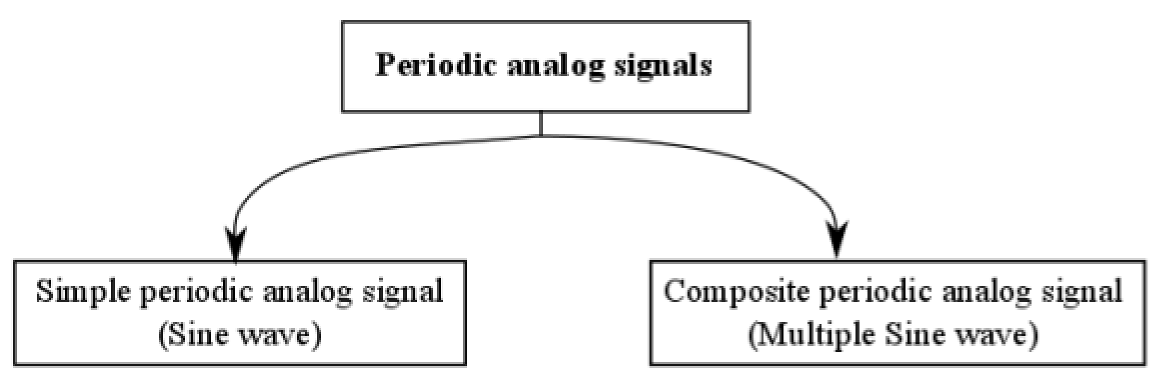
A **periodic signal** completes a pattern within a measurable time frame, called a period, and repeats that pattern over identical periods. The completion of one full pattern is called a cycle.

A **nonperiodic signal** changes without exhibiting a pattern or cycle that repeats over time. Both analog and digital signals can be periodic or nonperiodic.

In data communications, we commonly use ***periodic analog signals*** (because they need less bandwidth) and ***nonperiodic digital signals*** (because they can represent variation in data).

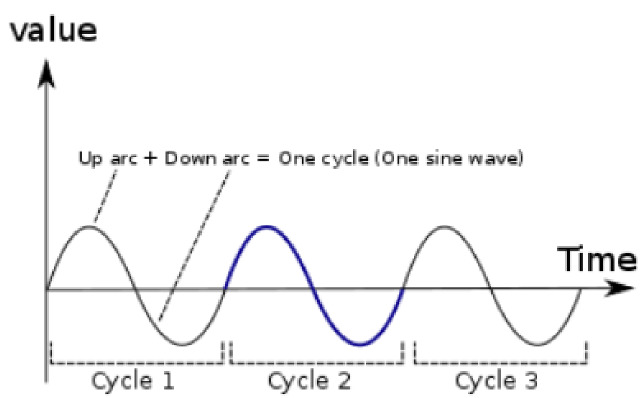
Periodic analog signals

Periodic analog signals can be classified as simple or composite.



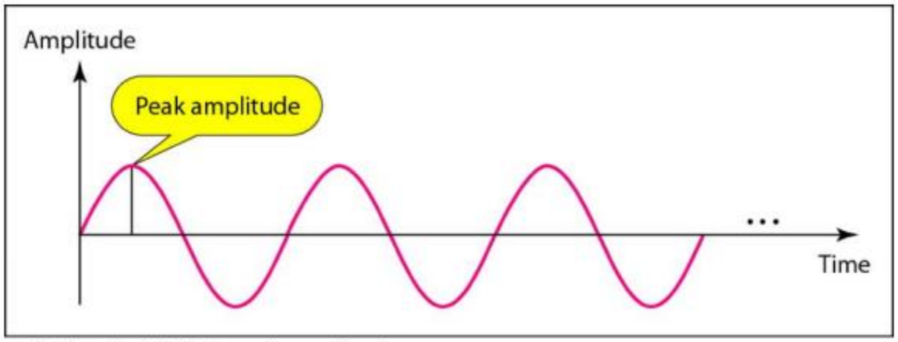
Sine Wave

Figure down below shows a sine wave. Each cycle consists of a single arc above the time axis followed by a single arc below it. A sine wave can be represented by three parameters: the **1) peak amplitude**, **2) the frequency**, and **3) the phase.**

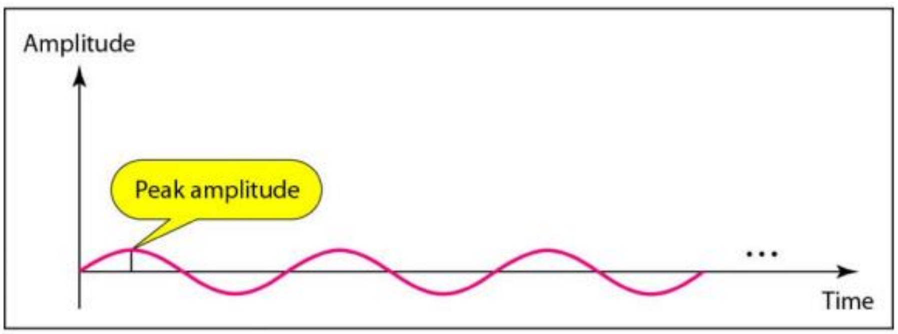


Peak amplitude

The peak amplitude of a signal is the absolute value of its highest intensity (the energy). Figure 4.4 shows two signals and their peak amplitudes. For electric signals, peak amplitude is normally measured in volts. The power in your house can be represented by a sine wave with a peak amplitude of 220 to 240 V, whereas the peak value of an AA battery is normally 1.5 V



a. A signal with high peak amplitude



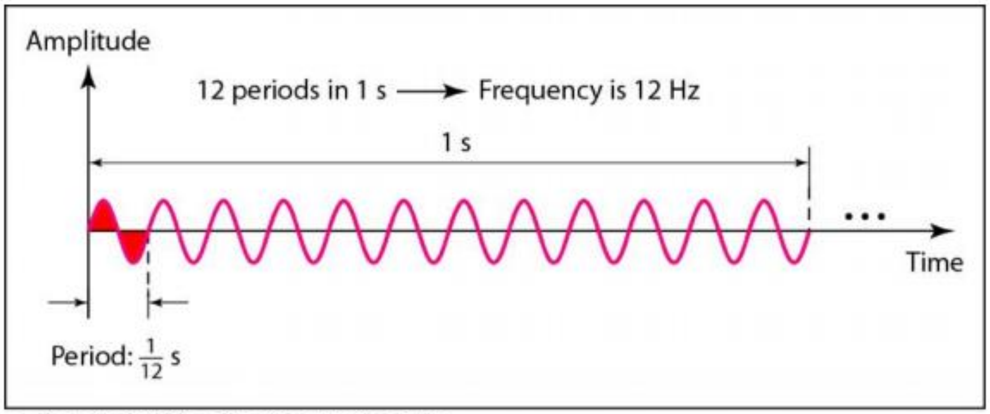
b. A signal with low peak amplitude

Period and Frequency

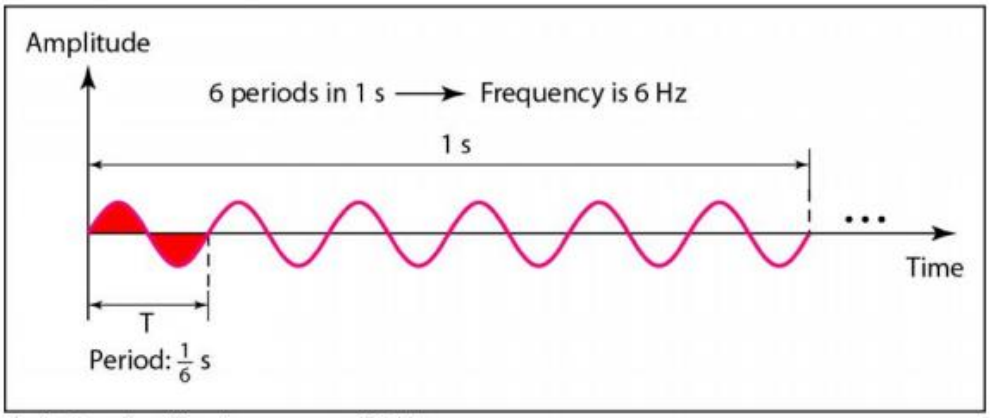
Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle. Frequency refers to the number of periods in 1 s. Note that period and frequency are just one characteristic defined in two ways. Period is the inverse of frequency, and frequency is the inverse of period, as the following formulas show.

$$f = \frac{1}{T} \text{ and } T = \frac{1}{f} \quad (f \text{ :frequency } T \text{ : time })$$

Figure down below shows two signals and their frequencies.



a. A signal with a frequency of 12 Hz



b. A signal with a frequency of 6 Hz

Two signals with the same amplitude and phase, but different frequencies

Period is formally expressed in seconds. Frequency is formally expressed in Hertz (Hz), which is cycle per second. Units of period and frequency are shown in Table down below:

Unit	*Equivalent*	*Unit*	*Equivalent*
Seconds (s)	1 s	Hertz (Hz)	1 Hz
Milliseconds (ms)	10^{-3} s	Kilohertz (kHz)	10^{3} Hz
Microseconds (μs)	10^{-6} s	Megahertz (MHz)	10^{6} Hz
Nanoseconds (ns)	10^{-9} s	Gigahertz (GHz)	10^{9} Hz
Picoseconds (ps)	10^{-12} s	Terahertz (THz)	10^{12} Hz

Units of Period Units of Frequency

Example 1

The power we use at home has a frequency of 60 Hz. The period of this sine wave can be determined as follows:

$$T\frac{1}{f} = \frac{1}{60} = 0.0166 \text{ s} = 0.0166 \text{ x } 10^{3} \text{ ms} = 16.6 \text{ ms}$$

This means that the period of the power for our lights at home is 0.0116 s, or 16.6 ms. Our eyes are not sensitive enough to distinguish these rapid changes in amplitude.

