Chapter 1
Introduction to Computer Network

- ***Outline:***

  1.1 Uses of Computer Network
  1.2 Networking model client/server, p2p, active network
  1.3 Protocols and Standards
  1.4 OSI model and TCP/IP model
  1.5 Comparison of OSI and TCP/IP model
  1.6 Example network: The Internet, X.25, Frame Relay, Ethernet, VoIP, NGN and MPLS, xDSL

What is a Network?

- A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
- Network is the collection of computer, software and hardware that are all connected to each other to help their work together.
- A network connects computers by means of cabling system (or wireless media), specialized software and devices that manage data traffic.
- A network enables users to share files and resources such as printer as well as send message electrically to each other.

Application of Network

- **Marketing and Sales:** use to collect, exchange, and analyze data relating to customer needs and product development cycles. *Teleshopping, online services etc.*
- **Financial Services:** *Foreign exchange, electronics fund transfer etc.*
- **Manufacturing:** *multiple users allow to work on a project simultaneously.*
- **Electronics Messaging:** email
- **Cable television**
- **Teleconferencing**
- **Sharing information** – collaborative documents, intranet, group calendaring, etc.
- **Facilitating communications** – email, chat, videoconferencing
- **Remote Services**: E-Commerce, e-governance, ATM
- **Resource sharing**: Printer, Software

Network Criteria

- The most important criteria are ***performance, reliability, and security***.
  - **Performance:** 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.
  - **Reliability:** In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.
  - **Security:** Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses. A good network is protected from viruses by hardware and software designed specifically for that purpose.

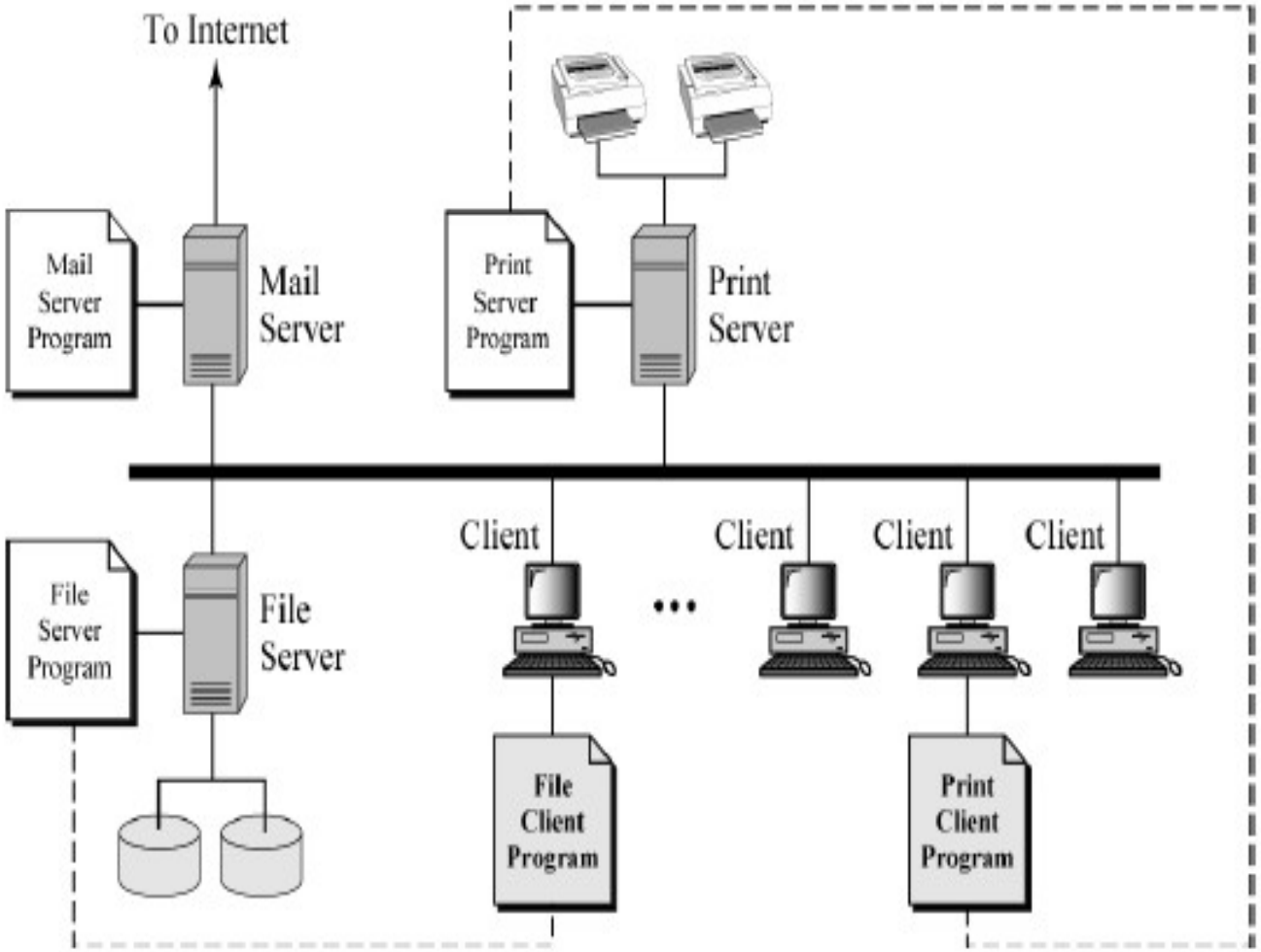
Networking Model: Client/Server network

- A network built around one or more dedicated servers and is administered from a central location.
- Clients connect to the dedicated servers through the network to access the resources, such as printers, servers, and so on.
- It supports many thousands of clients and multiple computer platforms. The clients have their own local storage and processing power.
- Communication takes the form of the client process sending a message over the network to the server process. The client process then waits for a reply message. When the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply.
- The server is a larger, faster more expensive computer that is designed to handle a number of tasks at once.
- **Thin client**: it is a network computer with no local storage. It processes information independently, but relies on servers for applications, data storage, and administration. Largely used for interaction with processing layer.
- **Thick client**: a typically powerful personal computer capable of handling independent application processes like notebook computer or PC.

Client Server

Common network services

- File services
- Print services
- Message services(e.g. email)
- Application services
- Database services



Networking Model: Client/Server network

Advantages

- Scalable and cost less than centralized networks
- Support many users
- More powerful than peer-to-peer networks
- Centralize security and administration while controlling access to resources
- Communicate with other networks and support remote access, Internet sites, and multiple computing platforms

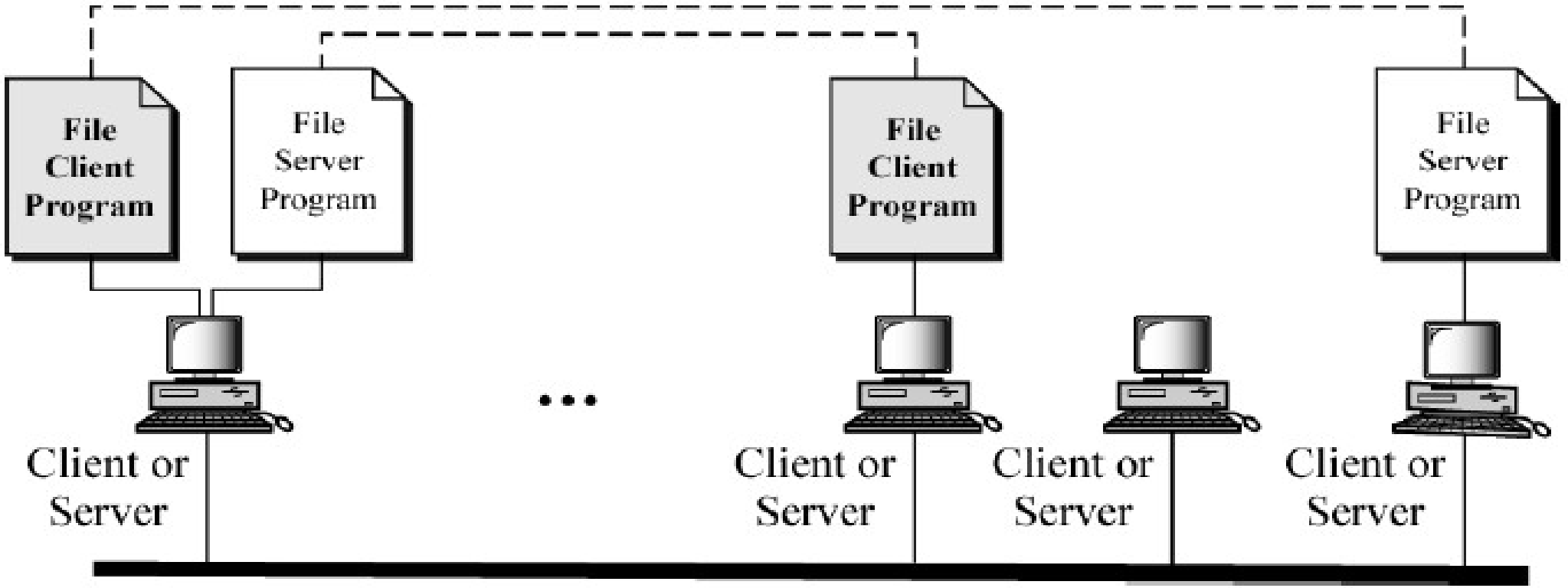
Disadvantages

- They are more expensive to implement and Running cost high
- More complicated to administer than peer-to-peer networks
- Server failures can bring down the entire network

Networking Model: Peer-to-Peer network

- In peer to peer networking architecture each computer (workstation) has equivalent capabilities and responsibilities.
- There is no server, and computers simply connect with each other in a workgroup to share files, printers, and internet access.
- It is practical for workgroups of dozen or less computers where each PC acts as an independent workstation that stores data on its own hard drive but which can share it with all other PCs on the network.
- All computers and users have equal authority and rights.
- Used at home or in small organisations with trusted users.
- Nodes are autonomous (no administrative authority)
- Network is dynamic (nodes enter and leave the network frequently)
- Nodes collaborate directly with each other with having widely varying capabilities.

