

Computer Network (CSE 3034)

Text book: Computer Networks by Andrew S. Tanenbaum

Introduction to the course

Syllabus :

- Introduction(Chapter 1)
- The Physical Layer(Chapter 2)
- The Data Link Layer(Chapter 3)
- The Medium Access Control Sublayer(Chapter 4)
- The Network Layer(Chapter 5)
- The Transport layer(Chapter 6)
- The Application layer(Chapter 7)
- Network security(Chapter 8)

Introduction

What is Computer Network?

S'O'A ITER

Computer Network :

- Formed by merging of **computers** and **communication technology**.



Computation/processing of data



Exchange of information

- Collection of autonomous computers interconnected by a single technology to carry out computation/processing of data and exchange of information.
- Wired (or cabled), Wireless
- Internet (Network of networks)
- Though looks same computer network is different from a **distributed system**.

- Copper wire
- Fibre optics
- Microwave

Distributed System :

- *High degree of cohesiveness and transparency*
- A software system built on top of a network

WWW a distributed systems run on the top of Internet.

Uses of Computer Network

- Business Applications
- Home Applications
- Mobile Users
- Social Issues

Uses of Computer Network (cont.)

Business Applications

Goals of Networks in this application :

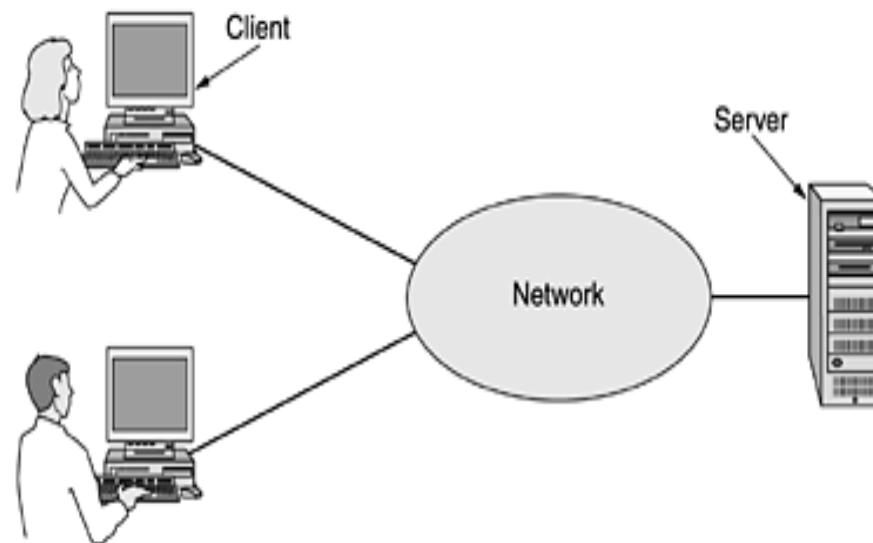
- *Resource sharing* : Programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource and the user
 - Ex: (i) Sharing of physical equipment like printer, CD burner, etc.
 - (ii) Sharing of customer records, inventories, accounts, financial statements, etc.
- *Establish a computer-assisted communication between individuals.*
 - Ex : (i) Electronic mail (i.e. e-mail).
 - (ii) VoIP (i.e. Voice over internet Protocol) /Videoconferencing.
- *Doing business electronically.*
 - Ex : E-commerce
 - Individual - company
 - Company - company

Uses of Computer Network (cont.)

Business Applications

Structure :

- The establishment varies from a single office in a single building to dozens of offices scattered over more than one place.
- Configured in the form of **client-server** model.



A network with two clients and one server

Server :

- Powerful computer where most of the data associated with an organization/company are stored.
- Physical equipment that is shared is also connected to the server system.
- Maintained by a system administrator.

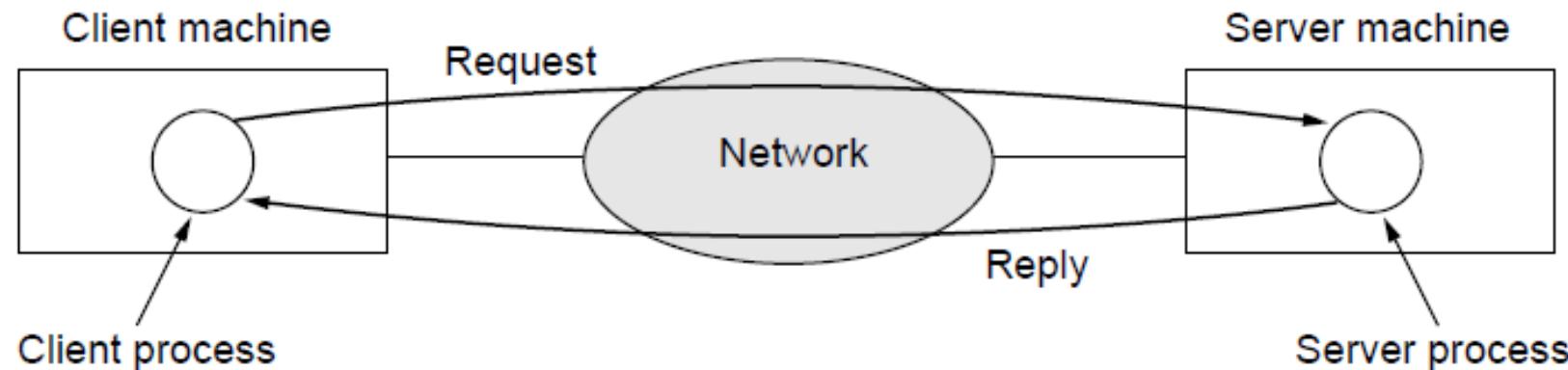
Client :

- Simpler computer systems used by employees of an organization/company/individual being connected to the same network.

Uses of Computer Network (cont.)

Business Applications

Communication in client – server model :



Client process : Sending message over the network to server & waits reply from server

Server process : Performs the requested work or looks up the requested data and sends back a reply to client.

Uses of Computer Network (cont.)

Home Applications

In 1977 Ken Olsen, President,

Digital Equipment Corporation (DEC), Second Largest Computer Company
(after IBM) said

“There is no reason for any individual to have a computer in his home”
(Initially for word processing)

Now : Why do people buy computers for home use?

Biggest Reason is Internet access.

Uses of Computer Network (cont.)

Home Applications

Popular uses of the **internet access** for home users :

- Access to remote information
- Person to person communication
- Interactive entertainment
- Electronic commerce

Uses of Computer Network (cont.)

Home Applications

Internet access for home users : Access to remote information

- Surfing the web is done for variety of reasons:
 - Arts, Business, Cooking, Government, Health, History, Hobbies, Recreation, Science, Sports, Travel, ...
- E-Newspaper
- Online Digital Libraries (magazines/journal)
(e.g. www.ieee.org)

Uses of Computer Network (cont.)

Home Applications

Internet access for home users : Person – to – person communication

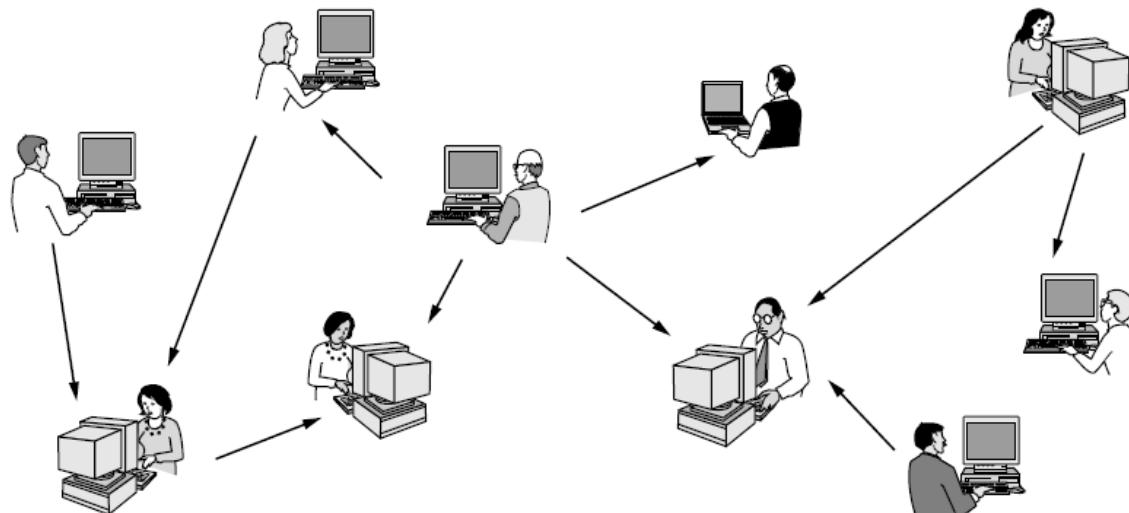
- Video conferencing/chating
- Instant Messaging (Whats app,Twitter)
- Telelearning
- Social Networking:
 - Facebook

Person - to – person communication often goes by the name of peer - to - peer communication

Uses of Computer Network (cont.)

Home Applications

Peer – to – peer communication (different from client –server model)



Example :

- BitTorrent
- Sharing Music and Videos (Napster)
- Email, etc.

In a peer-to-peer system there are no fixed clients and servers.

Uses of Computer Network (cont.)

Home Applications

Internet access for home users : Interactive entertainment

- MP3 and DVD-quality movies
- TV shows – IPTV (IP TeleVision)
- Interactive Live TV
- Multiperson real-time simulation games
- Smart Home Monitoring

Uses of Computer Network (cont.)

Home Applications

Internet access for home users : Electronic commerce

- Online shopping from home
- Online consultation about product with support team
- Payment of bills
- Managing bank accounts and financial investments
- Online auction of second hand goods – in the form of peer to peer system

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on-line
P2P	Peer-to-peer	File sharing

Some forms of e-commerce

Uses of Computer Network (cont.)

Mobile Users

- Mobile computers (handheld and laptops)
 - Fastest growing segments in computer history.
 - Individuals are able to use their mobile devices to:
 - Read and send email,
 - Tweet,
 - Watch Movies,
 - Download Music,
 - Play Games,
 - Surf the Web
- Internet connectivity allows for those applications to be easily built
 - Wireless Networks (Cars, Boats, and Airplanes can not have wired Connections)
 - Cellular Networks
 - Wireless hotspots (802.11 Standard).
 - Wireless Networking vs. Mobile Wireless Networks

Uses of Computer Network (cont.)

Mobile Users

S'0'A ITER

Combinations of wireless networks and mobile computing

Wireless	Mobile	Typical applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in unwired buildings
Yes	Yes	Store inventory with a handheld computer

Uses of Computer Network (cont.)

Mobile Users

- Smart Phones – Integration of Internet with Telephony
 - Driving the wireless-mobile applications
 - 3G & 4G cellular networks provides fast data services
 - GPS is a standard feature
 - m-commerce (mobile commerce)
- Sensor Networks
 - Notes that Sense/gather data about state of the physical world.
 - It is revolutionizing science
- Wearable Computers
 - Implantable Devices
 - Pacemakers, Insulin pumps, ...
 - Controllable wirelessly

Network Hardware

There is no generally accepted taxonomy into which all computer networks fit, but two dimensions stand out as important: **transmission technology** and **scale**.

Transmission technology : Two types of transmission technology are in widespread use.

1. Broadcast links.
2. Point to point links.

Network Hardware(cont.)

Broadcast network

- Single communication channel that is shared by all the machines connected to the network.
- Messages (in the form of **packets**) sent by one machine are received by all other machines belonging to the network.
- 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.
- **Multicast** : Transmission to a subset of machines



Broadcast transmission

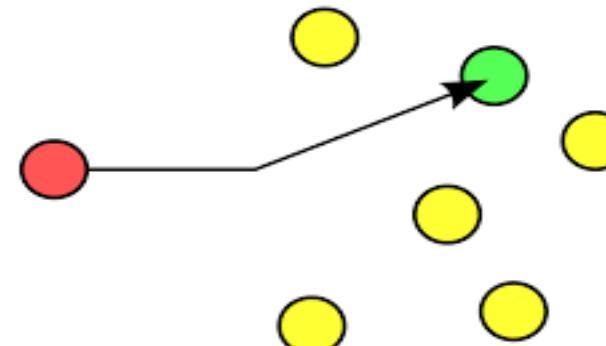


Multicast transmission

Network Hardware (cont.)

Point to point network

- Multiple individual pairs of machine communicate with each other.
 - Single hop : Directly, One route
 - Multi hop : Through one/more intermediate machines, Multiple routes possible
(Finding good one is important)
- Intermediate machines only forward the data packets from source to destination.
- **Unicast transmission**



Unicast transmission

Network Hardware (cont.)

Classification of network based on size of the network:

- Computer networks are also classified based on the **size**, **no. of machines** and **distance** among **machines** of a network.

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Networks (WAN)
- The internet

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

Classification of interconnected processors by scale

Network Hardware (cont.)

Local Area Networks (LANs):

- Privately owned
- Established within a single building or campus
- Widely used to connect personal computers and workstations in company offices and factories for share resources (e.g., printers) and exchange information.

Characteristics based on which different from other networks

(1) **Size** : Restricted and small

(2) **Transmission technology** :

Medium of communication : Mostly use **co-axial cable**

Speed : **10 Mbps to 100 Mbps**

Delay : low (**microseconds/nanoseconds**)

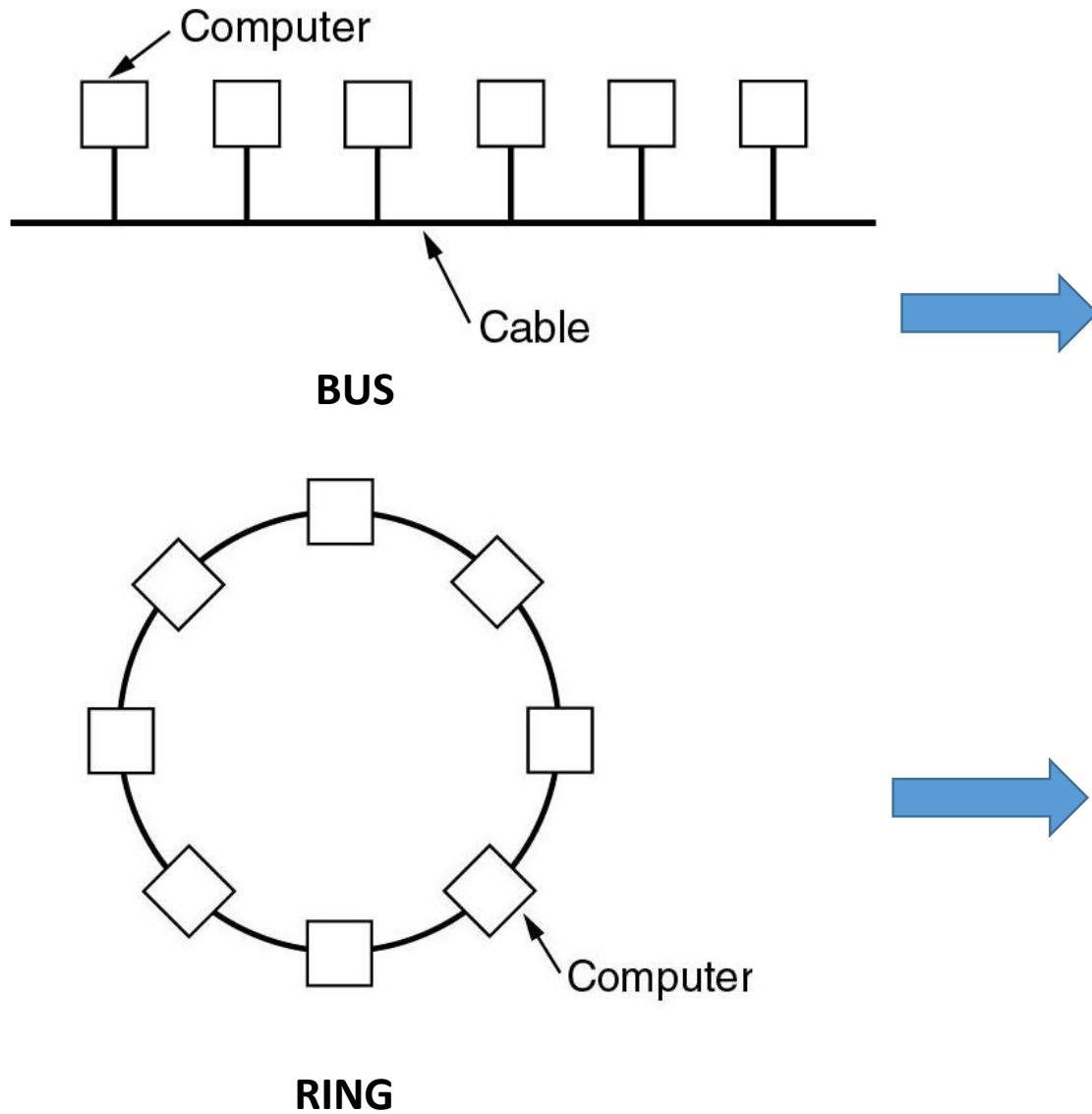
Transmission error : **Less**

(3) **Topology** : BUS , RING, STAR, MESH.

Network Hardware (cont.)

S'O'A ITER

Local Area Networks (LANs):



- At any instant at most one machine is the master and is allowed to transmit.
- Conflicts may occur when two or more machines try to transmit simultaneously.
(Requires proper arbitration mechanism)
- Ex : Ethernet (or IEEE 802.3)

- Each bit propagates around on its own, not waiting for the rest of the packet to which it belongs.
 - Each bit circumnavigates the entire ring.
 - Conflict due to simultaneous accesses to the ring can be avoided by arbitration mechanism.
- Ex : IEEE 802.5 and FDDI

Network Hardware (cont.)

Local Area Networks (LANs):

Categorized as **static or dynamic** based on the channel allocation strategy among the users wants to transmit their data.

Static :

- ❖ Uses a **round-robin algorithm** (i.e. each machine is allowed to broadcast only when its time slot comes up)
- ❖ Wastage of channel capacity (a drawback)

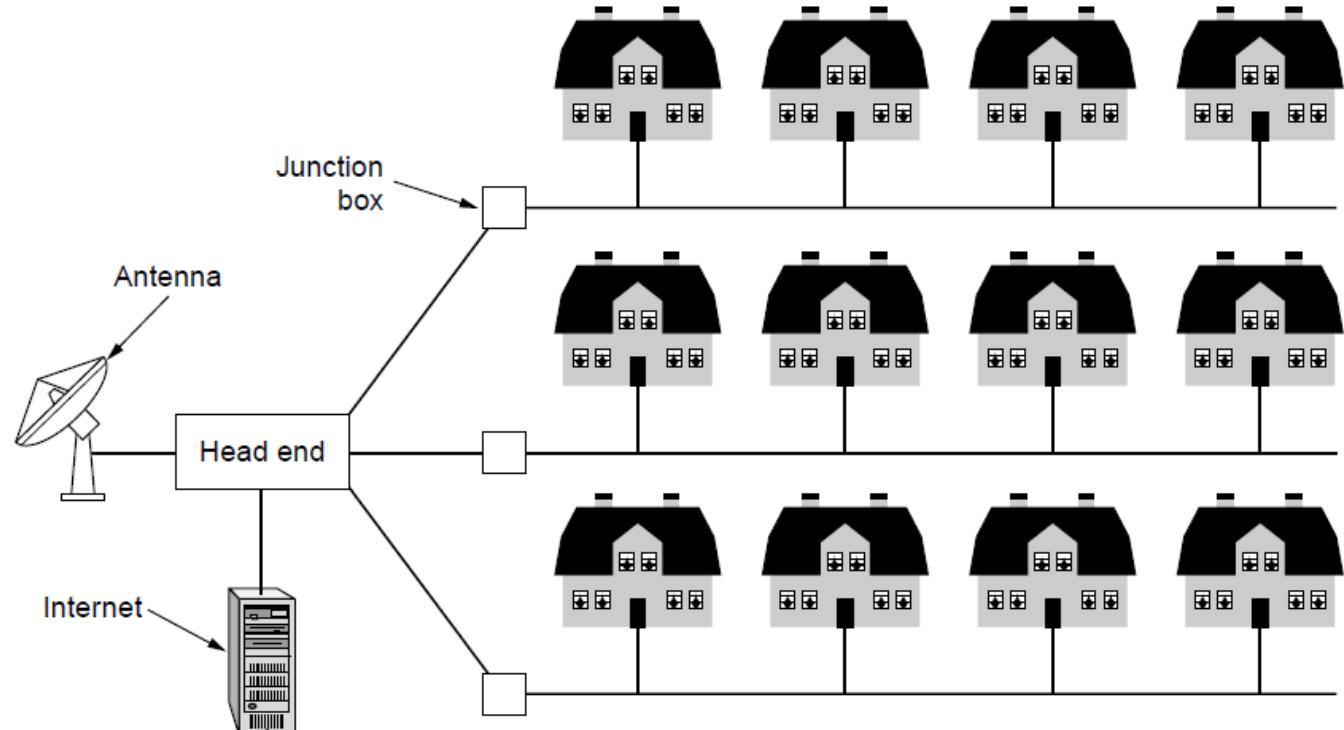
Dynamic :

- ❖ Centralized (**a bus arbitration unit used to determine who goes next**)
- ❖ Decentralized (each machine must decide for itself whether to transmit)

Network Hardware (cont.)

Metropolitan Area Network (MAN)

- Covers a city
- Ex : Cable television network
 - (Initially for TV signal transmission, currently for internet along with TV transmission)
- Concept : A large antenna was placed on top of a nearby hill or big building and then signal is piped to the subscribers' houses.



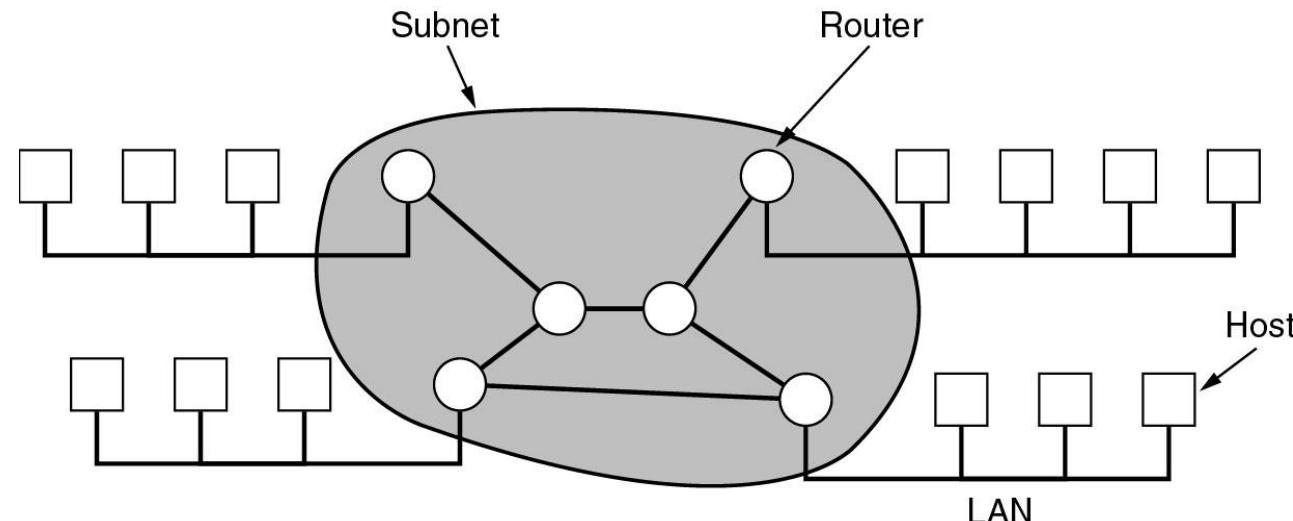
A metropolitan area network based on cable TV

Network Hardware (cont.)

S'0'A ITER

Wide Area Network (WAN)

- Spans a large geographical area, often a country or continent.
- Establish communication link between two machines (say **host computers**) belonging to two different networks.
- Major constituents of such a network
 - **Host** : Owned by customers
 - **Communication subnet** : Owned by the network service providers



Relation between hosts on LANs and the subnet

Network Hardware (cont.)

