F.Y.M.Sc.(Computer Applications)
Semester - II
CSA4204
Networking Concepts
Unit – I
Introduction to Computer Networks
Notes

Unit I. Introduction to Computer Networks

- Data Communication: characteristics of data communication, components, data representation, Data Flow
- Computer networks: Distributed processing, physical structures – point-to-point, broadcast, categories of topology (mesh, star, ring, bus, etc.)
- Categories of Network: LAN, MAN, WAN, INTERNET etc.
- Protocols and Standards: Definition of protocol, key elements, Defacto and Dejure standard, standards organizations

Unit 1. Introduction to Computer Networks

- Network Software - Protocol Hierarchies - layers, protocols, peers, interfaces
- Network architecture, protocol stack, Design Issues of the layers – addressing, error control, flow control, multiplexing and demultiplexing, routing, connection oriented and connectionless services
- Service primitives – listen, connect, receive, send, disconnect
- The relationship of services to protocol

Data Communication

- In data communication *data* refers to facts, concepts and instructions presented in various form and *communication* refers to actually exchange or share the information.
- Communication is local: face to face or remote: takes place over distance.
- Data communication is the exchange of data between two devices via some transmission medium.
- Four fundamental Characteristics: Delivery, Accuracy, Timeliness and Jitter.

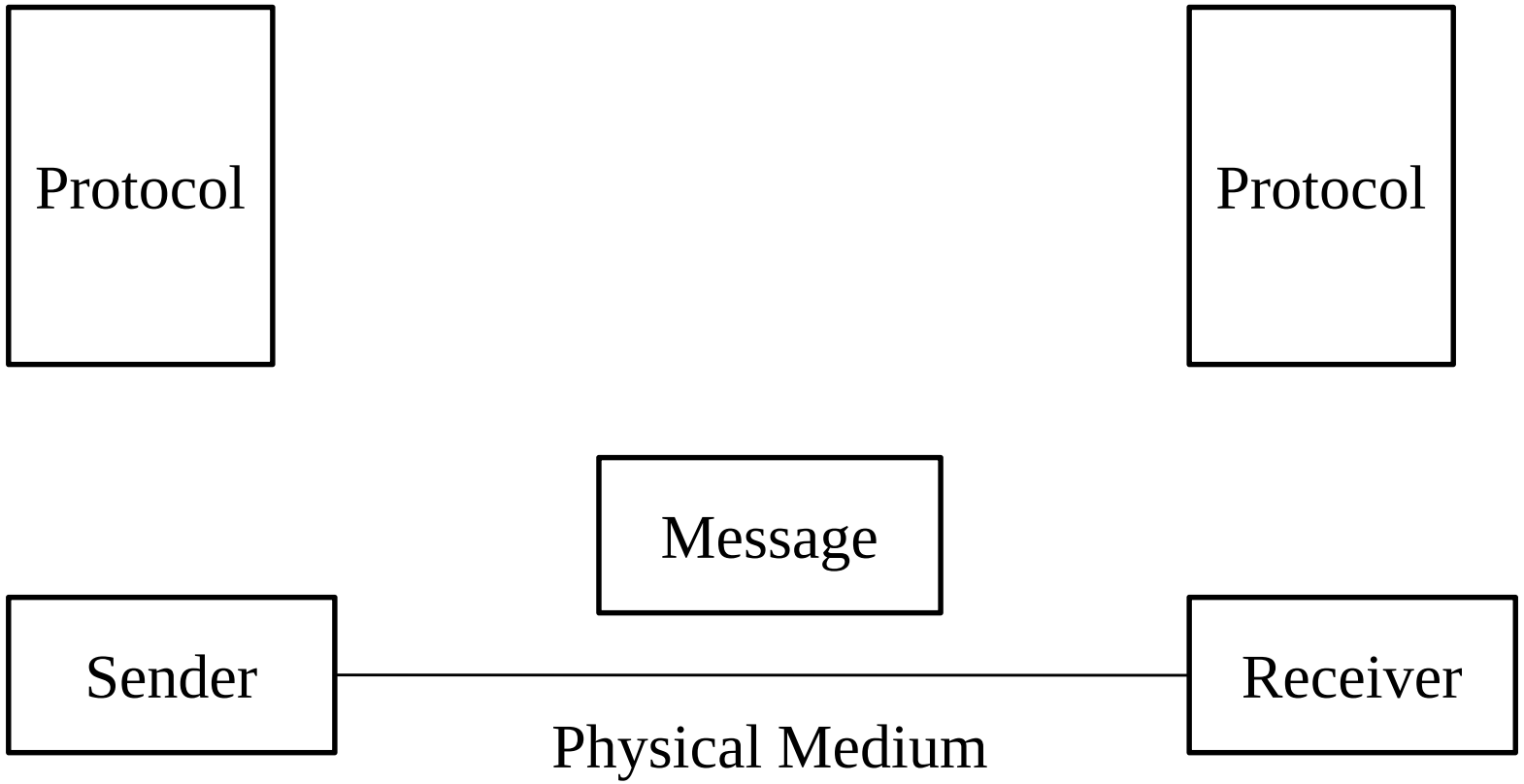
Data Communication

- Four fundamental Characteristics
  - 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
  - Accuracy – The sysem must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

Data Communication

- Four fundamental Characteristics
  - Timeliness – the system must delivered data in a timely manner. Data delivered late is useless. In the case of audio and video, timely delivery means delivering data as they are produced, in the same order that they are produced and without significant delay. Kind of delivery is called real-time transmission.
  - Jitter – refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

Components of Data Communication



Components of Data Communication

- **Message**

  Is the information to be communicated.
- **Sender**

  Which sends the data message.
- **Receiver**

  Which receives the message.
- **Medium**

  Physical path by which message travels from sender to receiver.
- **Protocol**

  set of rules that governs data communication. Its agreement between various communication devices.

Data Representation

- Text
  - represented as a bit pattern, a sequence of bits (0s or 1s).
  - Different set of bit pattern have been designed to represent text symbols.
  - Each set is called code, and the process of representing symbols is called coding.
  - Coding system called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world.
  - The American Standard Code for Information Interchange (ASCII), developed in US, constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

Data Representation

- Numbers
  - Also represented as a bit pattern.
  - However a code such as ASCII is not used to represent numbers, the number is directly converted to a binary number to simplify mathematical operations.

Data Representation

- Images
  - Also represented as a bit pattern. In this simplest form the image is composed of a matrix of pixels (Picture Elements), where each pixel is small dot. Size of pixel depends on the resolution.
  - After image is divided into pixels, each pixel is assigned a bit pattern. The size and value of the pattern depend on the image. For an image made of only black-and-white dots (chessboard), a 1-bit pattern is enough to represent a pixel.
  - If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale.

Data Representation

- Images
  - To show four levels of gray scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10 and white pixel by 11.
  - There are several methods to represent color images. One method is RGB - each color made of red, green and blue. Another method is YCM – each color made of yellow, cyan and magenta.

Data Representation

- Audio
  - Refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers or images.
  - It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuation signal.

Data Representation

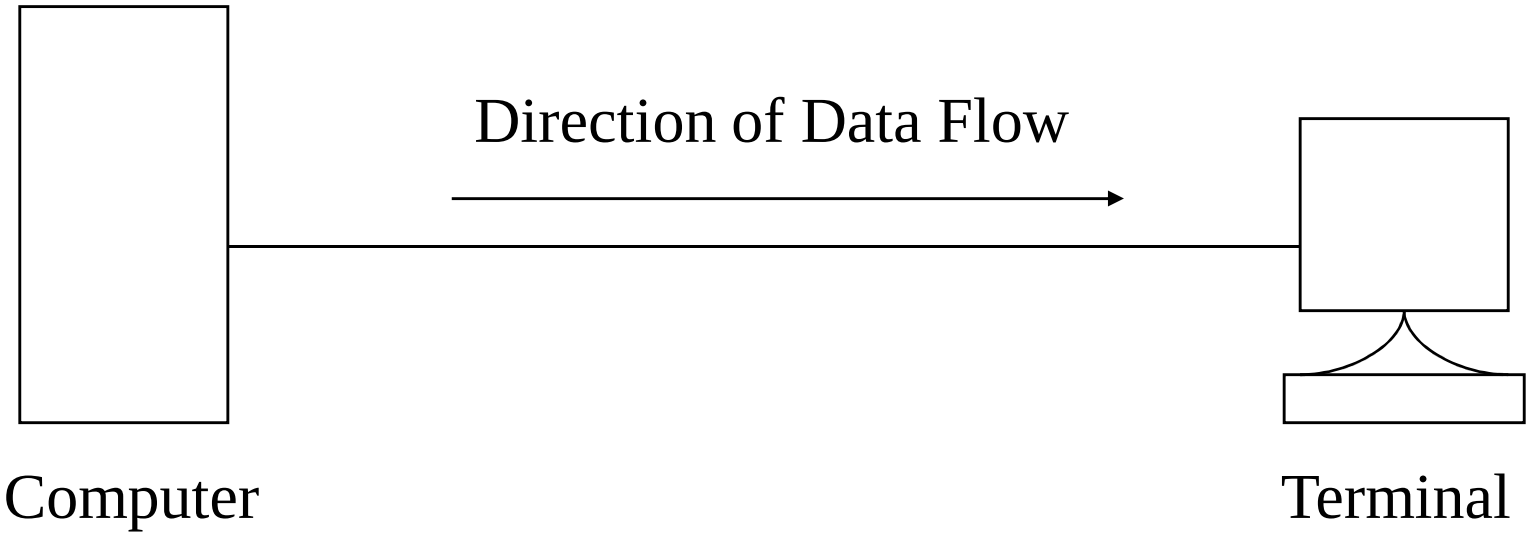
- Video
  - Refers to the recording or broadcasting of a picture or movie.
  - Video can either be produced as a continuous entity (e.g. by TV camera), or it can be combination of images, each a discrete entity, arranged to convey the idea of motion.
  - We can change video to a digital or an analog signal.