Example 2

Express a period of 100 ms in microseconds.

Solution

From the Units Table we find the equivalents of 1 ms (l ms is 10-3 s) and (1 s is 106 µs). We make the following substitutions:

$$100 \text{ ms} = \underbrace{100 \text{ x } 10^{-3}}\text{ x }\underbrace{10^{6}}\ \mu\text{s} = \underbrace{10^{2} \text{ x } 10^{-3} \text{ x } 10^{6}}\ \mu\text{s} = 10^{5}\ \mu\text{s}$$

لتحويل الوقت من وحدة الملي ثانية (milliseconds) الى وحدة الثانية (second)

لتحويل الوقت من وحدة الثانية (second) الى وحدة المايكرو ثانية (Microseconds)

عند الضرب تُجمع الأسس

Example 3

The period of a signal is 100 ms. What is its frequency in kilohertz? Solution First we change 100 ms to seconds, and then we calculate the frequency from the period (1 Hz = 10-3 kHz).

$$100 \text{ ms} = 100 \text{ x } 10^{-3} \text{ s} = 10^{-1} \text{ s}$$

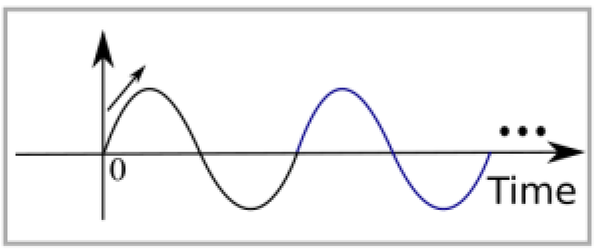
$$f = \frac{1}{T} = \frac{1}{10^{-1}} \text{ Hz} = 10 \text{ Hz} = 10 \text{ x } 10^{-3} \text{ kHz} = 10^{-2} \text{ kHz}$$

The Phase

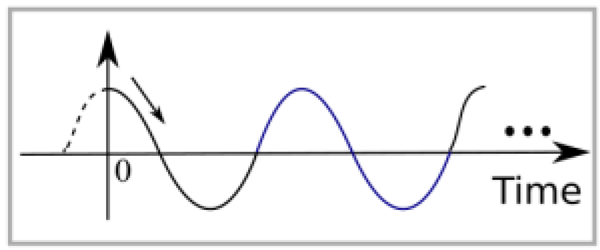
The term phase describes the position of the waveform relative to time 0. It indicates the status of the first cycle (how much the wave is shifted from 0 on the time axis).

Looking at Figure down below we can say that

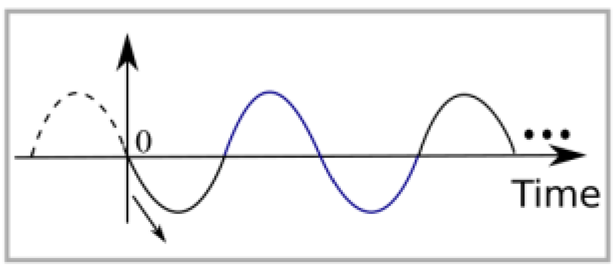
1. A sine wave with a phase of 0° starts at time 0 with a zero amplitude.
   The amplitude is increasing.
2. A sine wave with a phase of 90° starts at time 0 with a peak amplitude.
   The amplitude is decreasing.
3. A sine wave with a phase of 180° starts at time 0 with a zero amplitude.
   The amplitude is decreasing



a.0 degrees



b.90 degrees



c.180 degrees

Composite Signals

The previous section focused on simple sine waves which have many applications in daily life. We can send a single sine wave to carry electric energy from one place to another. For example, the power company sends a single sine wave with a frequency of 50 Hz to distribute electric energy to houses and businesses.

If we had only one single sine wave to convey a conversation over the phone, it would make no sense and carry no information. We would just hear a buzz. Therefore, we need to send a composite signal to communicate data; a singlefrequency sine wave is not useful in data communications.

The **composite signal** is a combination of simple sine waves with different frequencies, amplitudes, and phases.

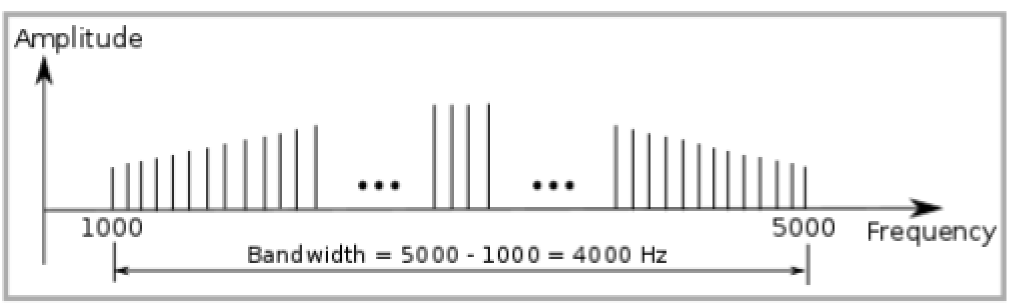
A composite signal can be periodic or nonperiodic as shown in the following:

- **A periodic composite signal** can be decomposed into a series of simple sine waves with discrete frequencies (the frequencies that have integer values: 1, 2, 3, and so on).
- **A nonperiodic composite signal** can be decomposed into a combination of an infinite number of simple sine waves with continuous frequencies (the frequencies that have real values: 0.1, 0.2, 0.3, and so on).

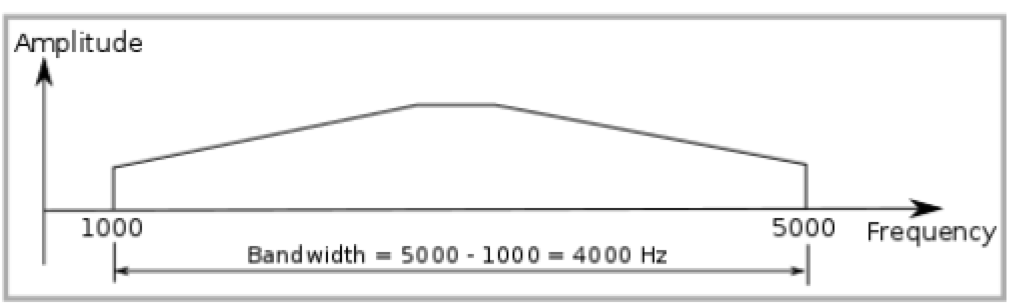
Bandwidth

Bandwidth is the range of frequencies contained in a composite signal. The bandwidth is normally a difference between two numbers. For example, if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 - 1000, or 4000.

Figure down below shows the concept of bandwidth. The bandwidth of the periodic signal contains all integer frequencies between 1000 and 5000 (1000, 1001, 1002, ...). The bandwidth of the nonperiodic signals has the same range, but the frequencies are continuous.



a. Bandwidth of a periodic signal



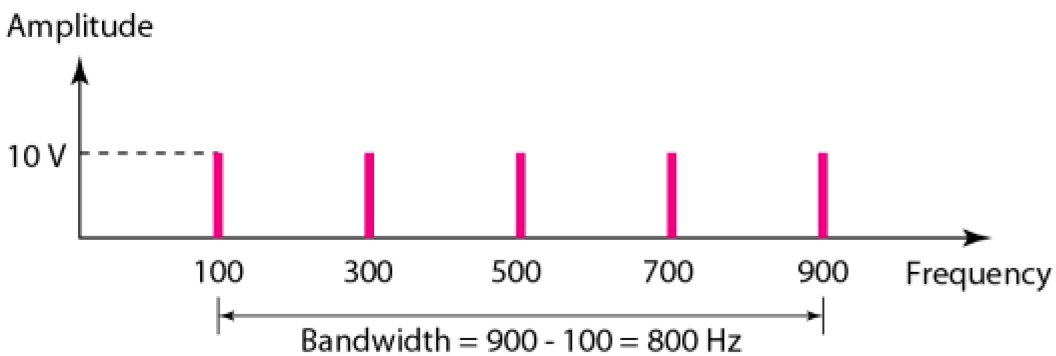
Example 4

If a periodic signal is decomposed into five sine waves with frequencies of 100, 300, 500, 700, and 900 Hz, what is its bandwidth? Draw the spectrum, assuming all components have a **maximum amplitude of 10 V.**

Solution

Let *fh* be the highest frequency, *fl* the lowest frequency, and *B* the bandwidth.
Then: $B = fh - fl = 900 - 100 = 800$ Hz

The spectrum has only five spikes, at 100, 300, 500, 700, and 900 Hz (see Figure down below).