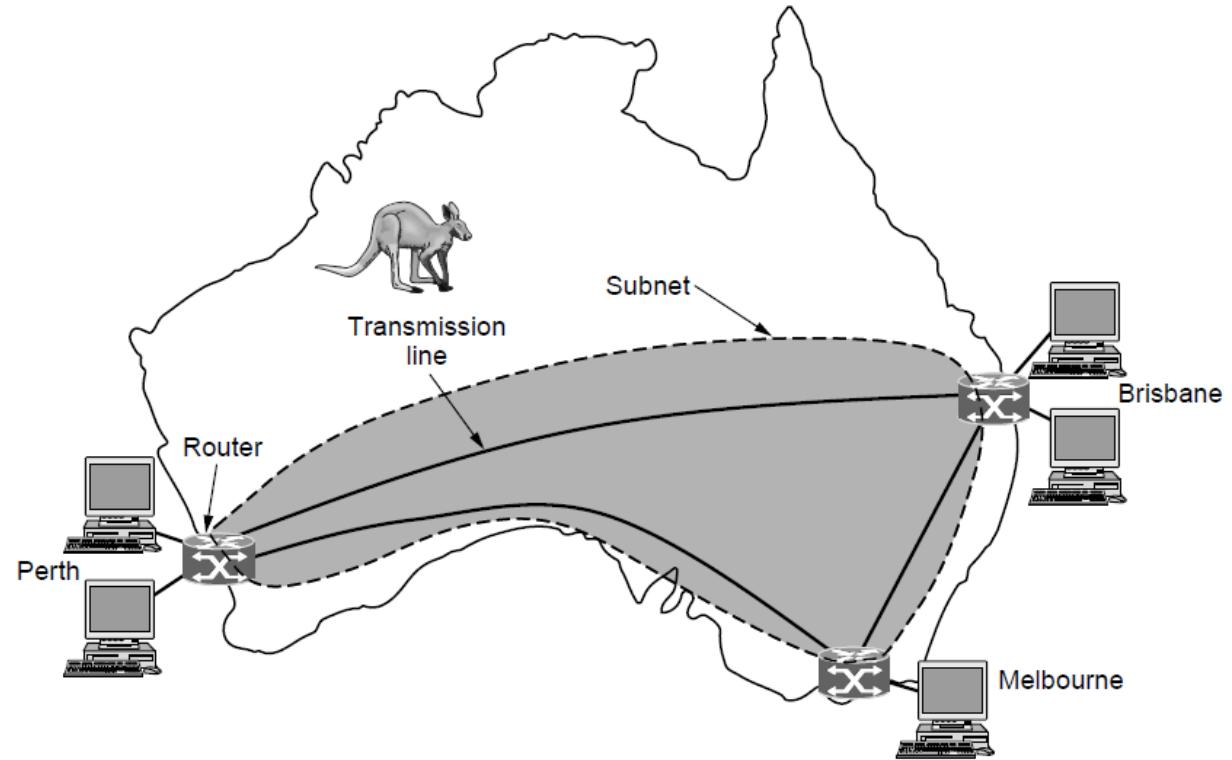
S'0'A ITER

Wide Area Network (WAN)

Subnet :

Comprises of two components.

- **Transmission lines :**
 - Used to move data packets between two machines
(Copper wire, optical fiber)
- **Switching elements :**
 - Popularly known as routers.
 - Connect more than two transmission lines.
 - Store -and-forward.



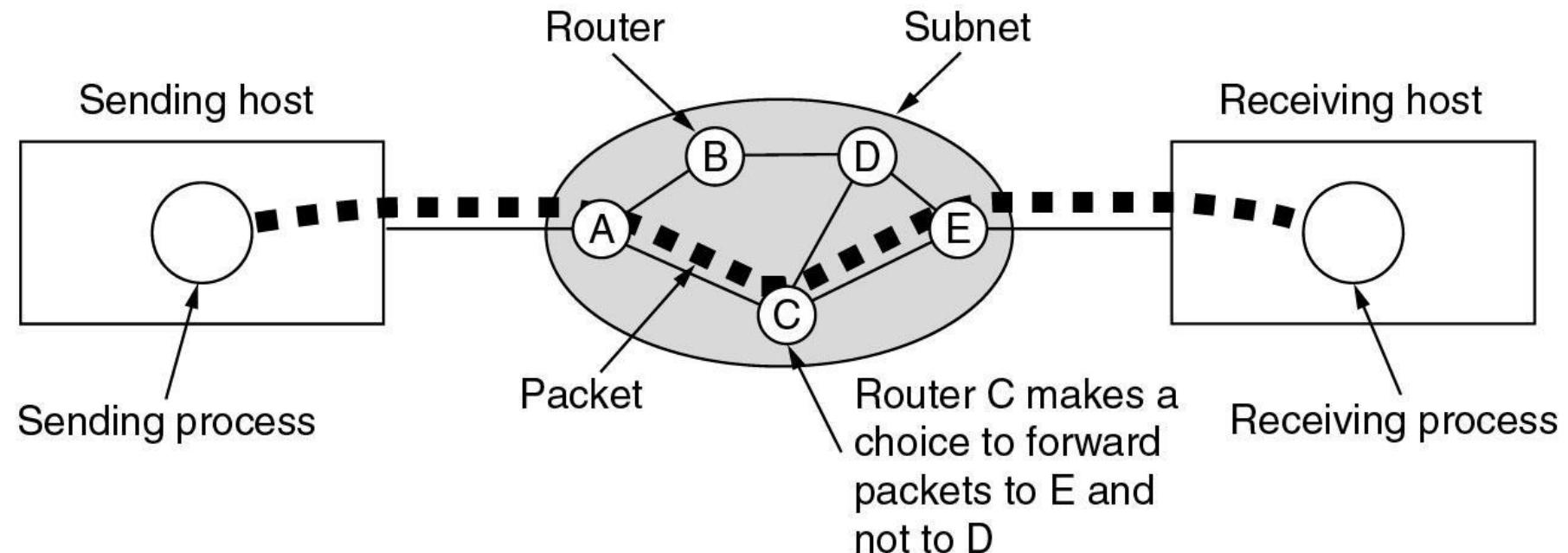
WAN that connects three branch offices in Australia

Network Hardware (cont.)

Wide Area Network (WAN)

The **WAN** often also referred as **packet switched network**, since the packets in the network are moved from one transmission line to other through the switching element (or router).

An example :



- Routing decisions are made locally.
- How A makes that decision is called the routing algorithm.

(Instead of ABDE it is ACE)

Network Hardware (cont.)

Wireless network

- Transmission line : Wireless (or radio channel)
- Wireless networks can be divided into three main categories:
 1. System interconnection.
 2. Wireless LANs.
 3. Wireless WANs.

Network Hardware (cont.)

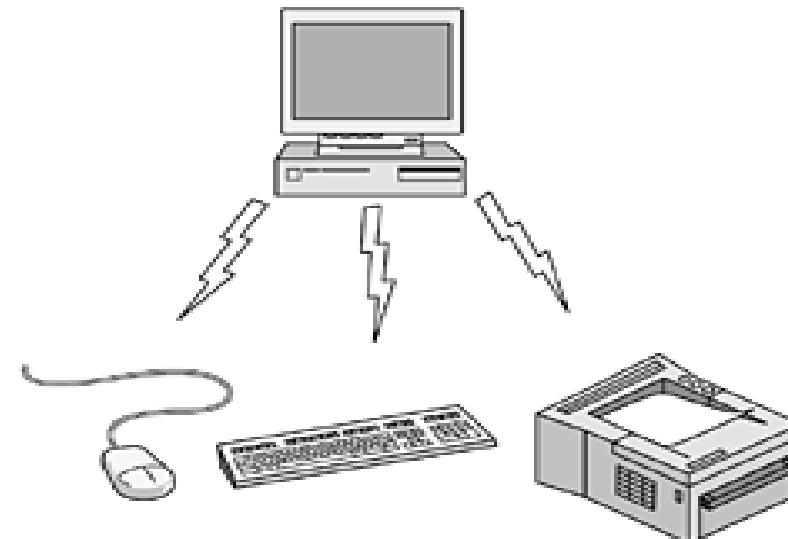
Wireless network

System interconnection :

- Uses **short range radio communication** technology (e.g. Bluetooth) to make interconnection between different digital machines in a room.
- Can be referred as a **PAN**.

Example:

A computer CPU and its subordinates like mouse, keyboard and monitor can be connected through a bluetooth based network system.



A Bluetooth configured network

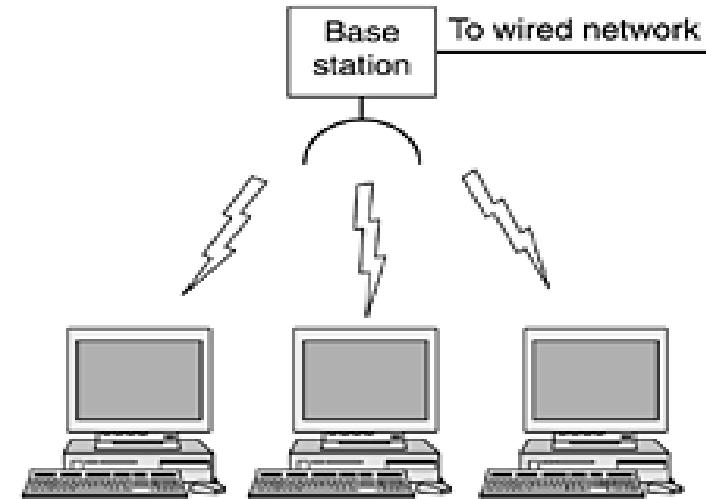
Network Hardware (cont.)

Wireless network

Wireless LANS :

- Every computer/computing machines should have a **radio modem and antenna**.
- Requires a **base station**.
- Follows the standard IEEE 802.11

Example : Offices, Hostels, Conference rooms etc.



An example of Wireless LAN

Wireless network

Wireless WANS :

- Structure is same as WLAN except to geographical area of coverage (quite a more than that in WLANs)
- Lesser speed than WLANs.
- Distance between base station and computing device is more than that in WLANs.

Example : Cellular networks (3G & 4G) meant for both voice and data.

High bandwidth wireless MANs are also being available in certain cities. A standard for it, called IEEE 802.16, has also been developed.

Note : Almost all wireless networks hook up to the wired network at some point to provide the internet service.

Network Hardware (cont.)

Home network

- Properly not categorized as a form of computer network.
- Smart home and IoT (a possibility).
- Requires smart devices that are capable to communicate with each other and (or) access internet.

Examples of smart devices in home :

1. Computers (desktop PC, notebook PC, PDA, shared peripherals).
2. Entertainment (TV, DVD, VCR, camcorder, camera, stereo, MP3).
3. Telecommunications (telephone, mobile telephone, intercom, fax).
4. Appliances (microwave, refrigerator, clock, furnace, airco, lights).
5. Telemetry (utility meter, smoke/burglar alarm, thermostat, babycam).

Network Hardware (cont.)

Home network

Home networking has some fundamentally different properties than other network types.

- The network and devices have to be easy to install.
- The network and devices have to be fool proof in operation.
- Low price is essential for success.
- The main application is likely to involve multimedia, so the network needs sufficient capacity.
- It must be possible to start out with one or two devices and expand the reach of the network gradually.
- Security and reliability will be very important.

Network Software

The network software structure plays an important role in the operation of the network.

- Protocol hierarchies
- Design issues for the layers
- Connection-oriented versus connectionless service
- Service primitives
- Relationship of services to protocols

Network Software

Protocol Hierarchies

- A stack of layers or levels, each one built upon the one below it.
- Number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- Lower layer provides service to higher layers.
- interaction/conversation between **n** layer of a machine with **n** layer of another machine carried following a **set of rules and convention** (normally known as **protocol**).

Network Software (cont.)

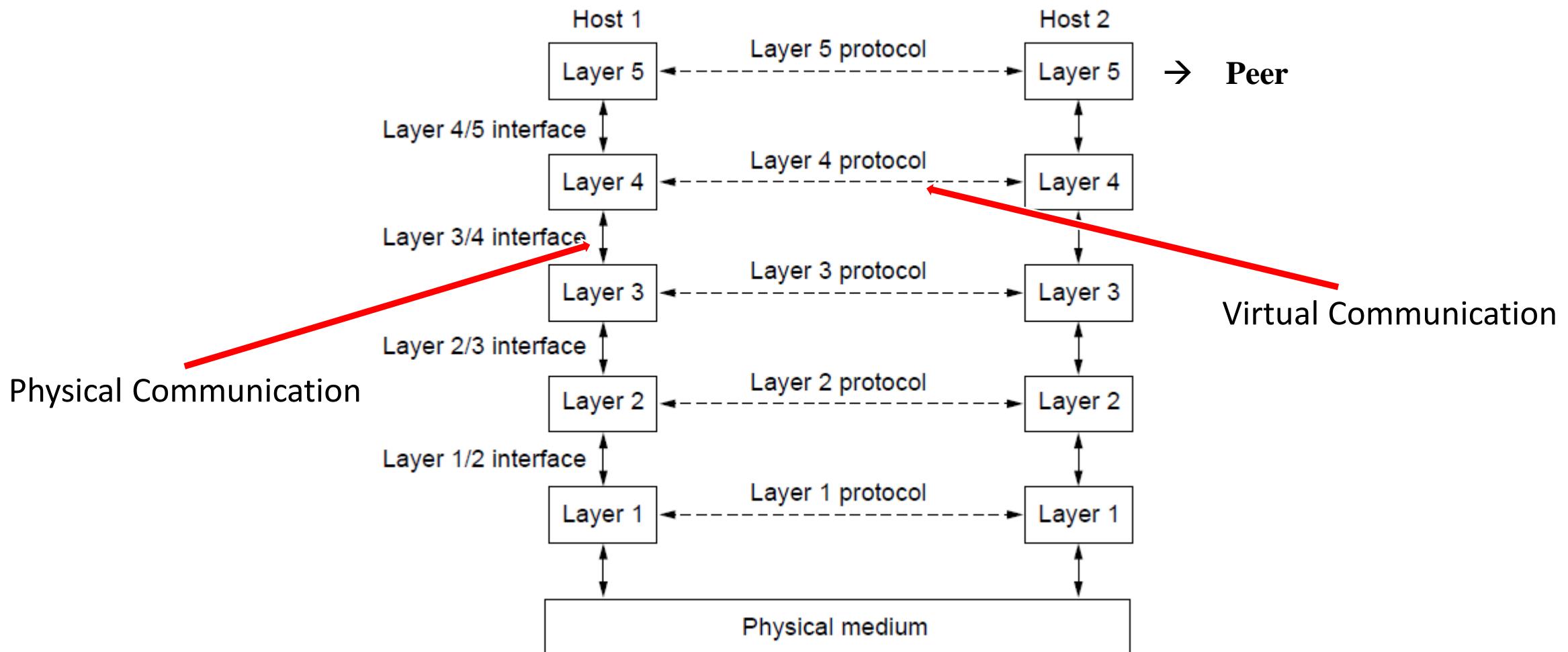
Protocol Hierarchies

- **Protocol** – An agreement between the communicating parties on how communication is to proceed.
- **Peers** – Entities comprising corresponding layers on different machines (e.g. hardware devices).
 - Peers use the protocol to communicate with each other.
- **No data is directly transferred from layer n on one machine to layer n on another machine.**
 - 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.
 - Between each pair of adjacent layers is an interface
- **Interface** - It defines which primitive operations and services the lower layer makes available to the upper one.

Network Software (cont.)

S'0'A ITER

Protocol Hierarchies



Layers, protocols, and interfaces in a network

Network Software (cont.)

Protocol Hierarchies

Layering

- ⇒ To make things simple: modularization container
- ⇒ Different layer has different functions
- ⇒ Create layer boundary such that
 - **description of services can be small**
 - **number of interactions across boundary are minimized**
 - **potential for interface standardized**
- ⇒ Different level of abstraction in the handling of data (e.g., syntax, semantics)
- ⇒ Provide appropriate services to upper layer
- ⇒ Use service primitives of lower layer

Network Software (cont.)

Protocol Hierarchies

➤ Network Architecture:

- A set of layers and protocols.
- The specification of the network architecture must contain enough information to allow an implementation of the program or the hardware for each layer so that it will obey appropriately the protocol.

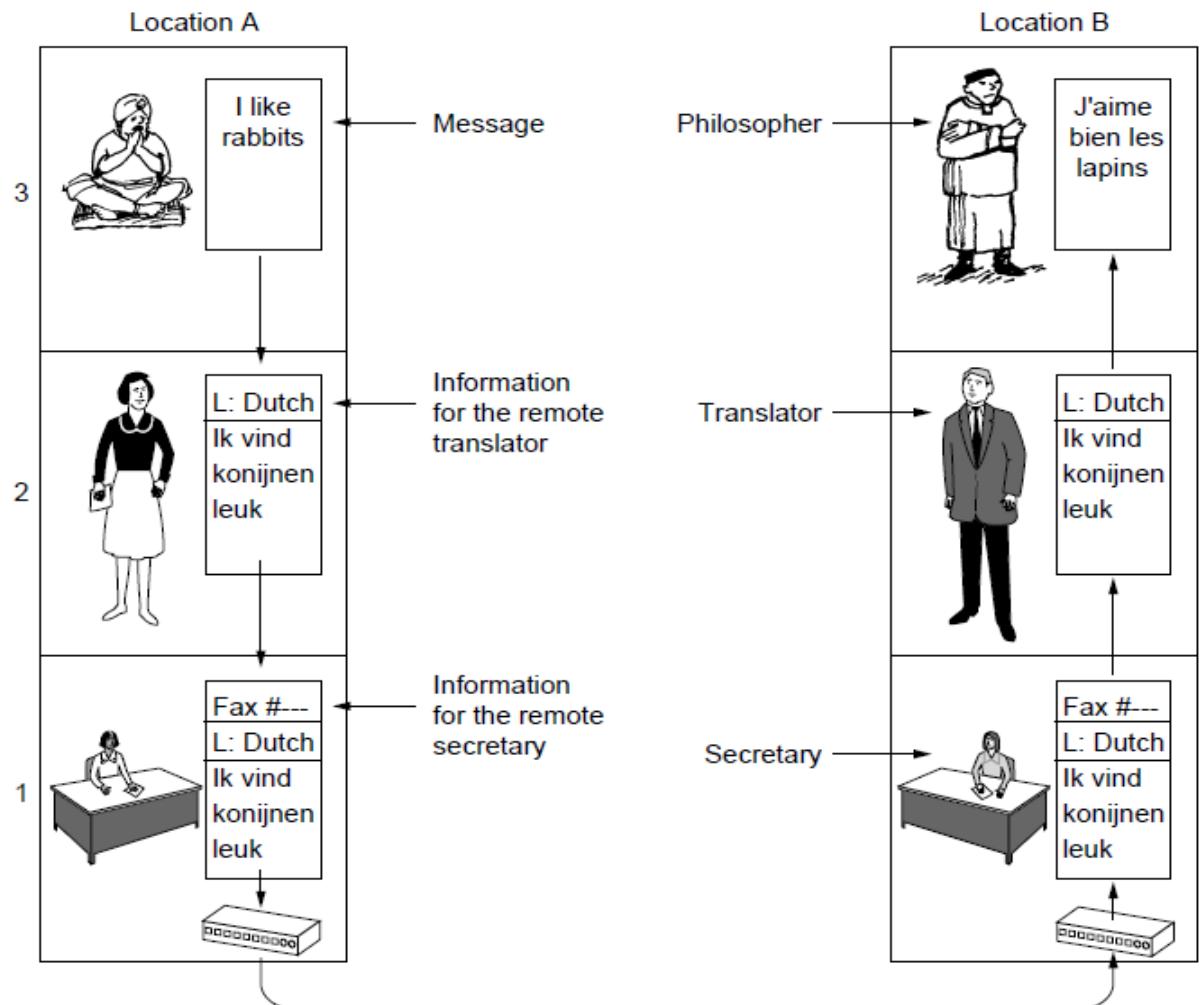
➤ Protocol Stack:

- The list of protocols used by a certain system – one protocol per layer.

Network Software (cont.)

Protocol Hierarchies

An analogy example:



Layer3 :

Two philosophers having no common language want to communicate with each other.

Layer2:

Each philosophers engages a translator.

Layer1:

Each translator takes the help of a secretary to transmit the message using the medium (e.g. Fax).

Note : Each protocol is completely independent of each other as long as interfaces are not changed.

(e.g. in layer1 the medium can be a telephone call or e-mail without the notice of translator)

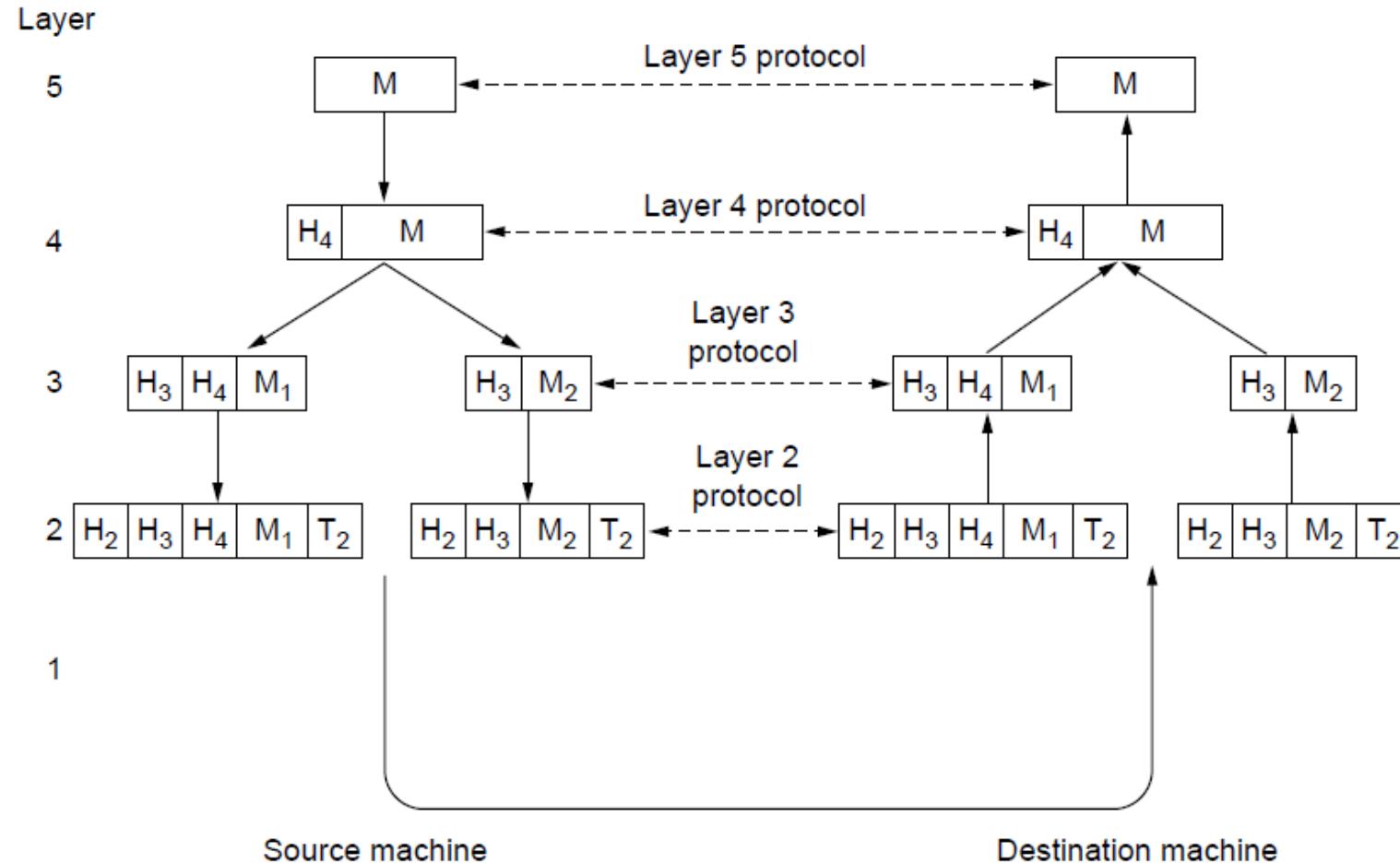
The philosopher-translator-secretary architecture

Network Software (cont.)

Protocol Hierarchies

S'0'A ITER

A technical example:



Example information flow supporting virtual communication in layer 5.

Network Software (cont.)

Protocol Hierarchies

S'0'A ITER

Illustration of technical example:

Let a message 'M' produced in **layer 5** in source machine is to be transmitted to **layer 5** in destination machine.

Step 1 : Message 'M' from layer 5 given to layer 4.