Data Flow

- Used to define direction of signal flow between two linked devices.
- Three modes are supported
  - Simplex
  - Half Duplex
  - Full Duplex

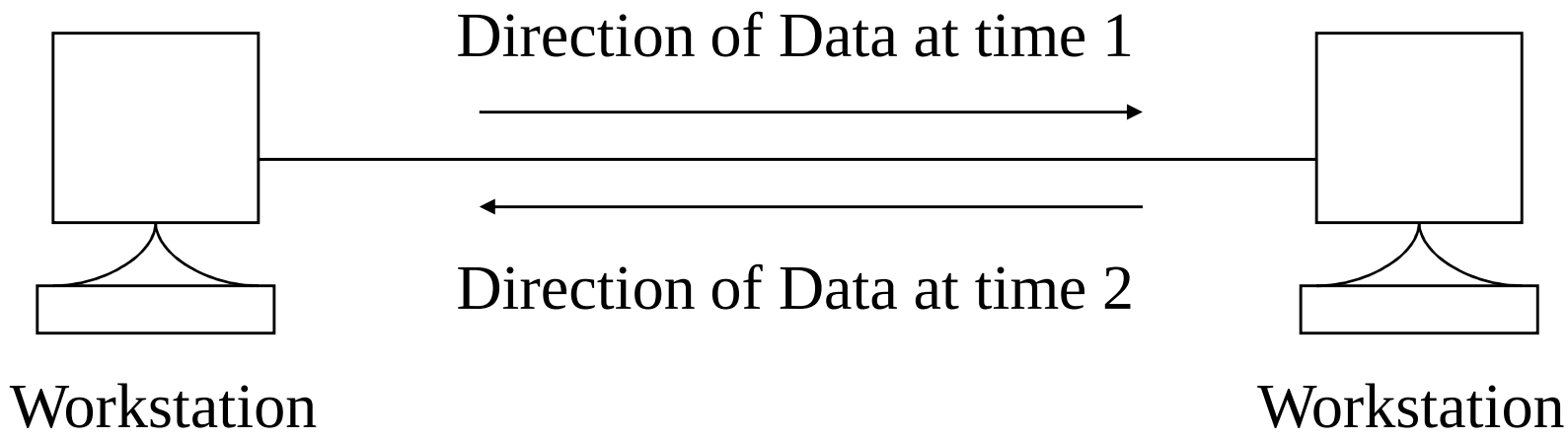
Data Flow

- Simplex
  - Communication is unidirectional. Only one of the two devices on a link can transmit; the other can only receive.
  - Example: keyboard and traditional output device



Data Flow

- Half Duplex
  - 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.
  - Example: Walkie-talkies

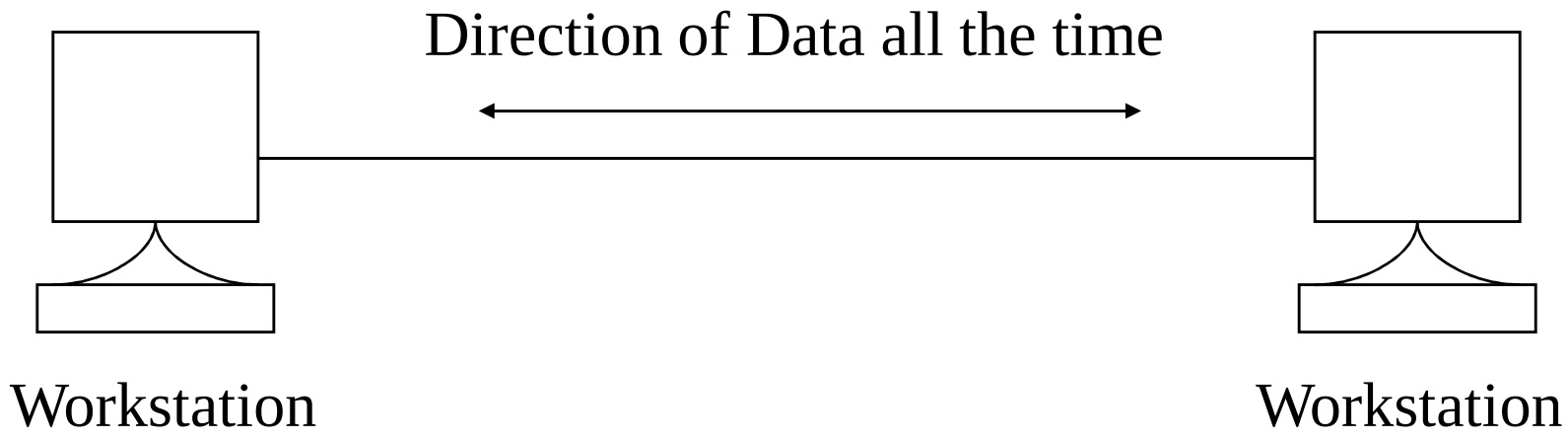


Data Flow

- Full Duplex
  - Both stations can send and receive simultaneously.
  - Signals going in either direction share the capacity of the link
  - Sharing occur in two ways: either 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 signals traveling in both directions.
  - Example: communication in telephone networks, both can talk and listen simultaneously.

Data Flow

- Full Duplex



Computer Networks

- Distributed Processing
  - A task is divided among multiple computers.
  - Instead of one single large machine being responsible for all aspects of a process, separate computers handle a subnet.

Computer Networks

- Physical Structures – Type of connection – Point-to-point
  - 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.
  - Example: Changing television channel by infrared remote control

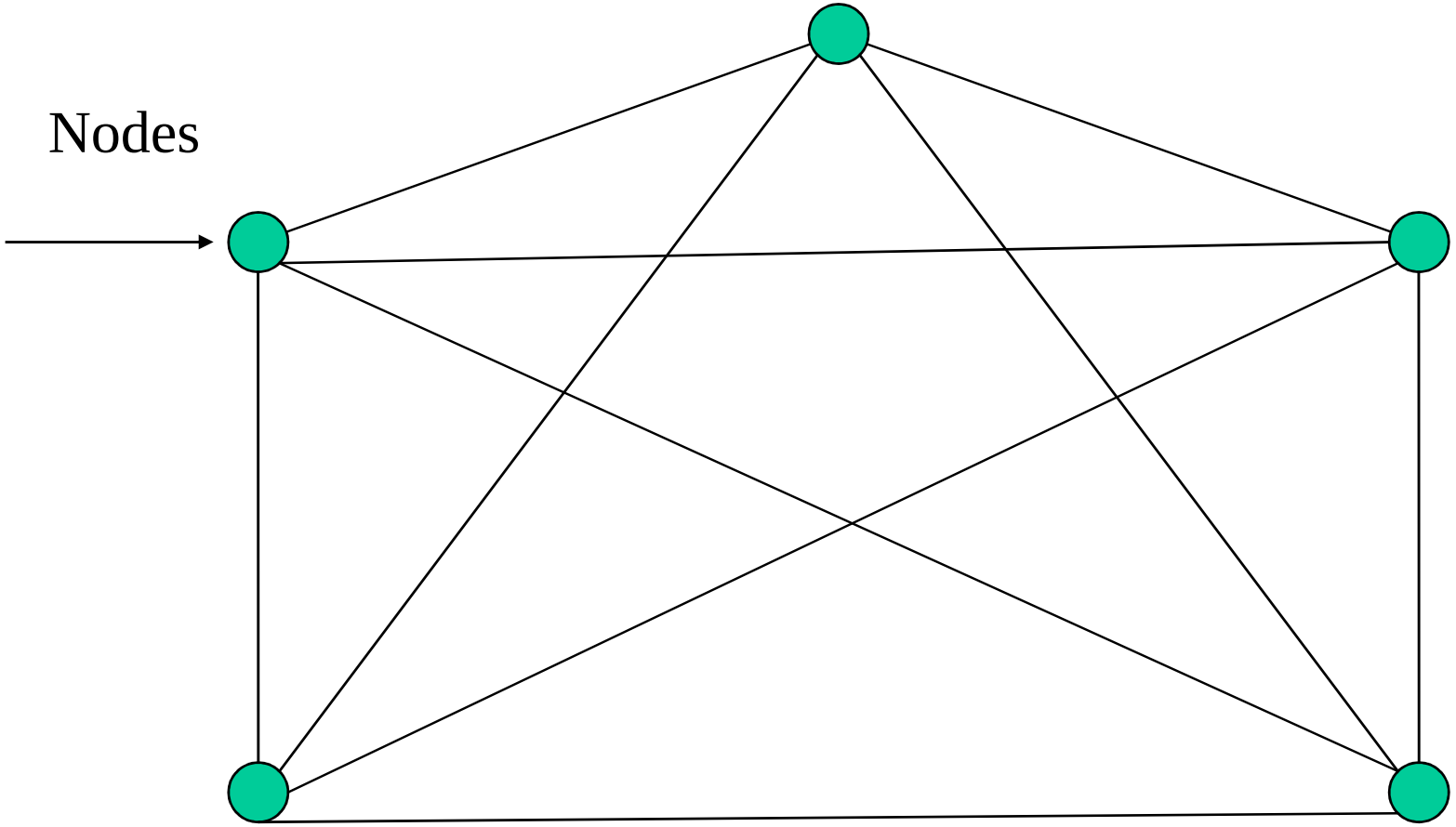
Computer Networks

- Physical Structures – Type of connection – Multipoint
  - One in which more than two specific devices share a single link.
  - The capacity of the channel is shared either spatially or temporally.
  - If several devices can use the link simultaneously, it is a spatially (local level) shared connection.
  - If users must take turns, it is a timeshared connection.