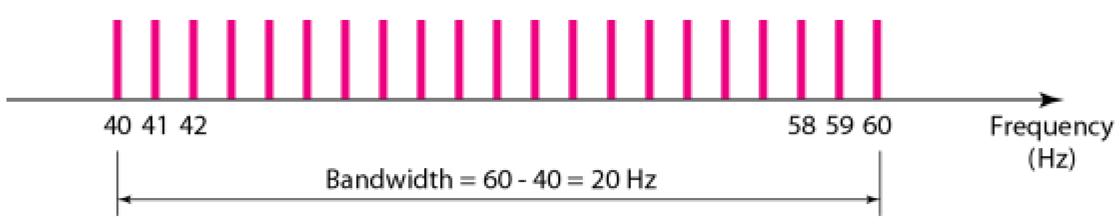
Example 5

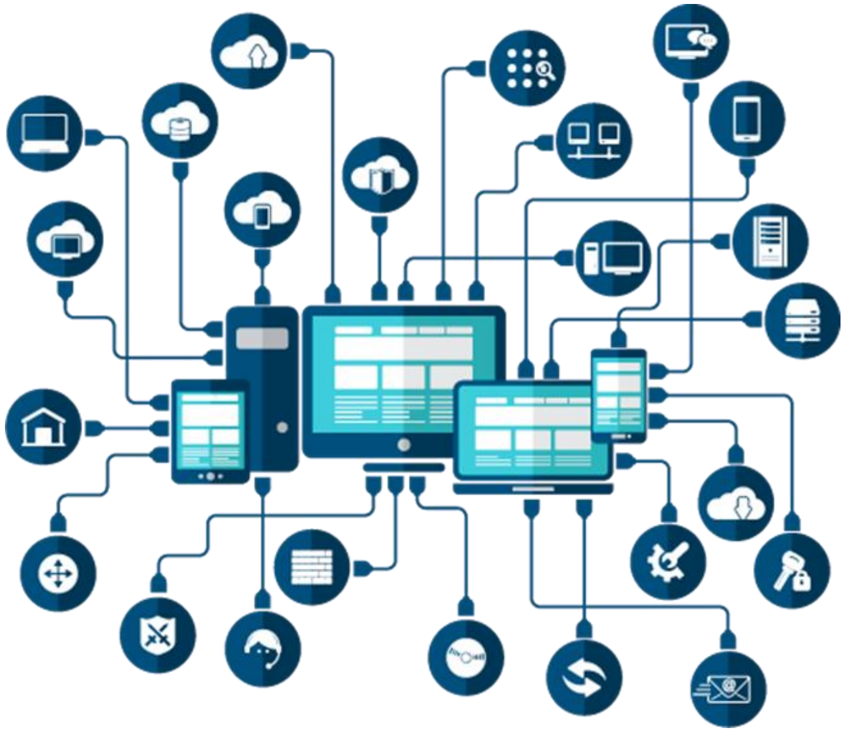
A periodic signal has a bandwidth of 20 Hz. The highest frequency is 60 Hz. What is the lowest frequency? Draw the spectrum if the signal contains all frequencies of the same amplitude.

Solution

Let *fh* be the highest frequency, *fl* the lowest frequency, and *B* the bandwidth.
Then: $B = fh - fl \quad \rightarrow 20 = 60 - fl \quad \rightarrow fl = 60 - 20 = 40$ Hz

The spectrum contains all integer frequencies. We show this by a series of spikes (see Figure down below)





COMPUTER NETWORKS 1

Stage Three

CHAPTER FOUR

Network Performance & Transmission Media

Network Performance

In previous sections, we have discussed the tools of transmitting data (signals) over a network and how the data behave. In this section we discuss quality of service, an overall measurement of network performance.

Bandwidth

One characteristic that measures network performance is bandwidth. However, the term can be used in two different contexts with two different measuring values: 1) ***bandwidth in hertz*** and 2) ***bandwidth in bits per second***.

1. **Bandwidth in Hertz**
   We have discussed this concept in Chapter 3. For example, we can say the bandwidth of a subscriber telephone line is 4 kHz.
2. **Bandwidth in Bits per Seconds**
   he terms bandwidth can refer to the number of bits per second that a channel or a network can transmit. For example, the bandwidth of an Ethernet network (or the links in this network) is a maximum of 100 Mbps.

Relationship

There is an explicit relationship between the bandwidth in hertz and bandwidth in bits per second. Basically, an ***increase in bandwidth in hertz*** means an ***increase in bandwidth in bits per second***. The relationship depends on whether we have baseband transmission or transmission with modulation.

In networking, we use the term bandwidth in two contexts.

• The first, bandwidth in **hertz**, refers to the range of frequencies in a composite signal or the range of frequencies that a channel can pass.

• The second, bandwidth in **bits per second**, refers to the speed of bit transmission in a channel or link.

Example

The bandwidth of a subscriber line is 4 kHz for voice or data. The bandwidth of this line for data transmission can be up to 56,000 bps using a sophisticated modem to change the digital signal to analog (modulation).

Example

If the telephone company improves the quality of the line and increases the bandwidth to 8 kHz, we can send 112,000 bps by using the same technology as mentioned in the Example above.

Therefore, an ***increase in bandwidth in hertz*** means an ***increase in bandwidth in bits per second***.

Throughput

The throughput is a measure of how fast we can actually send data through a network. The bandwidth in bits per second and throughput are different. For example, we may have a link with a bandwidth of 1 Mbps, but the devices connected to the end of the link may handle only 200 kbps. This means that we cannot send more than 200 kbps through this link.

Imagine a highway designed to transmit 1000 cars per minute from one point to another. However, if there is problem on the road, this number may be reduced to 100 cars per minute. The bandwidth is 1000 cars per minute; the throughput is 100 cars per minute.

Example

A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?

Solution

We can calculate the throughput as

Throughput = (12,000 x 10,000) / 60 = 2 Mbps

The ***throughput*** is almost one-fifth of the **bandwidth** in this case.

Latency (Delay)

The latency or delay defines how long it takes for an entire message to completely arrive at the destination. We can say that latency is made of four components: **propagation time, transmission time, queuing time and processing delay**.

Latency = propagation time + transmission time + queuing time + processing delay

Propagation Time

Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed.

Propagation time = Distance / (Propagation Speed)

The propagation speed of electromagnetic signals depends on the medium and on the frequency of the signal. For example, in a vacuum, light is propagated with a speed of 3×10^8 m/s. It is lower in air; it is much lower in cable.

Example

What is the propagation time if the distance between the two points is 12,000 km? Assume the propagation speed to be 2.4×10^8 m/s in cable.

Solution

We can calculate the propagation time as

Propagation time = (12,000 x 1000) / (2.4×10^8) = 0.05 s x 10^3= 50 ms

The example shows that a bit can go in only 50 ms: if there is a direct cable between the source and the destination.

Transmission Time

In data communications we don't send just 1 bit, we send a message. The transmission time of a message depends on the size of the message and the bandwidth of the channel.

Transmission time = (Message size) / Bandwidth

Example

What are the propagation time and the transmission time for a 2.5-KB (kilobyte) message (an email) if the bandwidth of the network is 1 Gbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4×108 m/s.

Solution

We can calculate the propagation and transmission time as

Propagation time = (12,000 x 1000) / (2.4×10^8) = 50 ms (dominant factor)

Transmission time = (2500 x 8) / 109= 0.00002 s = 0.02 ms

Note that in this case, because the message is short and the bandwidth is high, the **dominant factor** is the propagation time, not the transmission time. The transmission time can be ignored.

Example

What are the propagation time and the transmission time for a 5-MB (megabyte) message (an image) if the bandwidth of the network is 1 Mbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4 × 108 m/s.

Solution

We can calculate the propagation and transmission times as

Propagation time = (12,000 x 1000) / (2.4×10^8) = 50 ms

Transmission time = (5,000,000 x 8) /10^6 = 40 s (dominant factor**)**

Note that in this case, because the message is very long and the bandwidth is not very high, the **dominant factor** is the transmission time, not the propagation time. The propagation time can be ignored.

Jitter

Another performance issue that is related to delay is jitter. We can say that the jitter problem is happened because:

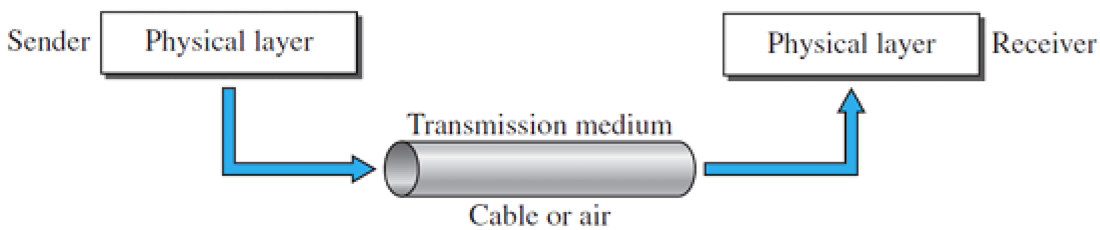
1) different packets of data encounter different delays.