Step 2 : In layer 4 a **header** (i.e. control information like sequence number) is added in front of the message and then given to layer 3. **No restriction in size of message.**

Step 3 : In layer 3 (if required) the message gets broken into small packets along with the prepend of layer 3 header to each packet following which the packets passed to layer 2. **Restriction in size of message.**
(In the picture the message 'M' is divided into 'M₁' and 'M₂' .)

Step 4 : Layer 2 adds not only a header to each piece, but also a trailer, and gives the resulting unit to layer 1 for physical transmission.

At the receiving machine the message 'M' moves upward from layer to layer, with headers being stripped off as it progresses.

The peer process abstraction is crucial to all network design.

Level 4 protocol conceptually think of their communication as being "horizontal":

SendToOtherSide or **GetFromOtherSide** even though these procedures actually communicate with lower layers across the 3/4 interface, not with the other side.

Network Software (cont.)

Key design Issues for the Layers

Addressing : Multiple computers and processes: addressing

- Identify senders and receivers (Ex : telephone number, e-mail address, IP address,...)

Error Control : Physical communication medium is not ideal : possibility of error at the receiving end

- error detection
- error correction

Flow control : A fast sender can communicate with slow receiver : proper handshaking before data transmission.

- feedback/acknowledgement from the receiver
- agreed upon transmission rate

Multiplexing and Demultiplexing : Scarcity of separate channels for each source destination pair in the network.

- Multiplexing at one(i.e. transmitting) end
- De-multiplexing at other(i.e. receiving) end

Routing : Possibility of multiple paths between source and destination: appropriate route using suitable routing algorithm

- High level: London -> France or Germany -> Rome
- Low level: many available circuits

Network Software (cont.)

Other design Issues for the Layers

Reliability:

- Network must operate correctly although it is made up of a collection of components that are themselves unreliable.

Protocol Layering:

- Networks grow larger over time and new designs emerge that need to connect to the existing networks.

Scalable:

- Designs that continue to work well when the network gets large.

Congestion:

- The problem may occur when the network is oversubscribed because too many computers want to send too much traffic and the network will not be able to deliver them all.
- Overloading problem of the network.
- One strategy is for each computer to reduce its demand.

Quality of Service:

- Additional Resources (other than Bandwidth),
- Real-time delivery (for applications that require high throughput),
- Live Video,

Network Security:

- How good is the network against different kinds of threats

Network Software (cont.)

S'OA ITER

Connection-Oriented and Connectionless Services

- Layers can offer two different types of service to the layers above them.
 - Connection-oriented
 - Connectionless
- Importance : Quality of service in terms of **reliability**.
- Reliability :
 - Accompanies an acknowledgement from the receiver to the sender after reception ensuring the information transmitted has not been lost.
 - In certain cases the unreliable service is also acceptable since acknowledgment introduces overhead and delays.

Connection-Oriented Service

- Modeled after telephone system: Pickup-the-phone, Dial the number, Talk, Hang-up
- In connection oriented service
 - Establishes a connection,
 - Uses a connection (sender pushes objects in at one end and the receiver takes them out at the other end).
 - Releases the connection
 - In some cases when connection is established, the sender, receiver, and a subnet conduct a negotiation about the parameters to be used:
 - Maximum message size,
 - Quality of service required
- Can be used in both **reliable** and **unreliable** form depending on requirement.

Network Software (cont.)

Connection-Oriented Service

- Reliable connection-oriented service: Two forms
 1. Message Sequences
 2. Byte Streams
- Message Sequences:
 - Message boundaries are preserved.
 - Example: Two 1024 byte messages are sent, they arrive as two distinct 1024-byte messages; Never as one 2048-byte message.
- Byte Streams:
 - Message is send as a stream of bytes with no concepts of message boundaries.
 - Example: When a 2048-byte message arrives at the receiver there is no way to tell if they were sent as
 - One 2048-byte message,
 - Two 1024-byte message, or 2048 1-byte messages.
- Unreliable connection-oriented service:
 - It is preferable for telephone users to hear a bit of noise on the line from time to time than to experience a delay waiting for acknowledgements.
 - Example : Digital voice transmission

Network Software (cont.)

Connectionless Service

- Modeled after a postal system.
 - Each message carries the full destination address
 - Each one is routed through the intermediate nodes inside the system independent of all the subsequent messages.
 - Possibility of arrival of second message prior to first message at the receiving end.
- Mostly used in unreliable form.
- Popularly known as **datagram** service.
 - Analogous to telegram service
 - Common example : E-mail
- Certain scenario appreciate acknowledgement from the receiver.

Connectionless Service

- Unreliable connectionless service :
 - The sender of such kind of messages does not worry for acknowledgement from the receiver.
 - Example : Junk e-mail
- Acknowledgement based connectionless service :
 - The sender in this service can be acknowledged by the receiver.
 - Example : Registered mail
- Request-reply connectionless service :
 - The sender transmits a single datagram containing a request; the reply contains the answer.
 - Example : Answering to queries through mail

Network Software (cont.)

Summary of connection oriented and connectionless service

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
Connection-less	Unreliable connection	Digitized voice
	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Six different types of services offered by network layers

Network Software (cont.)

Service primitives

- Set of **primitives (operations)** available to a user process to access the service.
- Primitives for connection-oriented service are different from those of connectionless service.

Example : Minimum service primitives required to implement a reliable byte stream in a client-server environment

Primitive	Meaning
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

Network Software (cont.)

Service primitives

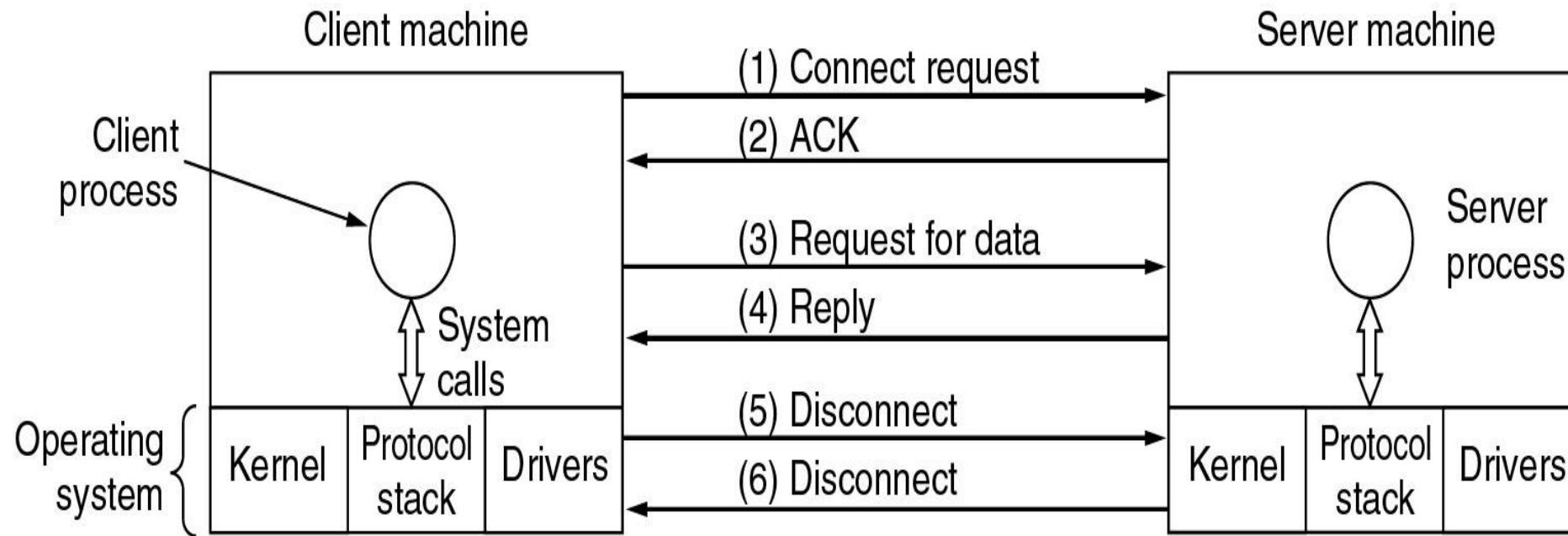
- First, the server executes **LISTEN** to indicate that it is prepared to accept incoming connections. After executing the primitive, the server process is blocked until a request for connection appears.
- Next, the client process executes **CONNECT** to establish a connection with the server. The client process is suspended until there is a response.
- The next step is for the server to execute **RECEIVE** to prepare to accept the first request.
- Then the client executes **SEND** to transmit its request followed by the execution of **RECEIVE** to get the reply.
- After receiving the reply from server, If the client has additional requests, it can make them now. If it is done, it can use **DISCONNECT** to terminate the connection.

Network Software (cont.)

S'0'A ITER

Service primitives

If the protocol stack is located in the operating system, the primitives are normally system calls.



Packets sent in a simple client-server interaction on a connection-oriented network

Network Software (cont.)

S'0'A ITER

Service primitives

1. Server executes **LISTEN** to indicate that it is prepared to accept incoming connections.
 - Blocking system call.
 - The server process is blocked until a request for connection appears.
2. Client process executes **CONNECT** to establish a connection (1) with the server.
 - Specifies who to connect to (parameter giving the server's address).
 - OS sends a packet to the peer asking it to connect.
 - Client process is suspended until there is a response.
3. The packet is processed at the server.
 - OS sees that the packet is requesting a connection upon reception of the packet.
 - OS checks to see if there is a listener and if so it unblocks it.
 - Sends an acknowledgement (2) back to the client process to accept the connection.
 - The arrival of this response then releases the client.
 - At this point both client and server are running and they have connection established.

Network Software (cont.)

Service primitives

4. The server will execute **RECEIVE** to prepare to accept the first request.
 - Server does this immediately upon being released from the LISTEN, before acknowledgment can get back to the client.
 - The RECEIVE is a blocking call.
5. The client will execute **SEND** to transmit its request (3) followed by **RECEIVE** to get the reply.
 - The arrival of the request packet at the Server unblocks it so it can handle the request.
 - After the server has done the work it will issue a SEND to return the answer to the client (4).
 - The arrival of the this packet unblocks the client which can now inspect the answer.
 - If further request are required it can make them now.

Network Software (cont.)

Service primitives

6. When the client is done it executed **DISCONNECT** to terminate the connection (5).
 - Initial DICONNECT 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 (6).
 - When the server's packet gets back to the client machine, the client process is released and the connection is broken.

Network Software (cont.)

S'0'A ITER

Service primitives

➤ Many things can go wrong:

- Timing (e.g., CONNECT is done before LISTEN)
- Packets can get lost, ...

➤ Why not using connectionless service:

- Only two (2) packets would be needed (i.e. request and reply) vs. six (6).
- If large messages then chances of transmission errors, lost packets, etc.

➤ Example:

- If the reply consisted of hundreds of packets, some of which could be lost during transmission, how would the client know if some pieces were missing?
- How would the client know whether the last packet actually received was really the last packet sent?

Note : However, in the case where the number of information packets to be communicated are very less and/or the loss of information is acceptable the system can make use of service primitives associated to a connectionless service.

Network Software (cont.)

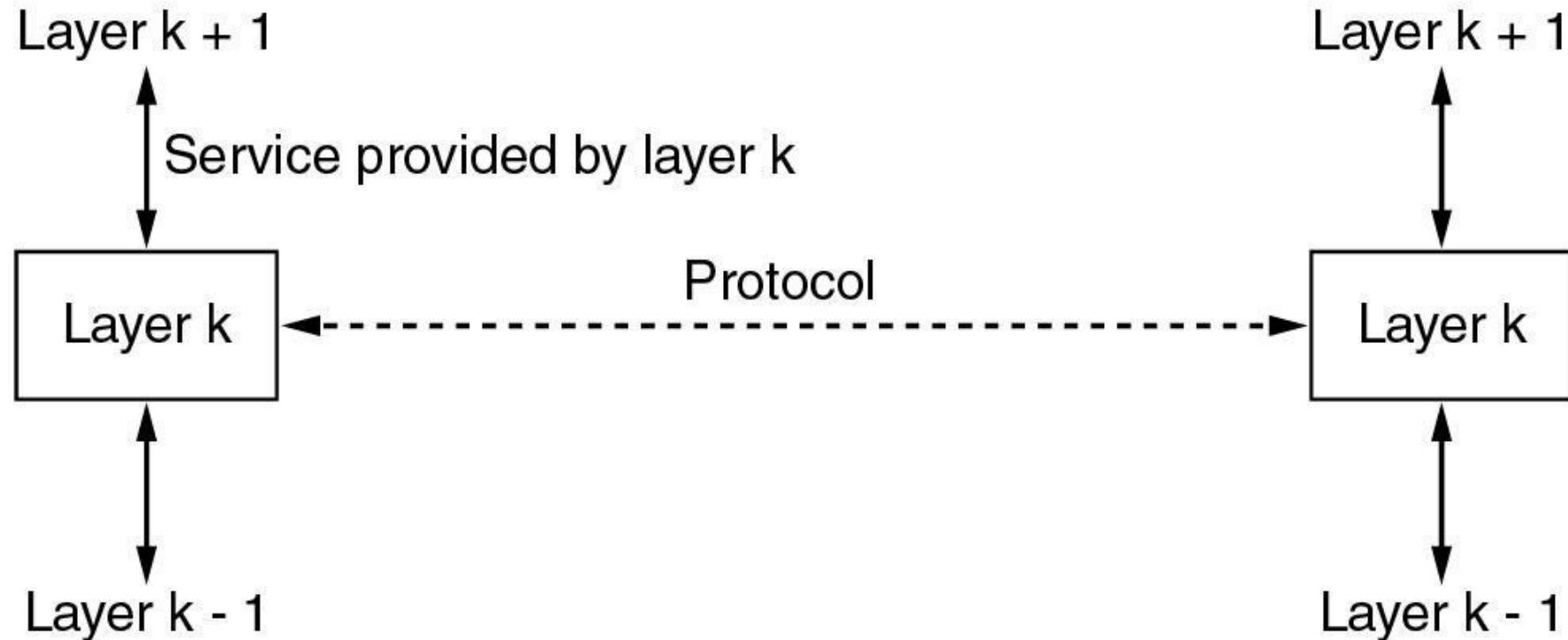
Relationship of Services to Protocols

- A *service* is a set of primitives (operations) that a layer provides to the layer above it.
 - Services relate to interfaces between layers
 - The service defines what operations the layer is prepared to perform on behalf of its users, but it does not say anything at all about how these operation are implemented.
- A *protocol* 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.
 - Protocols relate to the packets send between peer entities on different machines.
 - 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.

Network Software (cont.)

S'0'A ITER

Relationship of Services to Protocols



The relationship between a service and a protocol.

Reference Models

➤ OSI reference model :

- Although the protocols associated with the OSI model are rarely used any more, the model itself is actually quite general and still valid.

➤ TCP/IP reference model :

- The model itself is not of much use but the protocols are widely used.

Reference Models(cont.)

S'0'A ITER

The OSI Reference Model

- Designed in 1983 based on a proposal developed by the International Standards Organization (ISO).
- Revised in 1995, then after, the model is called the ISO **OSI (Open Systems Interconnection)**.
- Deals with connecting open systems (systems that are open for communication with other systems).
- Based on **seven layers**.

Reference Models(cont.)

The OSI Reference Model

Principles :

- Layers created where different abstraction needed.
- Each layer performs well-defined function.
- Function of layer chosen with definition of international standard protocols in mind.
- Minimize information flow across interfaces between boundaries.
- Number of layers optimum.

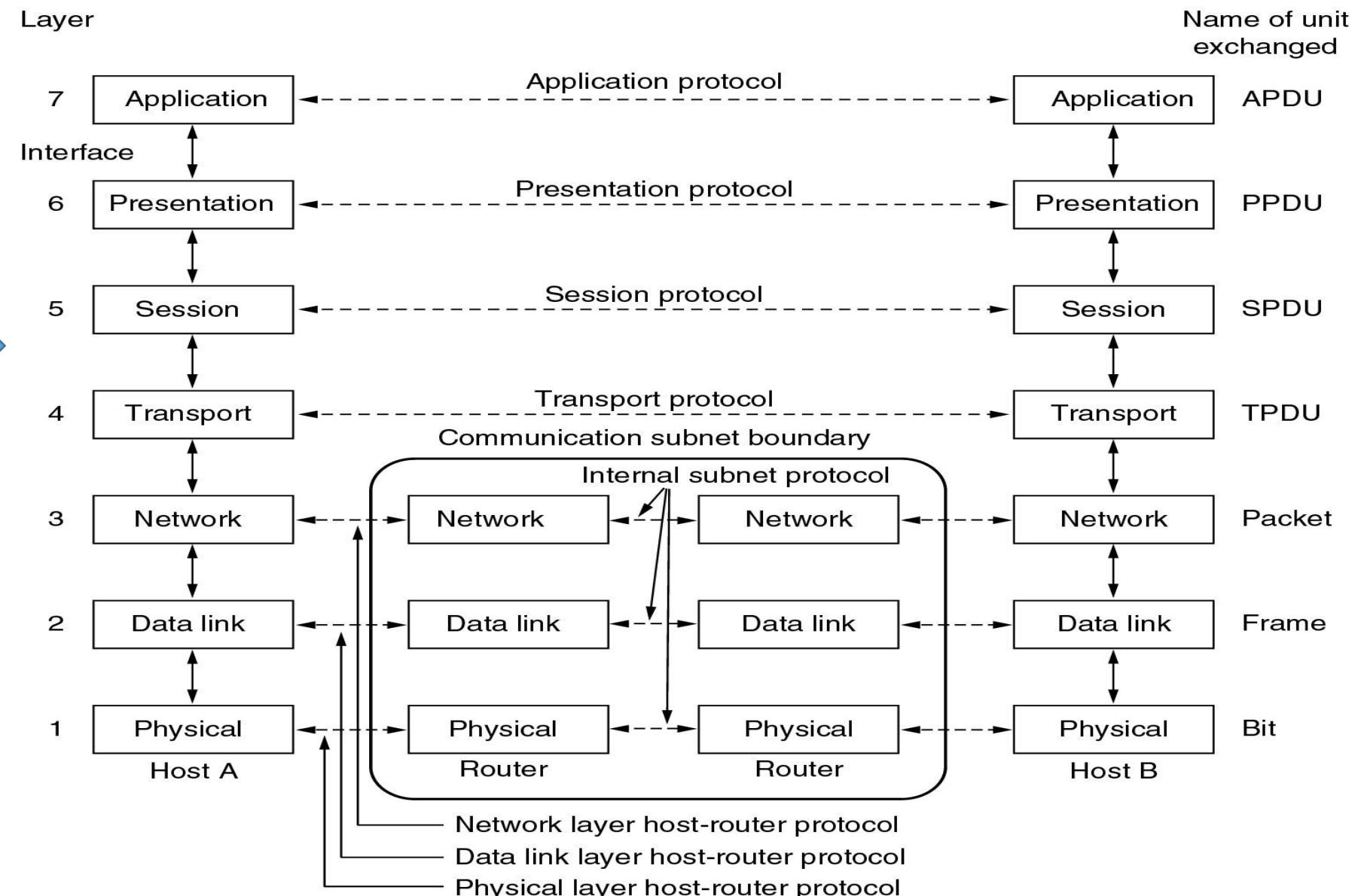
Layers :

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Reference Models(cont.)

The OSI Reference Model

Structure of
OSI reference model.



Reference Models(cont.)

The OSI Reference Model

Physical Layer:

- Concerned with transmitting raw bits over a communication channel.
- Converts data from the upper layers into '1's and '0's for transmission over media.
- Defines how data is encoded onto the media to transmit the data.
- Defined on this layer: Cable standards, wireless standards, and fiber optic standards.
- Copper wiring, fiber optic cable, radio frequencies, anything that can be used to transmit data is defined on the Physical layer of the OSI Model.

Design issues :

- Ensuring that when one side sends a 1 – bit of information it is received as 1-bit (not as 0-bit or 2-or more- bits).
- What type of signal should be used to represent “1” and “0”?
- How many nano seconds a bit lasts?
- Whether transmission can occur simultaneously in both direction?
- How many pins the network connector has?
- What each pin is used for?

Reference Models(cont.)

The OSI Reference Model

Data Link Layer:

- Transforms the raw data bits to a data frame (few hundred/thousand bits)
- Responsible for sequential transmission of frames from node to node or computer to computer
- In reliable service the receiver confirms correct receipt of each frame by sending back an *acknowledgment frame*.
- Protocols defined include Ethernet Protocol and Point-to-Point Protocol (PPP)
- Two sub layers: Logical Link Control (LLC) and the Media Access Control (MAC)
 - Logical Link Control (LLC)
 - Flow control, Error control
 - Media Access Control (MAC)
 - Determines which computer has access to the network media at any given time
 - Determines where one frame ends and the next one starts, called frame synchronization

Reference Models(cont.)

The OSI Reference Model

Network Layer:

- Controls the operation of the subnet.
- Responsible for moving (or routing) packets (data) from one end of the network to the other, called *end-to-end communications*.
- Determines how packets to be *routed* from source (in one network) to destination (in another network).
 - *Static table (rarely changed)*
 - *Dynamic table (Often changed to avoid failed components) : Route can be determined at the start of each conversion (or) new route for each packet depending on network load.*
- Responsible for congestion handling : If too many packets are present in the subnet at the same time, they will get in each other's way forming bottlenecks.
- Deals with quality of service (i.e. jitter, transit time, delay etc.)
- Handles the issues raised due to different physical addresses of machines belonging to different networks.

Reference Models(cont.)

The OSI Reference Model

Network Layer types :

In datagram networks

- Provides both routing and data forwarding

In connection-oriented network

- Separate data plane and control plane
- Data plane only forwards and schedules data (touches every byte)
- Control plane responsible for routing, call establishment, call-teardown (doesn't touch data bytes)

In Internet

- Network layer is provided by Internet Protocol
- Found in all **end-systems** and **intermediate systems**
- Packet-forwarding, routing, scheduling
- Unique IP addresses

Reference Models(cont.)

S'0'A ITER

The OSI Reference Model

Transport Layer:

- Accepts data from higher levels and splits it into smaller segments that can be sent to network layer.
- Also, reassembles data segments into data for the use of higher layers.
- Puts segments in correct order (called sequencing), so they can be reassembled in correct order at destination.
- Concerned with the reliability of the transport of sent data.
- May use a *connection-oriented protocol* such as TCP to ensure destination has received segments.
- May use a *connectionless protocol* such as UDP to send segments without assurance of delivery.
- It is a true end-to-end layer; it carries data all the way form the source to the destination.
 - In the lower layers (i.e. 1 to 3), the protocols are between each machine and its immediate neighbours (may be routers), and not between the ultimate source and destination machines.

Reference Models(cont.)

The OSI Reference Model

Session Layer:

- Allows users on different machines to establish *sessions* between them.
- Services:

Dialog control - Keeping track of whose turn is it to transmit

Token management – Preventing two parties from attempting the same critical operation simultaneously

Synchronization – Check pointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery.

- Establishes, manages, and terminates connections
- Provides duplex, half-duplex, or simplex communications between devices
- Internet – doesn't have a standard session layer

Reference Models(cont.)

The OSI Reference Model

Presentation Layer:

- Concerned with the syntax and semantics of the information transmitted.
- Since different computer may deal with different data representations a standard encoding is done, thus handles three primary tasks:
 - Translation , –Compression , –Encryption
- Ex : ASCII
- Internet
 - no standard presentation layer

Application Layer:

- Contains all services or protocols needed by application software or operating system to communicate on the network
- Example : **HTTP (Hyper Text Transfer Protocol)**, which is the basis for the World Wide Web.