Computer Networks

- Physical Structures – Physical Topology
  - Refers to the way in which a network is laid out physically.
  - Two or more devices connect to a link; two or more links forms a topology.
  - The topology of a network is the geometric representation of the relationship of all the links and linking devices called nodes to one another.
  - Four basic topologies are: mesh, star, bus and ring.

Mesh Topology



Mesh Topology

- Every device has dedicated point-to-point link to every device.
- Dedicated means links carries traffic between two devices if connected.
- Fully connected network has n(n-1)/2 physical channels to link ‘n’ devices and n-1 ports.

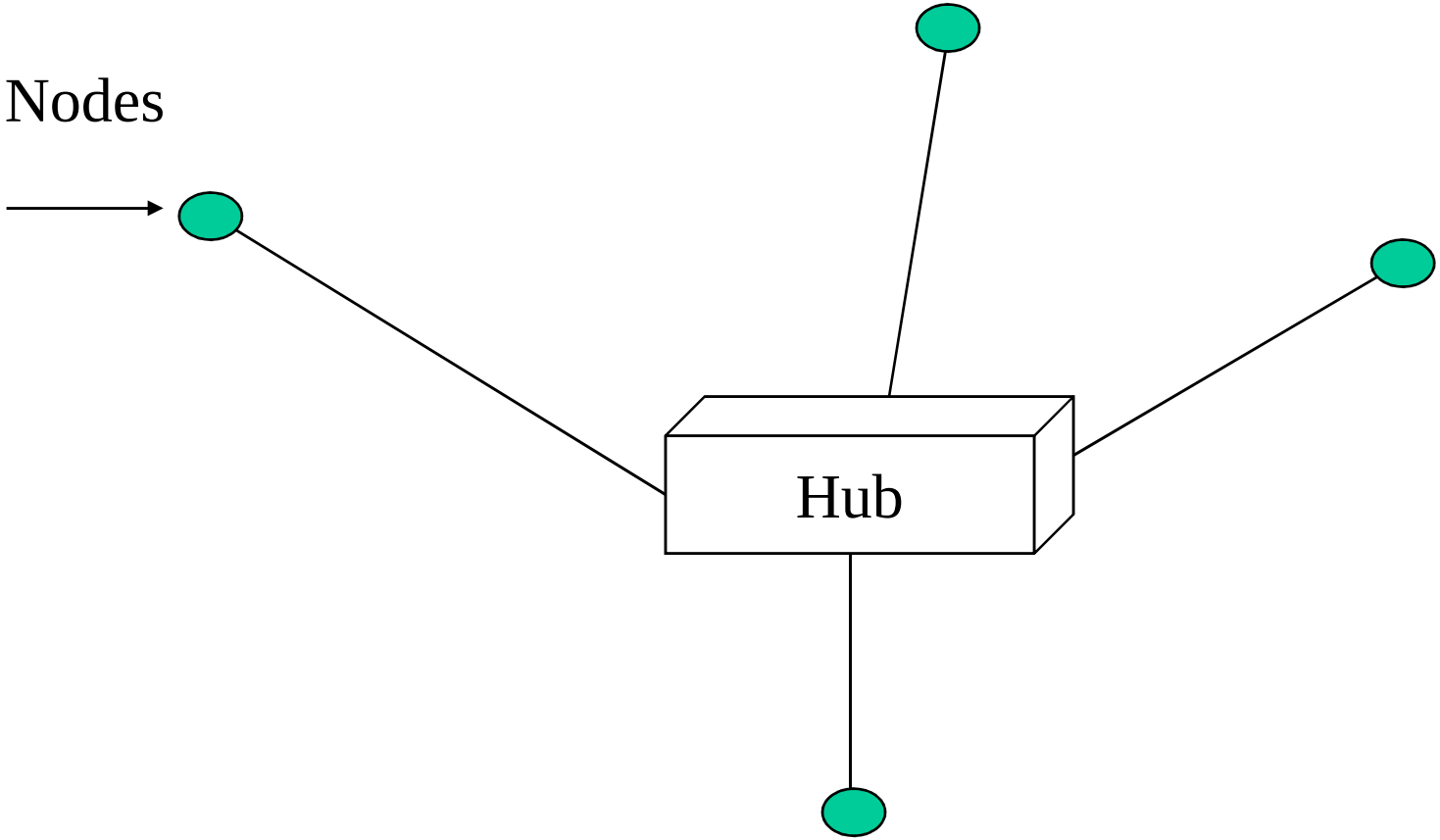
Advantages

- Dedicated links guarantees that connection carry its own data thus eliminating traffic problem
- Privacy and security since every message sent along dedicated line
- Fault isolation and identification is easy

Disadvantages

- Since every device must be connected to each other installation is difficult.
- Bulk of wires can be greater than available space.
- The hardware requirement is expensive.

Star Topology



Star Topology

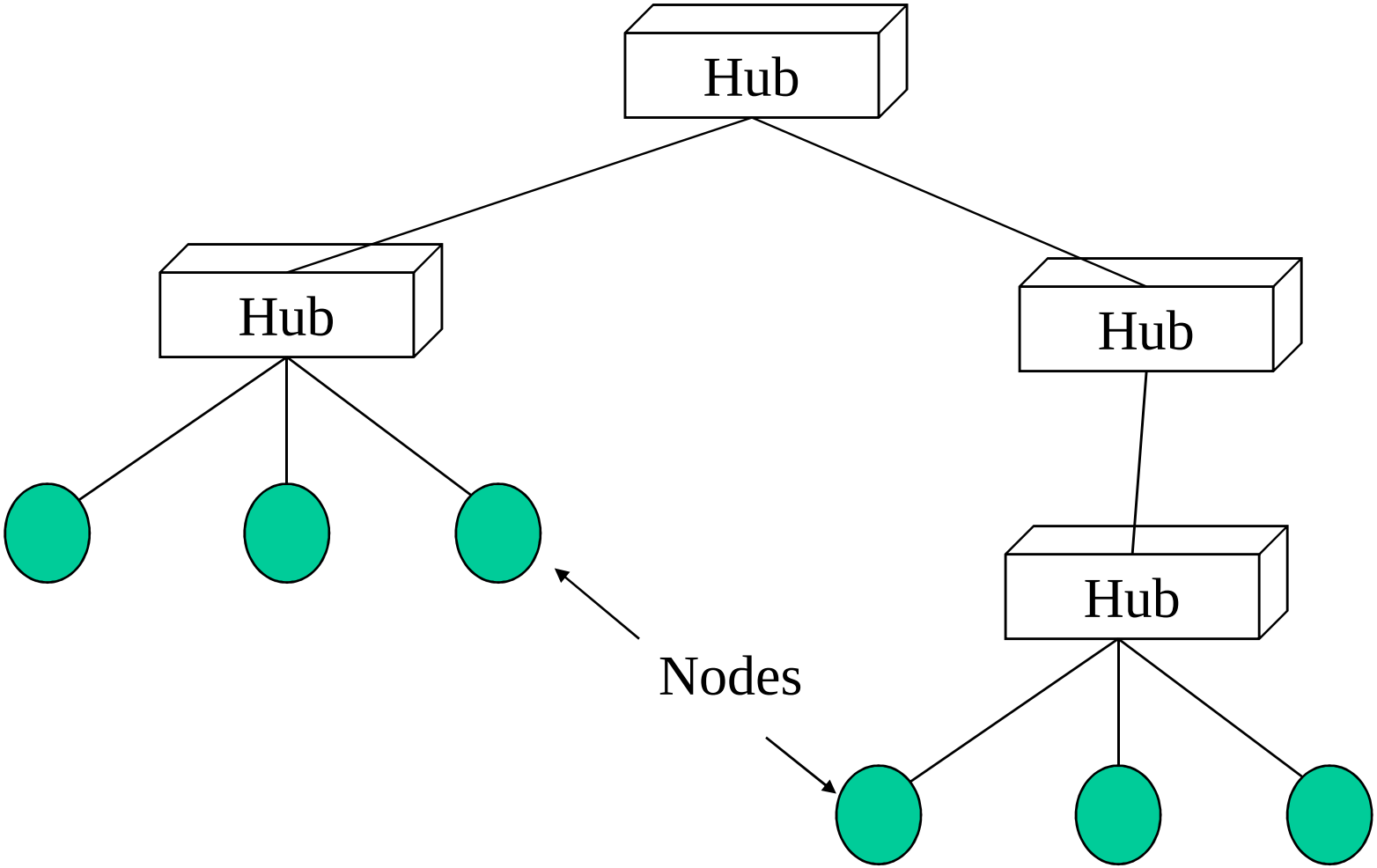
- Each device has dedicated point-to-point look to central controller, usually called HUB.
- Devices not connected directly hence no direct traffic
- Controller acts as exchange:

  data->controller->other device

Advantages

- Only one link and one I/O to connect it to many device.
- Easy to install and configure. Less expensive.
- Additions, deletion involves only one connection.
- Robust, only one link is affected.