2) the application using the data at the receiver site is time-sensitive (audio and video data, for example).

For example, if the delay for the first packet is 20 ms, for the second is 45 ms, and for the third is 40 ms, then the real-time application that uses the packets will make jitter.

Transmission Media

Transmission media are actually located below the physical layer and are directly controlled by the physical layer. Figure 6.1 shows the position of transmission media in relation to the physical layer.

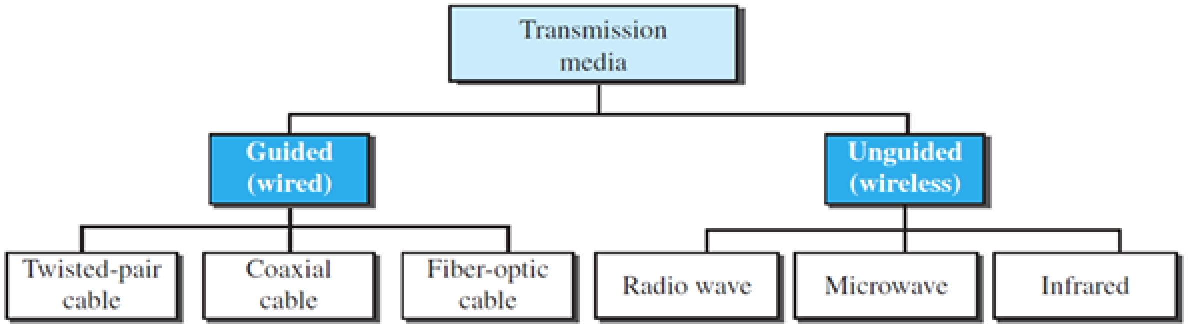


Transmission medium and physical layer

A **transmission medium** can be defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air.

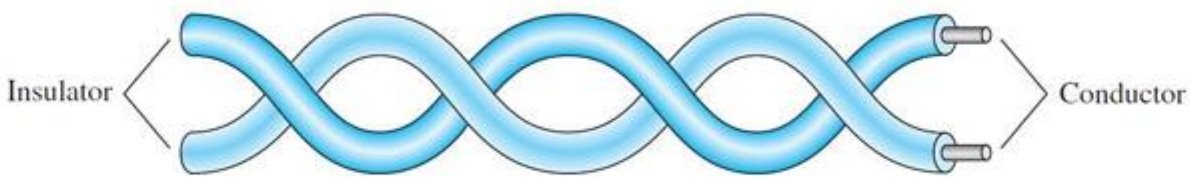
In data communications the transmission medium is usually free space, metallic cable, or fibre-optic cable. The information is usually a signal that is the result of a conversion of data from another form.

In telecommunications, transmission media can be divided into two broad categories: **guided and unguided**. Guided media include twisted-pair cable, coaxial cable, and fibre-optic cable. Unguided medium is free space. Figure 6.2 shows this taxonomy.



Twisted-Pair Cable

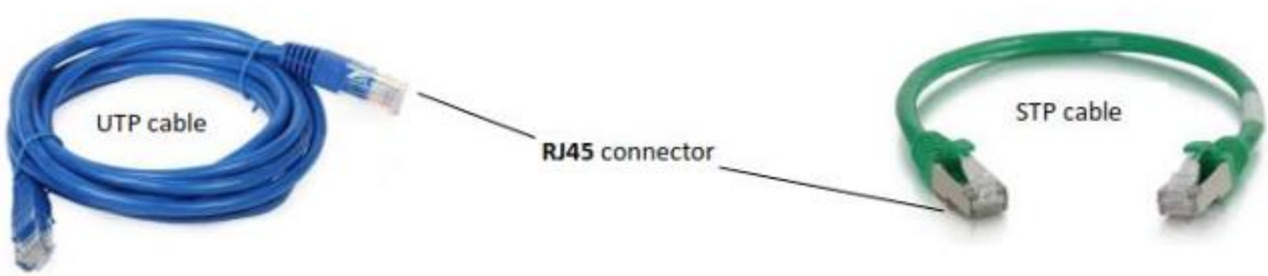
A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure down below.



One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.

In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

Twisting makes it probable that both wires are **equally affected** by external influences (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly cancelled out. **The number of twists** per unit of length (e.g., inch) has some effect on the **quality of the cable** (more twists → more quality).

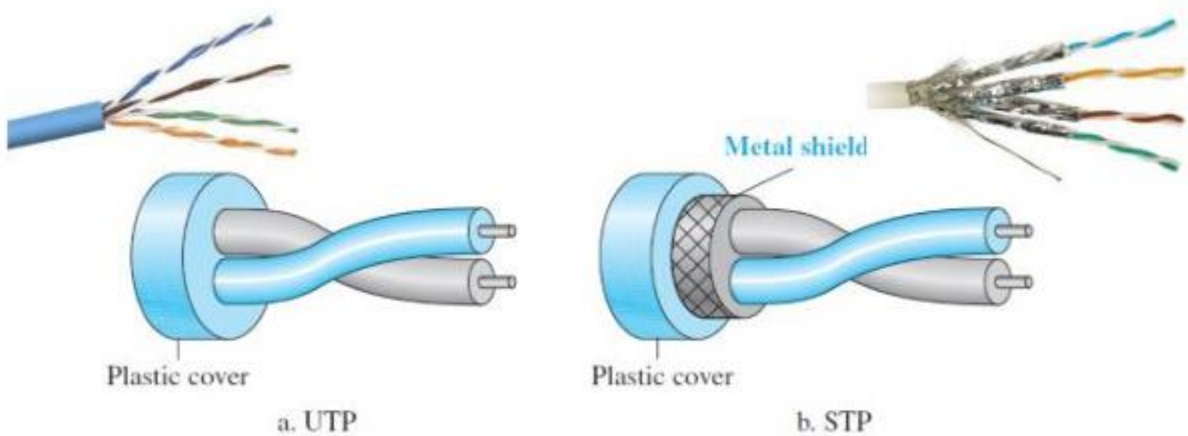


Unshielded Versus Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as **unshielded twisted-pair (UTP)**.

IBM has also produced a version of twisted pair cable for its use, called **shielded twisted-pair (STP).**

STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors. Figure 6.4 shows the difference between UTP and STP.



Categories

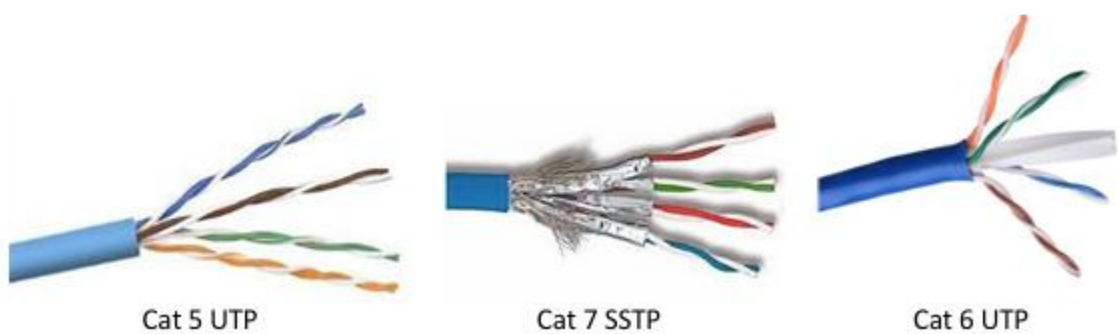
Twisted-pair cables are classified into seven categories. These categories are determined by cable quality, for example:

1. **Category 1** (Cat 1) Unshielded twisted-pair used in telephone.

2. **Category 5** (Cat 5) Unshielded twisted-pair used in LANs with 100 Mbps data rate.

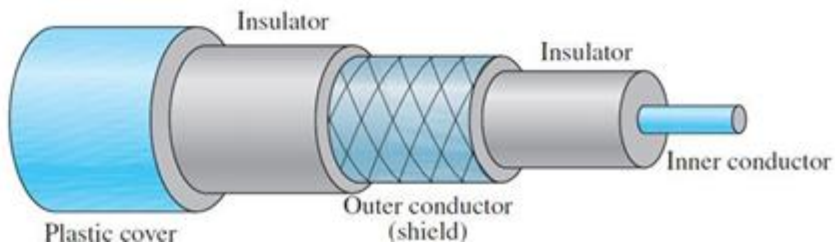
3. **Category 6** (Cat 6) A new category that must be tested at a 200-Mbps data rate.