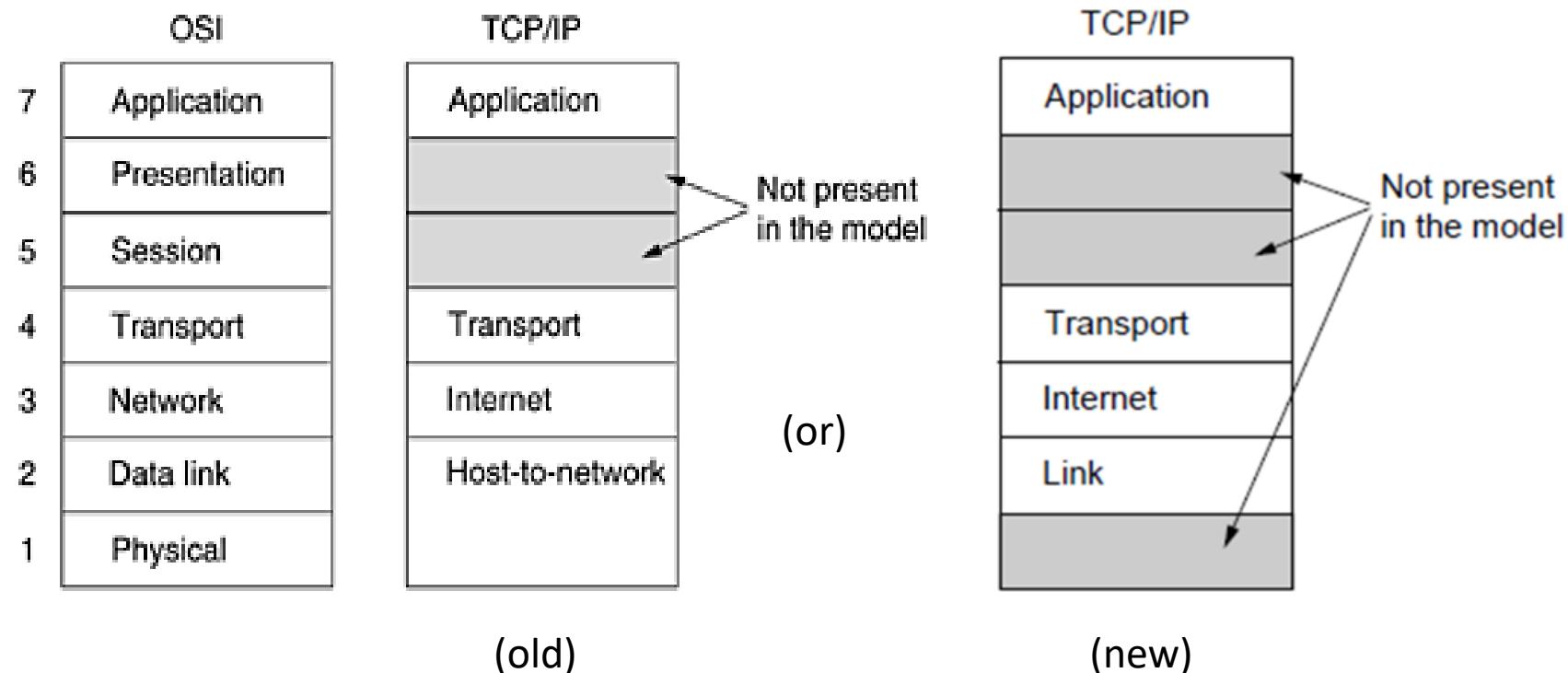
Reference Models(cont.)

The TCP/IP Reference Model

- Proposed earlier to OSI model.
- Used in **ARPANET**(grandparent of all wide area computer) and it's successor **the internet**
(Also used in private networks)
- Designed to support/interconnect different types of network (e.g. interconnection of radio network and computer network).
- Four protocol layers :
 - **Host-to-network/link**
 - **Internet**
 - **Transport**
 - **Application**
- Design criteria:
 - Network be able to survive loss of subnet hardware without existing conversations being broken off.
 - Applications with divergent requirements were supported ranging from file transfer to real-time speech transmission.

Reference Models(cont.)

The TCP/IP Reference Model



Note :

When TCP/IP is compared to OSI it can be seen that the host-to-network layer is equivalent to the combination of physical and data link layer. Also, the internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers

Reference Models(cont.)

The TCP/IP Reference Model

Link Layer :

- Describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer.
- It is not actual layer in the classical sense of the term rather is an interface between hosts and transmission links.

Internet Layer :

- Permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network).
- The packets may arrive in a completely random order from the original and the higher layer must rearrange them – if in-order of delivery is desired.

(An analogy example : Letters dropped in the post box in sequence may not reach in the same sequence)

- Defines an official packet format and protocol called **IP (Internet Protocol)**.
- Packet routing is a major issue and IP has not proven effective at avoiding congestion.

Reference Models(cont.)

The TCP/IP Reference Model

Transport Layer :

- Allow peer entities on the source and destination hosts to carry on a conversation.
- Uses either of the two types of transport protocol (i.e. **TCP** and **UDP**).

TCP(Transmission Control Protocol) :

- A reliable connection-oriented protocol.
- Allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.
- It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer.
- At the destination, the receiving TCP process reassembles the received messages into the output stream.
- TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

UDP(User Datagram Protocol):

- An unreliable, connectionless protocol for applications that do not want sequencing or flow control and wish to provide their own.
- 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.

Reference Models(cont.)

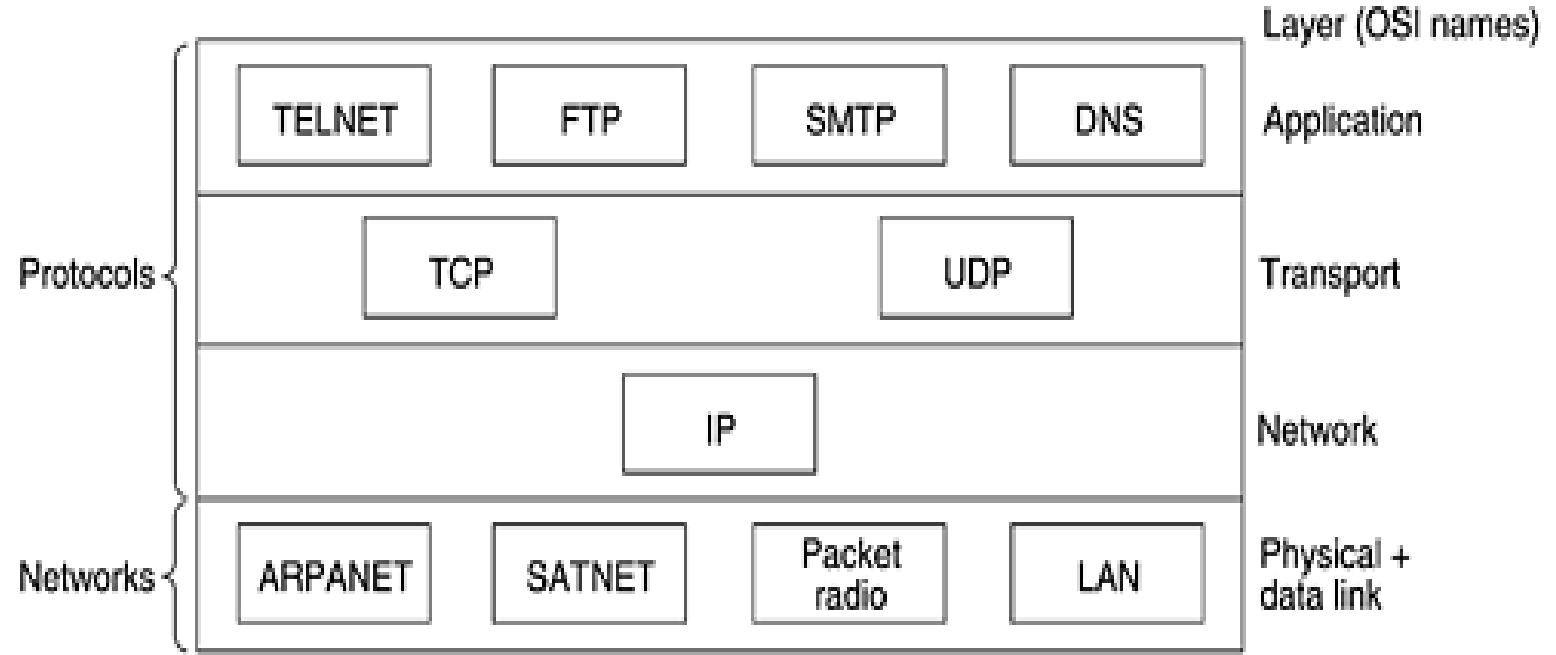
The TCP/IP Reference Model

Application Layer :

- Define the rules when implementing specific network applications.
- Applications simply include any session and presentation functions that they require.
- Rely on the underlying layers to provide accurate and efficient data delivery.
- Typical protocols:
 - FTP – File Transfer Protocol (For file transfer)
 - Telnet – Remote terminal protocol (For remote login on any other computer on the network)
 - SMTP – Simple Mail Transfer Protocol (For mail transfer)
 - HTTP – Hypertext Transfer Protocol (For Web browsing)

Reference Models(cont.)

The TCP/IP Reference Model



Protocols and networks in the TCP/IP model initially

Reference Models(cont.)

A Comparison of the OSI and TCP/IP Reference Models

Similarities :

1. Both lie on the concept of a stack of independent protocols.
2. Functionality of the layers is roughly similar (for example in both models, the layers above transport are application-oriented users of the transport service).

Differences :

OSI reference model	TCP/IP reference model
Uses 7 different layers.	Uses 4 different layers.
Supports both connectionless & connection oriented service in the network layer but only connection oriented service in transport layer.	Supports only connectionless service in the network layer but both connectionless & connection oriented service in transport layer.
Clearly distincts service, interface & protocol.	Doesn't clearly distinguish service, interface & protocol.
Protocols are better hidden and can be replaced relatively easily as the technology changes.	Protocols are not hidden and can not be replaced easily as the technology changes (e.g. Replacing IP with a different protocol is virtually impossible).
The reference model was devised before the corresponding protocols were invented.	The protocols came first, and the model was really just a description of the existing protocols since the protocols fit perfectly.

Example networks

S'0'A ITER

The computer networks that are functioning in the current scenario are associated with so many attributes like size, technology, goals etc.

- Internet
 - ARPANET
 - NSFNET
- Connection oriented network : ATM
- Ethernet
- Wireless LANs: 802.11

Example networks (cont.)

The Internet

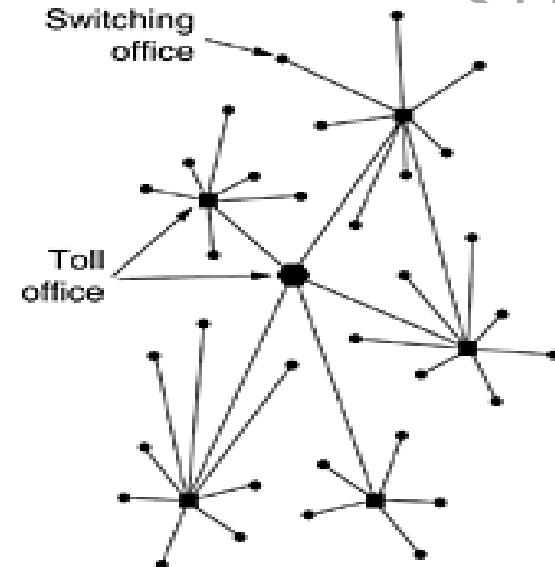
- Never be considered as a single network rather than a vast collection of different networks that use certain common protocols and provide certain common services.
- Not planned by anyone and not controlled by anyone.
- Revolutionized many aspects of our daily lives.
- People use internet for various reasons.
- History :
 - ARPANET
 - NSFNET

Example networks (cont.)

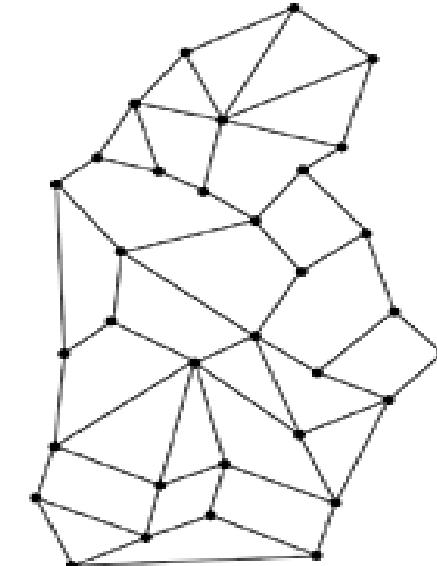
S'0'N ITER

ARPANET

- Started with the want from DoD in late 1950 to develop a command-and-control network.
- In the beginning uses the base of existing public telephone network.
- Issue : Structure is vulnerable (i.e. destroy of toll offices fragments the system into isolated islands).



Structure of the telephone system



- Around 1960 the DoD awarded a contract to the RAND Corporation.
- Paul Baran, proposed the incorporation of digital packet switching technology in a highly distributed and fault tolerant system.

(Idea was dismissed)



Baran's proposed distributed switching system

Example networks (cont.)

ARPANET

- Following several years, **ARPA (Advanced Research Projects Agency)** is created to find the solution related to design of the command and control network.
- In 1967, Lary Roberts (director of ARPA) presented an idea (Wesley clark) in the form of paper related to building of a packet switched subnet, where each host has it's own router.
- Following to this, the practical implementation of a network is determined by Roberts with a name **ARPANET**.
- A consulting firm named BBN had contracted to make practical implementation of ARPANET.
 - Built subnet
 - Wrote the subnet software
 - Transmission line leased from telephone companies.

Example networks (cont.)

ARPANET

Concept :

- ❖ Subnet consists of minicomputers called **IMPs (Interface Message Processors)**.
- ❖ 56-kbps transmission lines.
- ❖ Each IMP connected to at least two other IMPs.
- ❖ Datagram subnet (if some lines and IMPs were destroyed, messages could be automatically rerouted along alternative paths).
- ❖ Each node consists of an IMP and a host, in the same room, connected by a short wire.
- ❖ A host can send messages of up to 8063 bits to its IMP.
- ❖ IMPs break these up into packets of at most 1008 bits and forward them independently toward the destination.
- ❖ Each packet was received in its entirety before being forwarded.
- ❖ Store-and-forward packet-switching network.

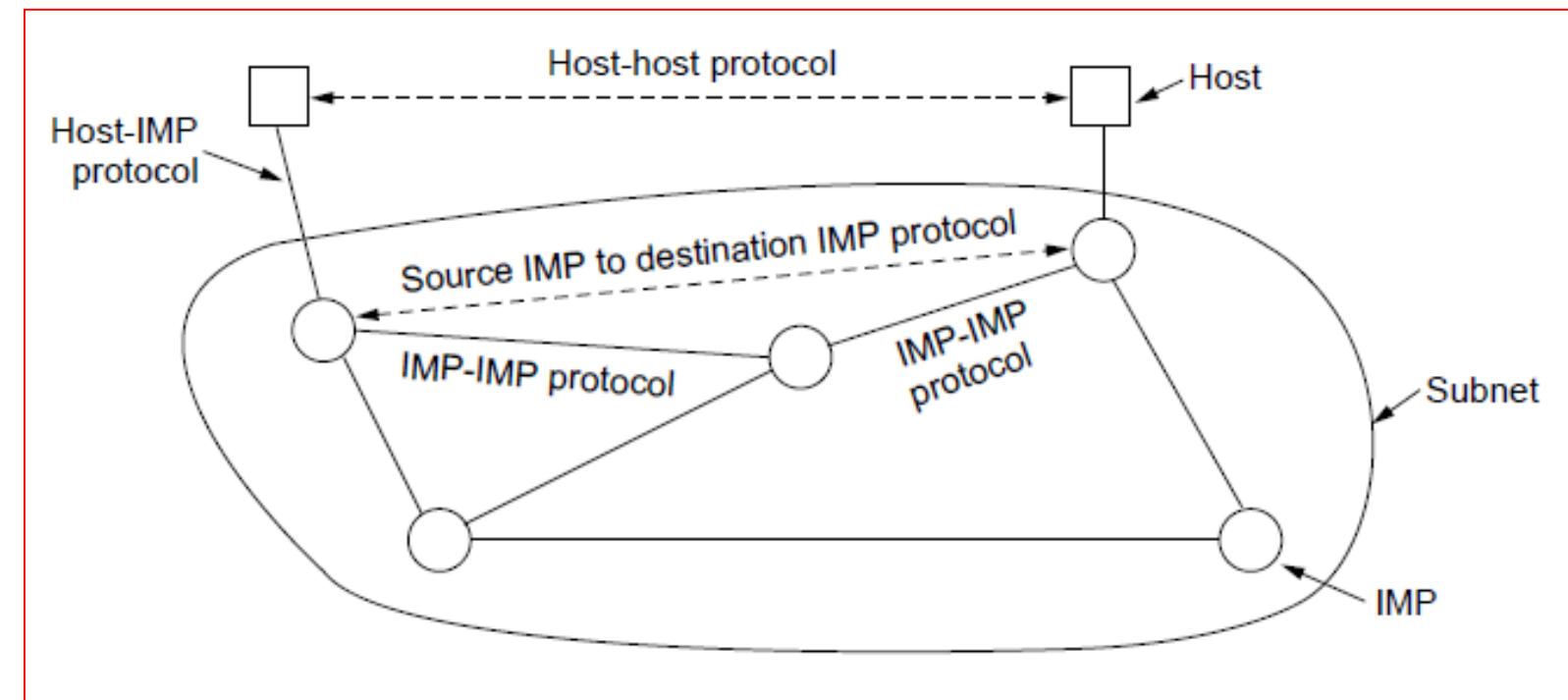
Example networks (cont.)

S'OA ITER

ARPANET

Software :

- **Subnet software** : required at the IMP end of the host-IMP connection
 - IMP-IMP protocol
 - Source IMP to destination IMP protocol
- **Host software** : Required at the host end of the host-IMP connection
 - Host-host protocol
 - Application software



The original ARPANET design

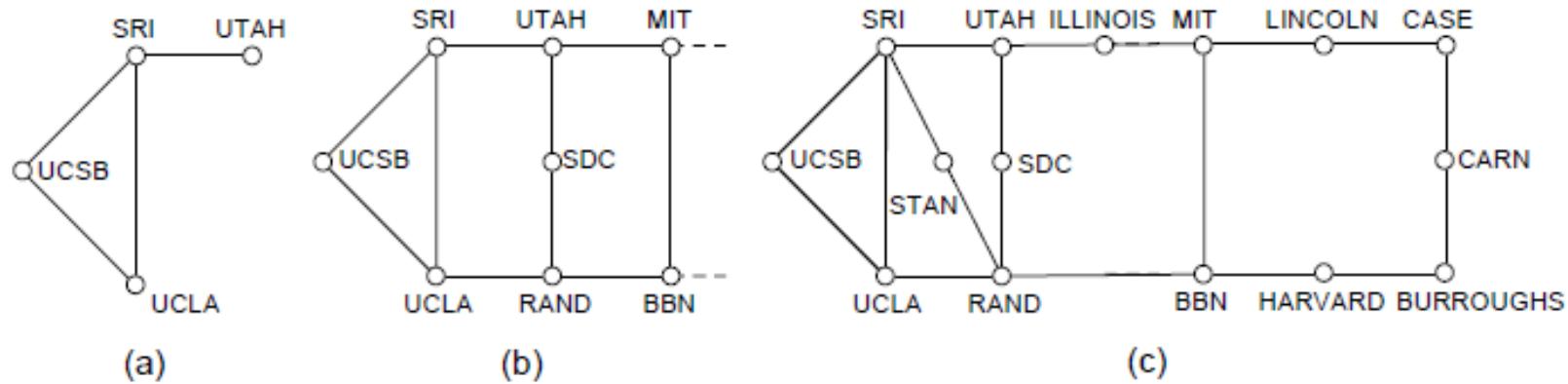
Example networks (cont.)

S'0'A ITER

ARPANET

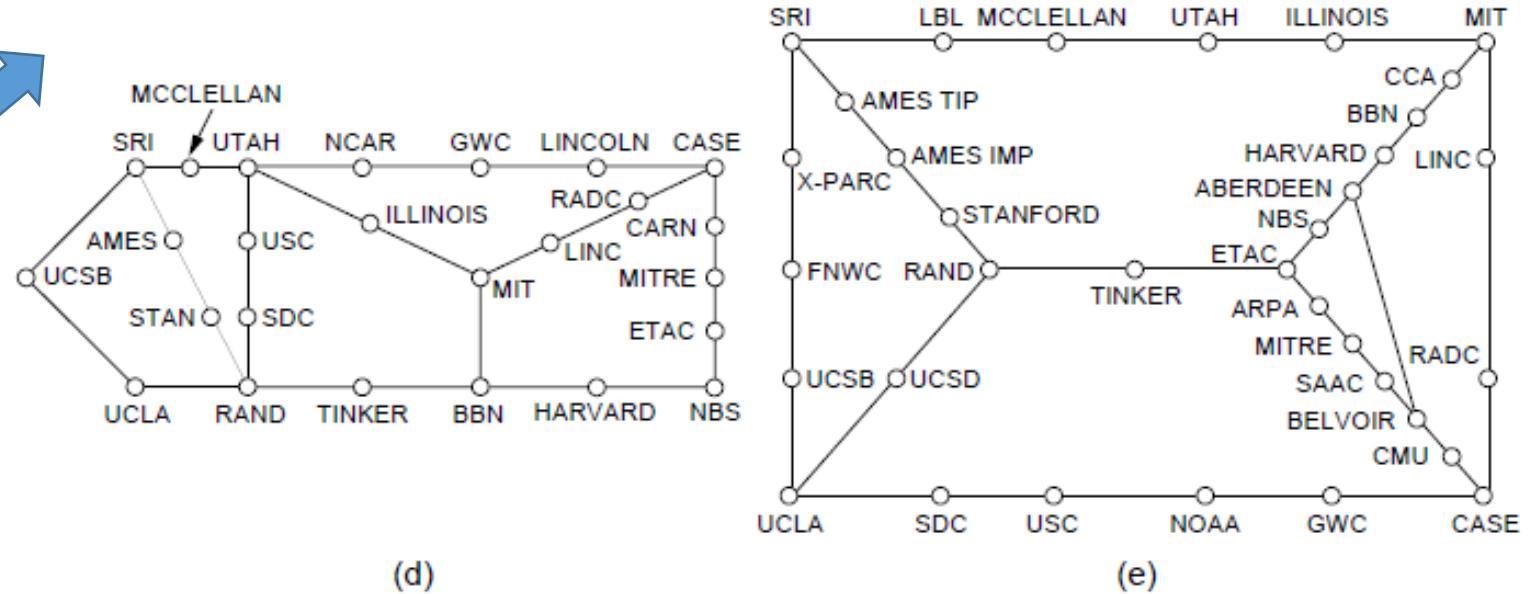
Growth :

- An experimental network implemented in December 1969 with four nodes: at UCLA, UCSB, SRI, and the University of Utah. (a)
- Installation of more IMPs make the ARPANET to grow rapidly. (b), (c), (d), (e)



Growth of the ARPANET.

- (a) December 1969.
- (b) July 1970.
- (c) March 1971.
- (d) April 1972.
- (e) September 1972.



Example networks (cont.)

ARPANET

Use of TCP/IP :

- ARPANET protocols were not suitable for running over multiple networks.
- Leads to invention and implementation of **TCP/IP**.
- In 1980s, many additional networks, especially LANs, were connected to the ARPANET.

Use of DNS :

- Increase in scale of network → Difficulty in identifying hosts
- Development of **DNS (Domain Name system)**.
- Host names mapped to IP addresses.
- DNS is still used in internet.