Peer-to-peer


File
Client
Program
File
Server
Program
File
Client
Program
File
Server
Program
Client or
Server
Client or
Server
Client or
Server
Client or
Server

Networking Model: Peer-to-Peer network

Advantages

- Ease of installation
- Easy to implement & operate.
- No dedicated server or NOS
- individual control of user resources
- Inexpensive – no specific device & configuration.
- No administrative stuff.

Disadvantages

- Multiple passwords.
- Lack of central repository (Central store house).
- Security distributed through out network terminals.
- Uncoordinated & inconsistent backup.
- Not for large number of computer.
- limitations in geographic area
- difficulty in ensuring security

Network Transmission Technology

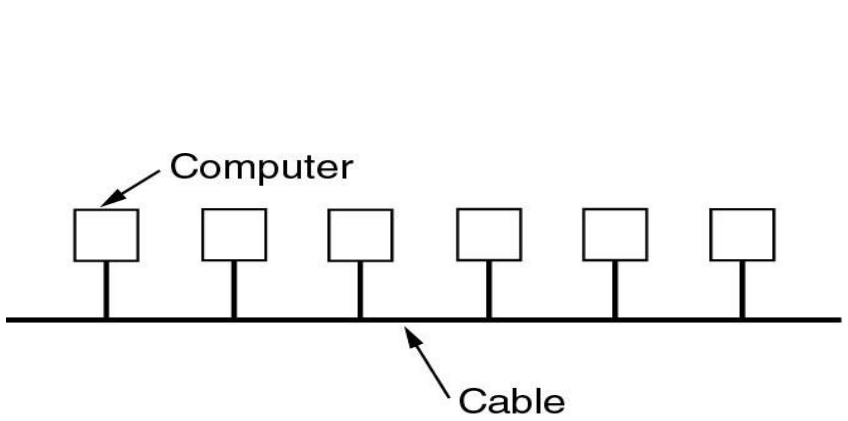
- There are two types of transmission technology that are in widespread use: **broadcast** links and **point-to-point** links.
- **Point-to-point links** connect individual pairs of machines. To go from the source to the destination on a network made up of point-to-point links, short messages, called **packets** in certain contexts, may have to first visit one or more intermediate machines. Often multiple routes, of different lengths, are possible, so finding good ones is important in point-to-point networks. Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called **unicasting**.
- In contrast, on a **broadcast network**, the communication channel is shared by all the machines on the network; packets sent by any machine are received by all the others. An address field within each packet specifies the intended recipient. Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.
- A wireless network is a common example of a broadcast link.

Type of Network

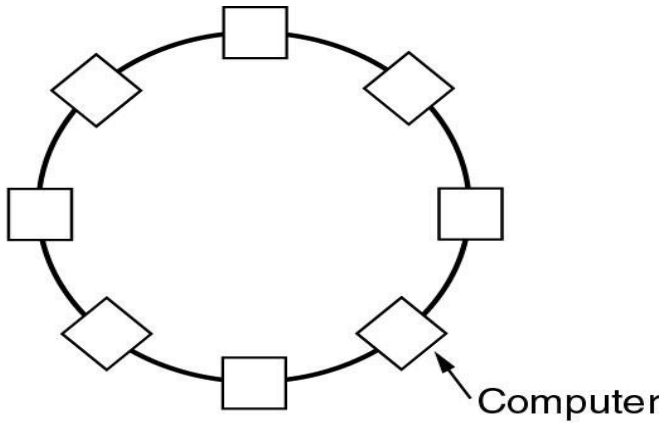
- It is classified by Scale:
  - Local Area network (LAN)
  - Metropolitan Area Network (MAN)
  - Wide Area Network (WAN)

Type of Network: LAN

- A LAN is a privately-owned networks within a single building or campus.
- LAN is limited in size, typically spanning a few hundred meters , and no more than a mile.
- The most common communication links used in LANs are twisted pair, coaxial cable, and fiber optics.
- A LAN utilizes high-speed data transfer capabilities. Transmission rates in LANs usually range from 10 Mbps to 1 Gbps.
- Nodes in LAN are linked together with a certain topology. These topologies may be Bus, Ring, Star etc.
- LAN technologies are: Token bus, Token Ring, FDDI



(a)



(b)

Type of Network: MAN

- A MAN is a large computer network that usually spans a city or a large Campus.
- The main objectives of MANs is to interconnect LAN located in an entire city or Campus.
- The MAN typically covers an area of between 5 and 50 KM diameter.
- The MAN speed is nearly around LAN speed.

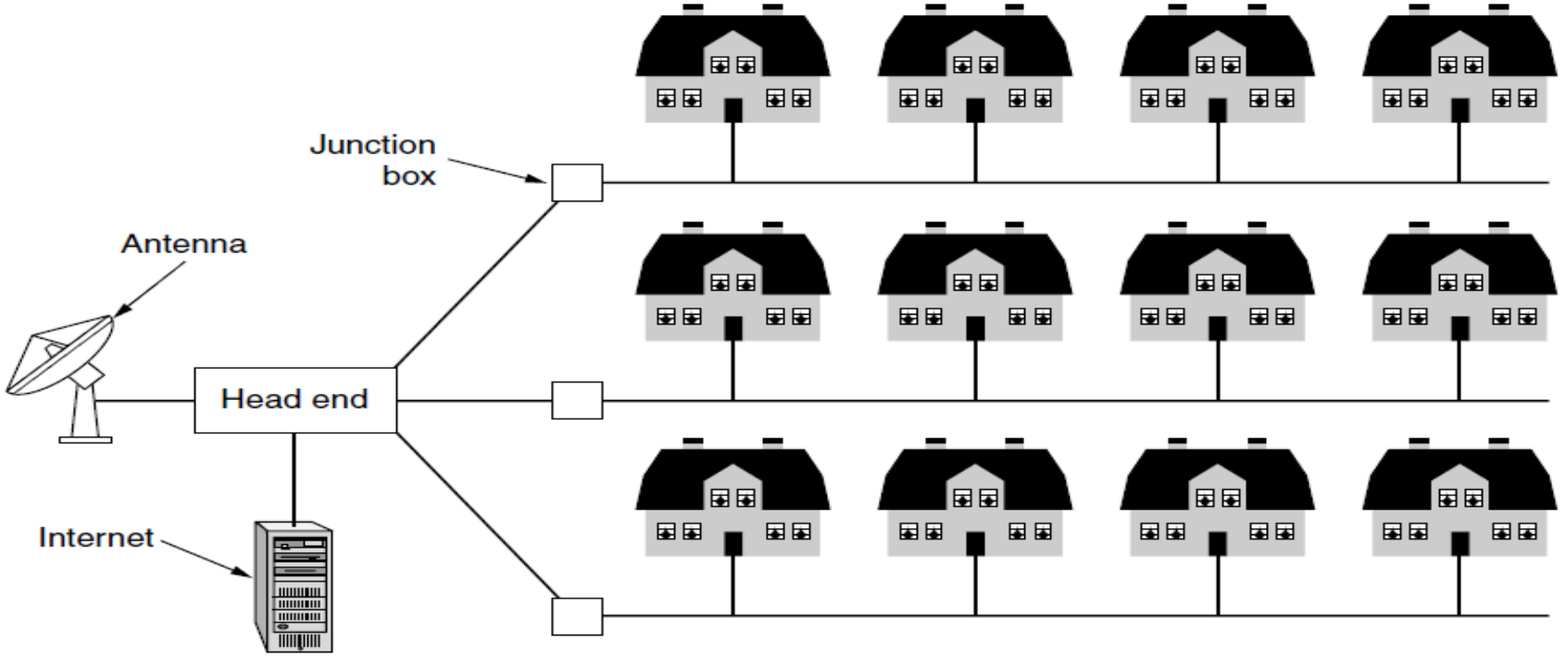
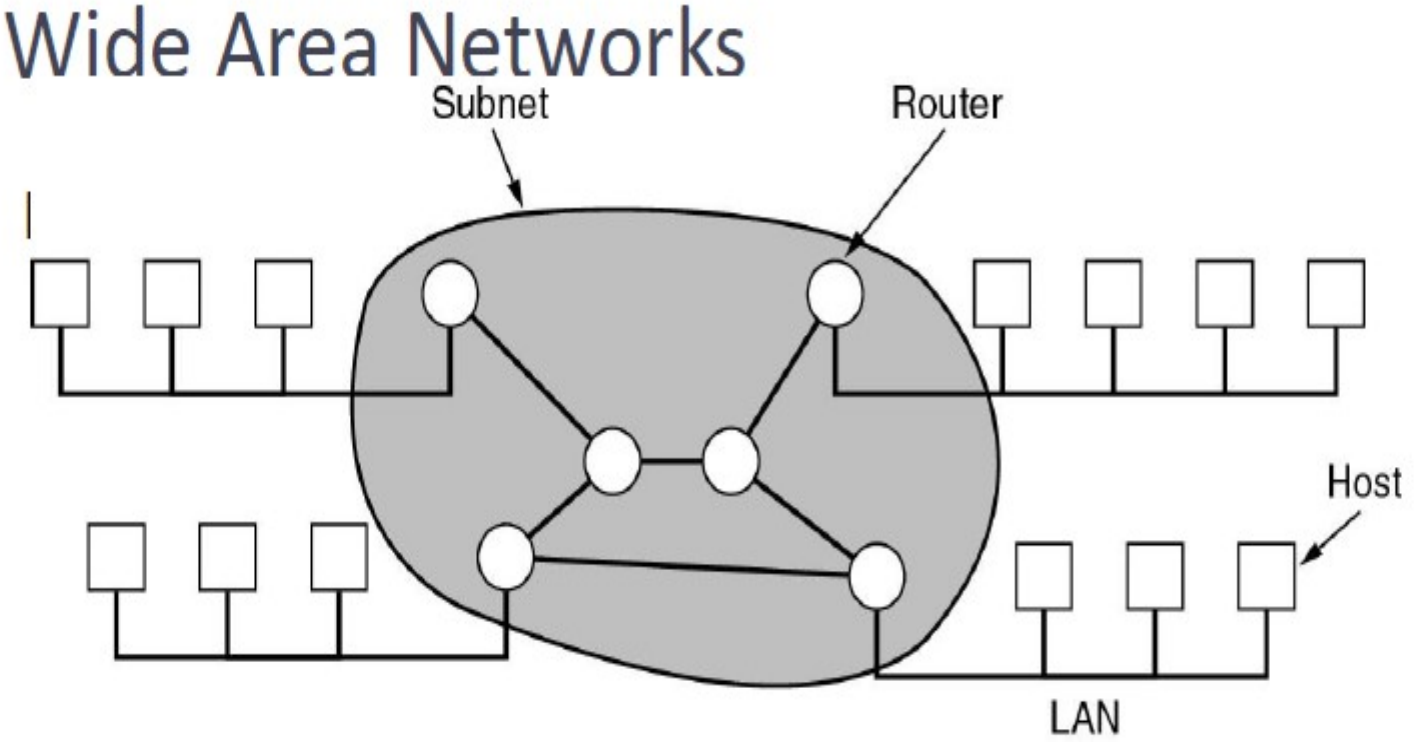