4. **Category 7** Sometimes called **SSTP** (shielded screen twisted-pair). Each pair is individually wrapped in a metallic foil. The data rate is 600 Mbps.



Coaxial Cable

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable. Instead of having two wires, coax has an **inner core conductor** of solid wire (usually copper) and **outer conductor** serves both as a shield against noise and as the second conductor to complete the circuit (see Figure down below).



Coaxial Cable Standards(للاطلاع فقط)

Coaxial cables are categorized by their Radio Government (RG) ratings. Each RG number denotes a unique set of physical specifications, such as the wire gauge of the inner conductor, the thickness and type of the inner insulator. Each cable defined by an RG rating is adapted for a specialized function, as shown in the following table.

Categories of coaxial cables (للاطلاع فقط)

Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

RG-59 cable and connectors

RG-58 cable and connectors

RG-11 cable and connectors

Coaxial cable applications

Coaxial cables are mainly used in the following:

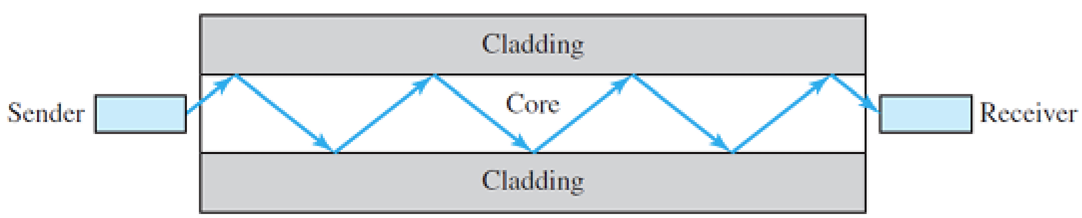
1. Telephone networks. Coaxial cable was widely used in telephone networks. However, coaxial cable has largely been replaced today with fiberoptic cable.

2. Cable TV networks. Coaxial cable was widely used in the traditional cable TV network. Later, however, cable TV providers replaced most of the media with fiber-optic cable.

3. Ethernet LANs. The 10Base-2 uses RG-58 coaxial cable with BNC connectors to transmit data at 10 Mbps with a range of 185 m. The 10Base5 uses RG-11 (thick coaxial cable) to transmit 10 Mbps with a range of 500 m.

Fiber-Optic Cable

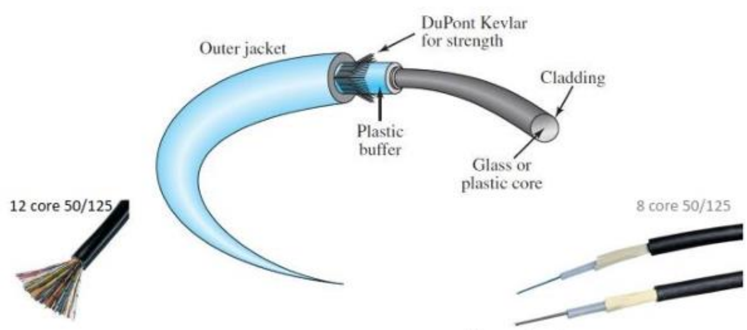
A **fiber-optic cable** is made of glass (or plastic) and transmits signals in the form of light. **The difference in density** of the glass and cladding must be such that a beam of light moving through the core is **reflected off** the cladding instead of being **refracted** into it, as shown in Figure down below.



Cable Composition (للاطلاع فقط)

Figure down below shows the composition of a typical fiber-optic cable. The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable. Kevlar is a strong material used in the fabrication of bulletproof vests. Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core.

Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding both expressed in micrometers (for example 50/125µm or 100/125µm).



Fiberoptic applications

Fiberoptics are mainly used in the following:

1. **Backbone networks**. Fiber-optic cable is often found in **backbone networks** (central large networks) because its wide bandwidth is cost-effective (with data rate of 1600 Gbps).

2. **Cable TV networks**. Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network.

3. **Ethernet LANs**. Local-area networks such as **100Base-FX** network (Fast Ethernet) and **1000Base-X** also use fiber-optic cable.

Advantages of Optical Fiber

Fiber-optic cable has several advantages over metallic cable (twisted-pair or coaxial).

• **Higher bandwidth**. Fiber-optic cable can support higher bandwidths (and hence data rates) than either cable. Bandwidth utilization are **limited not** by the fiber-optic cable **but by** the signal generation and reception technology available at LAN cards, switches, routers, etc.

• **Less signal attenuation**. A signal can run for 50 km without requiring regeneration.

• **No noise**. Electromagnetic noise cannot affect fiber-optic cables.

• **Resistance to corrosiveness**. Glass is more resistant to corrosive materials than copper.

• **Light weight**. Fiber-optic cables are much lighter than copper cables.

Disadvantages of Optical Fiber

• **Installation and maintenance**. Its installation and maintenance require expertise that is not yet available everywhere.

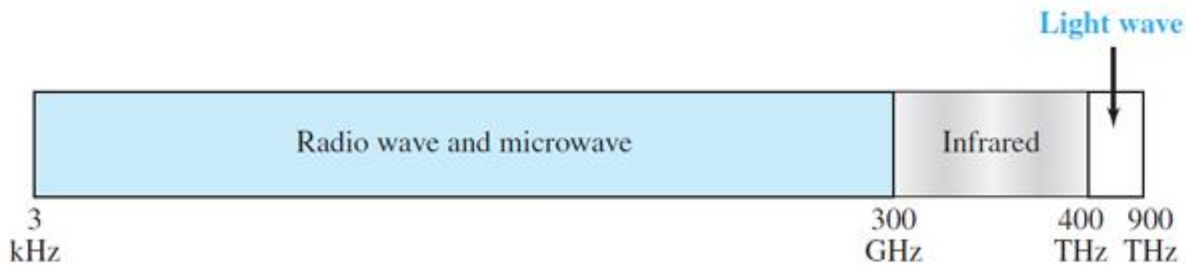
• **Unidirectional light propagation**. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.

• **Cost**. The cable and the interfaces are relatively more expensive than those of other copper media.

UNGUIDED MEDIA: WIRELESS

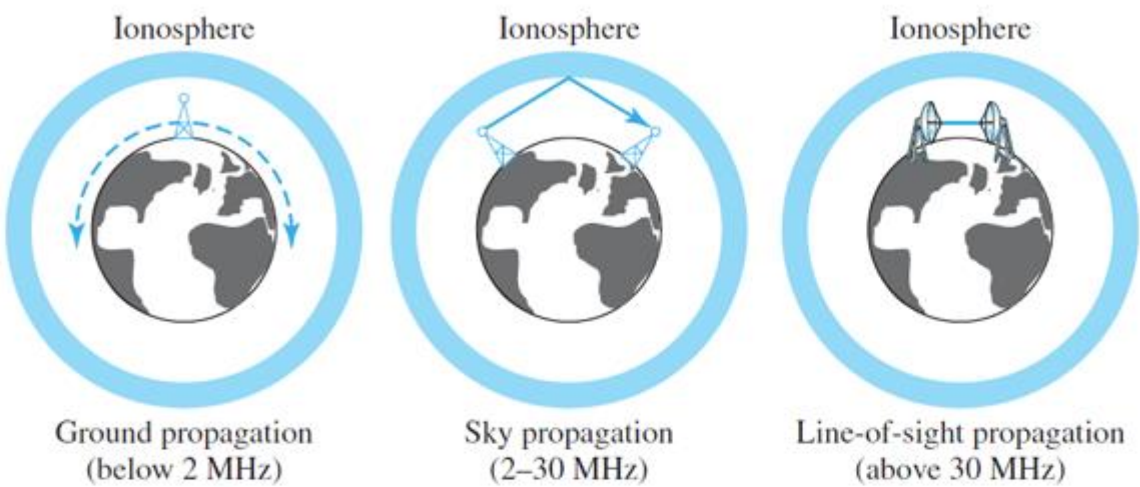
Unguided medium transport electromagnetic waves without using a physical conductor, signals are normally broadcast through free space and thus are available to anyone.

Figure down below shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication (Unguided medium).



Electromagnetic spectrum for wireless communication

Unguided signals can travel from the source to the destination in several ways: **ground propagation, sky propagation, and line-of-sight propagation**, as shown in Figure down below.



In **ground propagation**, radio waves travel through the lowest portion of the atmosphere, hugging the earth.

In **sky propagation**, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere) where they are reflected back to earth.

In **line-of-sight propagation**, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional.

The radio waves and microwaves are divided into eight ranges, called **bands**. These bands are rated from very low frequency (VLF) to extremely high frequency (EHF) as shown in the following table.

Band	*Range*	*Propagation*	*Application*
very low frequency (VLF)	3–30 kHz	Ground	Long-range radio navigation
low frequency (LF)	30–300 kHz	Ground	Radio beacons and navigational locators
middle frequency (MF)	300 kHz–3 MHz	Sky	AM radio
high frequency (HF)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft
very high frequency (VHF)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
ultrahigh frequency (UHF)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
superhigh frequency (SF)	3–30 GHz	Line-of-sight	Satellite
extremely high frequency (EHF)	30–300 GHz	Line-of-sight	Radar, satellite

(للاطلاع فقط)

We can divide wireless transmission into three broad groups: **radio waves**, **microwaves**, and **infrared waves**.