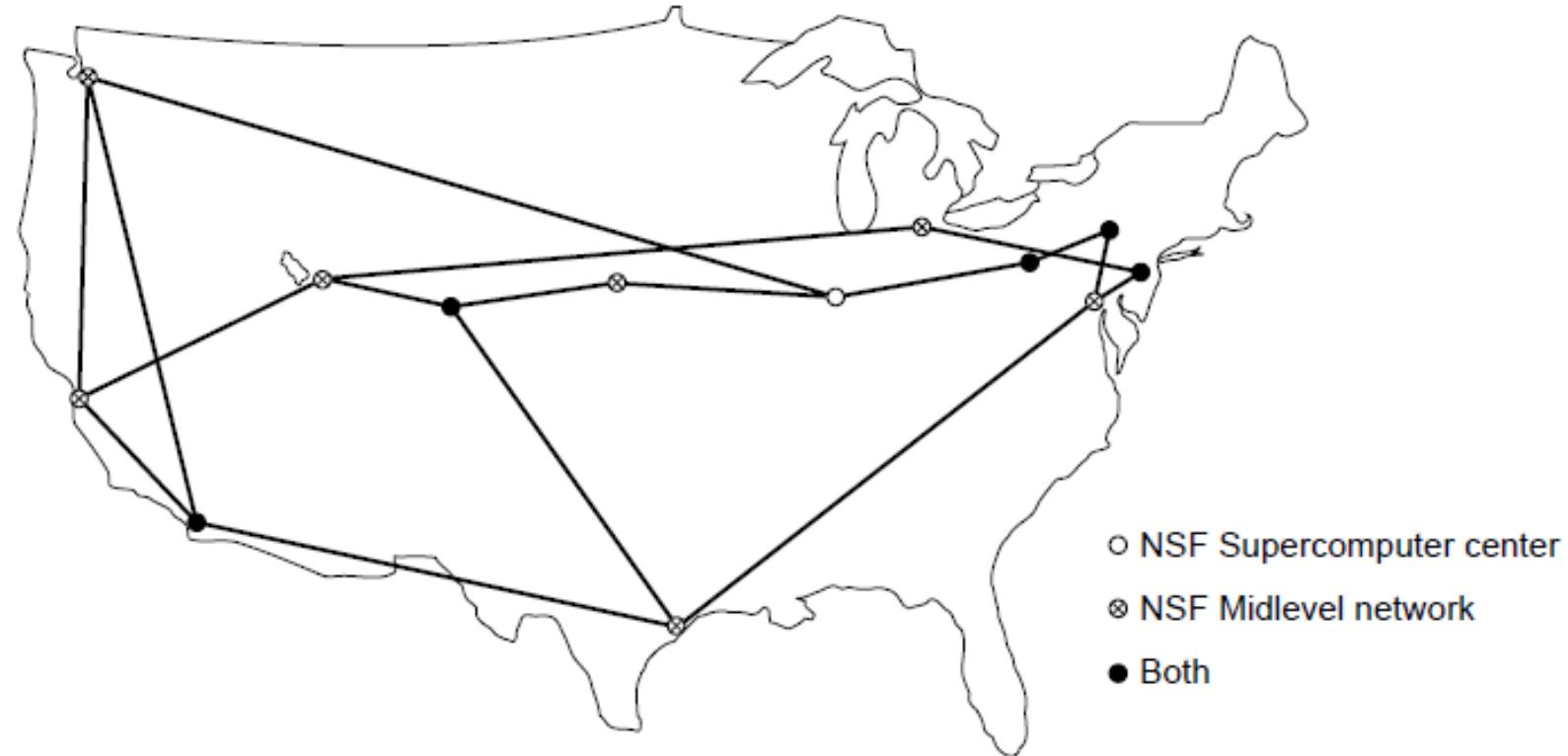
Example networks (cont.)

NSFNET

- Late 1970's : NSF (the U.S. National Science Foundation) had taken a response to design a successor to the ARPANET.
- Open to all university research groups.
- Initial step to built a backbone network to connect its six supercomputer centres.
- Each supercomputer was attached with a microcomputer called a **fuzzball**.
- **Fuzzballs** were connected with 56-kbps leased lines and formed the subnet.
- TCP/IP was used from the beginning.
- Regional networks also connected to the backbone getting the financial support from NSF.
 - Allow users at thousands of universities, research labs, libraries, and museums to access any of the supercomputers and to communicate with one another.
- Combined structure of backbone and regional networks named as **NSFNET**.
- **NSFNET** was also connected with ARPANET through link between fuzzball and IMP.

Example networks (cont.)

NSFNET



The NSFNET backbone in 1988

Example networks (cont.)

NSFNET

NSFNET to ANSNET:

- By 1990s version 2 backbone designed and implemented with the use of fiber channel to provide a speed of 1.5 Mbps.
- NSF with non government organizations forms **ANS (Advanced Networks and Services)**.
- In 1990s, ANS took over the NSFNET and renamed it **ANSNET** with a speed 45 Mbps.

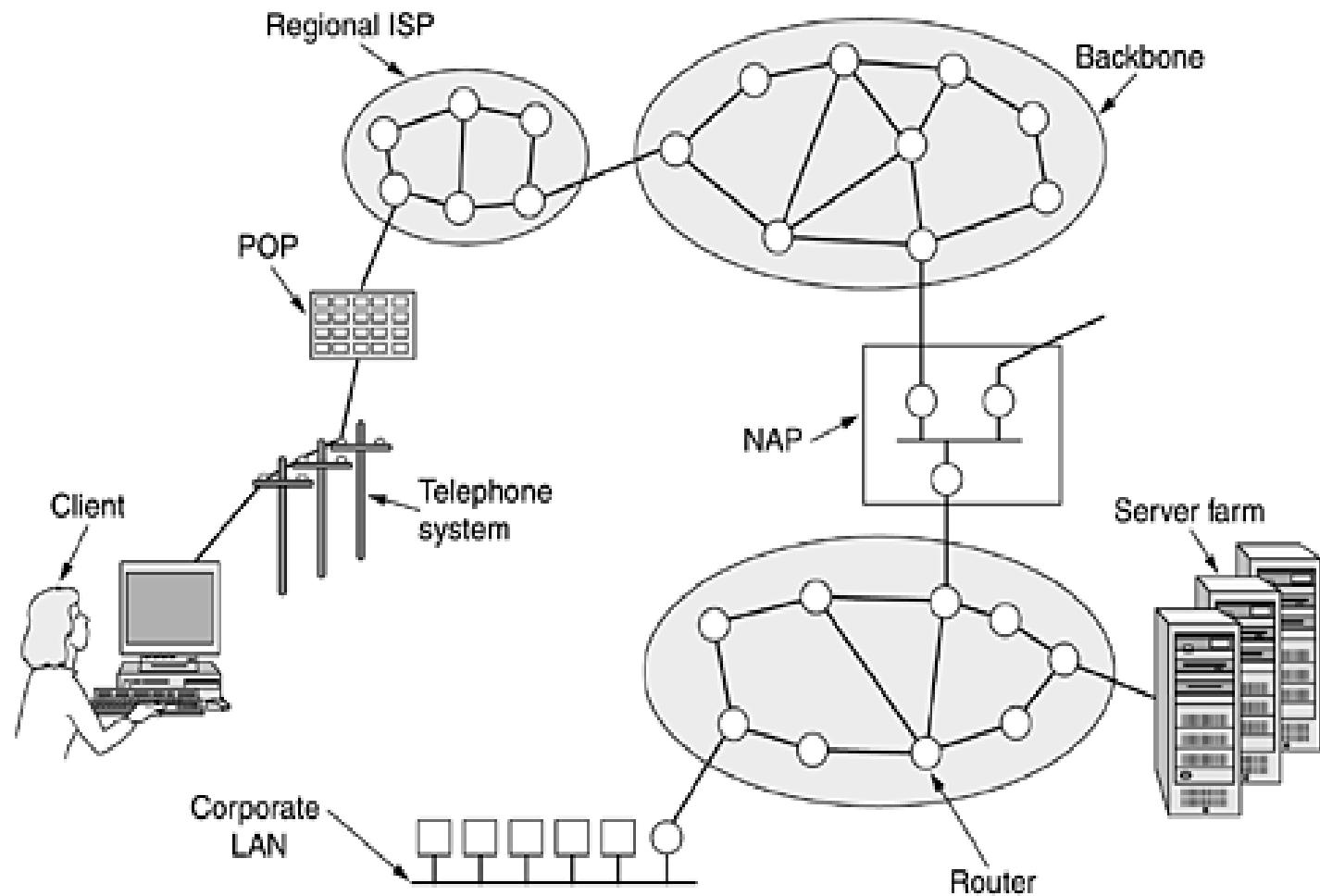
NAP (Network Access Point):

- Four different network operators get contract from NSF to set up **NAPs** for providing communication service between regional networks.
- Network operators also provide backbone service to regional networks.
- A packet originating on any regional network had a choice of backbone carriers to get from its NAP to the destination's NAP.
- More than one backbone like competitive structure came into action.

Example networks (cont.)

Architecture of the Internet

- Client machine gets connected to Regional ISP through POP centre.
 - Dial up service (for telecom company as ISP).
 - Direct cable (ISP other than telecom company).
- ISP's regional network consists of interconnected routers in cities.
- If destination host served by same ISP, then packet delivered to destination host, else forwarded to ISP's backbone operator.
 - If destination host directly connected to backbone, then Packet delivered to host, else forwarded to other ISP regional network/ other backbone (through NAP).
- Packet delivered to host.



Overview of the Internet

Example networks (cont.)

Internet usage

Definition :

A machine is on the Internet if it runs the TCP/IP protocol stack, has an IP address, and can send IP packets to all the other machines on the Internet.

1970 – early 1990 : The Internet and its predecessors had four main applications.

- E-mail.
- News.
- Remote login.
- File transfer.

- Until the early 1990s, the Internet was largely populated by academic, government, and industrial researchers.
- **WWW (World Wide Web)** changed all that and brought millions of new, non-academic users to the net.
- Together with the **browser**, the WWW made it possible for a site to set up a number of pages of information with embedded links between pages.
 - For example, many companies have a home page with entries pointing to other pages for product information, price lists, customer support and more.
- With the facility available in home, the network character has taken the shape of public utility.

Example networks (cont.)

S'OA ITER

Connection-Oriented Network: ATM

- Telephone companies were supporting the connection-oriented network because of two reasons:
 - 1) Quality of service
 - 2) Billing
- **X.25** (1970s) and **frame delay** (1980s) : works on synchronous transmission characteristics.
- In early 1990s, **ATM (Asynchronous Transfer Mode)** network designed to work with asynchronous transmission system.
- Merging of voice, data, cable television and many more signals into a single integrated system that could do everything for everyone.
- Initially not happened due to bad timing, technology and implementation, however later on, found to be successful.

Example networks (cont.)

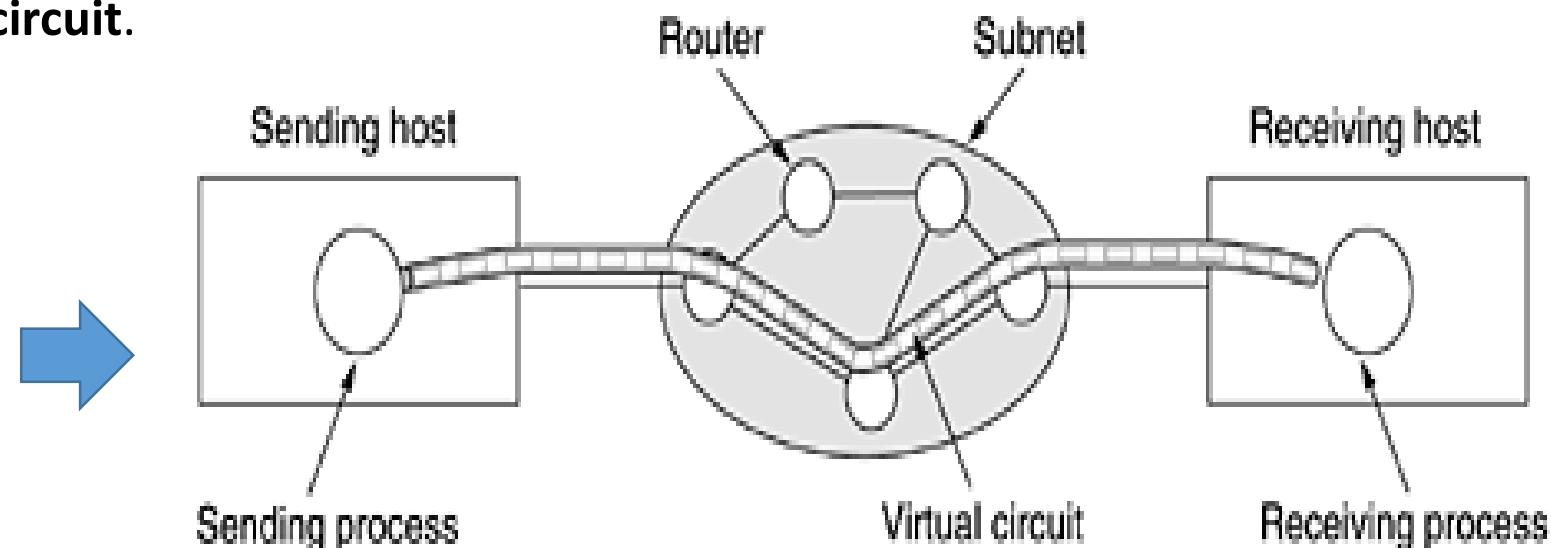
S'0'A ITER

Connection-Oriented Network: ATM

ATM Virtual Circuits:

- Set up packet transmission prior to sending of data from source host to destination host.
- Routers in the path followed by set up packet make an entry to their routing table indicating path information till the end of the data transmission.
- Connection between two hosts through subnet/routers can be temporary/permanent and is referred as **ATM virtual circuit**.

A virtual circuit in
ATM network



Example networks (cont.)

Connection-Oriented Network: ATM

Connection identifier, ATM cell, Information flow

- Each connection, temporary or permanent, has a unique **connection identifier**.
- The information in ATM is transmitted in the form of small, fixed-size packets called **cells**.
- The cells are 53 bytes long, of which 5 bytes are header and 48 bytes are payload.



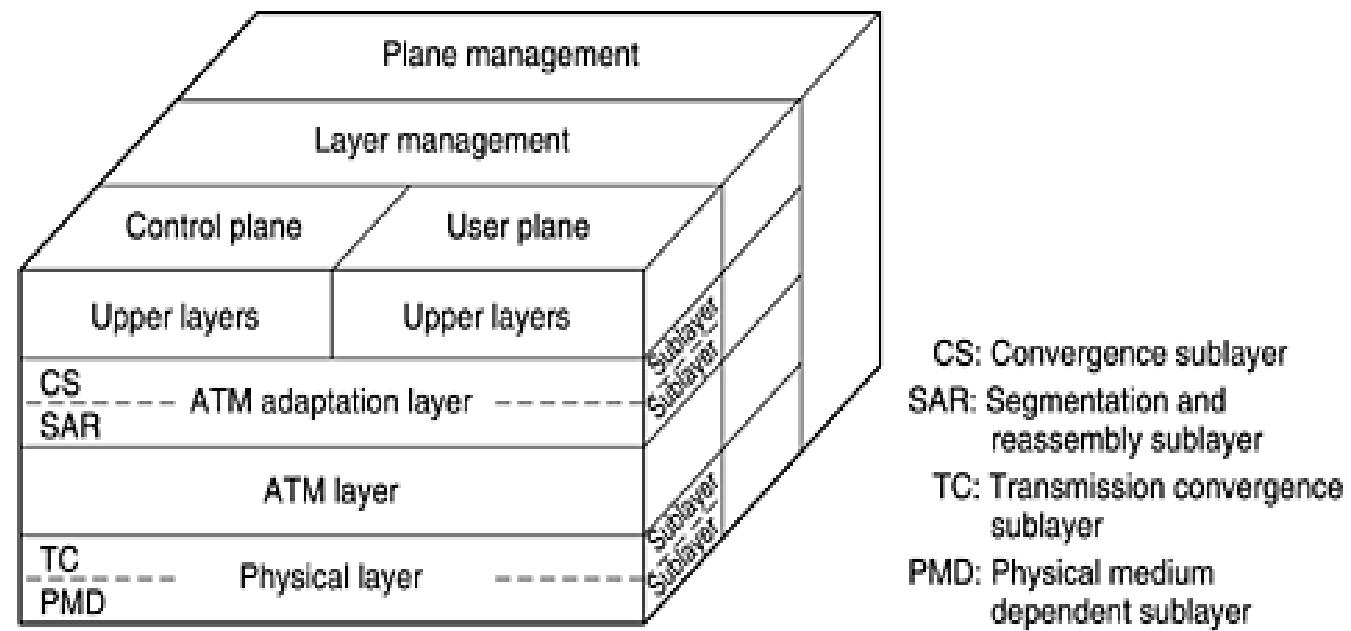
An ATM cell

- Part of the header is the connection identifier to identify the source and destination host for a packet.
- Helps the router to know how to route each incoming cell.
- Cells transmitted in a sequence order.
- Most common speeds for ATM networks are 155 Mbps and 622 Mbps.

Example networks (cont.)

The ATM Reference Model

- ATM has its own reference model, different from the OSI model and also different from the TCP/IP model.
- Three layers, **the physical**, **ATM**, and **ATM adaptation layers** with a flexibility for an **user defined upper layer(s)** above that.



The ATM reference model

Example networks (cont.)

The ATM Reference Model

Physical layer :

- Deals with the physical medium: voltages, bit timing, and various other issues.
- No specific rules for the cells regarding the choice of transmission medium.
- ATM cells can be sent on a wire or fibre by themselves.
- ATM cells can also be packaged inside the payload of other carrier systems.
- Two sub layers.

- *PMD (Physical Medium Dependent) sub layer:*

- Make the bits on and off to move through transmission medium (say cable)/carrier.
- Handles the bit timing.
- For different carriers and cables, this layer will be different.

- *TC (Transmission Convergence) sub layer:*

- Converts the cells into bit stream in transmitting end and the reverse in receiving end.
- Handles all the issues related to telling where cells begin and end in the bit stream.

Example networks (cont.)

The ATM Reference Model

ATM layer :

- Deals with cells and cell transport.
- Defines the layout of a cell and tells what the header files mean.
- Deals with establishment and release of virtual circuits.
- Handles congestion control issues.

ATM adaption layer :

- Allow users to send packets larger than a cell.
- The ATM interface segments these packets, transmits to lower layer.
- Reassembles the segments (if any) at the other end.
- Two sub layers.

- *SAR (Segmentation And Reassembly) sub layer:*

- Breaks up packets into cells on the transmission side and puts them back together again at the destination.

- *CS (Convergence Sub layer):*

- Handles different kinds of services to different applications (e.g., file transfer and video on demand have different requirements concerning error handling, timing, etc.).

Example networks (cont.)

The ATM Reference Model

User defined upper layer :

- User plane deals with data transport, flow control, error correction, and other user functions.
- Control plane is concerned with connection management.
- Layer and plane management functions relate to resource management and interlayer coordination.

Example networks (cont.)

The ATM Reference Model

ATM layer	ATM sublayer	Functionality
AAL	CS	Providing the standard interface (convergence)
	SAR	Segmentation and reassembly
ATM		Flow control Cell header generation/extraction Virtual circuit/path management Cell multiplexing/demultiplexing
Physical	TC	Cell rate decoupling Header checksum generation and verification Cell generation Packing/unpacking cells from the enclosing envelope Frame generation
	PMD	Bit timing Physical network access

The ATM layers and sub layers, and their functions

Example networks (cont.)

Ethernet

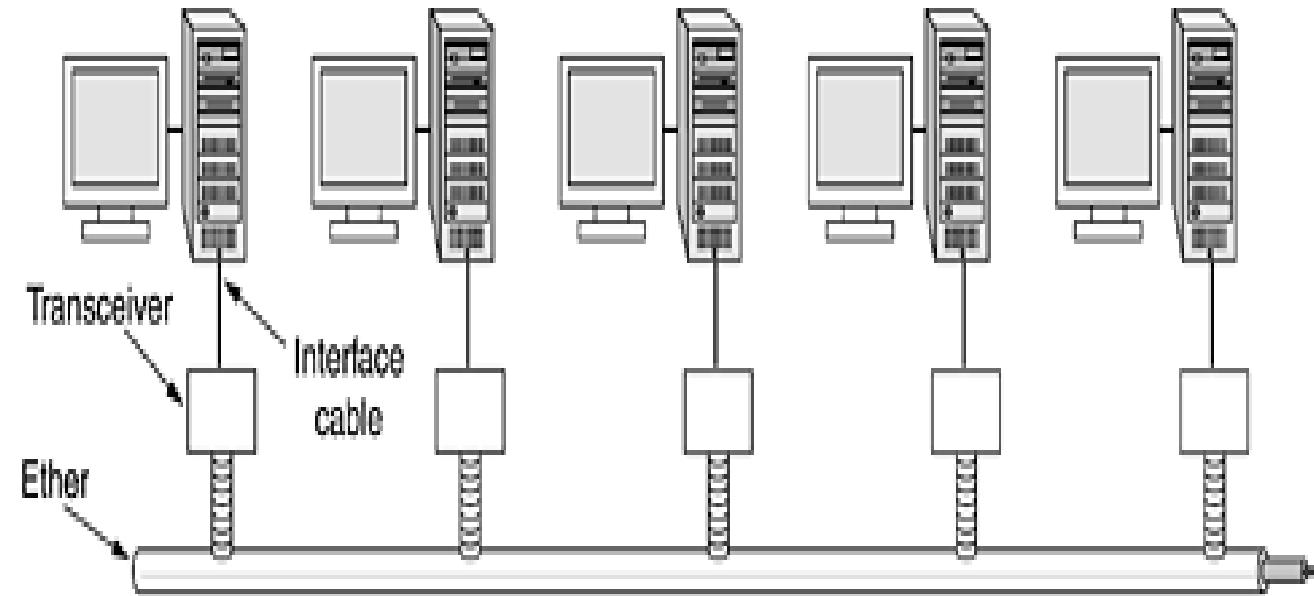
- Most popular local area network.
- Implemented in Xerox PARC (Palo alto Research centre) in 1976.
- Named after the *luminiferous ether*, through which electromagnetic radiation was once thought to propagate.
- Considered as a sucedeer to ALOHANET.
- Uses thick coaxial cable (the ether) as transmission medium.
- Cable length : 2.5 km
(Repeaters at every 500m)
- 256 machines can be connected.
- Speed : 2.94 Mbps.

- Prior to Ethernet (in 1970s)
- Uses short range radio devices.
- Communication between user terminals through central computer.
- Uses two frequencies.
 1. Upstream (user terminal to central computer)
 2. Downstream (Central computer to user terminal).
- Worked fine with low traffic.
- Poor performance with heavy traffic in upstream.

Example networks (cont.)

S'0'A ITER

Ethernet



Architecture of the original Ethernet

Example networks (cont.)

Ethernet

Advantage of Ethernet over ALOHANET :

- Before transmitting, a computer first listened to the cable to see if someone else was already transmitting.
- If so, the computer held back and wait until the current transmission finished.
- Avoids interfering with existing transmissions, giving a much higher efficiency.
- (ALOHANET : Not possible to sense the transmission line.)
- Still a possibility of simultaneous transmission ?
- Can be resolved with random wait time which can be doubled if still collision chance is there.

Example networks (cont.)

Ethernet

Ethernet as IEEE standard :

- Following to success in implementation of Ethernet the speed enhanced to 10 Mbps in 1978.
- In 1983, considered as **IEEE 802.3** standard.
- In the due course of time with the improvement in technology it provides higher speed (100 Mbps).

Other IEEE standards for LAN : [IEEE 802.4](#), [IEEE 802.5](#)

- **802.4** : **Token** bus introduced by General motors, BUS topology
- **802.5** : **Token** ring introduced by IBM, RING topology
- **Token** : A short packet and is used to make a turn for a computer being allowable for transmission of its data.
- A computer could only send if it possessed the token, thus avoiding collisions.
- In due course of time 802.4 has vanished from sight .
- 802.5 had its existence and still in use at some IBM site (popular in the name **IBM token ring**).

In the war of LAN, Ethernet has taken the highest utility in compare to others like token bus and token ring.

Example networks (cont.)

S'OA ITER

Wireless LANs: 802.11

- To equip both the office and the notebook computers with short-range radio transmitters and receivers and to allow them to communicate.
- **Issue in the beginning : Some systems faces problem because of technical incompatibility between devices.**

Example: A computer equipped with a brand X radio could not work in a room equipped with a brand Y base station.

- **Issue solved through standardisation of Wireless LAN (IEEE 802.11).**
- Popular in the term **WIFI**.

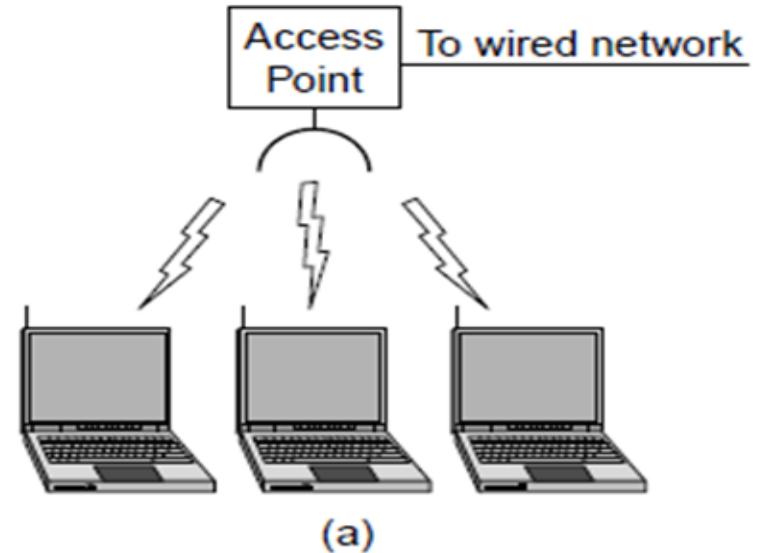
Example networks (cont.)