Figure 1-9. A metropolitan area network based on cable TV.

Type of Network: WAN

- WAN covers a large geography area such as country, continent or even whole of the world.
- The worlds most popular WAN is the internet.
- A WAN is formed by connecting Multiples LANs which may belongs to different organizations.
- WAN Technologies: Frame Relay, ISDN, Point to point protocol etc.



Network Topology

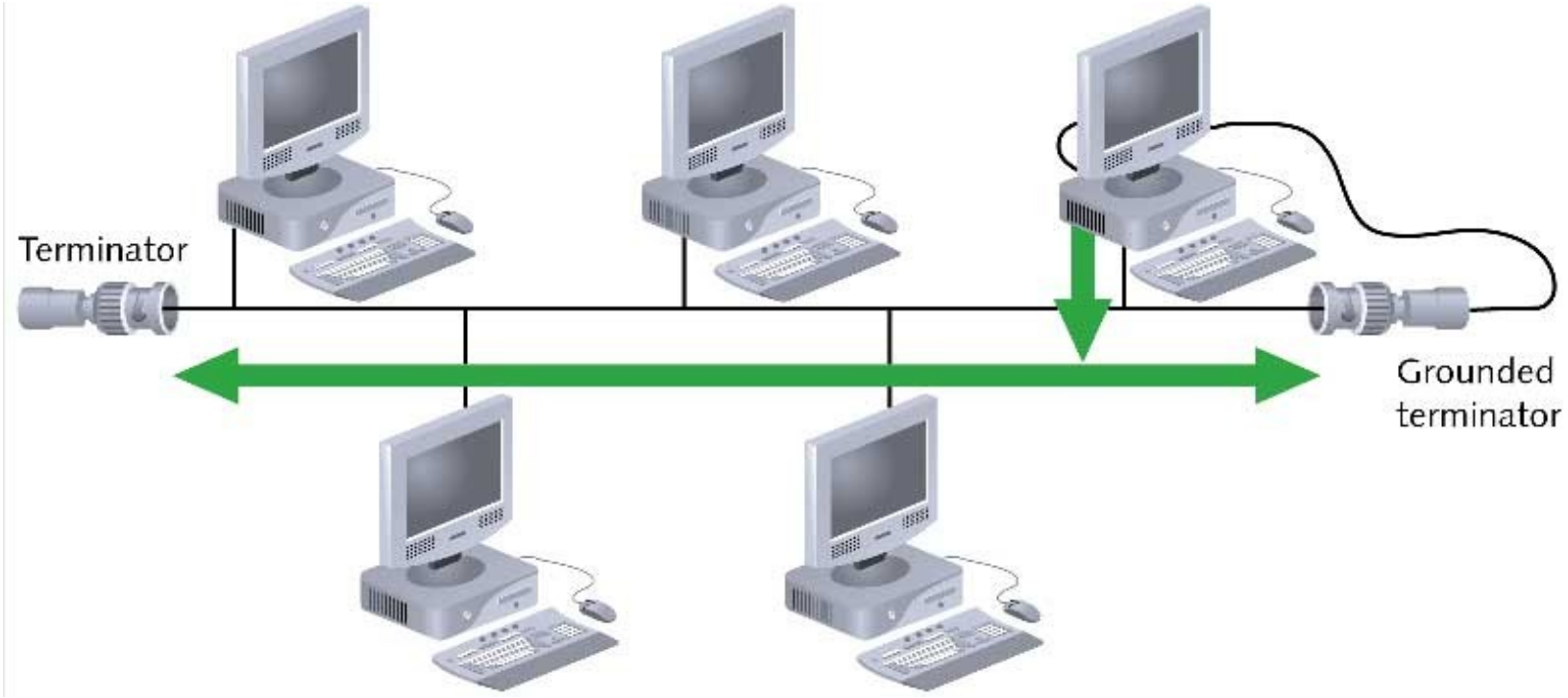
- Network topology is the arrangement of the various elements of a communications networks.
- Two types:
  - **Physical Topology**: It describes the geometric arrangement of components that make up the LAN. It refers to the way the computers are cabled together.
  - **Logical Topology:** It describes the possible connections between pairs of networked end –points that can communicate.
- Physical Topologies are Bus topology, Ring topology, Star topology, Mesh topology, Tree topology, Hybrid topology, and Daisy Chain topology.
- Logical topologies are Token Bus, Token Ring, CSMA/CD etc.

Bus Topology

- All nodes are connected to a single common cable known as the backbone.
- Both end of the backbone must be terminated with a terminating resister to prevent signal bounce and complete the circuit.
- If the backbone cable fails, the entire network effectively becomes unusable.
- Bus (backbone) carries all network data.
- Bus networks work best with a limited number of devices.
- Ethernet (IEEE 802.3) is the protocols used for this type of LAN.
- When one computer send a signal up the wire all the computers receive the information but only one with the address that matches accepts the information, the rest disregard the message.
- **Advantages**
  - Easy to implement.
  - Requires least amount of cable to connect the computers together.
  - Failures of one station does not affect the others.

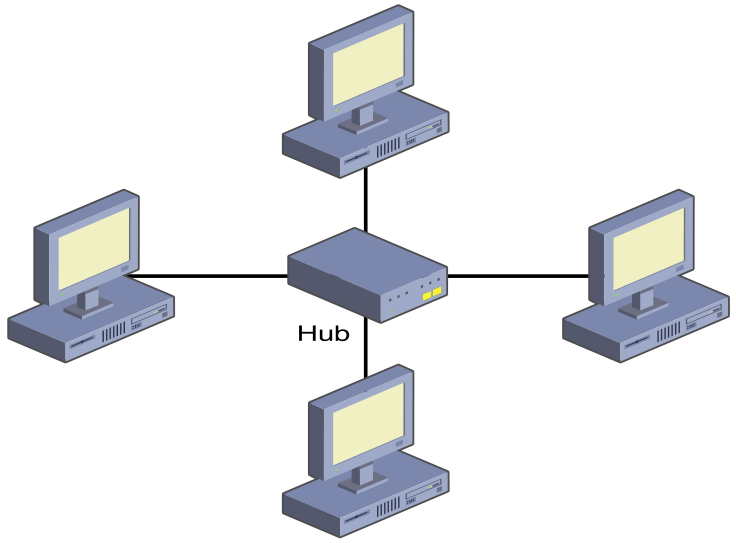
Bus Topology

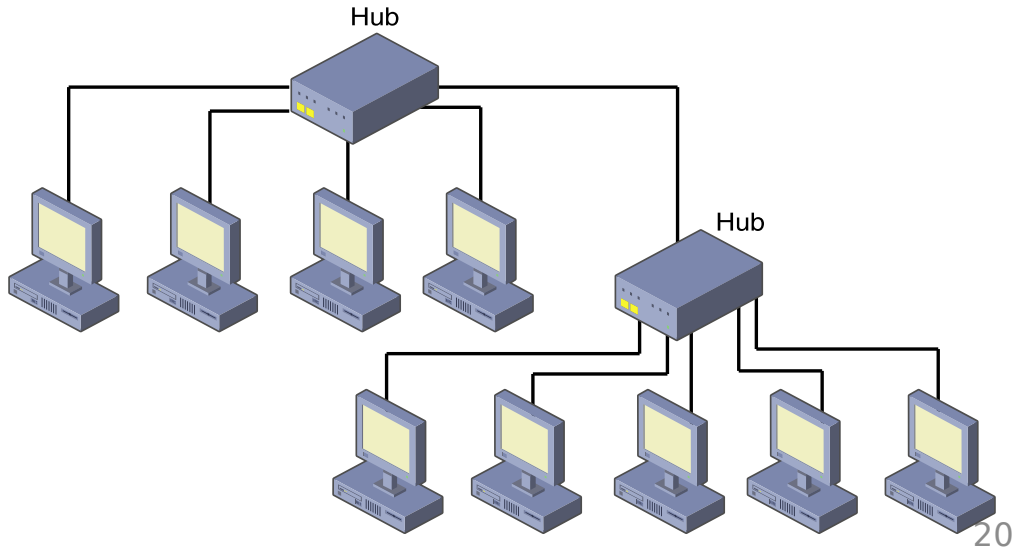
- **Disadvantages**
  - A central cable break can disable the entire network.
  - Difficult to troubleshoot.
  - A cable break or loose connector causes reflection and stops all the activity.
  - Collisions occurs when two nodes send message simultaneously.