Radio Waves

Radio waves are omnidirectional, when an antenna transmits radio waves; they are propagated in all directions. **This means** that the sending and receiving antennas **do not have to be aligned**.

Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. **This makes** radio waves a good candidate for long distance broadcasting such as AM radio.

1. **Omnidirectional Antenna**
   Radio waves use omnidirectional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas. Figure down below shows an omnidirectional antenna.

2. **Radio waves applications**
   The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. **AM radio, FM radio and television** are examples of multicasting.

Microwaves

Microwaves have frequencies between 1 and 300 GHz. Microwaves are unidirectional. A pair of antennas can be aligned without interfering with another pair of aligned antennas. Following describes some characteristics of microwave propagation:

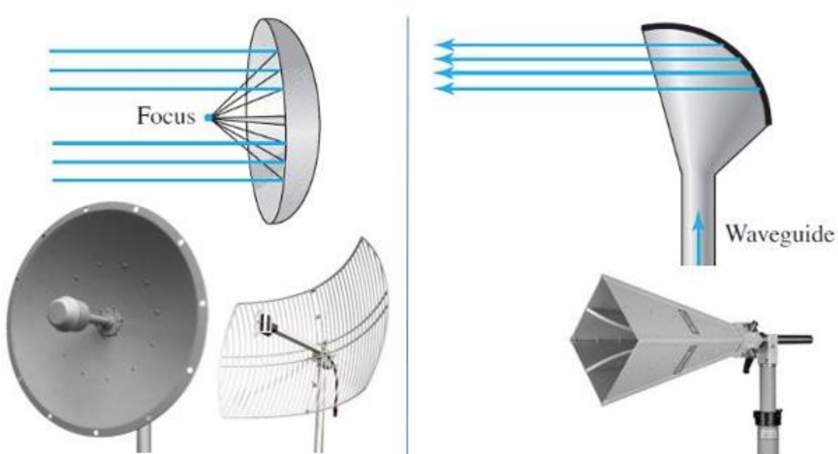
• **Microwave propagation is line-of-sight**. Since the towers with the mounted antennas need to be in direct sight of each other.

• **Very high-frequency microwaves cannot penetrate walls**.

• **The microwave band is relatively wide**, almost 299 GHz.

Unidirectional Antenna

Microwaves need unidirectional antennas that send out signals in one direction. **Two types of antennas** are used for microwave communications: **the dish antenna** and the **horn antenna** (see Figure down below).



a. Dish antenna **b.** Horn antenna

Microwave Applications

Microwaves, due to their unidirectional properties, are very useful when unicast (one-to-one) communication is needed between the sender and the receiver. They are used in **cellular phones, satellite networks, and wireless LANs**

Infrared waves

Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short-range communication.

Infrared waves, having high frequencies, cannot penetrate walls. This **advantageous characteristic** prevents interference between one system and another. When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors.

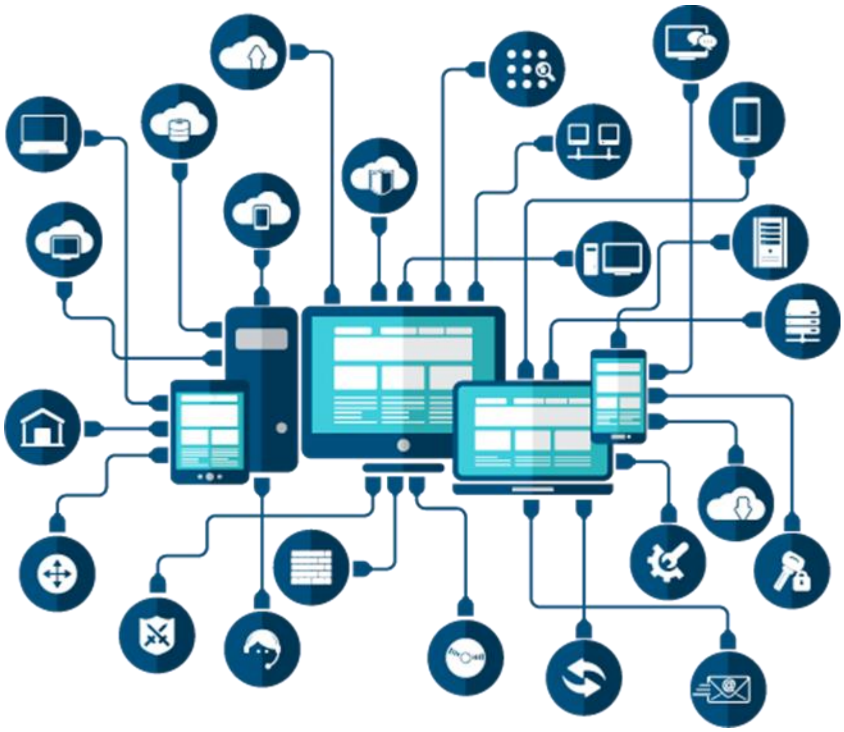
We cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Infrared Applications

The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.

The **Infrared Data Association** (IrDA), an association which has established standards for using these signals for communication between devices such as **keyboards, mice, PCs, and printers**.

Infrared signals defined by IrDA transmit through **line of sight**; the IrDA port on the keyboard needs to point to the PC for transmission to occur.

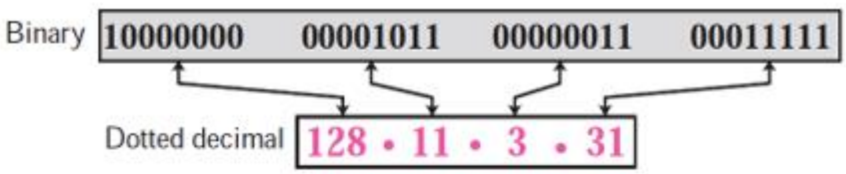


COMPUTER NETWORKS 1

المرحلة الثالثة

CHAPTER FIVE

IP addressing



IPv4 address

The identifier used in the IP layer of the TCP/IP protocol suite to identify each device connected to the Internet is called **the Internet address** or **IP address**. **An IPv4 address** is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.

Two devices on the Internet can **never have the same address** at the same time. However, if a device has two connections to the Internet, via two networks, **it has two IPv4 addresses**.

Address Space

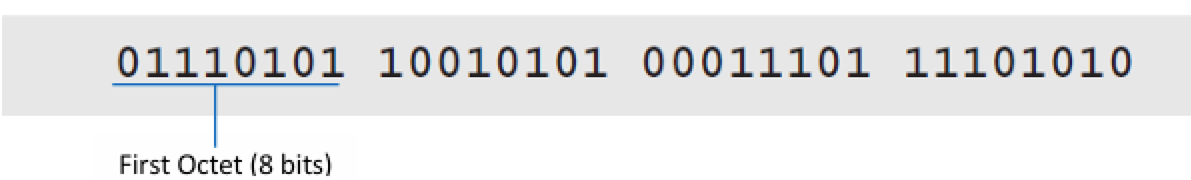
An address space is the total number of addresses used by the protocol. If a protocol uses b bits to define an address, the address space is 2b because each bit can have two different values (0 or 1). IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than four billion). Theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet.

Notation

There are three common notations to show an IPv4 address: binary notation (base 2), dotted-decimal notation (base 256), and hexadecimal notation (base 16).

Binary Notation: Base 2

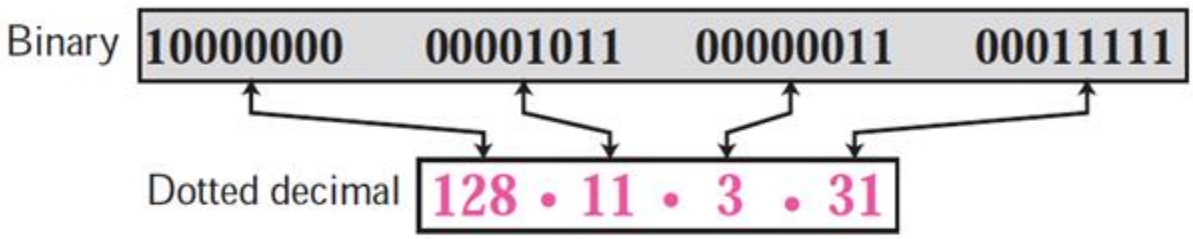
In binary notation, an IPv4 address is displayed as 32 bits (in four octets). Each octet (8 bits) is often referred to as a byte. The following is an example of an IPv4 address in binary notation:



Dotted-Decimal Notation: Base 256

To make the IPv4 address more compact and easier to read, an IPv4 address is usually written in decimal form with a decimal point (dot) separating the bytes.

Note that because each byte (octet) is only 8 bits, each number in the dotted decimal notation is between 0 and 255 (see Figure down below).