Wireless LANs: 802.11

The proposed standard had to work in two modes:

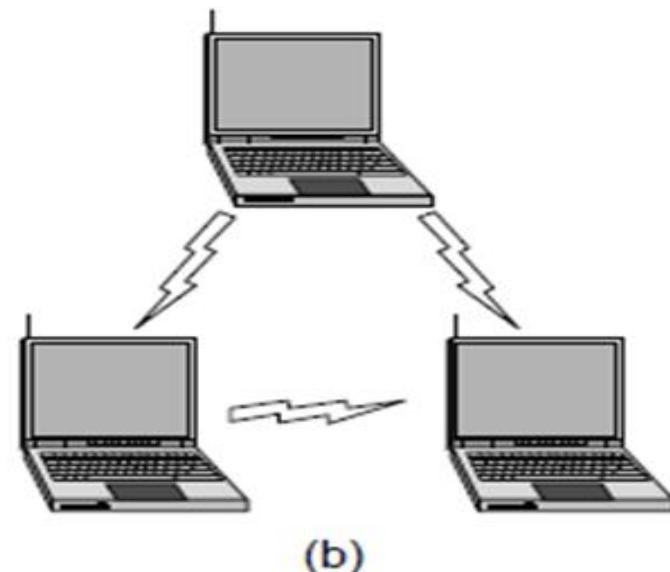
(a) In the presence of a base station.

- All communication was to go through the base station, called an **access point**.



(b) In the absence of a base station.

- The computers would just send to one another directly.
- This mode is now sometimes called **ad hoc networking**.



Example networks (cont.)

S'0'A ITER

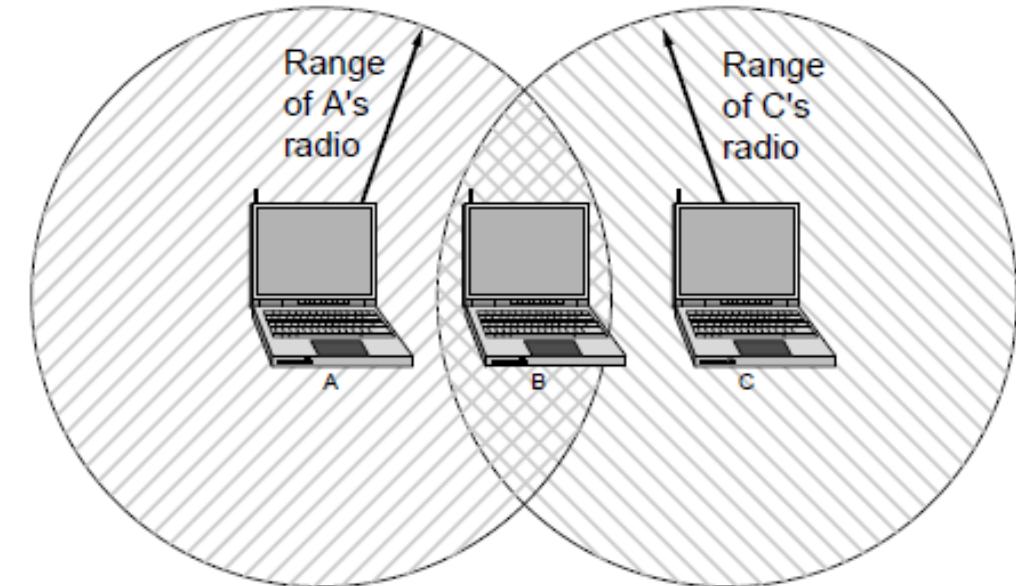
Problems encountered during implementation of Wireless LANs: 802.11

Carrier sense before transmission :

- Though works in Ethernet to avoid simultaneous transmission may not work always in 802.11.

Example :

Let's assume that computer A is transmitting to computer B, but the radio range of A's transmitter is too short to reach computer C. If C wants to transmit to B it can listen to the ether before starting, but the fact that it does not hear anything does not mean that its transmission will succeed.



The range of a single radio may not cover the entire system

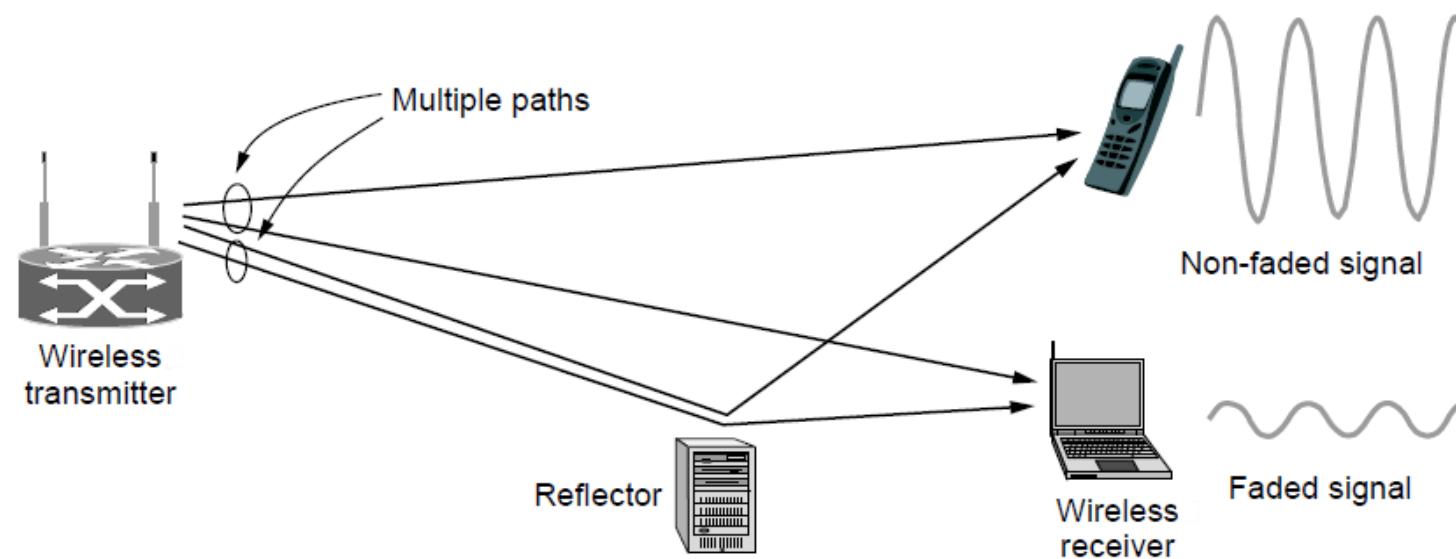
Example networks (cont.)

S'0'A ITER

Problems encountered during implementation of Wireless LANs: 802.11

Multipath fading:

- A radio signal can be reflected off solid objects.
- Same signal may be received multiple times (along multiple paths).
- May lead to interference what is called **multipath fading**.



Example networks (cont.)

S'0'A ITER

Problems encountered during implementation of Wireless LANs: 802.11

Compatibility with software :

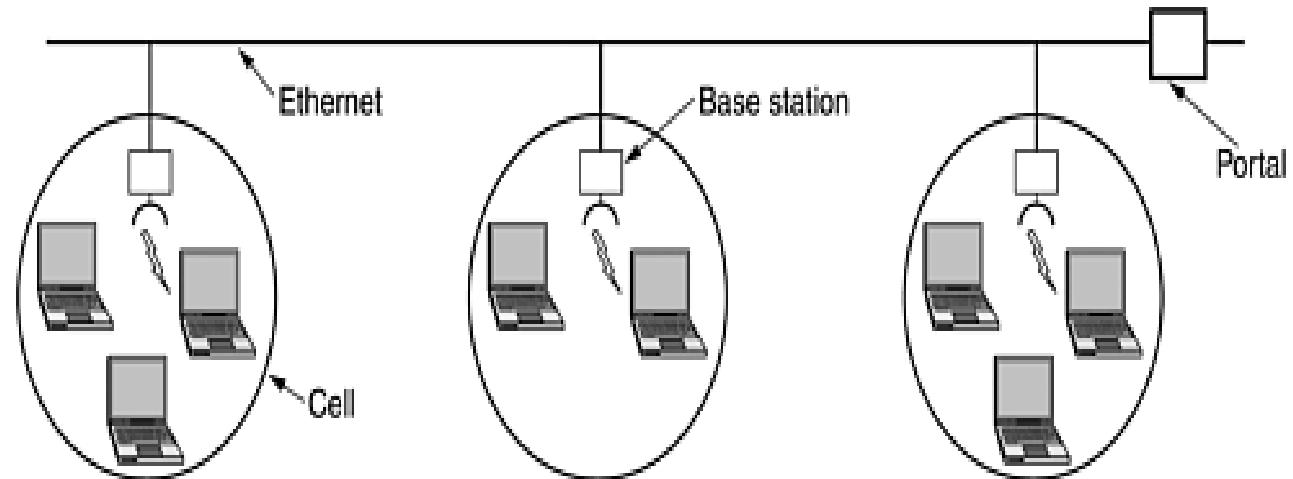
- Software is not aware of mobility of computer system compatible with other device.

Example :

Many word processors have a list of printers that users can choose from to print a file. When the computer on which the word processor runs is taken into a new environment, the built-in list of printers becomes invalid.

Hand off:

- A notebook computer moving from the range of one ceiling-mounted base station into the range of a different base station, requires hand off.



A multi-cell 802.11 network

Example networks (cont.)

Versions of 802.11

Though the problem cited earlier were solved in the due course of time dissatisfaction lies among users with speed.

- The initial standard (i.e. 802.11 in 1997) ran at either 1 Mbps or 2 Mbps.
(Frequency hopping and signal spreading technology)
- **802.11a** and **802.11b** (1999)

802.11a : Speed up to 54 Mbps (wider frequency band)

802.11b : 11 Mbps (same frequency band as 802.11 but different modulation technique)

Besides these 802.11g (2003) is also used currently in some networks that employs OFDM transmission.

Computer Network

(CSE 3034)

Text book: Computer Networks by Andrew S. Tanenbaum

Introduction to the course

Syllabus :

- Introduction(Chapter 1)
- **The Physical Layer(Chapter 2)**
- The Data Link Layer(Chapter 3)
- The Medium Access Control Sublayer(Chapter 4)
- The Network Layer(Chapter 5)
- The Transport layer(Chapter 6)
- The Application layer(Chapter 7)
- Network security(Chapter 8)

The Physical Layer

The Physical Layer

- Theoretical analysis of data transmission
- Transmission media.
 - Guided (copper wire and fiber optics)
 - wireless (terrestrial radio)
 - Satellite
- Examples of communication systems used in practice for wide area computer networks

Theoretical Basis for Data Communication

Pre -requisite

- Involvement of two signals : Digital and Analog

Analog signal

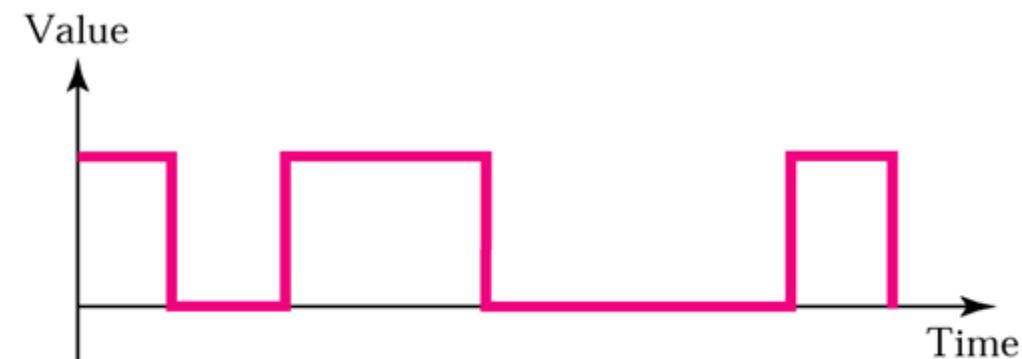
- Continuous waveform
- Can have a infinite number of values in a range
- Ex : Human voice



a. Analog signal

Digital signal

- Discrete
- Can have only a limited number of values
E.g., 0 and 1, i.e., two levels, for binary signal
- Ex : Computer data



b. Digital signal

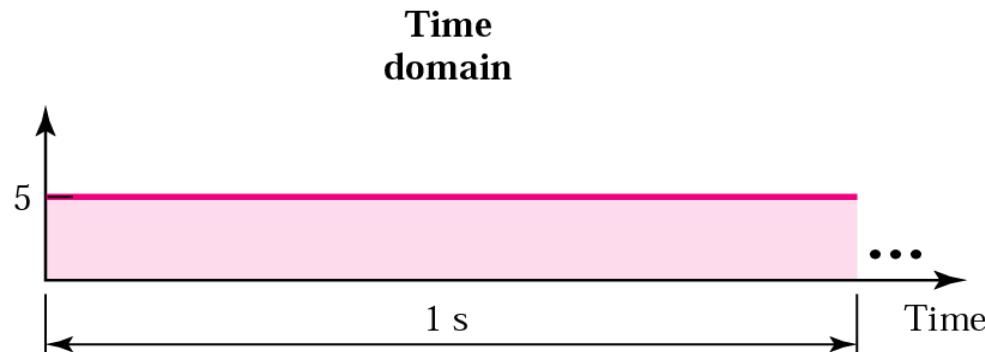
- Computer to modem : Digital
- Modem to modem : Analog

Theoretical Basis for Data Communication(cont.)

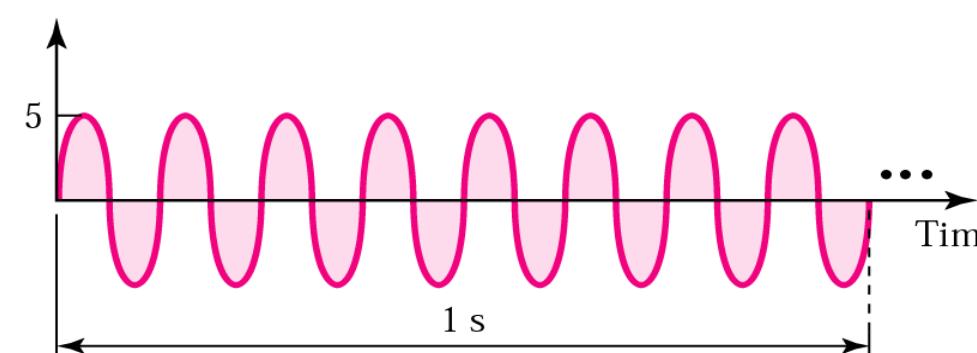
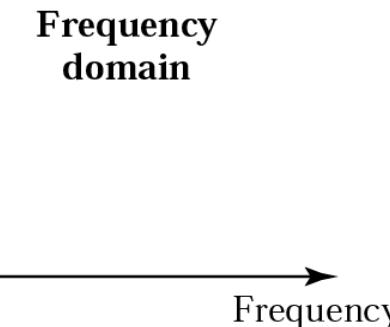
Pre -requisite

Time Vs. Frequency Domain:

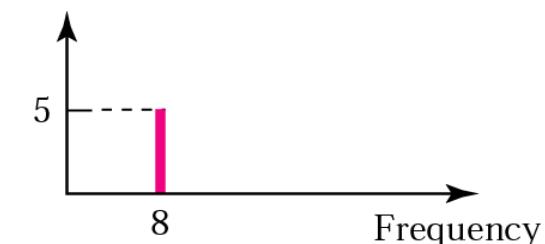
- A signal can be represented in either the **time** domain or the **frequency** domain.
- An analog signal is best analyzed in the **frequency** domain.



a. A signal with frequency 0



b. A signal with frequency 8



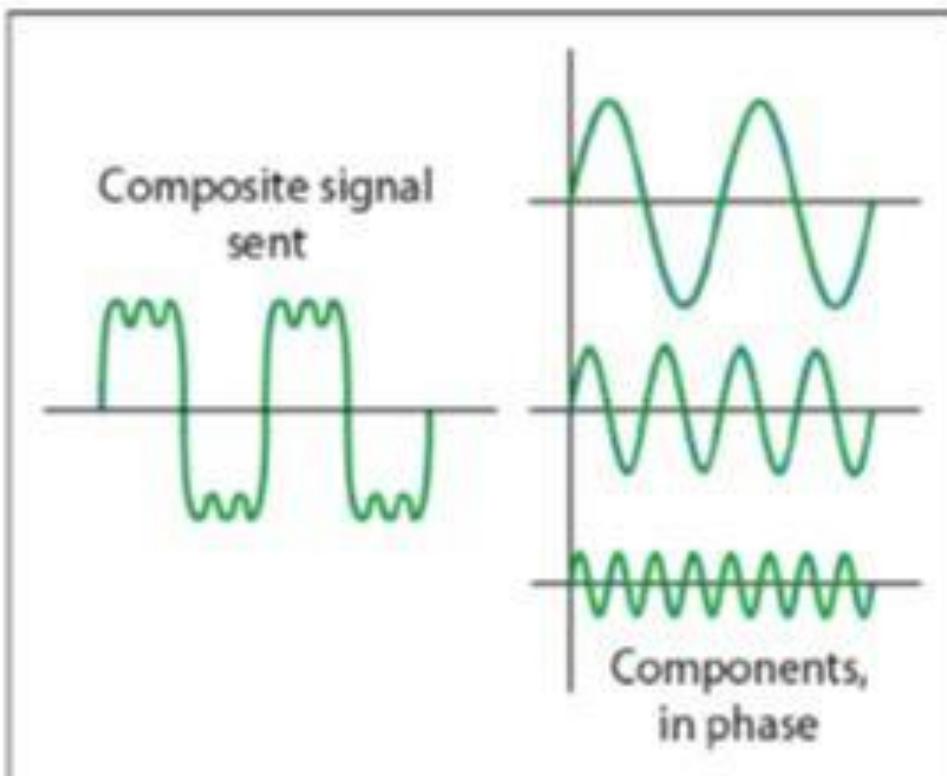
Theoretical Basis for Data Communication(cont.)

Pre -requisite

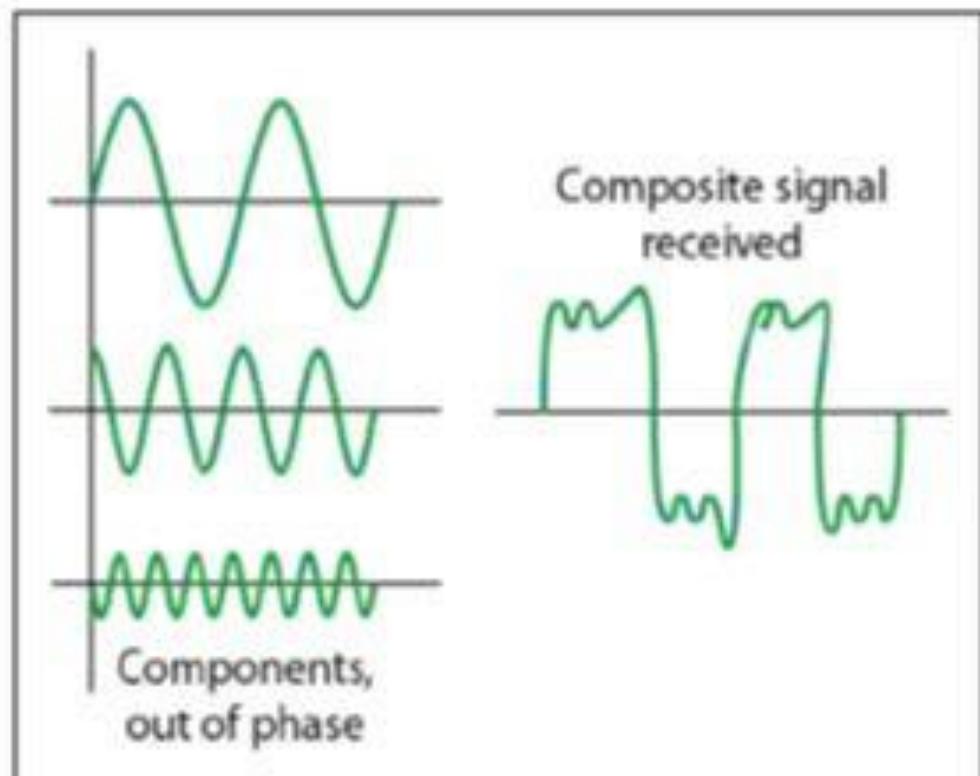
Composite signal:

- Single-frequency sine wave is not useful for data communication.
 - If a single sine wave was used to convey conversation over the phone, we would always hear just a buzz.
 - If we sent one sine wave to transfer data, we would always be sending alternating 0's and 1's, which does not have any communication value.
- If we want to use sine wave for communication, we need to change one or more of its characteristics. For e.g., to send 1 bit, we send a maximum amplitude, and to send 0, the minimum amplitude.
- When we change one or more characteristics of a single-frequency signal, it becomes a **composite signal** made up of many frequencies (**or harmonics**).
- A composite signal is well analyzed in frequency domain.

Composite signal:



At the sender



At the receiver

Theoretical Basis for Data Communication(cont.)

Pre -requisite

Frequency spectrum:

- The description of a signal using the frequency domain and containing all its components is called the **frequency spectrum of the signal**.



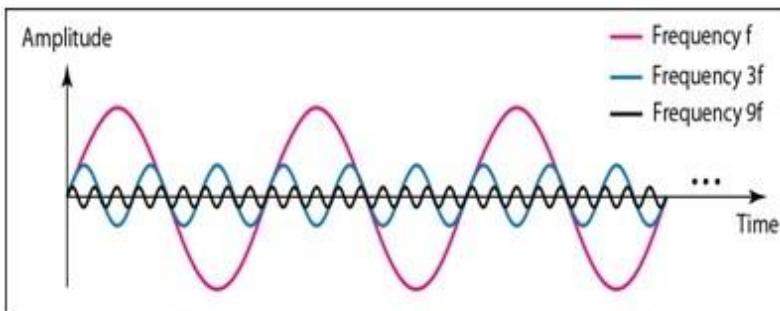
Frequency spectrum of an approximation with only three harmonics

- **Fourier analysis** : Used to analyze the composite signal in frequency domain.
 - **Fourier series** : For periodic signal
 - **Fourier transform** : For aperiodic signal

Periodic Signal

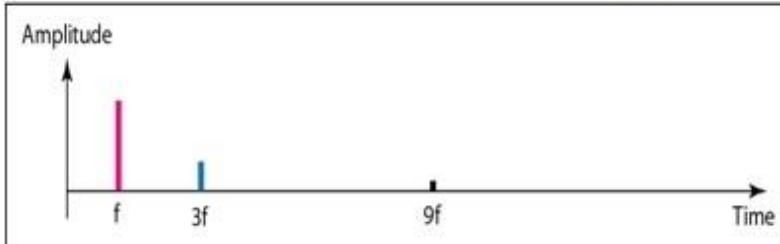
- Definition: A signal is periodic signal when it is repeated over cycle of time or regular interval of time. This means periodic signal repeats its pattern over a period. The function $f(x)$ can be periodic if it satisfies following equation.

$$f(x + p) = f(x)$$

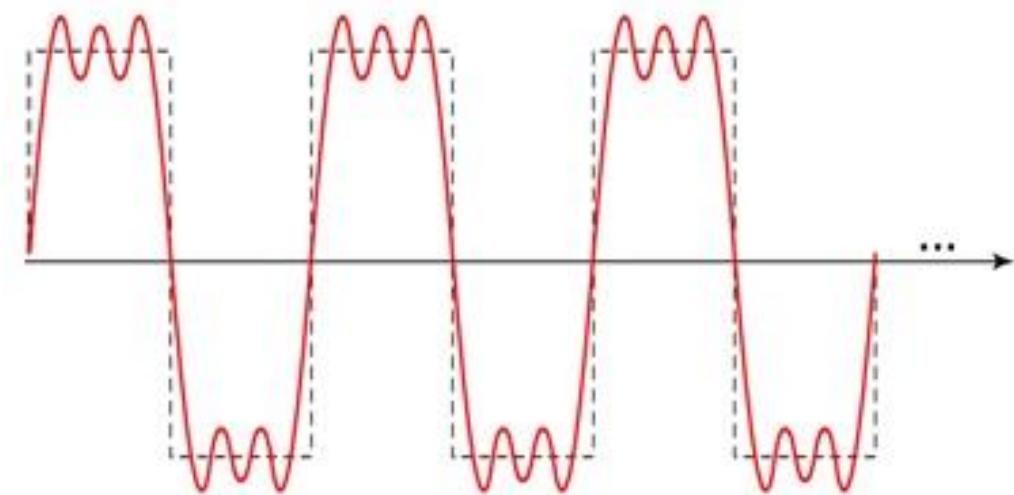


a. Time-domain decomposition of a composite signal

Periodic Signal



b. Frequency-domain decomposition of the composite signal



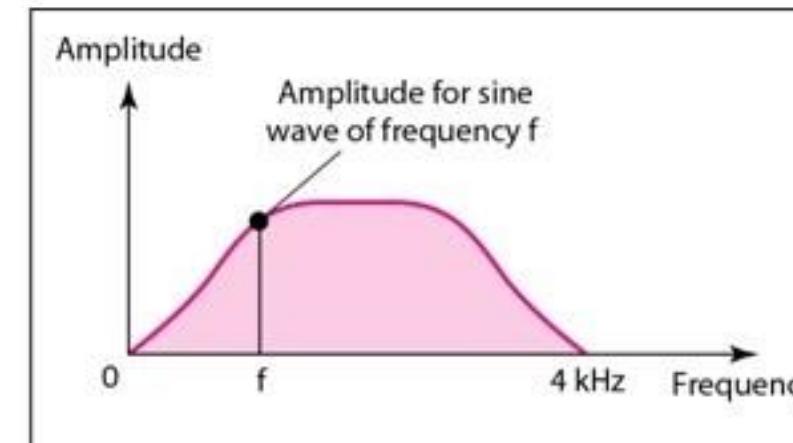
Composite Periodic Signal

Aperiodic Signal or Non-periodic Signal

- Definition: A signal is non-periodic or aperiodic signal when it does not repeat its pattern over a period (i.e., interval of time).



a. Time domain



b. Frequency domain

Aperiodic Signal

Theoretical Basis for Data Communication(cont.)