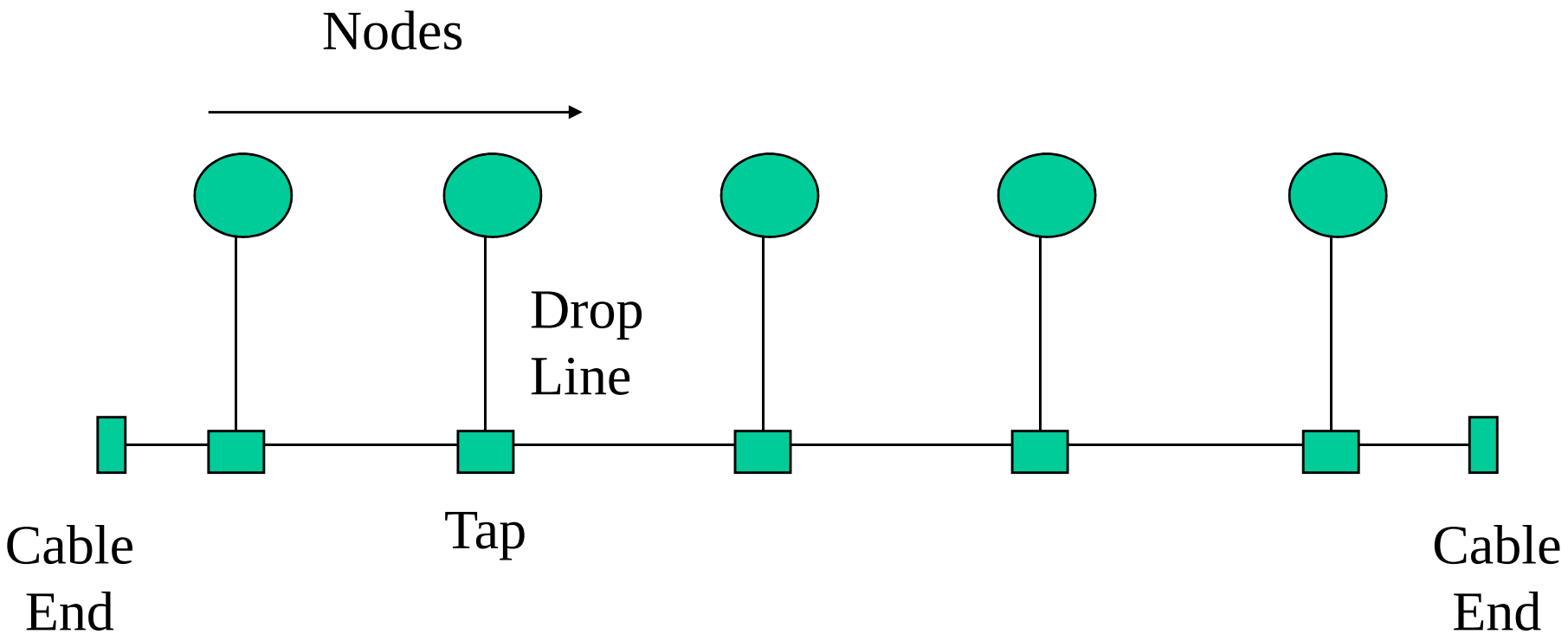
Tree Topology



Tree Topology

- Variation over star. Every device is not connected to central hub directly but through secondary hub.
- The central hub is active hub having repeaters to regenerate signal before sending out.
- Secondary hubs can be active or passive. Passive hubs simply provides physical connection between device.
- Secondary hub adds two additional advantages to star.
  - Allows more device connected to central hub.
  - Allows network isolation and priority communication
- Example Cable TV

Bus Topology



BUS Topology

- It is multipoint. One long cable acts as backbone to link all devices in network.
- Drop lines: connection running between device and main cable.
- Tap:punctures the sheathing of cable to create a contact with metallic core.
- Limitation on number of taps.

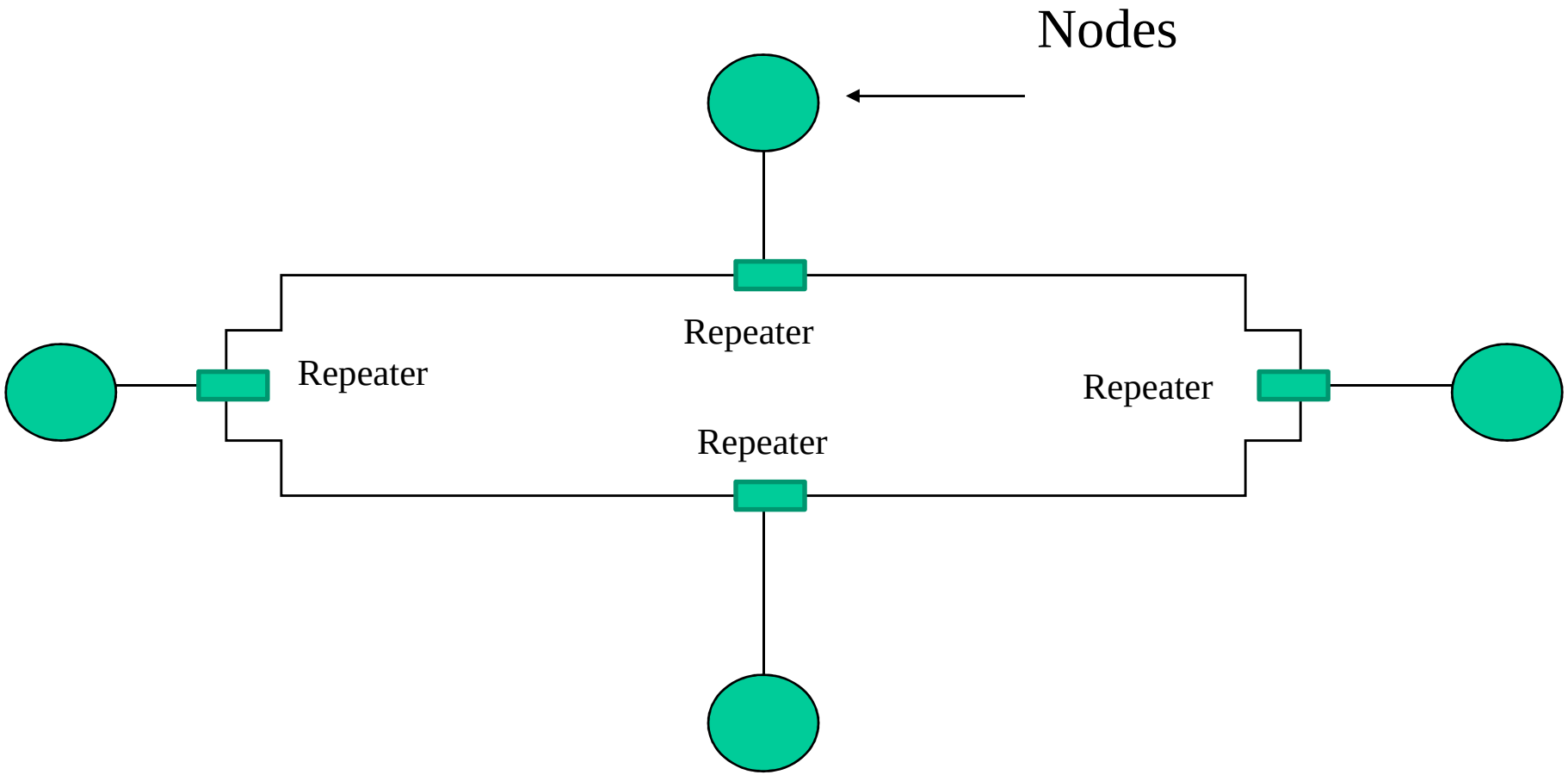
Advantages

- Backbone cable can laid along most efficient path and then connected to node, hence less cabling than other topologies. Redundancy of cable is eliminated.

Disadvantages

- Difficult to add new device
- Signal reflection at taps can cause degradation in quality.
- The fault or break in cable stops all transmission

Ring Topology



Ring Topology

- Here each device has dedicated point-to-point line with two devices either side of it.
- Signal reaches to destination through device to device in one direction.
- Repeater is present.
- To add or remove device only one connection to move.
- Signal is circulating all the time. If destination is unreachable it issues alarm.
- Break in cable can affect entire network.

Hybrid Topology

- Network can be hybrid.
- Example: we can have a main star topology with each branch connecting several stations in bus topology.

Categories of Networks - LAN

- LANs usually privately owned networks within single building or campus of up to a few KM in size.
- Widely used to connect personal computers and workstations in company offices and factories to share resources (printers) and exchange information.
- LANs are distinguished from other kinds of networks by three characteristics: their size, their transmission technology and their topology.
- LANs are restricted in size, means that the worst case transmission time is bounded and known in advance. Simplifies network management.

Categories of Networks - LAN

- LANs may use a transmission technology consisting of a cable to which all the machines are attached.
- Traditional LANs run at speeds of 10Mbps to 100Mbps, have low delay and make very few errors. Newer LANs operate at up to 10Gbps.
- Various topologies are possible for broadcast LANs
  - Bus topology
  - Ring topology

Categories of Networks - LAN

- In bus network, at any instant at most one machine is the master and is allowed to transmit.
- All other machines are required to refrain from sending.
- An arbitration mechanism is needed to resolve conflicts when two or more machines want to transmit simultaneously. May be centralized or distributed.
- IEEE 802.3, called Ethernet, is bus based broadcast network with decentralized control usually operates at 10Mbps to 10Gbps.
- Computers on an Ethernet can transmit whenever they want to; if two or more packets collide, each computer just waits a random time and tries again later.

Categories of Networks - LAN

- In ring, each bit is propagates around on its own, not waiting for the rest of the packet to which it belongs.
- Typically, each bit circumnavigates the entire ring in the time it takes to transmit a few bits, often before the complete packet has even been transmitted.
- IEEE 802.5 is ring based LAN operating at 4 to 16Mbps. FDDI is another example of a ring network,

Categories of Networks - LAN

- Broadcast networks can be further divided into static and dynamic depending on how the channel is allocated.
- Static allocation
  - Divide time into discrete intervals and use round-robin algorithm, allowing each machine to broadcast only when its time slot comes up.
  - Wastes channel capacity when a machine has nothing to say during its allocated slot, so most systems attempt to allocate the channel dynamically (i.e. on demand).