Example 1

Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number and add dots for separation:

a. 129.11.11.239

b. 193.131.27.255

Example 2

Change the following IPv4 addresses from dotted-decimal notation to binary notation.

a. 111.56.45.78

b. 221.34.7.82

Solution

We replace each decimal number with its binary equivalent:

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

Example 3

Find the error, if any, in the following IPv4 addresses:

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

Solution

a. There should be no leading zeroes in dotted-decimal notation (045).

b. We may not have more than 4 bytes in an IPv4 address.

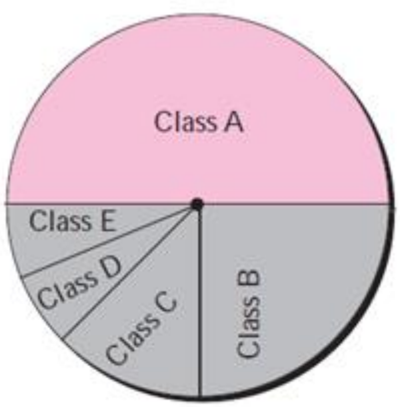
c. Each byte should be less than or equal to 255; 301 is outside this range.

d. A mixture of binary notation and dotted-decimal notation is not allowed.

Classful addressing

In classful addressing, the IP address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the whole address space.

Figure down below shows the class occupation of the address space.



Class A: 2^{31} = 2,147,483,648 addresses, 50%

Class B: 2^{30} = 1,073,741,824 addresses, 25%

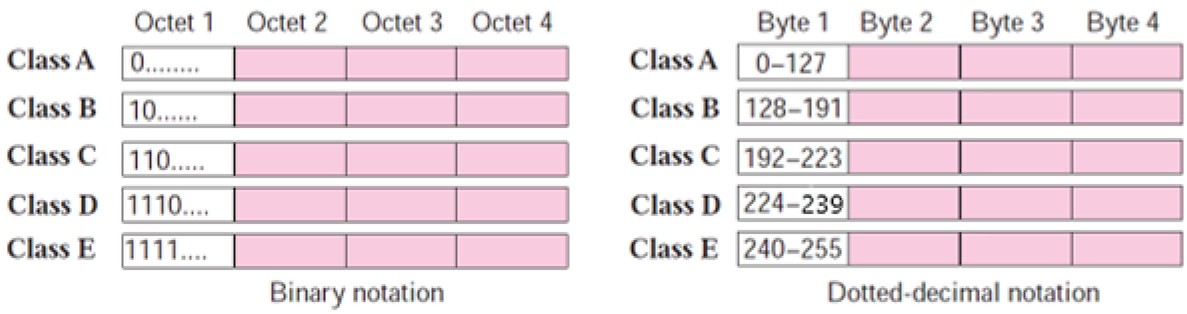
Class C: 2^{29} = 536,870,912 addresses, 12.5%

Class D: 2^{28} = 268,435,456 addresses, 6.25%

Class E: 2^{28} = 268,435,456 addresses, 6.25%

Recognizing Classes

We can find the class of an address when the address is given either in binary or dotted decimal notation. In the binary notation, the first few bits can immediately tell us the class of the address; in the dotted-decimal notation, the value of the first byte can give the class of an address (Figure down below).



Example 5

Find the class of each address:

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 10100111 11011011 10001011 01101111

d. 11110011 10011011 11111011 00001111

Solution

a. The first bit is 0. This is a class A address.

b. The first 2 bits are 1; the third bit is 0. This is a class C address.

c. The first bit is 1; the second bit is 0. This is a class B address.

d. The first 4 bits are 1s. This is a class E address.

Example 6

Find the class of each address:

a. 227.12.14.87

b. 193.14.56.22

c. 14.23.120.8

d. 252.5.15.111

Solution

a. The first byte is 227 (between 224 and 239); the class is D.

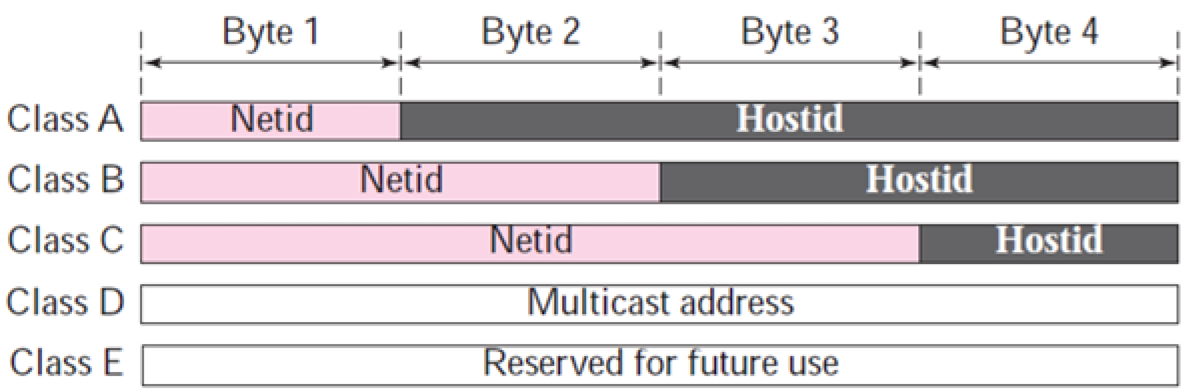
b. The first byte is 193 (between 192 and 223); the class is C.

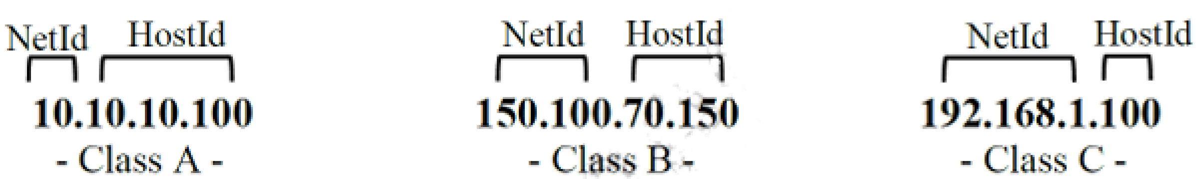
c. The first byte is 14 (between 0 and 127); the class is A.

d. The first byte is 252 (between 240 and 255); the class is E.

NetId and HostId

In classful addressing, an IP address in classes A, B, and C is divided into NetId and HostId. Figure down below shows the NetId and HostId bytes. Note that classes D and E are not divided into NetId and HostId.





Class D

There is just one block of class D addresses. It is designed for **multicasting**. Each address in this class is used to define **one group of hosts** on the Internet. When a group is assigned an address in this class, every host that is a member of this group will have a multicast address in addition to its normal (unicast) address.

Class E

There is just one block of class E addresses. It was designed for use as reserved addresses for **future purposes**.

Extracting Information in a Block

The **block size** shows the number of IP addresses contained in a specific range. Given any address in the block, we normally like to know three pieces of information about the block: the number of addresses, the first address, and the last address. After the class of the block is found, **we know the value of n** (the length of NetId in bits). We can now find these three pieces of information as shown in the following:

1. The number of addresses in the block, N, can be found using $\mathbf{N = 2^{32-n}}$.

2. To find the first address, we keep the n leftmost bits and set the **(32− n)** rightmost bits all to 0s.

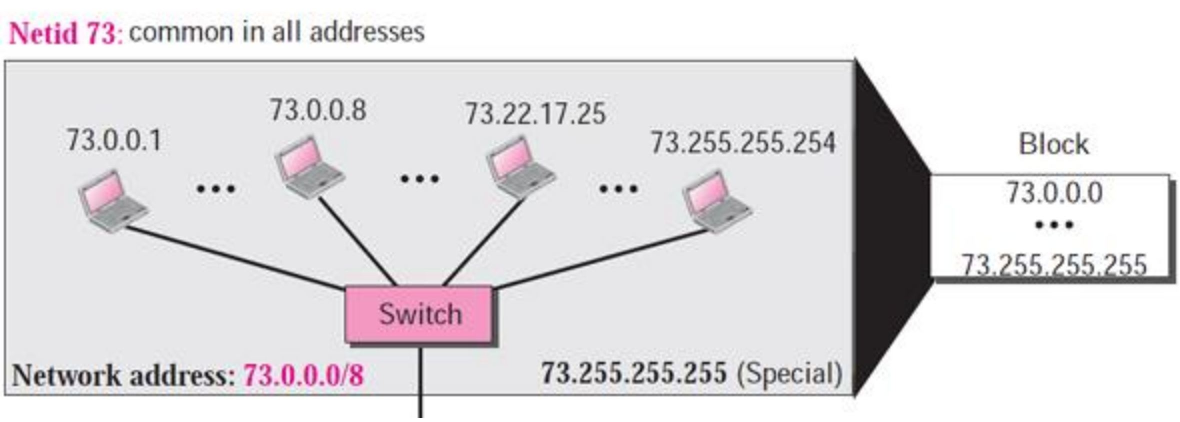
3. To find the last address, we keep the n leftmost bits and set the **(32− n)** rightmost bits all to 1s.

Example 7

An address in a block is given as 73.22.17.25. Find the number of addresses in the block, the first address, and the last address.