Star Topology

- Most dominant topology type in contemporary LANs.
- Every node on the network is connected through a central device.
- Each computer on a star network communicates with a central device that resends the message either to each computer or only to the destination computer.
- A central device (hub) connects hubs and nodes to the network.
  - ✓ Each node connects to its own dedicated port on the hub.
  - ✓ Hubs broadcast transmitted signals to all connected devices.
  - ✓ we can connect multiple hubs to form a hierarchical star topology.





Star Topology

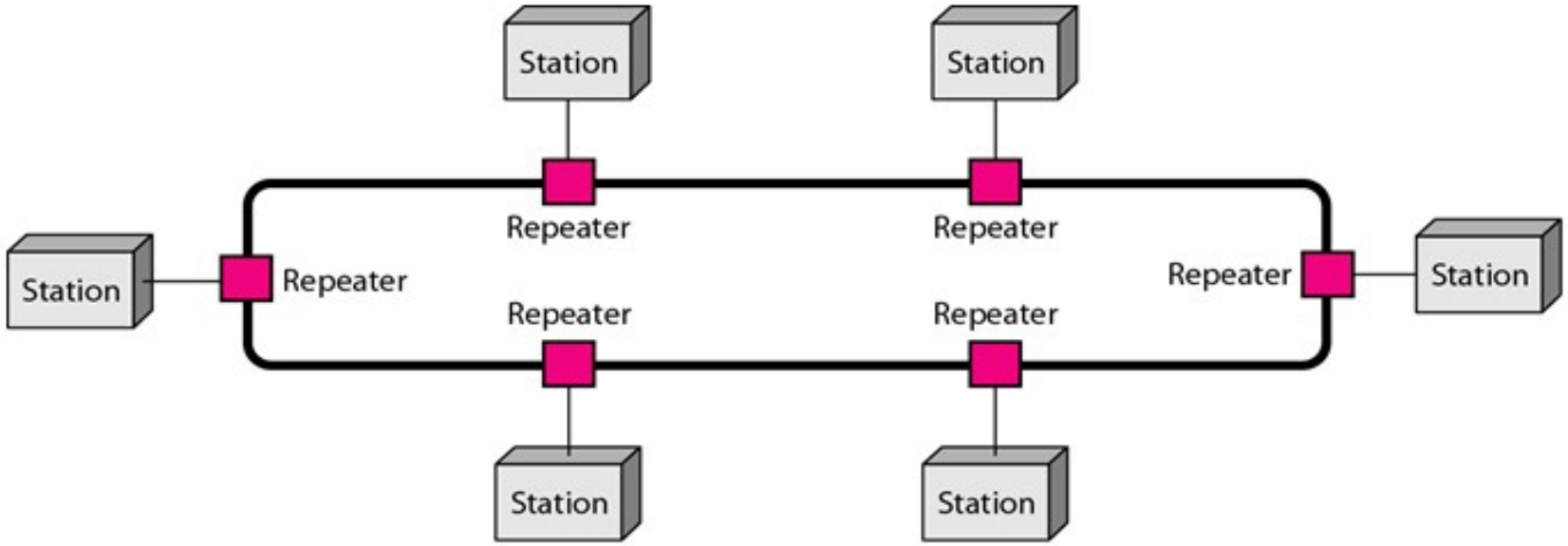
- **Advantages:**
  - Single computer failure does not necessarily bring down the whole star network
  - Easy to connect new nodes or devices.
  - Centralized management.
  - Most popular topology in use; wide variety of equipment available
  - The center of the star network is a good place to diagnose the faults.
  - Compared to Bus topology it gives far much better performance.
- **Disadvantages:**
  - If central device fails, the entire network goes down.
  - Requires more cable than the bus topology.
  - Performance is depends on central device.

Ring Topology

- Each node is connected to the two nearest nodes so the entire network forms a circle.
- Ring network consists of nodes that are joined by point- to- point connections to form a ring.
- Data are transmitted around the ring using token passing either clockwise or counterclockwise.
- No central hub
- Each node will repeat any signal that is on the network regardless its destination. The destination station recognizes its address and copies the frame into a local buffer as it goes by. The frame continues to circulate until it returns to the source station, where it is removed.
- A failure in any cable or device breaks the loop and can take down the entire network.
- Token Ring (IEEE 802.5) is the most popular Ring topology protocol.
- **Advantages:**
  - Each computer has equal access to resource.
  - Performance is better than that of Bus topology
  - Network is point- to- point connections. Hence, easier to locate defective node.

Ring Topology

- **Disadvantages:**
  - Failure of one computer on the ring can affect the whole network.
  - Each packet of data must pass through all the computers between source and destination, slower than star topology.
  - If diameter of a network is high, the number of edges involved in each communications will also be very high resulting in high signal attenuation and network blocking probability.



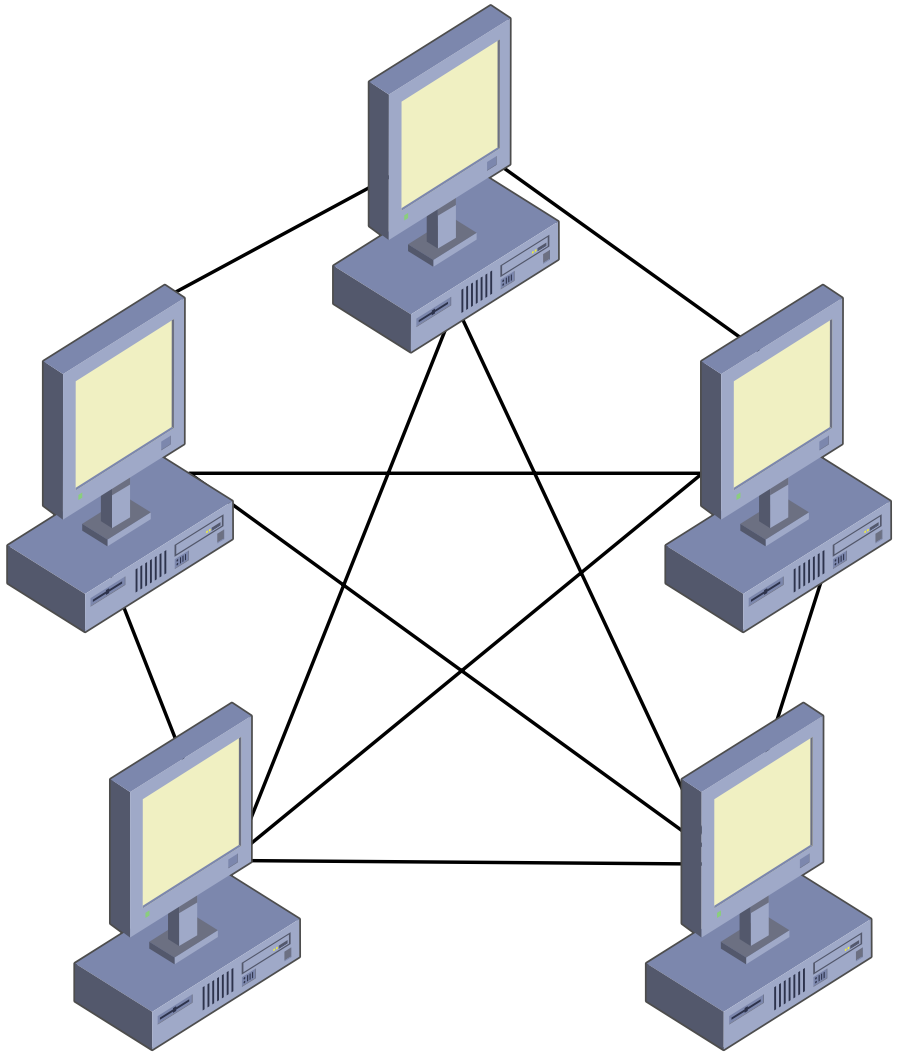
Mesh Topology

- The Internet is a mesh topology.
- **Two Types:**
  - Fully Connected
  - Partially Connected
- **Fully Connected Mesh Topology**
  - All nodes are interconnected.
  - Each and every node has a unique point to point link with all the other nodes. This features leads to the reliability and fault tolerance.
  - In mesh topology it will connect or share traffic between two nodes only.
  - Messages sent on a mesh network can take any of several possible paths from source to destination. Hence, static routing impractical. Use dynamic routing practical,
- In **Partial mesh topology**, nodes are connected to only some, not all, of the other nodes.