- Information can be transmitted on wires in the form of variation in voltage or current with time (say $f(t)$).
- Signal behaviour can be modelled and analysed mathematically.

Fourier Analysis:

- A time-varying periodic signal can be represented as a series of frequency components (harmonics): Normally termed as **Fourier series**

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft)$$

$f = 1/T$ – **fundamental frequency**.

a_n, b_n – are the sine and cosine amplitudes of the n 'th **harmonic**.
 c – is a constant.

Theoretical Basis for Data Communication (cont.)

The function can be reconstructed; that is, if the period, T, is known and the amplitudes are given.

$$a_n = \frac{2}{T} \int_0^T g(t) \sin(2\pi n f t) dt$$

$$b_n = \frac{2}{T} \int_0^T g(t) \cos(2\pi n f t) dt$$

$$c = \frac{2}{T} \int_0^T g(t) dt$$

Note :

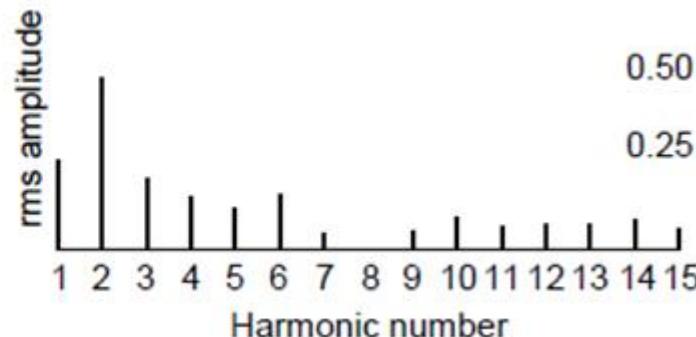
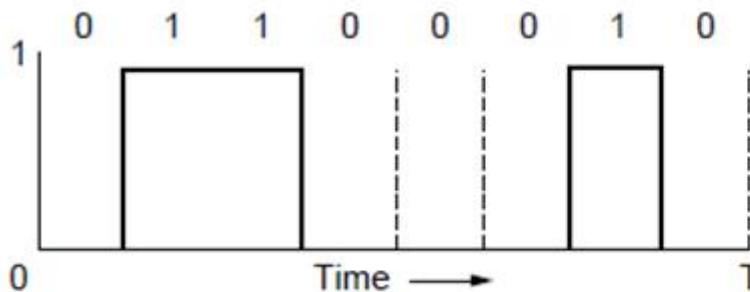
A data signal that has a finite duration thus can be handled by just imagining that it repeats the entire pattern over and over forever (i.e., the interval from T to 2T is the same as from 0 to T, etc.).

Theoretical Basis for Data Communication (cont.)

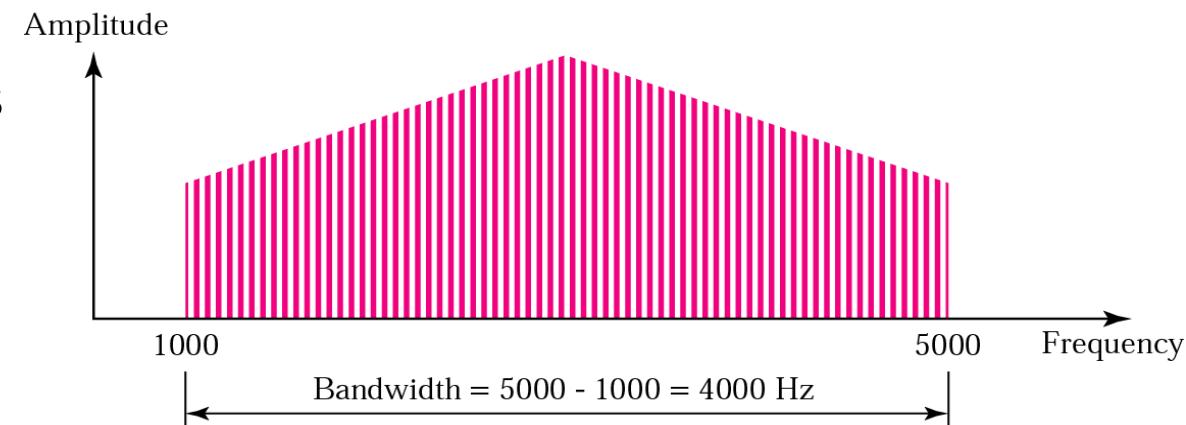
Bandwidth limited signal

- The range of frequencies that a medium can **pass** without loosing one-half of the power contained in that signal is called its **bandwidth**.
- At the signal level, bandwidth is also considered as cut-off frequency (HZ).
- For data transmission it is bits/sec.

Ex: 8-bit (01100010) data transmission



A binary signal and its root-mean-square Fourier amplitudes.



Theoretical Basis for Data Communication (cont.)

Bandwidth limited signal

- Having less bandwidth (harmonics) degrades the signal.

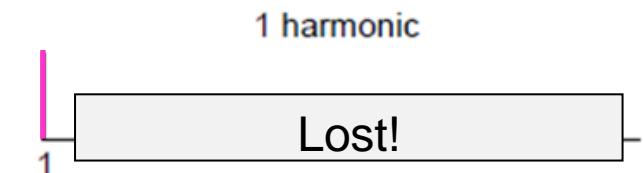
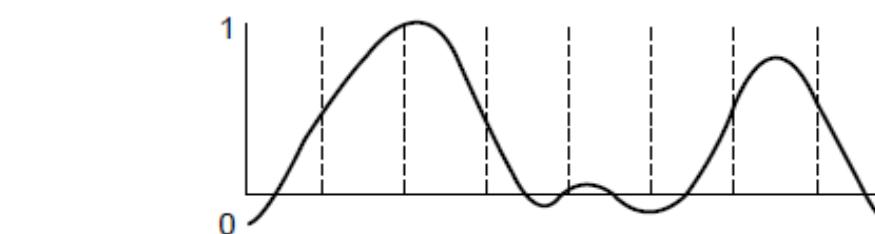
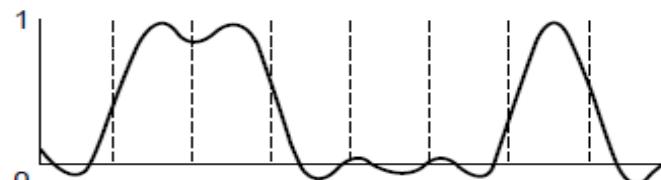
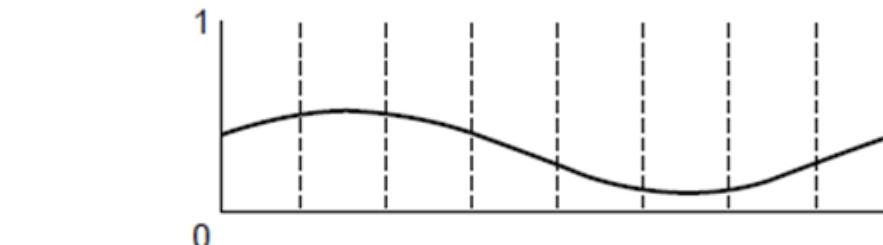
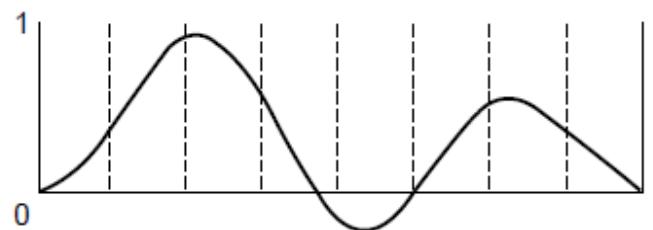
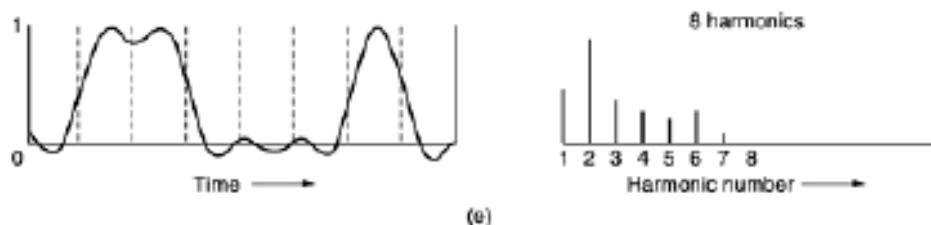
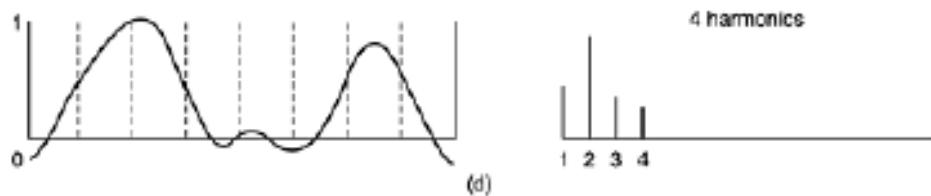
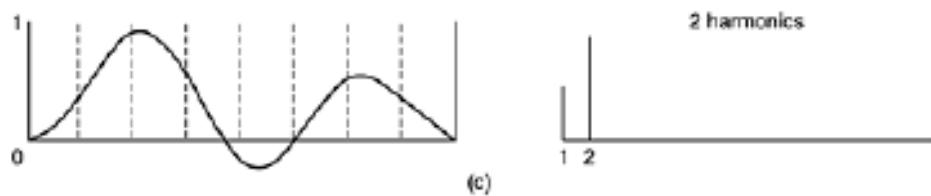
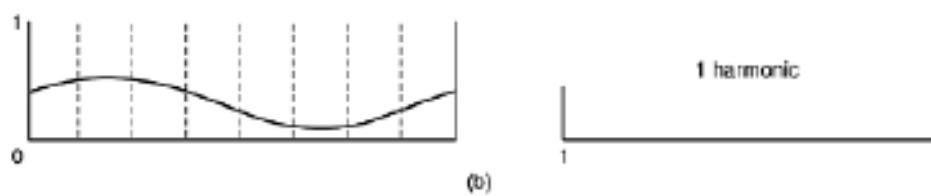
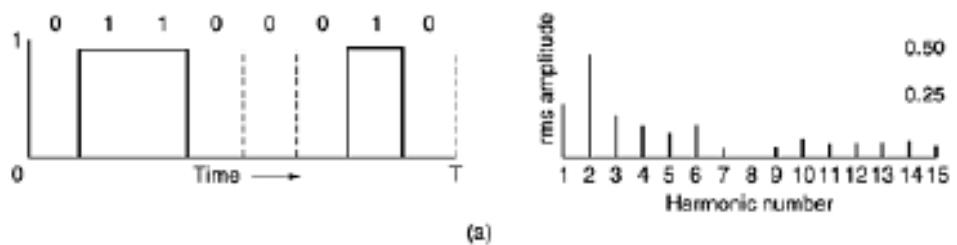


Figure 2-1. (a) A binary signal and its root-mean-square Fourier amplitudes. (b)-(e) Successive approximations to the original signal.



Having less bandwidth
(harmonics) degrades
the signal

Theoretical Basis for Data Communication (cont.)

Bandwidth limited signal

Let a bit rate is b bits/sec.

Time to send 8 bits is $8/b$ sec.

The frequency of the first harmonics is $b/8$ Hz.

The voice-grade line, has cut off frequency just above 3000 Hz. This restriction means that the number of the highest harmonic passed through is roughly $3000/(b/8)$ or $24000/b$, (the cut-off is not sharp).

Bps	T (msec)	First harmonic (Hz)	# Harmonics sent
300	26.67	37.5	80
600	13.33	75	40
1200	6.67	150	20
2400	3.33	300	10
4800	1.67	600	5
9600	0.83	1200	2
19200	0.42	2400	1
38400	0.21	4800	0

Theoretical Basis for Data Communication (cont.)

Maximum Data Rate of a Channel

- Two theorems.
 - Nyquist
 - Shannon
- Nyquist theorem : For noiseless channel
- Shannon's theorem : For noisy channel

Theoretical Basis for Data Communication (cont.)

Maximum Data Rate of a Channel

Nyquist theorem

- If an arbitrary signal passes through a low-pass filter of bandwidth H, the filtered signal can be completely reconstructed by making only $2H$ (exact) samples per second.
- Relates the data rate to the bandwidth (H) and number of signal levels (V) on a noiseless channel.

$$\text{Max. data rate} = 2H \log_2 V \text{ bits/sec}$$

- Ex : A noiseless 3-kHz channel cannot transmit binary (i.e., two-level) signals at a rate exceeding 6000 bps.

$$\text{Max data rate} = 2 \times 3000 \times \log_2 2 = 6000 \times 1 = 6000 \text{ bps}$$

Theoretical Basis for Data Communication (cont.)

Maximum Data Rate of a Channel

Shannon's theorem

- Assumes the presence of thermal noise in the channel due to movement of molecules always.
- The strength of the signal is expressed in the form of $10 \log_{10} (\text{signal power/noise power})$ (i.e. in dB)
- Relates the data rate to the bandwidth (H) and signal strength (S) relative to the noise (N).

$$\text{Max. data rate} = H \log_2(1 + S/N) \text{ bits/sec}$$

- A channel of 3000-Hz bandwidth with a signal to thermal noise ratio (S/N) of 30 dB can never transmit much more than 30,000 bps.

$$10\log_{10}(S/N) = 30 \rightarrow \log_{10}(S/N) = 3 \rightarrow (S/N) = 10^3 \rightarrow 1000$$

Max data rate

$$= 3000 \times \log_2(1 + 1000) = 3000 \times \log_2 1001 = 3000 \times 9.967 < 30000$$

Example

We have a channel with a 1 MHz bandwidth. The SNR for this channel is 63; what is the appropriate bit rate and signal level?

Solution

First, we use the Shannon formula to find our upper limit.

$$\text{Max. data rate} = H \log_2(1 + S/N) \text{ bits/sec}$$

$$C = H \log_2 (1 + S/N) = 10^6 \log_2 (1 + 63) = 10^6 \log_2 (64) = 6 \text{ Mbps}$$

Then we use the Nyquist formula to find the number of signal levels.

$$\text{Max. data rate} = 2H \log_2 V \text{ bits/sec}$$

$$6 \text{ Mbps} = 2 \times 1 \text{ MHz} \times \log_2 V \rightarrow L = 8$$

Theoretical Basis for Data Communication (cont.)

Maximum Data Rate of a Channel

Q1. A noiseless 8-kHz channel is sampled every 1 sec. What is the maximum data rate if the 2 level digital signal are used?

Answer :

$$\text{Number of samples/sec} = 2 \times 8\text{KHz} = 16,000 \text{ samples/sec}$$

Assuming each sample is represented by 2 bits, the data rate = $16,000 \times 2 = 32 \text{ Kbps}$

Q2. Television channels are 6 MHz wide. How many bits/sec can be sent if four-level digital signals are used? Assume a noiseless channel.

Answer :

$$\text{Max. data rate} = 2H \log_2 V \text{ bits/sec}$$

Given $H = 6 \text{ MHz}$, $V = 4$

$$\text{Data rate} = 2 \times 6 \times 10^6 \times (\log_2 4) = 24 \text{ Mbps}$$

Theoretical Basis for Data Communication (cont.)

Maximum Data Rate of a Channel

Q3. If a binary signal is sent over a 3-kHz channel whose signal-to-noise ratio is 20 dB, what is the maximum achievable data rate?

Answer :

$$\text{Max. data rate} = H \log_2(1 + S/N) \text{ bits/sec}$$

Given $S/N = 20 \text{ dB} = 100$, $H = 3 \text{ KHz}$

$$\text{Data rate} = 3 \times 10^3 \times (\log_2 101) = 19.975 \text{ Kbps}$$

However according to Nyquist theorem with this data rate the signal can't be reconstructed at the receiving end.

So, the maximum data rate = $2 \times 3 \text{ KHz} = 6 \text{ Kbps}$ (assuming 1 bit/sample)

Guided transmission media

- Magnetic media
- Twisted pairs
- Coaxial cable
- Fiber optics

Guided transmission media (cont.)

Magnetic media

- Exactly not satisfying the criteria of a computer network.
- Can be used when the transmission rate is slow and a higher amount of data is to be transferred in a stipulated time.
- **Uses magnetic tape or removable media.**
- Physically transported to the destination machine.

Example :

For a bank with **many gigabytes of data** to be backed up **daily on a second machine** (so the bank can continue to function even in the face of a major flood or earthquake), it is likely that no other transmission technology can even begin to approach magnetic tape for performance.

Guided transmission media (cont.)

Twisted Pair

- One of the oldest and still most common transmission media.
- Consists of two insulated copper wires(typically about 1 mm thick) twisted together in a helical form, just like a DNA molecule.
- Effectively less radiation from each wire.
(Two wires in parallel can act as antenna, when twisted waves from different twists cancel out)
- Low cost.
- Adequate performance.
- Most common application of the twisted pair is the telephone system.
- Can run several kilometres without amplification, but for longer distances, repeaters are needed.
- More than one twisted pairs can run in parallel for a substantial distance being bundled together and encased in a protective sheath.
- Can be used for transmitting either analog or digital signals.
- Bandwidth depends on the thickness of the wire and the distance travelled.
(several megabits/sec can be achieved for a few kilometres)

Guided transmission media (cont.)

Twisted Pair

Types :

➤ UTP (unshielded twisted pair)

• Category 3 :

- Two insulated wires gently twisted together and four such pairs grouped in a plastic sheath
- 16 MHz

• Category 5 :

- Similar to category 3, but more twists per centimeter.
- Less crosstalk.
- Better-quality signal over longer distances
- More suitable for high-speed computer communication.
- 100 MHz.

➤ STP (shielded twisted pair) : Not popularly used, bulky than UTP



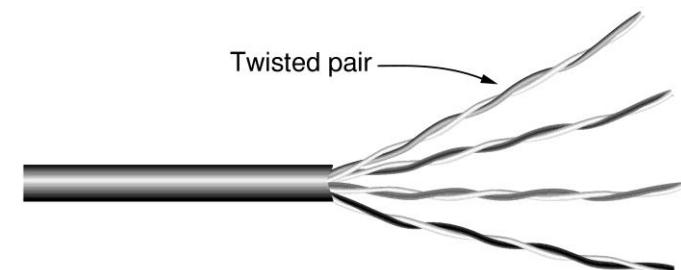
(a)

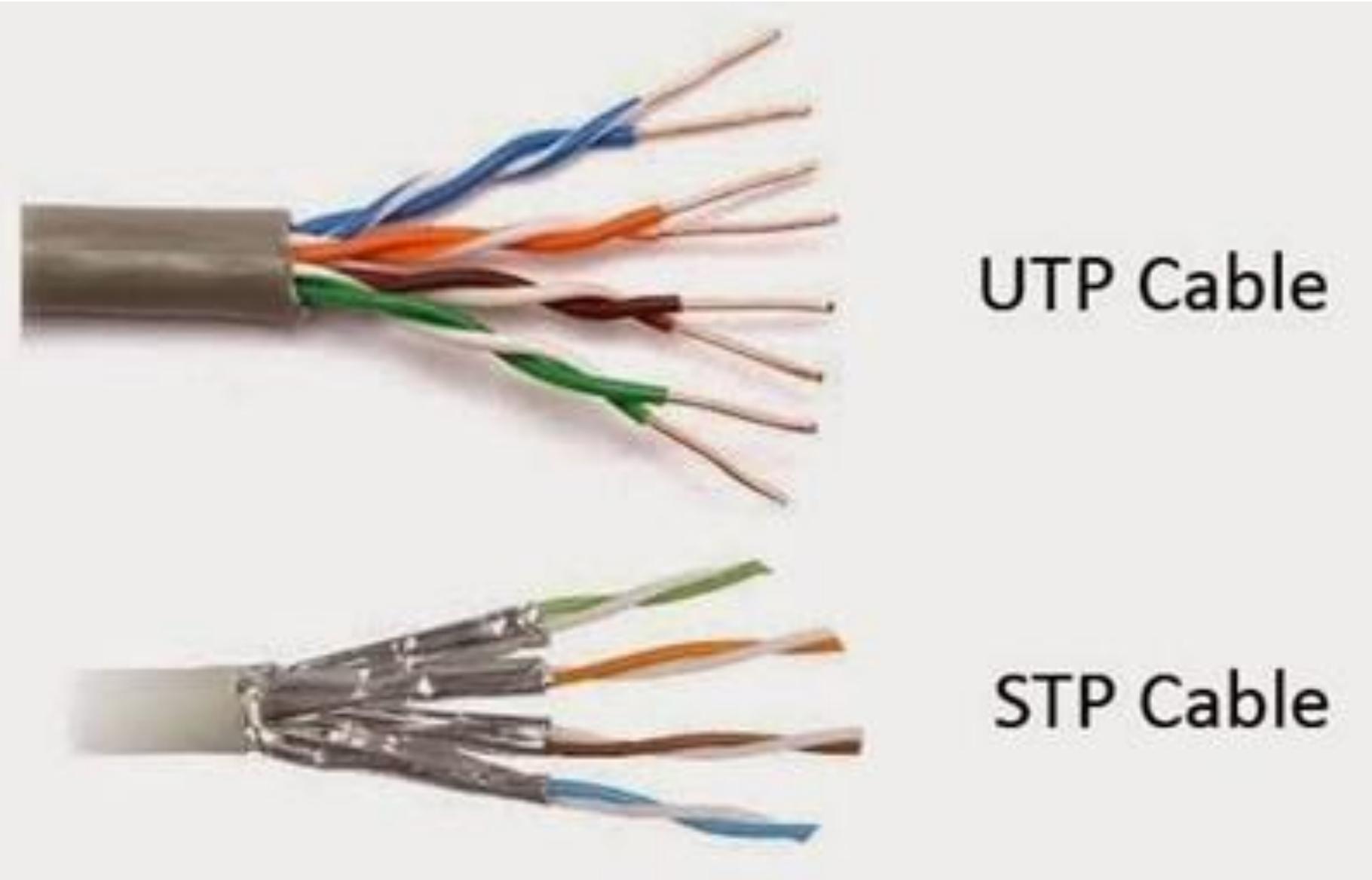


(b)

(a) Category 3 UTP. (b) Category 5 UTP.

Category 5 UTP cable with four twisted pairs





UTP Cable

STP Cable

Guided transmission media (cont.)