Categories of Networks - LAN

- Dynamic allocation
  - Are either centralized or decentralized.
  - In the centralized channel allocation method, there is single entity, a bus arbitration unit, which determines who goes next. It do this by accepting requests and making a decision according to some internal algorithm.
  - In the decentralized channel allocation method, there is no central entity, each machine must decide for itself whether to transmit.

Categories of Networks - MAN

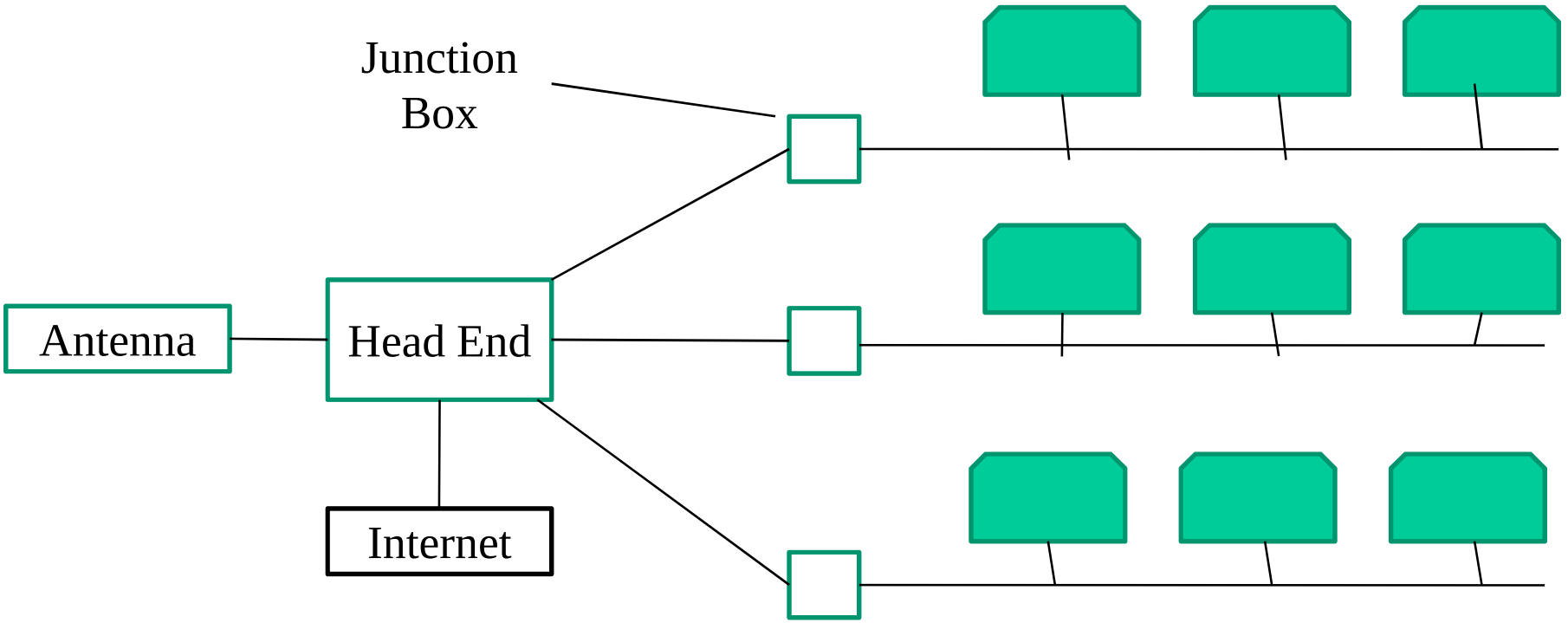
- To extend over an entire city.
- Best-known example of a MAN is the cable television network available in many cities.
- System grew from earlier community antenna systems used in areas with peer over-the-air television reception.
- Here a large antenna was placed on top of a nearby hill and signal was then piped to the subscriber’s home.

Categories of Networks - MAN

- As companies began jumping into the business, getting contracts from city government to wire up an entire city.
- The next step was television programming and even entire channels designed for cable only.
- Often these channels were specialized, such as all news , all sports, all cooking and so on, but from their inception they were intended for television reception only.
- When the Internet attracted a mass audience, the cable TV network operators began to realize that with some changes to the system, they could provide two-way Internet service in unused parts of the spectrum.

Categories of Networks - MAN

- At that point, the cable TV system began to morph from a way to distribute television to metropolitan area network.
- First approximation, a MAN might look like



Categories of Networks - MAN

- We can see that both television signals and Internet being fed into the centralized head end for subsequent distribution to people’s homes.
- Cable television is not the only MAN. Recent developments in high speed wireless Internet access resulted in another MAN standardized as IEEE 802.16.

Categories of Networks - MAN

- It may be single network or means of connecting number of LANs into larger network to share resources LAN-LAN
- MAN can be wholly owned and operated by private company or may be service provided by public company such as telephone company.
- There is broadcast medium to which all computers are connected.

Categories of Networks - WAN

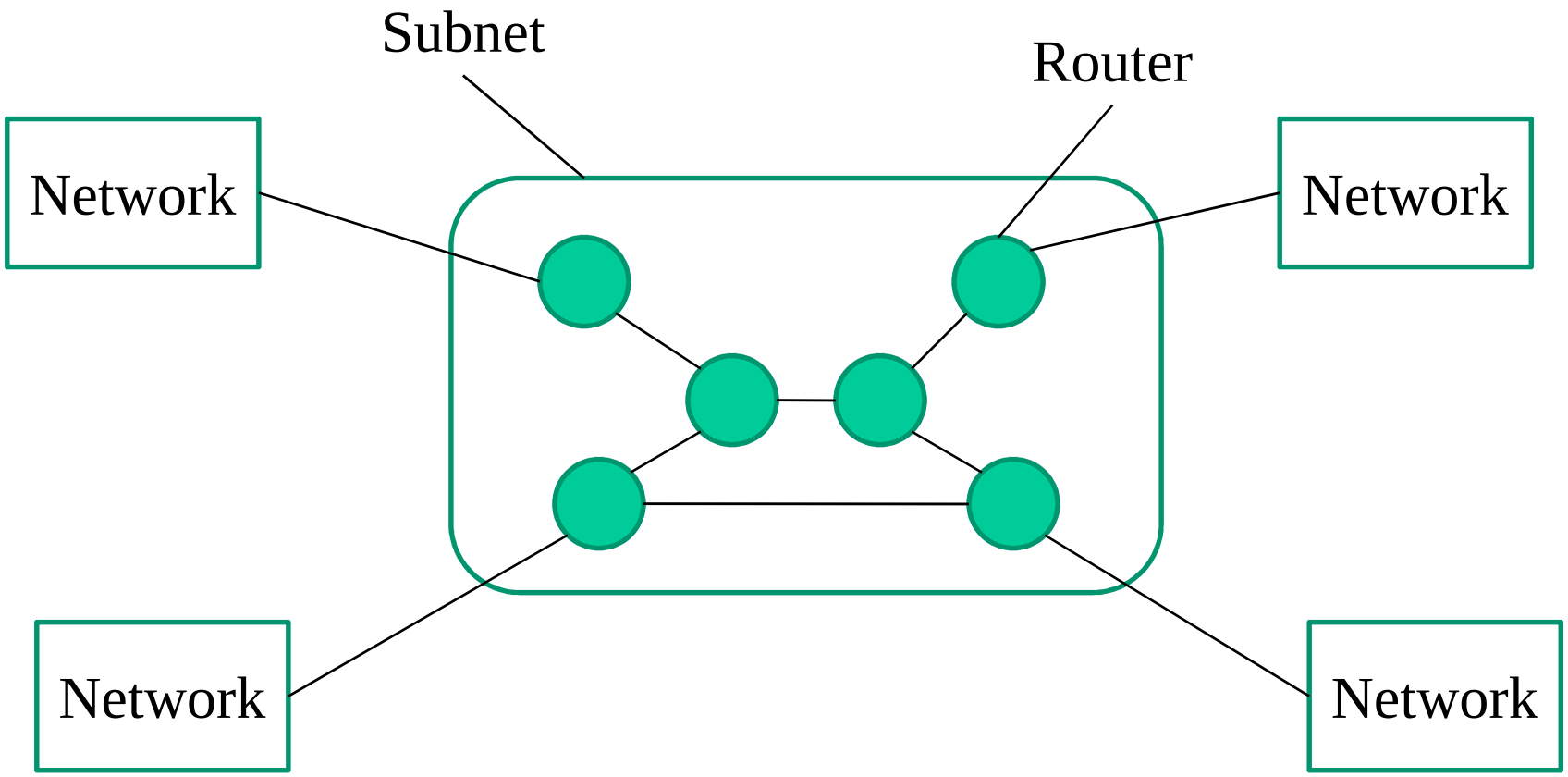
- Spans a large geographical area, often a country or continent.
- Contains collection of machines (hosts) intended for running user (i.e. application) programs.
- The hosts are connected by communication subnet, or just subnet for short. The hosts are owned by the customers, whereas communication subnet is typically owned and operated by a telephone company or Internet service provider.
- Job of subnet is to carry messages from host to host.

Categories of Networks - WAN

- In most wide area networks, the subnet consists of two distinct components:
  - Transmission line: moves bits between machines. Made of copper wire, optical fiber, or even radio links.
  - Switching elements: specialized computers that connect two or more transmission lines.
- When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them.
- Switching computers, now most commonly called as routers.