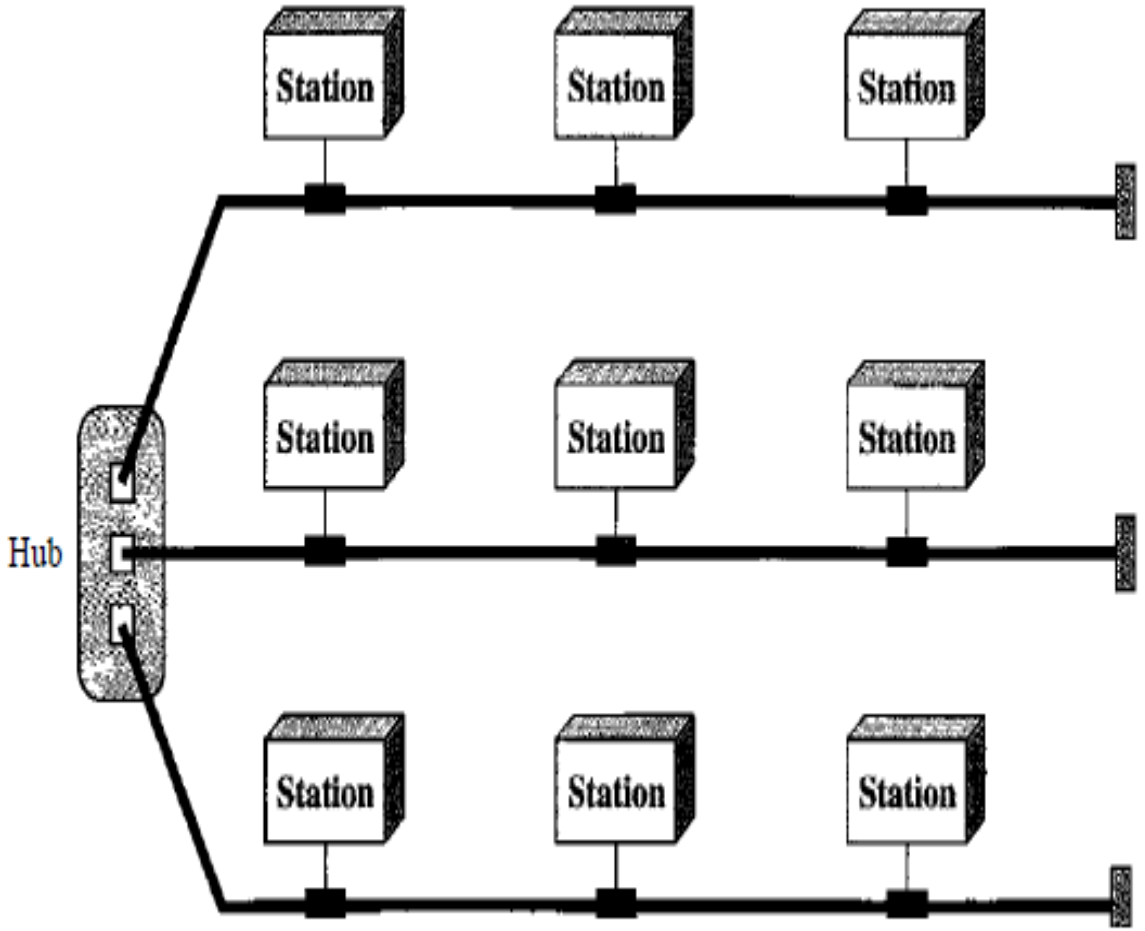
Mesh Topology

- **Advantages:**
  - When a link of other nodes fail to connect it will not affect the entire network.
  - There is a facility of a unique link between nodes to ensure higher finest data rate and remove traffic issues.
  - Error identification and error isolation can be found easy.
  - It is robust.
- **Disadvantages:**
  - It is most expensive network from the point of view of link cost i.e. cost of cable.
  - Bulk wiring is required.
  - Installation and configuration are difficult if the connectivity gets more.

Mesh Topology

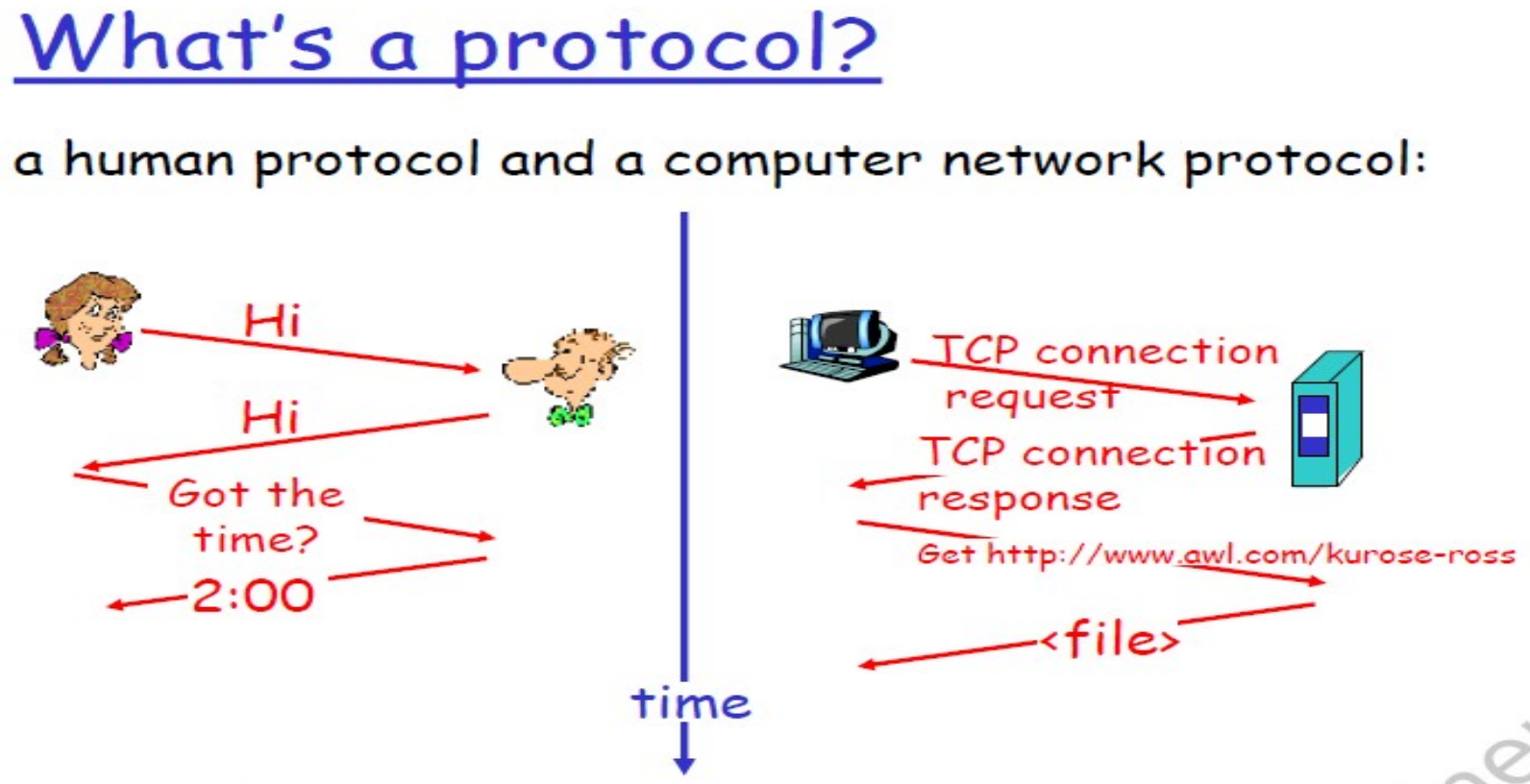


A *hybrid topology: a star backbone with three bus networks*



Protocol

- Basically, **a protocol** is an agreement between the communicating parties on how communication is to proceed.
- A **protocol** is a formal description of a set of rules and conventions that govern a particular aspect of how devices on a network communicate.