Solution

Since 73 is between 0 and 127, the class of the address is A. The value of n for class A is 8. Figure down below shows a possible configuration of the network that uses this block. Note that we show the value of n in the network address after a slash.



1. The number of addresses in this block is $\mathbf{N = 2^{32-n} = 2^{24} = 16,777,216.}$

2. The first address is **73.0.0.0/8** in which 8 is the value of n. The first address is called the network ID and is not assigned to any host. It is used to define the network.

3. The last address is **73.255.255.255**. The last address (or called the broadcast ID) is normally used for a special purpose.

Example 8

An address in a block is given as 180.8.17.9. Find the number of addresses in the block, the first address, and the last address.

Solution

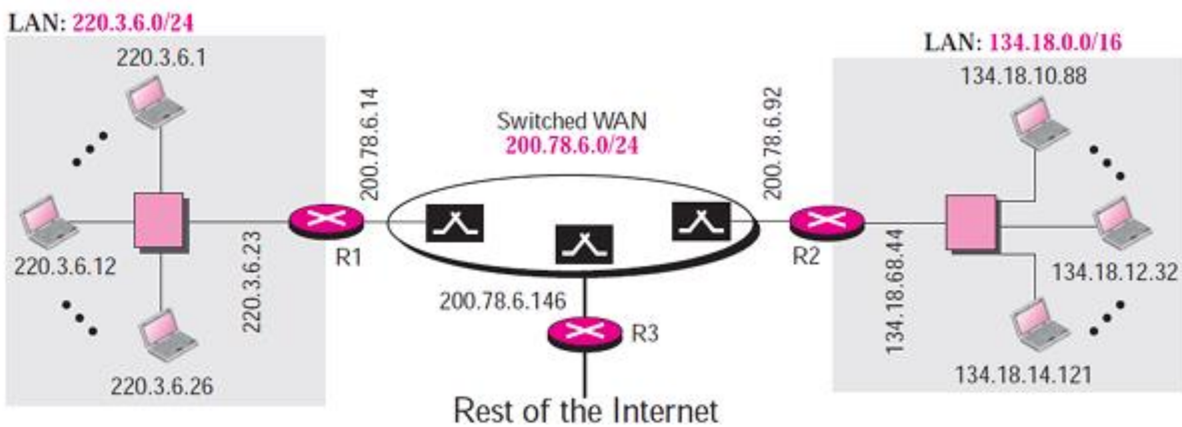
1.The number of addresses in this block is $N = 2^{32-n} = 2^{16} = 65{,}536$.

2. The first address (network address) is 180.8.0.0/16, in which 16 is the value of n.

3. The last address is 180.8.255.255.

Example 9

Figure down below shows a hypothetical part of an internet with three networks.



We have

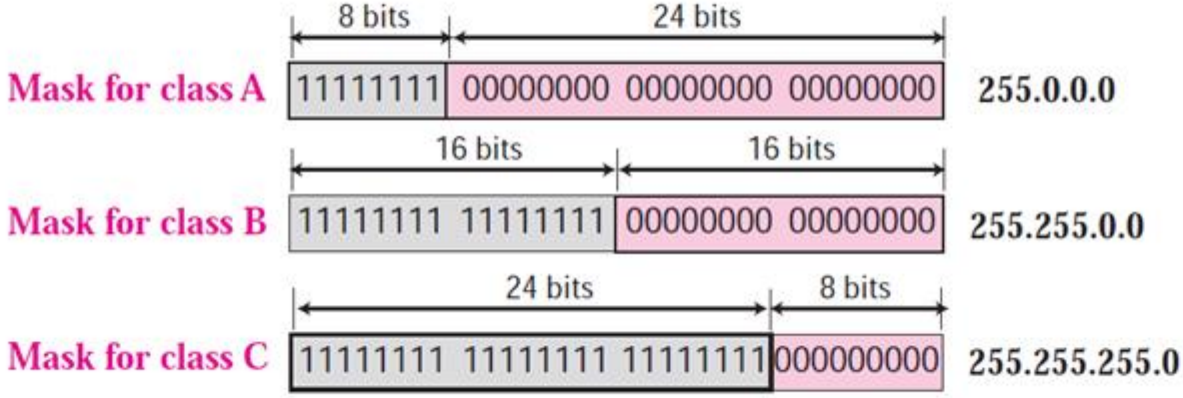
1. A LAN with the network address 220.3.6.0 (class C).

2. A LAN with the network address 134.18.0.0 (class B).

3. A switched WAN (class C), that can be connected to many routers. We have shown three. One router connects the WAN to the left LAN, one connects the WAN to the right LAN, and one connects the WAN to the rest of the internet.

Network Mask

A network mask or a default mask in classful addressing is a 32-bit number with n leftmost bits all set to 1s and (32 − n) rightmost bits all set to 0s. Since n is different for each class in classful addressing, we have three default masks in classful addressing as shown in Figure down below.



The routers in the Internet normally use an algorithm to extract the network address from the destination address of a packet. A router uses the AND operation. When the destination address is ANDed with the default mask, the result is the network address.

Example 10

A router receives a packet with the destination address 135.24.67.32. Show how the router finds the network address of the packet.

Solution

Since the class of the address is B, we assume that the router applies the default mask for class B, 255.255.0.0 to find the network address.

Destination address	→	201	.	24	.	67	.	32
Default mask	→	255	.	255	.	0	.	0
Network address	→	**135**	.	24	.	0	.	0

The destination address is ANDed with the default mask as described in the previous section. The network address (or ID) is 135.24.0.0.

Special Addresses

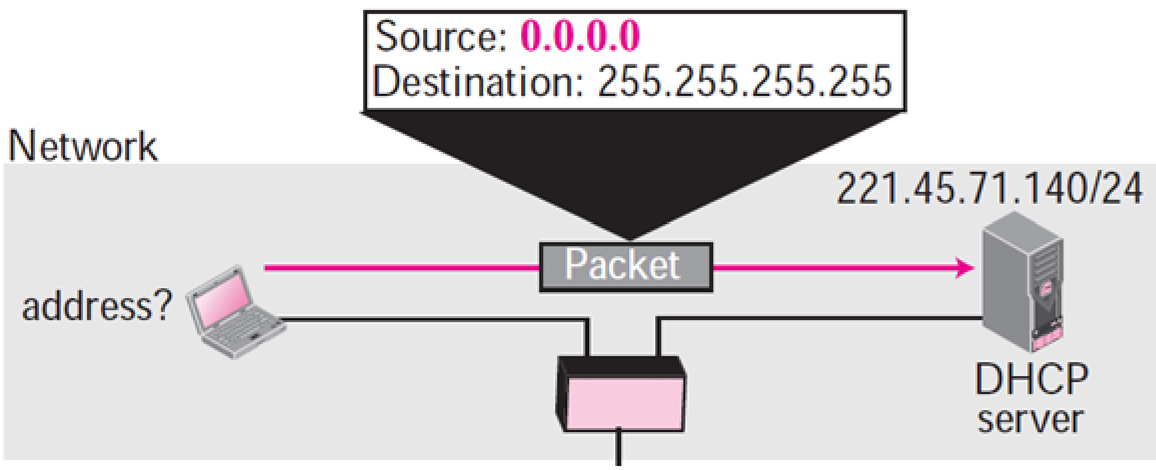
Some blocks of addresses are reserved for special purposes and cannot be used as normal IP addresses as shown in the following:

1- **All-Zeros Address** The block **0.0.0.0/32**, which **contains only one single address**, is reserved for communication when a host needs to send an IPv4 packet but it does not know its own address. The host sends an IPv4 packet to a bootstrap server (called DHCP server) using this address as the source address and a **limited broadcast address (255.255.255.255)** as the destination address to find its own address (see figure down below).

2- **All-Ones Address** The block 255.255.255.255/32, which contains one single address, is reserved for **limited broadcast address** in the current network.

3- **Loopback Addresses** The block 127.0.0.0/8 is used to test the software on a machine. When this address is used, **a packet never leaves the machine**; it simply returns to the protocol software.

4- **Network ID and broadcast ID** As we have already discussed, the network ID is the first address (with the suffix set all to 0s) in a block **defines the network address**. Broadcast ID is the last address in a block or subnet (with the suffix set all to 1s) can be used as a direct broadcast address. This address is usually used by a router to send a packet to all hosts in a specific network.



Internet Protocol version 6 (IPv6)

IPv6 was developed to deal with the problem of IPv4 address. IPv6 is intended **to replace** IPv4. With the rapid growth of the Internet after the 1990s, far more addresses would be needed to connect devices than the IPv4 address space had available.

By 1998, the IPv6 had been formalized with **128-bit**, theoretically allowing 2^{128}, or approximately 3.4×1038 addresses, whereas IPv4 uses only **32-bit** addresses and provides approximately 2^{32}, or 4.3 billion addresses.

IPv6 addresses are represented **as eight groups of four hexadecimal digits** with the groups being separated by colons, for example

3501:0cb8:0000:0052:0000:7a5e:0b70:9335