Categories of Networks - WAN

- WAN Model



Categories of Networks - WAN

- Each host is frequently connected to a LAN on which a router is present, in some cases a host can be connected directly to a router.
- The collection of communication lines and routers form the subnet.
- Originally subnets' meaning was the collection of routers and communication lines that moved packets from the source to destination host.

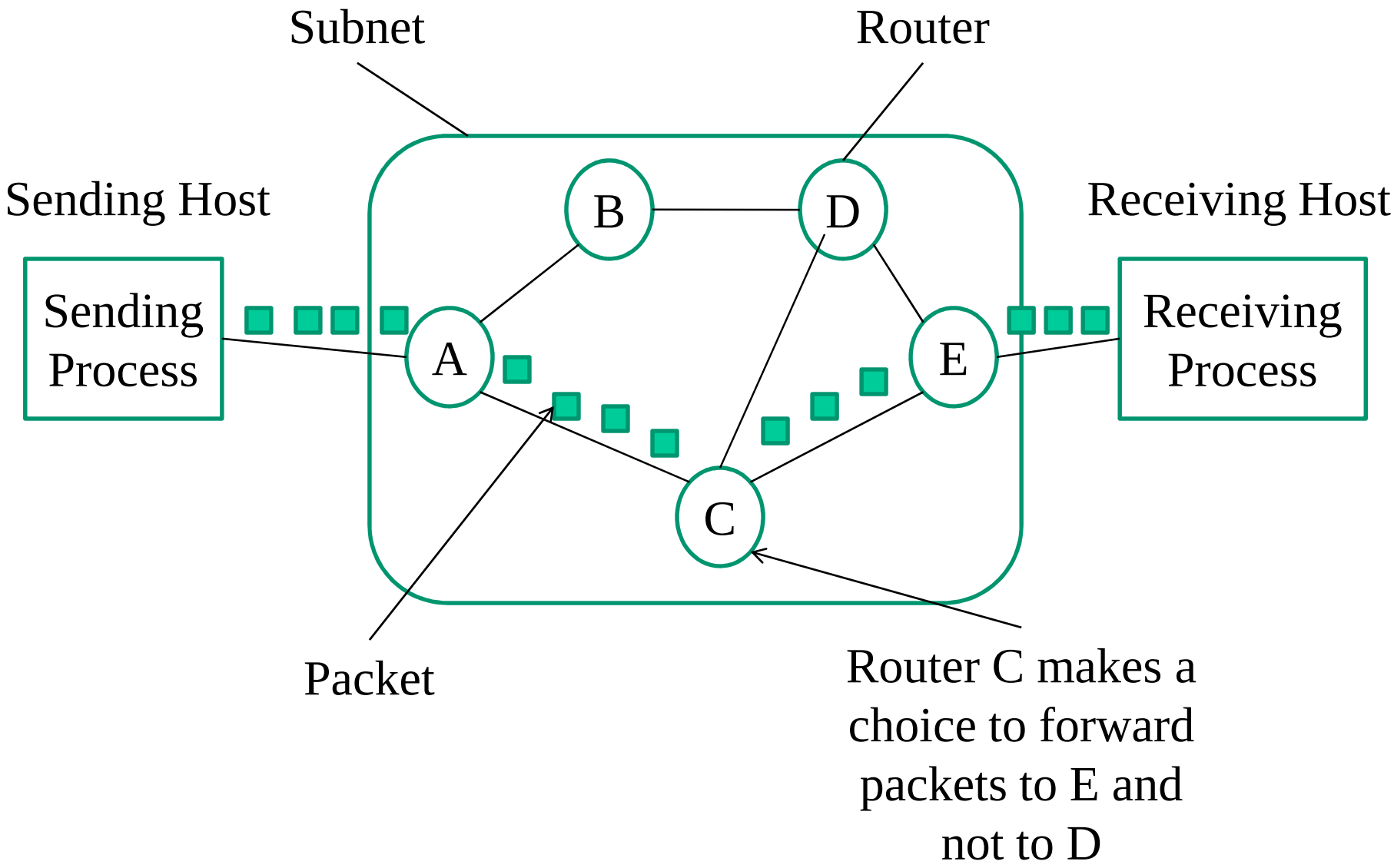
Categories of Networks - WAN

- In most WANs, the network contains numerous transmission lines, each one connecting a pair of routers.
- If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers.
- When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirely, store there until the required output line is free and then forwarded.
- A subnet organized according to this principle is called store-and-forward or packet switched subnet. All wide area networks have store-and-forward subnets.
- When the packets are small and all same size, called as cells

Categories of Networks - WAN

- In packet switched WAN, when a process has a message to be sent to another process, the sending host cuts the message into packets, each one bearing its number in the sequence.
- These packets are then injected into the network one at a time in quick succession. The packets are transported individually over the network and deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process.

Categories of Networks - WAN



Categories of Networks - WAN

- Routing decisions are made locally.
- When packet arrives at A, it is up to A to decide if this packet should be sent on the line to B or the line to C. A makes decision depending on routing algorithm.

Categories of Networks - WAN

- Not all WANs are packet switched. Second possibility is satellite system.
- Each router has antenna through which it can send and receive.
- All routers can hear the output from the satellite, and in some cases they can also hear the upward transmission of their fellow routers to the satellite as well.
- Sometimes the routers are connected to a substantial point-to-point subnet, with only some of them having a satellite antenna.
- Satellite networks are inherently broadcast.

Categories of Networks– Internetworks

- Many networks exists in the world with different hardware and software. People connected to one network often want to communicate with people attached to a different one.
- The fulfillment of this desire requires that different, and frequently incompatible networks, be connected, sometimes by means of machines called gateways to make the connection and provide the necessary translation, both in terms of hardware and software.
- A collection of interconnected networks is called an Internetwork or Internet.

Categories of Networks– Internetworks

- A common form of internet is a collection of LANs connected by a WAN.
- If we were to replace the label “subnet” by WAN nothing else would have to change.
- The only real technical distinction between a subnet and a WAN in this case is whether hosts are present.
- If the system contains only routers, it is a subnet; if it contains both routers and hosts, it is WAN.
- The real differences relate to ownership and use.

Categories of Networks– Internetworks

- subnets, networks, and internetworks are often confused.
- Subnet makes the most sense in the context of a wide area network, where it refers to the collection of routers and communication lines owned by the network operator.
- The combination of a subnet and its hosts forms a network.
- An internetwork is formed when distinct networks are interconnected. Connecting different LAN and a WAN or connecting two LANs forms an internetwork.

Protocols and Standards

- Protocols
  - Define it as set of rules that governs data communication.
  - An entity which is capable of sending or receiving information will not send any bit stream to other place till both not agreed on set of rules.
  - A protocol defines what is communicated, how it is communicated and when it is communicated.
  - The key elements of protocol
    - **Syntax** : refers to the structure or format of the data, meaning the order in which they are presented.
    - **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
    - **Timing** : refers to two characteristics: when data should be sent and how fast can be sent.

Protocols and Standards

- Standards
  - Are agreed upon rules
  - 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 process.
  - Provide guidelines to manufacturers, vendors, and other service providers to ensure the kind of interconnectivity necessary in today's market.
  - Fall in two categories:
    - **De facto** (by fact or by convention): standards that have not been approved by an organized body but have been adopted as standards through widespread use. They are established by manufacturers
    - **De jure** (by law or by regulation): standards that have been legalized by an officially recognized body.

Protocols and Standards

- Standard organizations
  - ISO (International Organization for Standardization)
  - ITU-T (International Telecommunication Union – Telecommunication Standards Sector)
  - ANSI (American National Standards Institute)
  - IEEE (Institute of Electrical and Electronics Engineers)
  - EIA (Electronic Industries Association)

Network Software

- Protocol Hierarchies
  - To reduce the design complexity of network software, 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, shielded 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.