Network Software

- Network software is highly structured.
- The software structuring technique in detail is below:
- **Protocol Hierarchies**
  - To reduce their design complexity, most networks are organized as a stack of **layers** or **levels**, each one built upon the one below it.
  - The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
  - The purpose of each layer is to offer certain services to the higher layers while shielding those layers from the details of how the offered services are actually implemented.
  - In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.
  - Each layer talks to the ones above & below it

Network Software: Protocol Hierarchies

- The entities comprising the corresponding layers on different machines are called **peers**.
- The peers may be software processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol to talk to each other.
- **A five-layer network :**

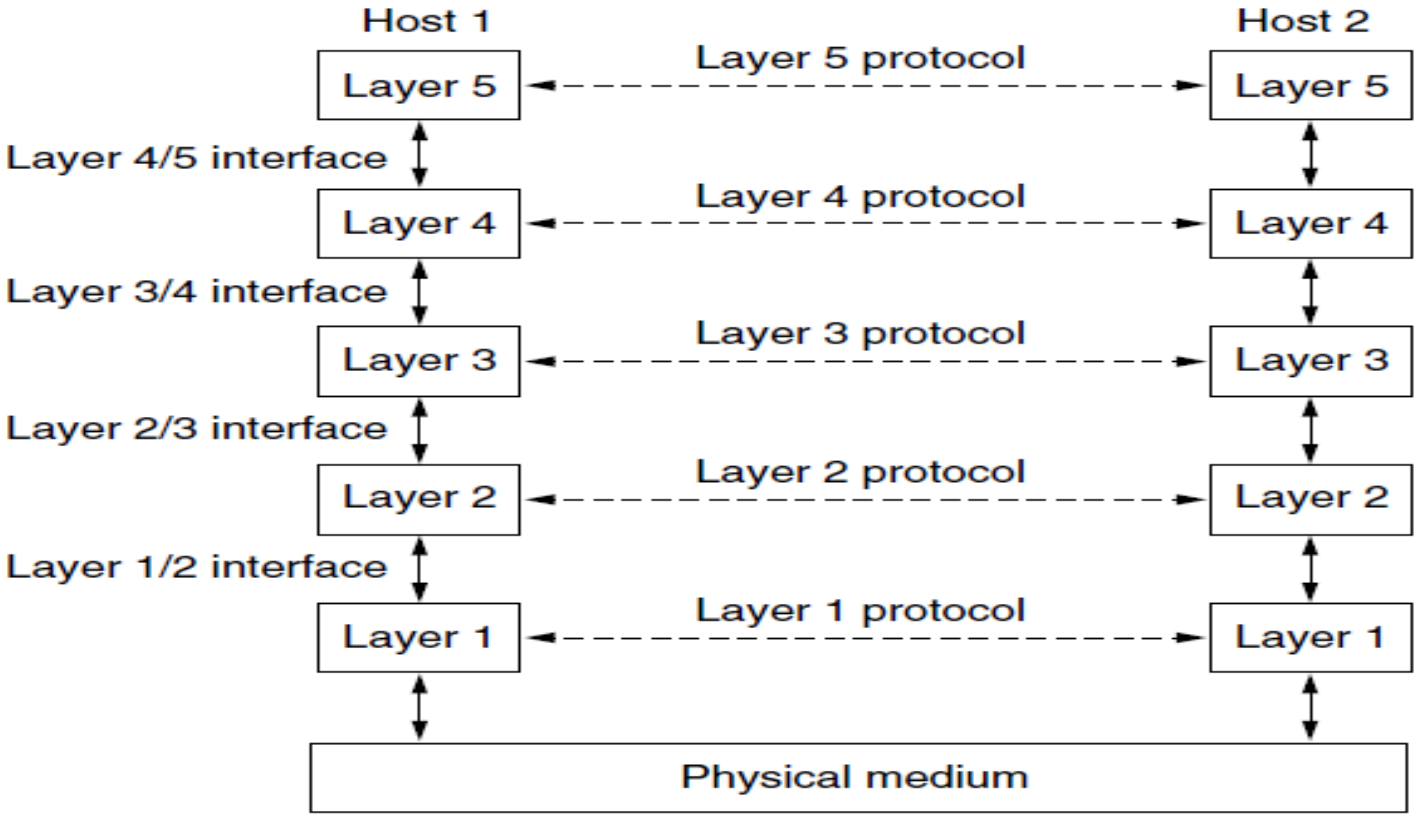
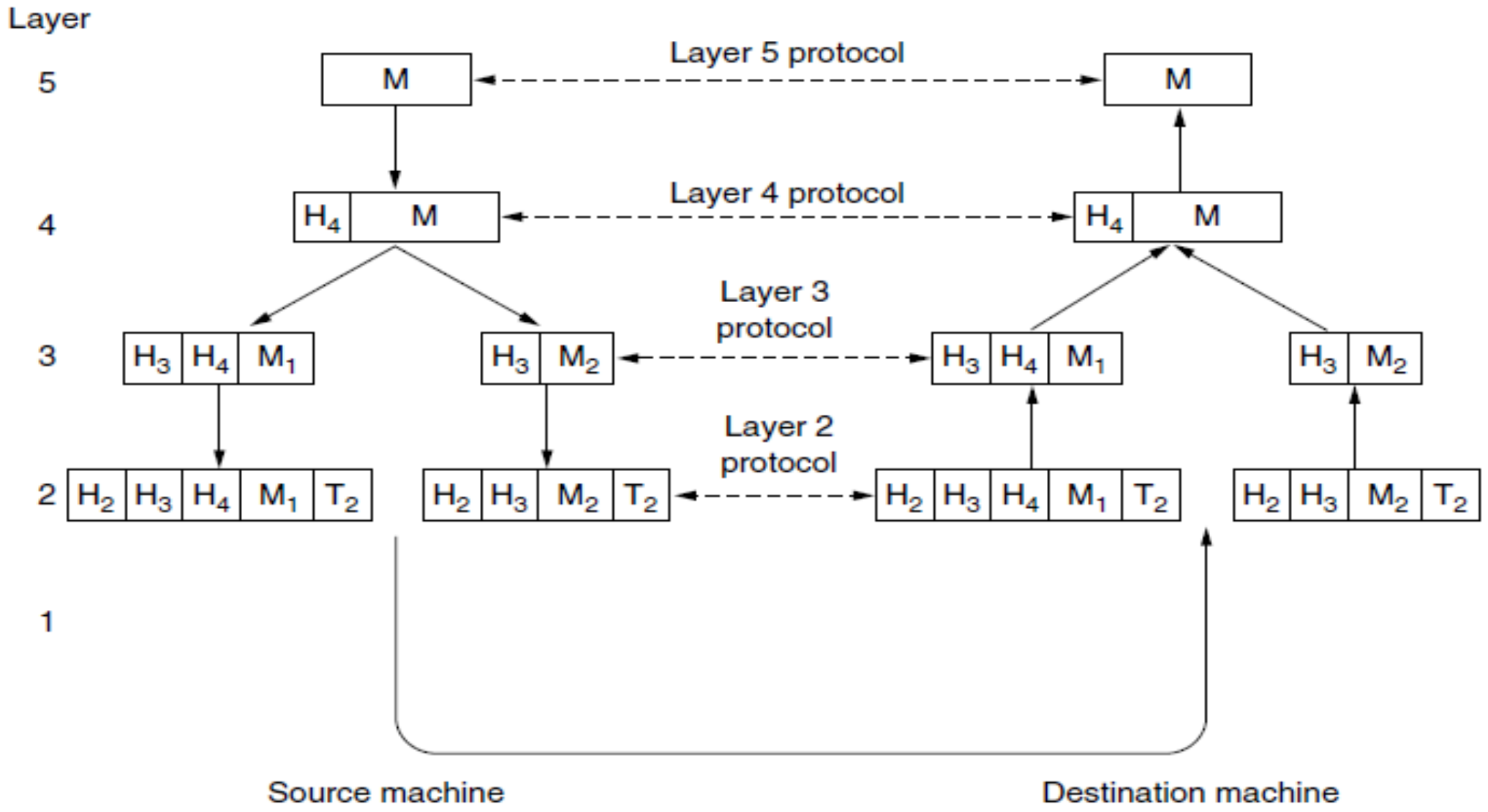


Figure 1 . Layers, protocols, and interfaces.

Network Software: Protocol Hierarchies

- No data is transferred directly from one machine to another on that layer – the layers can only talk to the ones above or below them on their host.
- A message from layer 5 will have to travel to layer 1, move across the physical medium, and then back up to layer 5 on the different machine.
- Layer 1 is the only layer able to move data from one machine to another, through the physical medium.
- Between each pair of adjacent layers is an **interface**. The interface defines which primitive operations and services the lower layer makes available to the upper one.
- A set of layers and protocols is called a **network architecture**. The specification of an architecture must contain enough information to allow an implementer to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol.
- A list of the protocols used by a certain system, one protocol per layer, is called a **protocol stack**.

Header and Trailer Addition



Header and Trailer Addition

- A message, *M*, is produced by an application process running in layer 5 and given to layer 4 for transmission.
- Layer 4 puts a **header** in front of the message to identify the message and passes the result to layer 3.
- The header includes control information, such as addresses, to allow layer 4 on the destination machine to deliver the message.
- Consequently, layer 3 must break up the incoming messages into smaller units, packets, prepending a layer 3 header to each packet. In this example, *M* is split into two parts, *M*1 and *M*2, that will be transmitted separately.
- Layer 3 decides which of the outgoing lines to use and passes the packets to layer 2.
- Layer 2 adds to each piece not only a header but also a **trailer**, and gives the resulting unit to layer 1 for physical transmission.
- At the receiving machine the message moves upward, from layer to layer, with headers being stripped off as it progresses.
-

Design Issue for the Layers

- **Error detection and Error correction:** *One mechanism for finding errors in received information uses codes for* ***error detection.*** *Information that is incorrectly received can then be retransmitted until it is received correctly. More powerful codes allow for* ***error correction****, where the correct message is recovered from the possibly incorrect bits that were originally received.*
- **Routing Algorithm:** *finding a working path through a network. Often there are multiple paths between a source and destination, and in a large network, there may be some links or routers that are broken.*
- **Addressing:** *every layer needs a mechanism for identifying the senders and receivers that are involved in a particular message.*
- **Flow control:** *An allocation problem that occurs at every level is how to keep a fast sender from swamping a slow receiver with data. Feedback from the receiver to the sender is often used.*

Design Issue for the Layers

- **Confidentiality:**
  - The design issue is to secure the network by defending it against different kinds of threats. One of the threats is that of eavesdropping on communications. Mechanisms that provide **confidentiality** defend against this threat, and they are used in multiple layers.
  - Mechanisms for **authentication** prevent someone from impersonating someone else. They might be used to tell fake banking Web sites from the real one, or to let the cellular network check that a call is really coming from your phone so that you will pay the bill.
  - Other mechanisms for **integrity** prevent surreptitious changes to messages, such as altering "debit my account 10" to "debit my account 1000.'

Connection Types

- **Connection-Oriented service**
  - like the phone system
  - to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection.
  - a “live” connection must be established
  - data is sent in “real time” and received by the other end
  - the other end will respond back as data is received
- **Connectionless Service**
  - like the postal system.
  - Each message (letter) carries the full destination address, and each one is routed through the intermediate nodes inside the system independent of all the subsequent messages.
  - data is packaged and sent to the destination
  - no time limit is placed on the transport of the data
  - each packet of data is determined to be a single message in and of itself with no relation to other messages.

Service Primitives

- Service is formally specified by a set of **primitives** (operations) available to user processes to access the service.
- These primitives tell the service to perform some action or report on an action taken by a peer entity.
- If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls.
- The primitives for connection-oriented service are

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
ACCEPT	Accept an incoming connection from a peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Figure 1-17. Six service primitives that provide a simple connection-oriented service.

Service Primitives

- These primitives might be used for a request-reply interaction in a client-server environment. To illustrate how, sketching a simple protocol that implements the service using acknowledged datagrams.

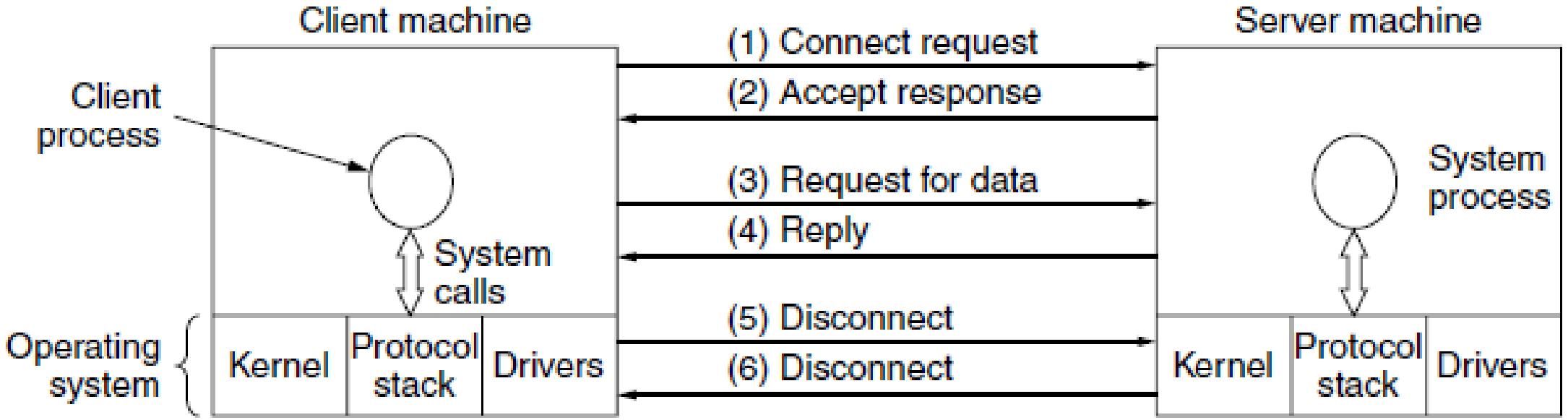


Figure 1-18. A simple client-server interaction using acknowledged datagrams.

The relation of services to protocols

- A service is a set of primitives (operations) that a layer provides to the layer above it.
- The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented.
- A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.
- A protocol, in contrast, is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer.
- Entities use protocols to implement their service definitions.

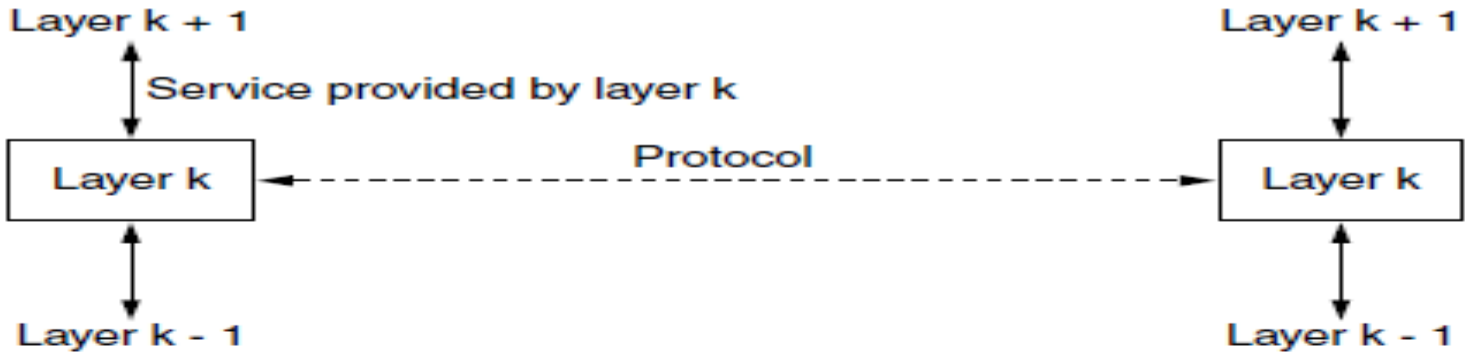


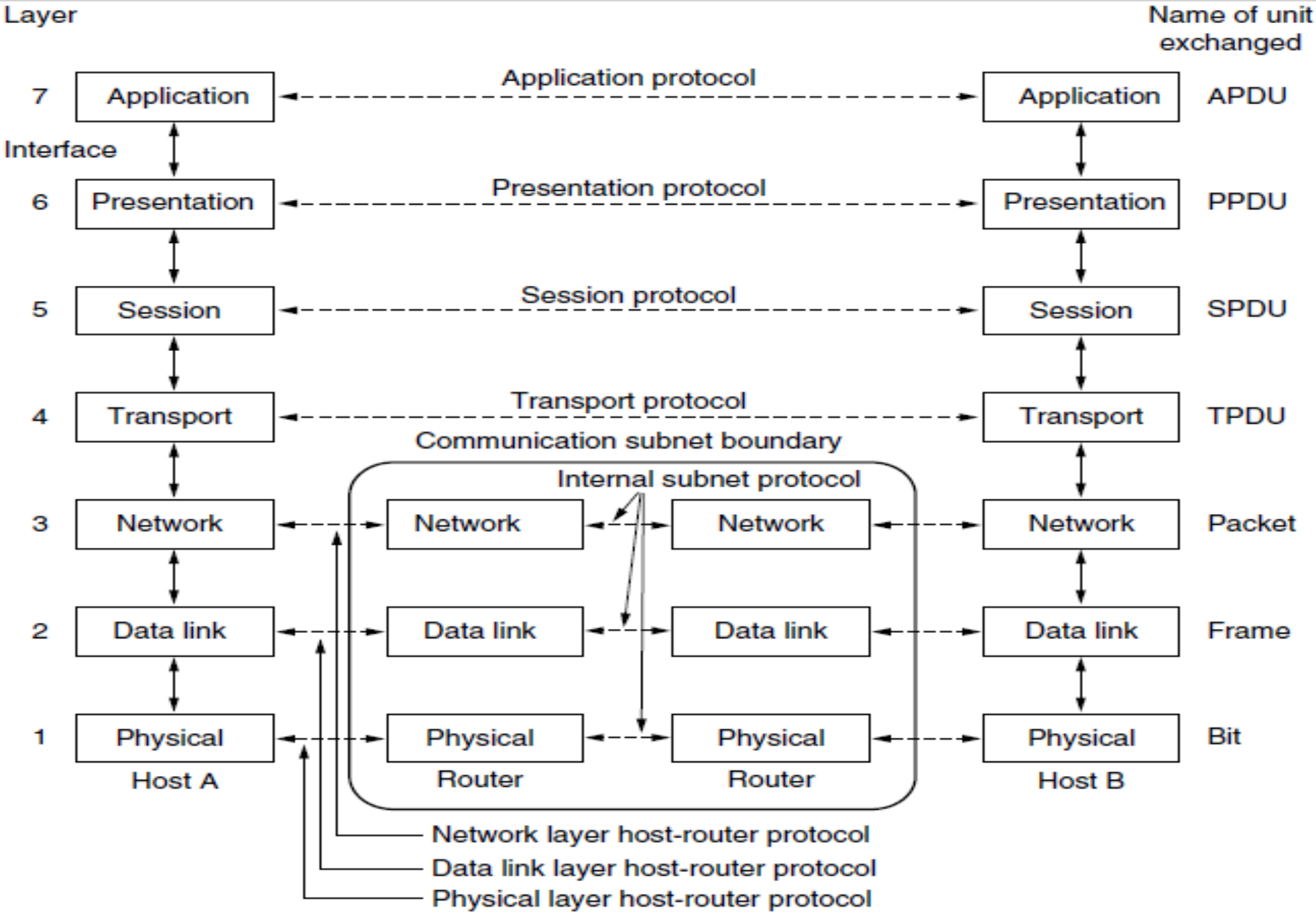
Figure 1-19. The relationship between a service and a protocol.