Network Software

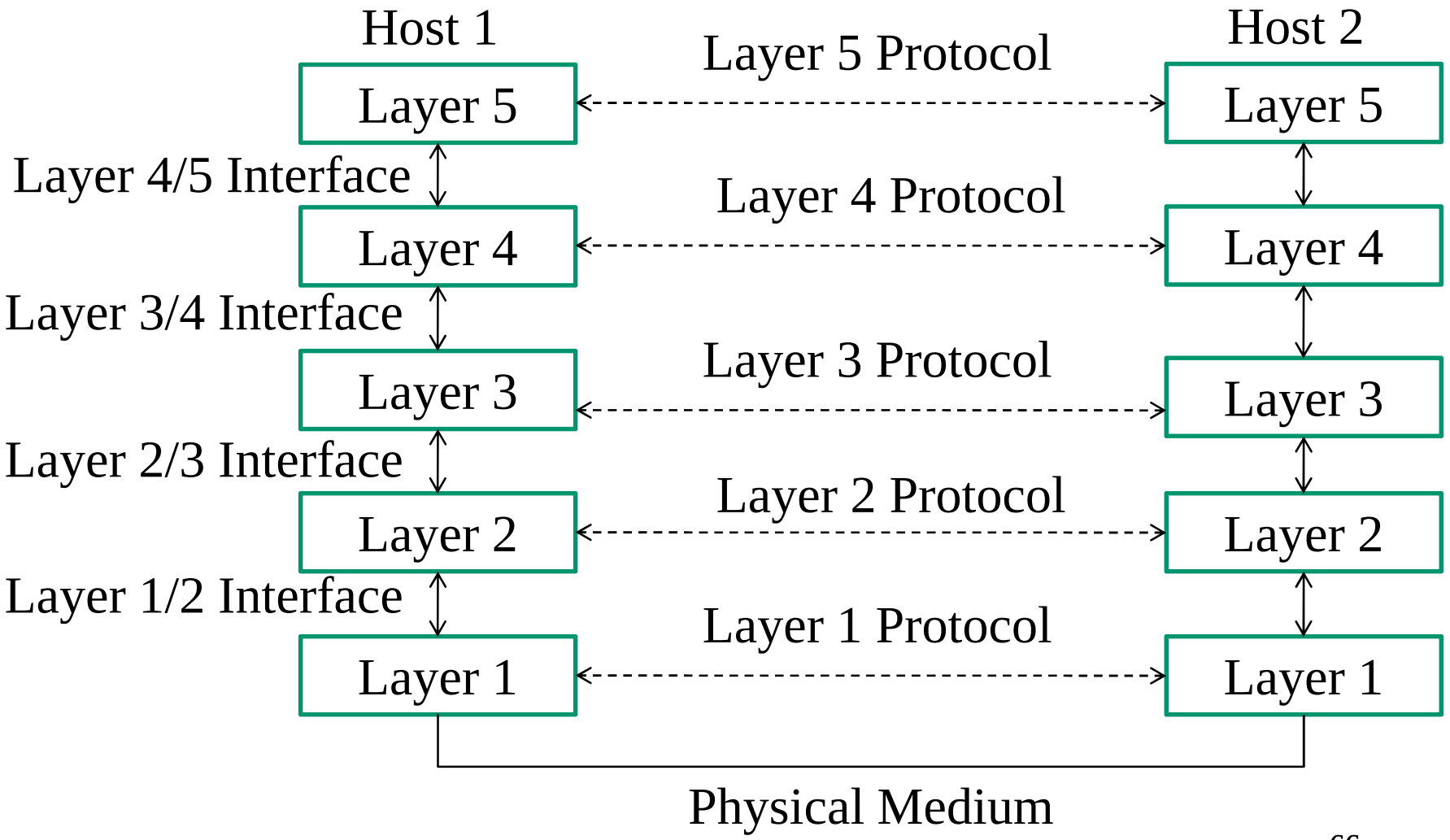
- Protocol Hierarchies
  - The concept is familiar and used throughout computer science, where it is variously known as information hiding, abstract data types, data encapsulation and object-oriented programming.
  - The fundamental idea is that a particular piece of software (or hardware) provides a service to its users but keeps the details of its internal state and algorithms hidden from them.

Network Software

- Protocol Hierarchies
  - Layer *n* on one machine carries on a conversation with layer *n* on another machine. The rules and conversations used in this conversation are collectively known as the layer *n* protocol. Protocol is an agreement between the communicating parties on how communication is to proceed.
  - Consider the five layer network as showed next.

Network Software

- Protocol Hierarchies



Network Software

- Protocol Hierarchies
  - The entities comprising on the corresponding layers on different machines are called peers. Peers may be processes, hardware devices or even human being. It is the peers that communicate by using the protocol.
  - Each layer passes data and control information to the layer immediately below it, until the lowest layer is reached.
  - Below layer 1 is the physical medium through which actual communication occurs. In figure virtual communication is shown by dotted lines and physical communication by solid lines.

Network Software

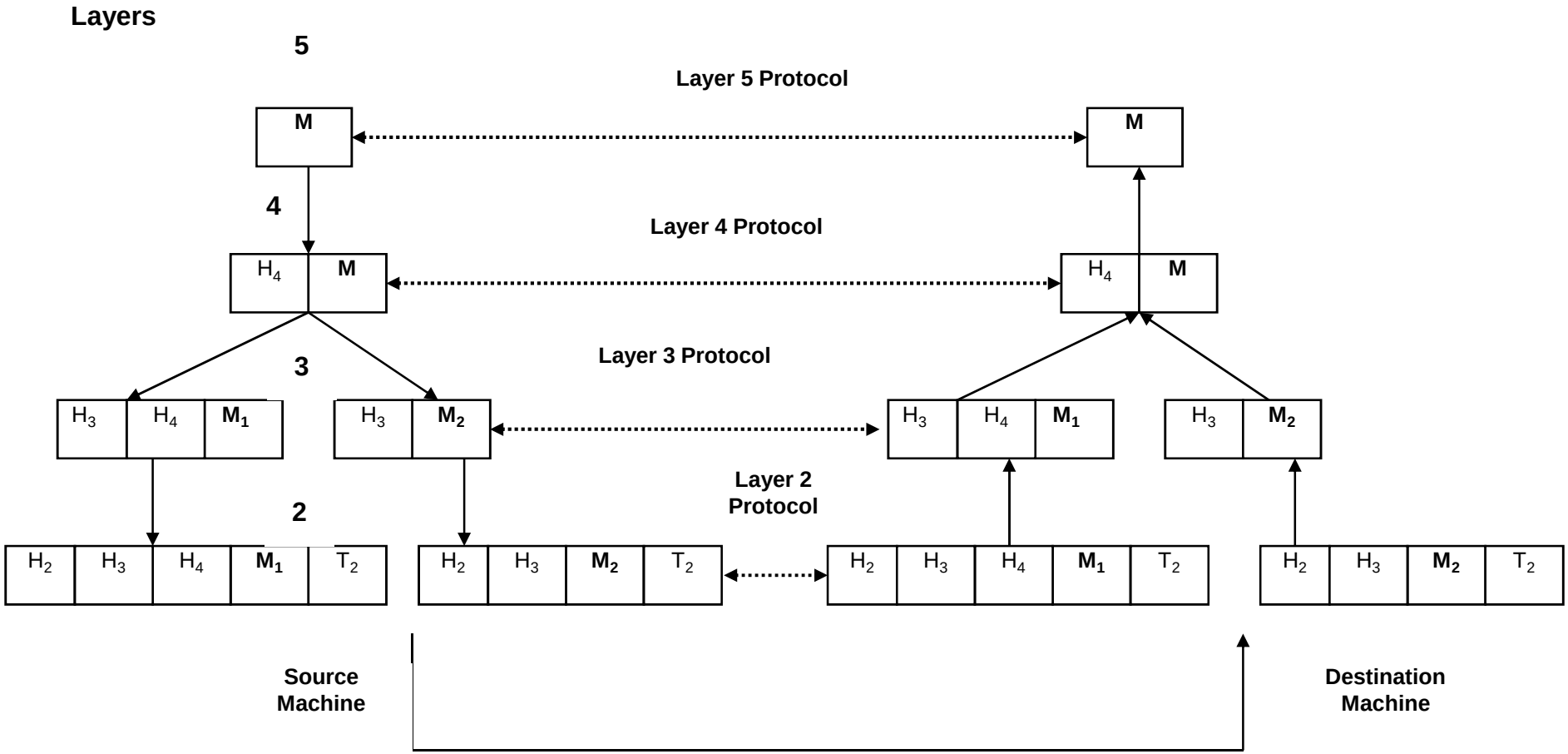
- Protocol Hierarchies
  - Between each pair of adjacent layers is an interface – defines which primitive operations and services the lower layer makes available to the upper one.
  - One of the most important considerations is defining clean interfaces between the layers. Doing so requires that each layer perform a specific collection of well-understand functions.
  - In addition to minimizing the amount of information that must be passed between layers, clear-cut interfaces also make it simpler to replace the implementation of one layer with a completely different implementation because all that is required of the new implementation is that it offer exactly the same set of services to its upstairs neighbor as the old implementation did.

Network Software

- Protocol Hierarchies
  - 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.
  - Neither the details of the implementation nor the specification of the interface is part of the architecture because these are hidden away inside the machines and not visible from the outside.
  - It is not even necessary that the interfaces on all machines in a network be the same, provided that each machine can correctly use all the protocols.
  - A list of protocols used by a certain system, one protocol per layer is called protocol stack.

Network Software

- Message Passing In 5 Layers Protocol



Network Software

- Message Passing in N Layers Protocol
  - A message M is produced by an application process of 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 contains the control information, such as sequence numbers, to allow layer 4 on the destination machine to deliver messages in the right order. Sometimes it has sizes, times, and other fields.
  - In many networks there is no limit to the size of messages transmitted in the layer 4, but there is always a limit imposed by layer 3 protocol.

Message Passing In N Layers Protocol

- So layer 3 must break up the incoming messages into smaller units, packets pretending layer 3 header to each packet. So M is split into two parts M1 and M2.
- Layer 3 decides which of outgoing lines to use and passes the packet to layer 2.
- Layer 2 adds not only header to each piece, but also trailer and gives the resulting unit to layer 1 for physical transmission.
- At receiving machine the message moves upward from layer to layer, with headers being stripped off as it progress.
- None of the headers for layers below *n* are passed up to layer *n*.

Design Issues for Layers

- Every layer needs a mechanism for identifying senders and receivers.
- Network normally has many computers some of which have multiple processes, a means is needed for a process on one machine to specify with who it wants to talk. Because of having multiple destinations, some form of addressing is needed in order to specify a specific destination.
- Another set of design decisions concerns the rules for data transfer. Some times data travel in one direction; or it can go both ways. The protocol must determine how many logical channels the connection corresponds to and what their priorities are.

Design Issues for Layers

- Many networks provide at least two logical channels per connection, one for normal data and one for urgent data.
- Error control is an important aspect of protocol design because physical communication circuits are not perfect. Many error-detecting and correcting codes are known but both ends must agree on one of them. The receiver must have some way of telling the sender which messages have been correctly received and which have not.
- Not all communication channels preserve the order of messages sent on them. To deal with possible loss of sequencing, the protocol must make provision for receiver to allow the pieces to be reassembled properly.

Design Issues for Layers

- Solution is to number the pieces. But what to do with the pieces arrived out of order.
- An issue that occurs at every level is how to synchronize the sender's and receiver's clock. To handle this protocol must have facility of feedback from the receiver to sender, either directly or indirectly about receiver's current situation. Technique is called flow control.
- Protocol must give the facility of disassembling, transmitting and then reassembling messages.

Design Issues for Layers

- When it is expensive or inconvenient to set up a separate connection for each pair of communicating processes, the layers may decide to use the same connection for multiple, unrelated conversations. As long as this multiplexing and demultiplexing is done it can be use by any layer.
- When their are multiple paths between source and destination, a route must be chosen. Sometimes this decision must be split over two or more layers. Concept is called routing.

Connection Oriented and Connectionless services

- Connection Oriented Services
  - Modeled after the telephone system, pick up phone, dial number, talk, and then hang up.
  - Similarly, to use connection oriented service, the service user first establishes a connection, uses the connection and then releases the connection.
  - Connection acts like a tube: sender pushes objects (bits) in at one end, and the receiver takes them out at the other end.
  - The order is preserved so that the bits arrive in the order they were sent.
  - In some cases when a connection is established, the sender, receiver, and subnet conduct a negotiation about parameters to be used, such as maximum message size, quality of service required, and other issues.

Connection Oriented and Connectionless services

- Connectionless Services
  - Modeled after the postal system. Each message carries the full destination address, and each one is routed through the system independent of all the others.
  - When two messages are sent to the same destination, the first one sent will be the first one to arrive.
  - However it is possible that the first one sent can be delayed so that the second one arrived first.

Connection Oriented and Connectionless services

- Each service can be characterized by a quality of service.
- Some services are reliable in the sense that they never lose data.
- Reliable service is implemented by having the receiver acknowledge the receipt of each message so the sender is sure that it arrived.
- Acknowledgement process introduces overhead and delays, which are often worth it but are sometimes undesirable. Service is appropriate in file transfer situation.

Connection Oriented and Connectionless services

- Reliable service has two variations:
  - Message Sequencing
    - The message boundaries are preserved. When two 1024 bytes messages are sent, they arrive as two distinct 1024 bytes messages, never as one 2048 byte message.
  - Byte streaming
    - The connection is simply a stream of bytes, with no message boundaries.
    - When 2048 bytes arrive at the receiver, there is no way to tell if they were sent as on 2048 byte message or two 1024 byte messages.

Connection Oriented and Connectionless services

- Not all applications require connections. Nor is 100 percent reliable delivery essential, especially if it costs more. All that needed is a way to send a single message that has a high probability of arrival, but no guarentee.
- Unreliable (meaning not acknowledged) connectionless service is often called datagram service, in analogy with telegram service, which does not return an acknowledgement to sender.
- In other situations, the reliability becomes essential. The acknowledged datagram service can be provided for these applications. It is likely sending a registered letter and requesting a return receipt.

Connection Oriented and Connectionless services

- Another service is the request-reply service. Here the sender transmits a single datagram containing a request; the reply contains the answer.
- Commonly used to implement communication in the client-server model; the client issues a request and the server responds to it.

Connection Oriented and Connectionless services

- Why would anyone actually prefer unreliable communication to reliable communication?
  - First of all, reliable communication may not be available. Packets are occasionally be damaged in transit. It is upto higher protocol levels to deal with this problem.
  - Second, the delays inherent in providing a reliable service may be unacceptable, especially in real-time applications such as multimedia.
  - For these reasons, both reliable and unreliable communication coexist.

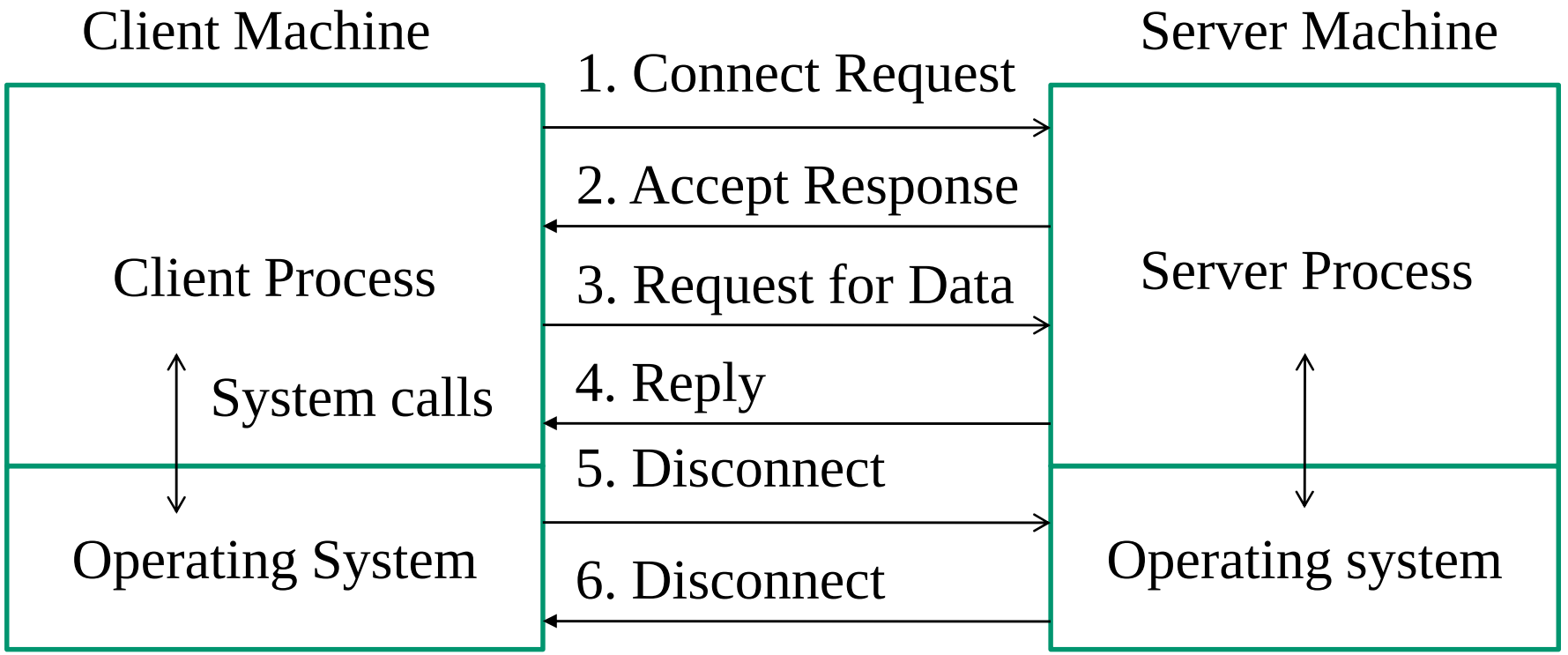
Service Primitives

- A service is specified by a set of primitives (operations) available to a user process to access service. 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, the primitives are normally system calls – cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets.
- The set primitives available depends on the nature of the service being provided.

Service Primitives

- The primitives for connection oriented service are different from those of connectionless service.
- Five service primitives for implementing a simple connection oriented service are listed as below
  - Listen: Block waiting for an incoming connection
  - Connect: Establish a connection with a waiting peer
  - Receive: Block waiting for an incoming message.
  - Send: Send a message to the peer
  - Disconnect: Terminate a connection

Service Primitives



Service Primitives

- Primitives are used as follows: - First server executes LISTEN to indicate that it is prepared to accept incoming connections. A common way to implement LISTEN is to make it a blocking system call. After execution the server process is blocked until a request for connection appears.
- Next the client process executes CONNECT to establish a connection with the server. The CONNECT call needs to specify who to connect to, so it might have parameter giving the server's address. The operating system then typically sends a packet to the peer asking it to connect.

Service Primitives

- The client process is suspended until there is a response. When packet arrives at the server, it is processed by the operating system there. When the system sees that the packet is requesting a connection, it checks to see if there is a listener. If so,it does two things: unblocks the listener and sends back an acknowledgement. The arrival of this acknowledgement then releases the client. At this point the client and server are both running and they have connection established.

Service Primitives

- The next step is for the server to execute RECEIVE to prepare to accept the first request. Normally, the server does this immediately upon being released from the LISTEN, before the acknowledgement can get back to the client. The RECEIVE call blocks the server.
- Then the client executes SEND to transmit its request followed by the execution of RECEIVE to get the reply.
- The arrival of the request packet at the server machine unblocks the server process so it can process the request. After it has done the work, it uses SEND to return the answer to client. The arrival of this packet unblocks the client, which can now inspect the answer.

Service Primitives

- If it is done, it can use DISCONNECT to terminate the connection. Usually, an initial DISCONNECT is a blocking call, suspending the client and sending a packet to the server saying that the connection is no longer needed.
- When the server gets the packet, it also issues a DISCONNECT of its own, acknowledging the client and releasing the connection. When the server's packet gets back to the client machine, the client process is released and the connection is broken.

Relationship of Services to Protocol

- The service is set of primitives 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.

Relationship of Services to Protocol

- 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. They are free to change their protocols at will, provided they do not change the service visible to their users.
- In other words, services relate to the interfaces between layers. In contrast, protocols relate to the packets sent between peer entities on different machines.

Relationship of Services to Protocol

- A service defines operations that can be performed on an object but does not specify how these operations are implemented.
- A protocol relates to the implementation of the service and as such is not visible to the user of the service.

References

- Andrew S. Tanenbaum, Computer Networks, Pearson Education. [4th Edition]
- Andrew S. Tanenbaum, David J. Wetherall, Computer Networks, Pearson. [5th Edition]
- Behrouz A. Forouzan, Data Communications and Networking, Tata McGraw Hill. [4th Edition]