The OSI Reference Model

- Open Systems Interconnection (OSI)
- The OSI model explains how packets travel through the various layers to another device on a network, even if the sender and destination have different types of network media.
- The principles that were applied to arrive at the seven layers can be briefly summarized as follows:
  1. A layer should be created where a different abstraction is needed.
  2. Each layer should perform a well-defined function.
  3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
  4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
  5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

The OSI Reference Model

- Dividing the network into seven layers provides the following advantages:
  - It breaks network communication into smaller, more manageable parts.
  - It standardizes network components to allow multiple vendor development and support.
  - It allows different types of network hardware and software to communicate with each other.
  - It prevents changes in one layer from affecting other layers.
  - It divides network communication into smaller parts to make learning it easier to understand.


Layer
Name of unit exchanged
7
Application
Application protocol
Application
APDU
Interface
6
Presentation
Presentation protocol
Presentation
PPDU
5
Session
Session protocol
Session
SPDU
4
Transport
Transport protocol
Transport
TPDU
Communication subnet boundary
Internal subnet protocol
3
Network
Network
Network
Network
Packet
2
Data link
Data link
Data link
Data link
Frame
1
Physical
Physical
Physical
Physical
Bit
Host A
Router
Router
Host B
Network layer host-router protocol
Data link layer host-router protocol
Physical layer host-router protocol

The OSI Reference Model

- **Physical layer**
  - It is concerned with transmitting raw bits over a communication channel.
  - It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.
  - The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical.
  - **The transmission rate-**the number of bits sent each second-is also defined by the physical layer.
  - **Transmission Mode:** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.
  - **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**: The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.

The OSI Reference Model

- **Data link Layer**
  - **Framing:** The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
  - **Physical addressing:** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame.
  - **Flow control:** If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
  - **Error control :** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames.
  - **Access control :** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

The OSI Reference Model

- **Network Layer**
  - The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links), whereas the data link layer oversees the delivery of the packet between two systems on the same network (links).
  - If two systems are connected to the *same link*, there is usually *no need for a network layer*.
  - However, if the two systems are attached to *different networks (links)* with connecting devices between the networks (links), there is *often a need for the network layer* to accomplish source-to-destination delivery.
  - **Logical addressing:** If a packet passes the network boundary, need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that includes the logical addresses of the sender and receiver.
  - **Routing:** When independent networks or links are connected to create intemetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.

The OSI Reference Model

- **Transport Layer**
  - **Service-point addressing:** The transport layer header must include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
  - **Segmentation and reassembly:** A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
  - **Connection control:** The transport layer can be either connectionless or connection oriented.
  - **Flow control:** Flow control at this layer is performed end to end rather than across a single link.
  - **Error Control:** Error control at this layer is performed process-to process rather than across a single link.

The OSI Reference Model

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

The OSI Reference Model

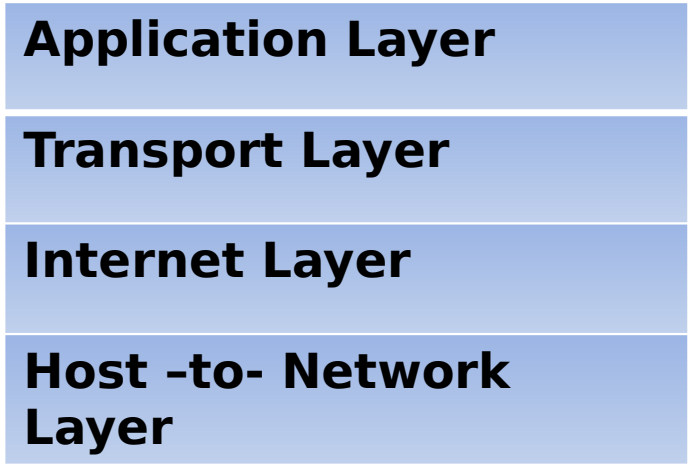
- **Presentation Layer**
  - The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems e.g.. ASCII, UNICODE etc.
  - **Translation:** The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
  - **Data Encryption and Compression**

The OSI Reference Model

- **Application Layer**
  - It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
  - One widely used application protocol is HTTP (Hyper Text Transfer Protocol), which is the basis for the World Wide Web.
  - **Network virtual terminal:** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
  - **File transfer, access, and management:** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
  - **Mail services**: This application provides the basis for e-mail forwarding and storage.
  - **Directory services:** This application provides distributed database sources and access for global information about various objects and services.

TCP/IP Reference Model

- **Host to Network Layer/ Network Access Layer**
  - Network Access Layer is the first layer of the four layer TCP/IP model.
  - Network Access layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.
  - The protocols included in Network Access layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.
  - Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media.

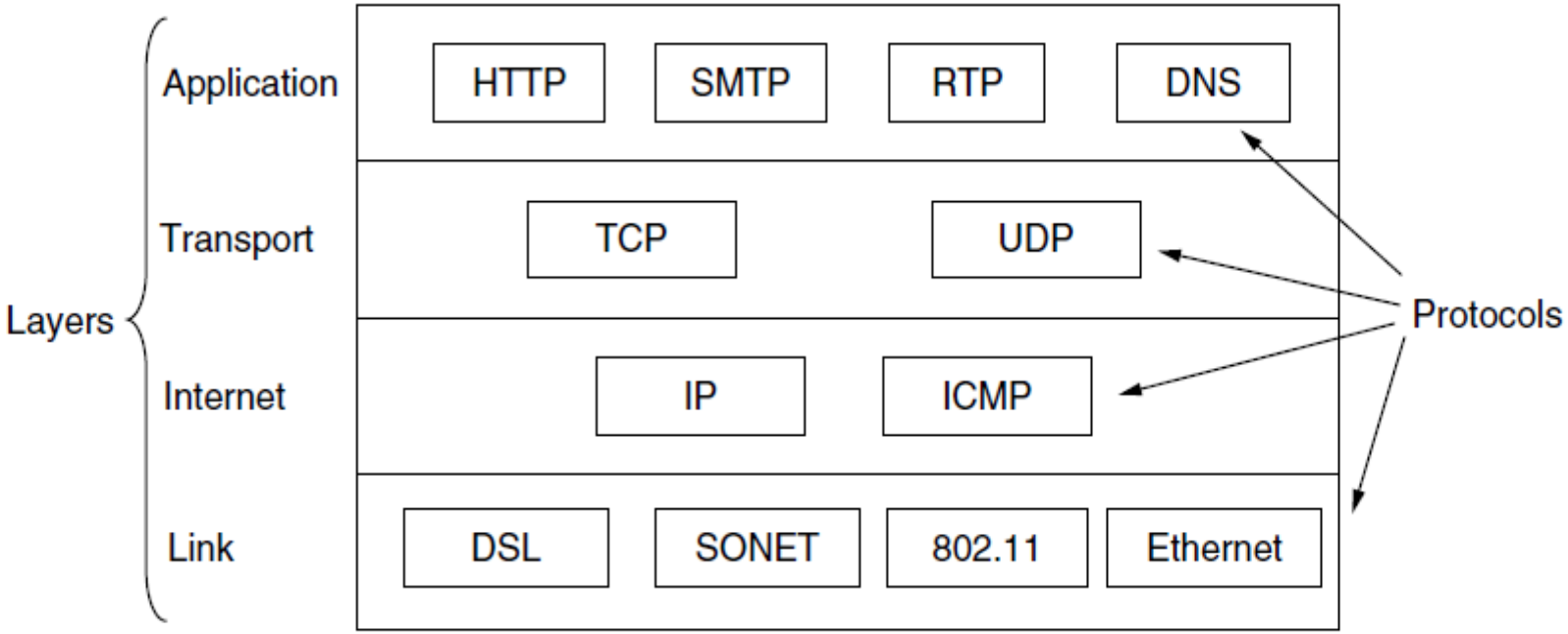


TCP/IP Reference Model

- **Internet Layer**
  - At the internet layer , TCP/IP supports the Internetworking Protocol.
  - The internet layer defines an official packet format and protocol called IP (Internet Protocol). IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.
  - The job of the internet layer is to deliver IP packets where they are supposed to go.
- **Transport Layer**
  - Two end-to-end transport protocols have been defined here.
  - The first one, ***TCP (Transmission Control Protocol),*** is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.
  - The second protocol, ***UDP (User Datagram Protocol),*** is an unreliable, connectionless protocol for applications. It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video.

TCP/IP Reference Model

- **Application Layer**
  - On top of the transport layer is the **application layer**. It contains all the higher- level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP).
  - The Domain Name System (DNS), for mapping host names onto their network addresses, HTTP, the protocol for fetching pages on the World Wide Web, and RTP, the protocol for delivering real-time media such as voice or movies.



OSI Vs. TCP/IP Reference Model

- Both are based on the concept of a stack of independent protocols. Also, the functionality of the layers is roughly similar.
- The OSI model has Seven layers and TCP/IP has four layers.
- The OSI model makes the distinction between the *Services, Interfaces, and Protocols*, whereas TCP/IP did not originally clearly distinguish between *Services, Interfaces, and Protocols.*
- The OSI reference model was devised *before* the corresponding protocols were invented. With TCP/IP the reverse was true: the protocols came first, and the model was really just a description of the existing protocols.
- The OSI model supports both connectionless and connection oriented communication in the network layer, but only connection-oriented communication in the transport layer.
- The TCP/IP model supports only one mode in the network layer (connectionless) but both in the transport layer, giving the users a choice.

Assignment 1

- Prepare Notes on Following
  - PAN: Personal Area Network
  - CAN: Campus Area Network
  - SAN: Storage Area Network
  - Active Networks

Thank You

References:

- Data Communications and Networking " Behrouz A. Forouzan" Fourth Edition.
- Computer Networks "A. S. Tanenbaum" Fifth Edition
- Data and Computer Communications "William Stallings" Tenth Edition.