Co-axial Cable

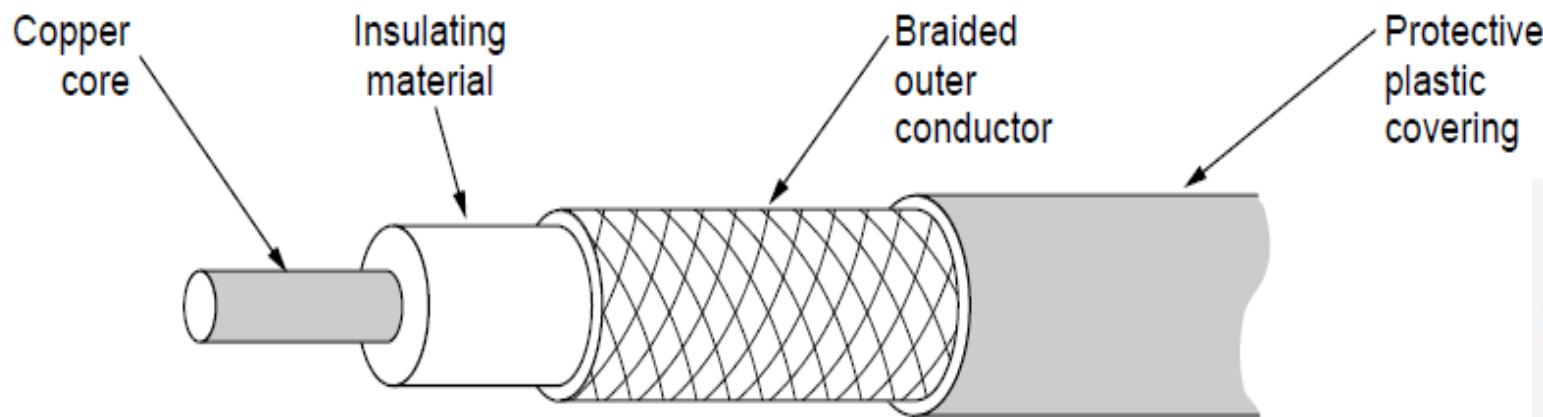
- Better shielding than twisted pairs.
- Span longer distances at higher speeds.
- Two kinds :
 - 50 ohm : Intended for digital transmission.
 - 75 ohm : Mostly analog (Initially for cable TV and now also for internet).
- High bandwidth (close to 1 GHz).
- Excellent noise immunity.

Guided transmission media (cont.)

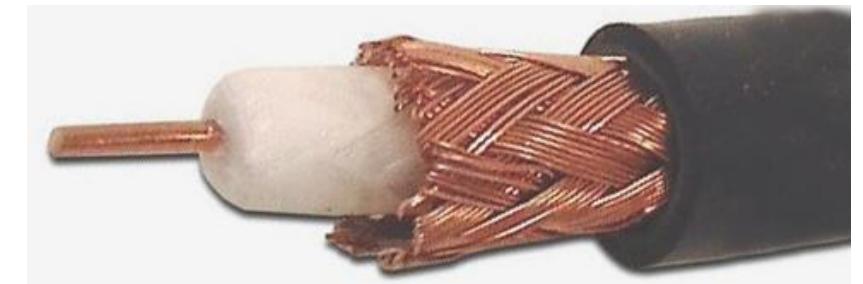
Coaxial Cable

Construction :

- Two conductors : **Inner** and **outer**
- **Inner conductor** : Consists of a stiff copper wire as the core, surrounded by an insulating material.
- The insulator is encased by a cylindrical conductor (**outer conductor**), often as a closely-woven braided mesh.
- The outer conductor is covered in a protective plastic sheath.



Cutaway view of a coaxial cable



Guided transmission media (cont.)

Fiber Optics

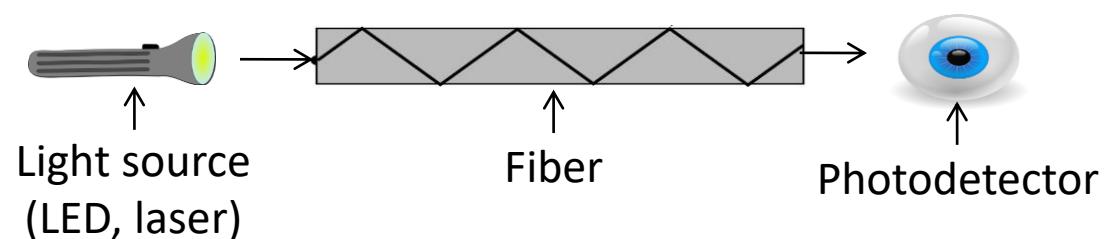
- Widely accepted high speed data communication technology.
- Most common is 1Gbps (but also possible up to 10 Gbps).
- Common for high rates and long distances.
- Popular in the term FTTH (fiber to the home) for internet access.

Optical transmission system:

Three key components :

- (1) Light source : Generates a pulse of light (bit '1') and absence of light (bit '0').
- (2) Transmission medium : Ultra-thin fiber of glass.
- (3) Photo detector : Generates an electrical pulse when light falls on it.

By attaching a light source to one end of an optical fiber and a detector to the other, we have a unidirectional data transmission system that accepts an electrical signal, converts and transmits it by light pulses, and then reconverts the output to an electrical signal at the receiving end.

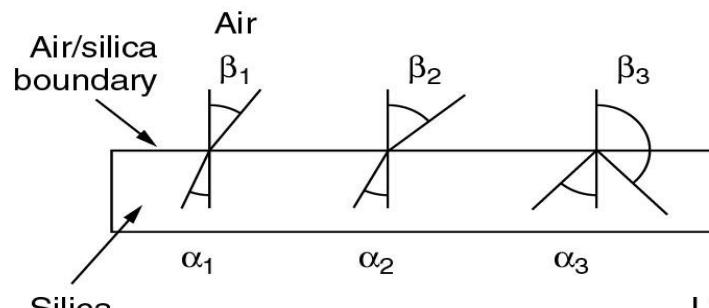


Guided transmission media (cont.)

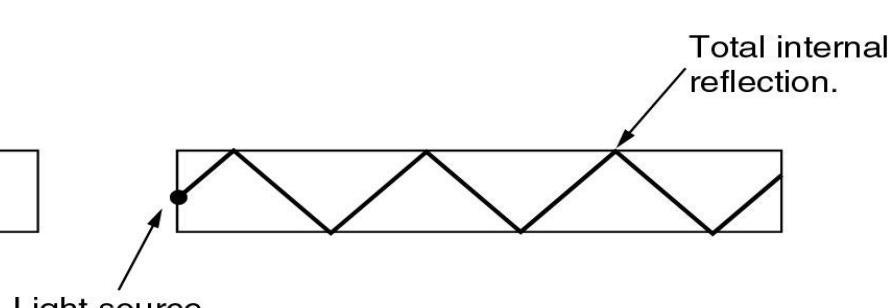
Fiber Optics

Physics behind transmission of light :

- Aim : To avoid loss of light in transmission medium.
- When a light ray passes from one medium to another (e.g. fused silica to air), the ray is refracted (bent) at the silica/air boundary.
- For angles of incidence above a certain **critical value**, the light is reflected back into the silica; none of it escapes into the air.
- Thus, a light ray incident at or above the **critical angle** is trapped inside the fiber, and can propagate for many kilometers with virtually no loss.



(a)



(b)

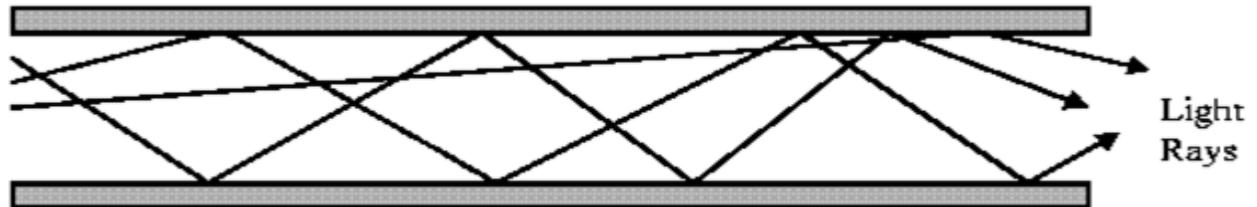
- (a) Three examples of a light ray from inside a silica fiber impinging on the air/silica boundary at different angles.
- (b) Light trapped by total internal reflection.

Guided transmission media (cont.)

Fiber Optics

Multi mode Vs Single mode:

- Multiple light ray can incident at different angles (but above critical angle), to transmit from one end of the transmission medium to other through reflection.
- Fiber used with this property is called a **multimode** fiber.



- If the fiber's diameter is reduced to a few wavelengths of light, the light can propagate only in a straight line, without bouncing.
- Fiber used with this property is called a **singlemode** fiber.
- Single-mode fibers are more expensive but are widely used for longer distances.



Guided transmission media (cont.)

Fiber Optics

Fiber Cables:

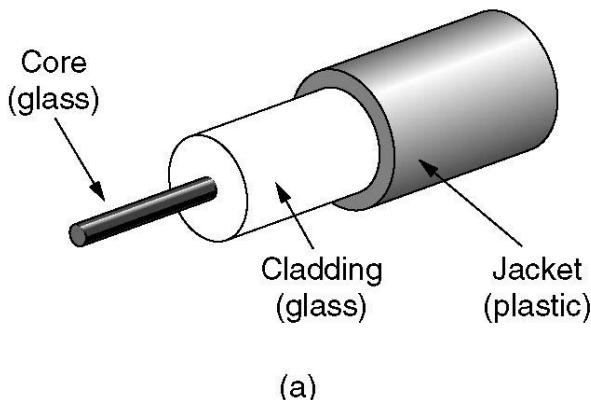
Core : Thin glass fiber at the center through which the light propagates that carries the information.

- 50 microns in diameter for multimode.
- 8 to 10 microns in diameter for singlemode.

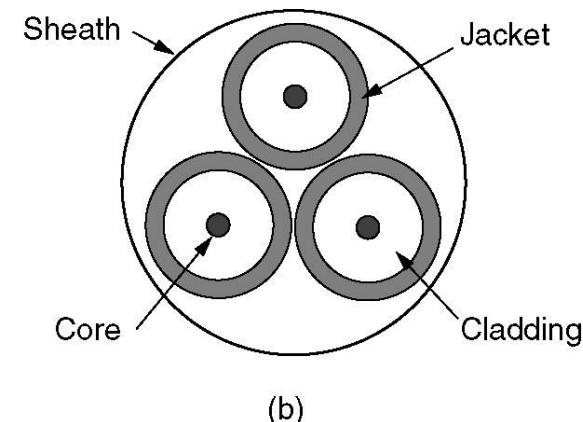
Cladding : The core is surrounded by a glass cladding with a lower index of refraction than the core, to keep all the light in the core.

Jacket : Thin plastic jacket to protect the cladding.

Sheath : Fibers are typically grouped in bundles, protected by an outer sheath.

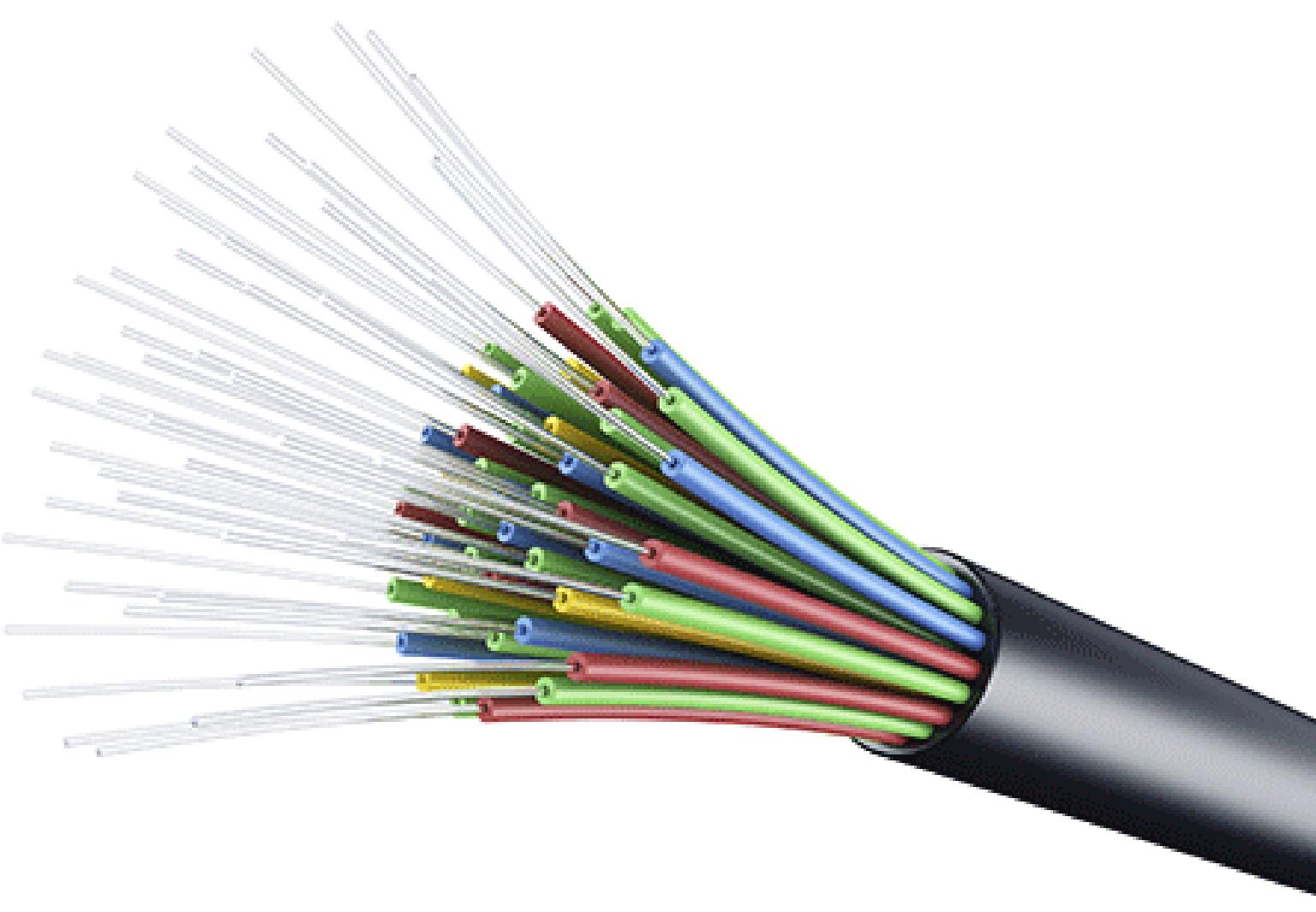


(a)



(b)

(a) Side view of a single fiber. (b) End view of a sheath with three fibers.



Optical fiber



Guided transmission media (cont.)

Fiber Optics

Connection between fibers:

Three different ways.

- They can terminate in connectors and be plugged into fiber sockets.
- Mechanical splices just lay the two carefully-cut ends next to each other in a special sleeve and clamp them in place.
- Two pieces of fiber can be fused (melted) to form a solid connection.

For all three kinds of splices, reflections can occur at the point of the splice (i.e. attenuation/loss).

Guided transmission media (cont.)

Fiber Optics

Light source and comparison:

1. Light emitting diode (LED).
2. Semiconductor LASER.

Item	LED	Semiconductor laser
Data rate	Low	High
Fiber type	Multi-mode	Multi-mode or single-mode
Distance	Short	Long
Lifetime	Long life	Short life
Temperature sensitivity	Minor	Substantial
Cost	Low cost	Expensive

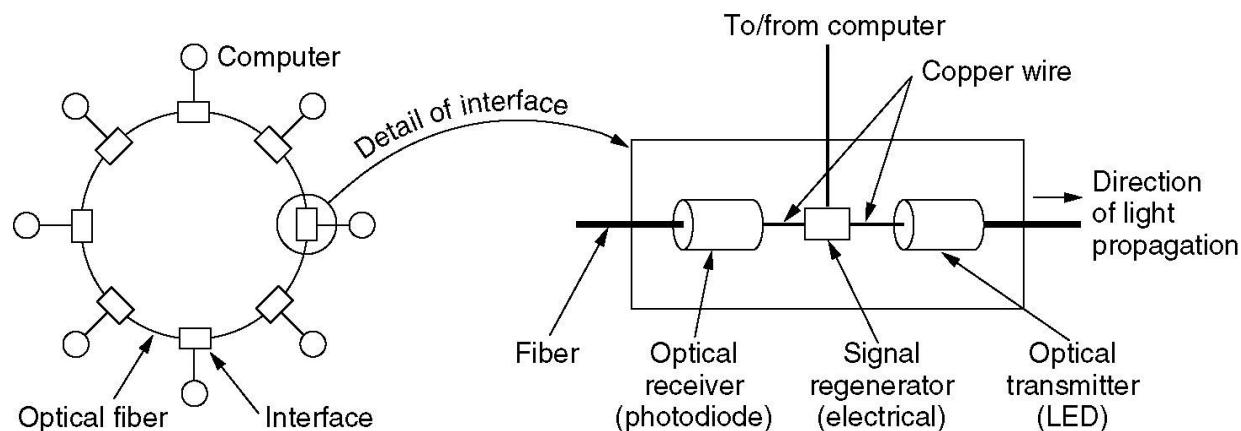
A comparison of semiconductor laser and LEDs as light sources

Guided transmission media (cont.)

Fiber Optics

Fiber Optic Networks:

- Used for LANs as well as for long-haul transmission, although tapping into it is more complex than connecting to an Ethernet.
- Two types of interface :
 - Passive : At the transmitting and receiving end.
 - Active : In between two fiber cable for increasing the strength of the signal (if falls down)



A fiber optic ring with active repeaters

Guided transmission media (cont.)

Fiber Optics Vs Copper Wire: A comparison

Property	Wires	Fiber
Distance	Short (100s of m)	Long (tens of km)
Bandwidth	Moderate	Very High
Cost	Inexpensive	Less cheap
Convenience	Easy to use	Less easy
Security	Easy to tap	Hard to tap

Wireless Transmission

- Fulfils the need of mobile users to get connected with network for accessing data in their laptops, notebooks etc.
- Use radio waves or infrared light to transmit data.
 - The Electromagnetic Spectrum
 - Radio Transmission
 - Microwave Transmission
 - Infrared and Millimeter Waves
 - Light wave Transmission

Wireless Transmission(cont.)

The Electromagnetic Spectrum

- When electrons move, they create **electromagnetic waves** that can propagate through space (even in a vacuum).
- **Electromagnetic waves** are characterized with two variables:
 1. Frequency (f)
 2. Wavelength (λ)
- In vacuum, all **electromagnetic waves** travel at the same speed (speed of light (c), no matter what their frequency.
- The fundamental relation between f , λ , and c (in vacuum) is
$$c = f\lambda$$
- When an antenna of the appropriate size is attached to an electrical circuit, the **electromagnetic waves can be broadcast efficiently and received by a receiver** some distance away.(Basic principle behind wireless communication)

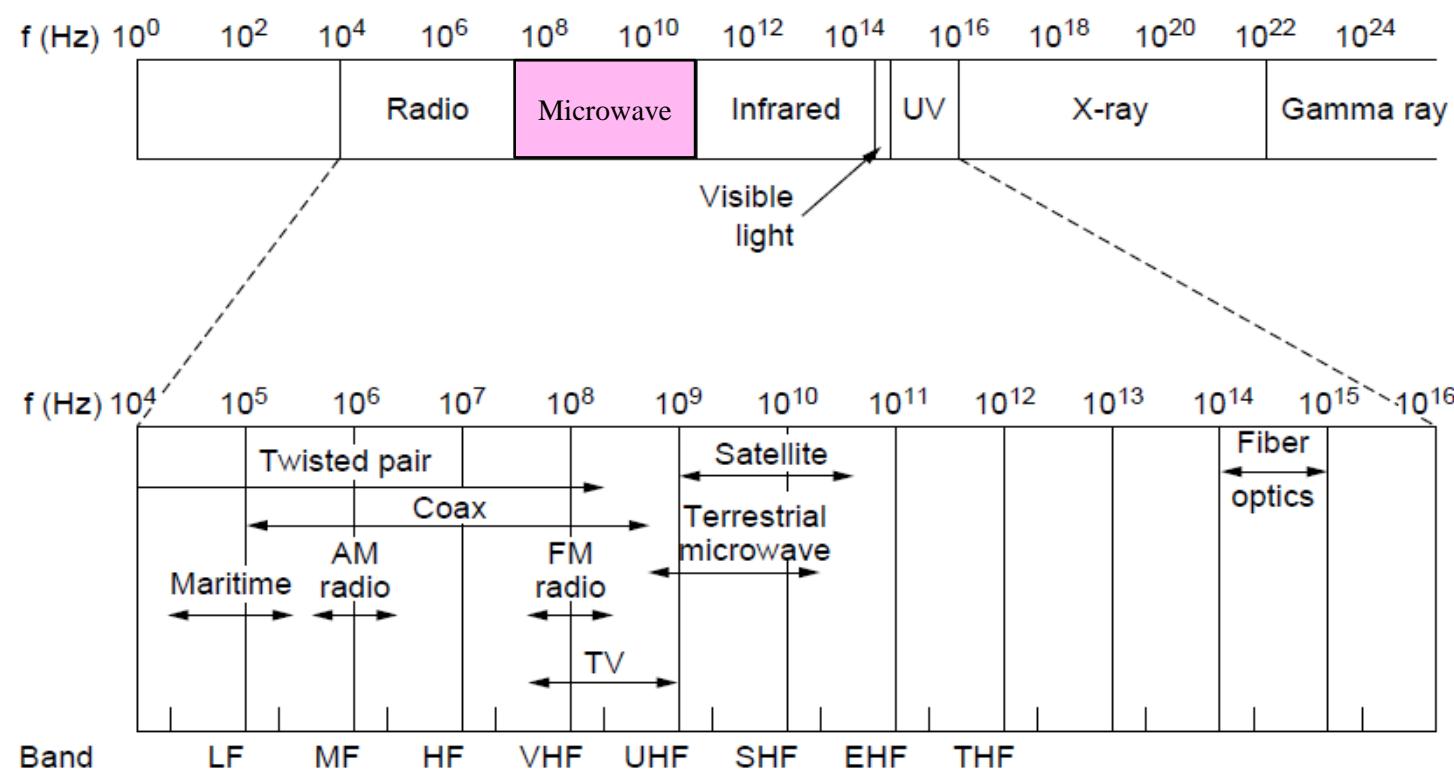
Wireless Transmission(cont.)

The Electromagnetic Spectrum

- Different bands have different uses:
 - Radio: wide-area broadcast; Infrared/Light: line-of-sight
 - Microwave: LANs and 3G/4G; ← Networking focus

- The radio, microwave, infrared, and visible light portions of the spectrum can be used for transmitting information through modulation.

- UV light, X-rays, and gamma rays would be even better, due to their higher frequencies.
- They are hard to produce and modulate, do not propagate well through buildings, and are dangerous to living things.



Wireless Transmission(cont.)

The Electromagnetic Spectrum

- The amount of information that an electromagnetic wave can carry is related to its bandwidth.
- At low frequencies it is possible to encode a few bits per Hertz.
- At high frequencies it is possible to encode as many as 8 bits per Hertz.

(e.g. a coaxial cable with a 750 MHz bandwidth can carry several gigabits/sec.)

- Bandwidth depends on width of the wavelength of the EM wave.

$$\Delta f = \frac{c \Delta \lambda}{\lambda^2}$$

- wider the band, the higher the data rate.

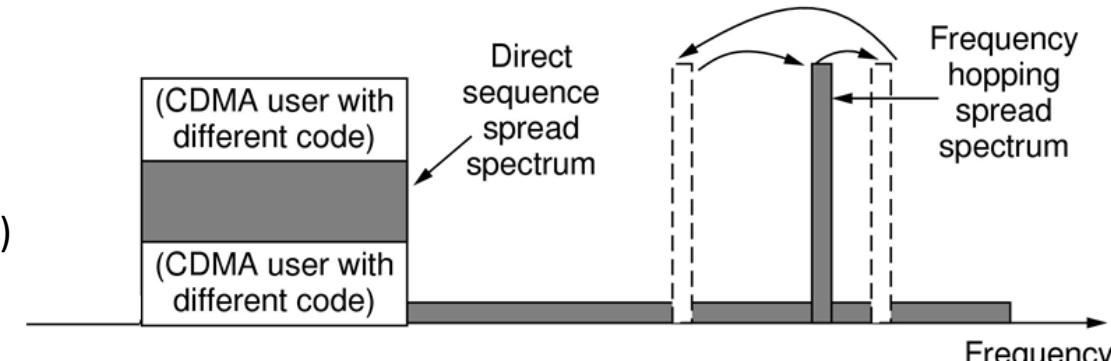
(e.g. a 1.3 micron band with $\Delta \lambda = 0.17 \times 10^{-6}$ supports 30 THz bandwidth or data rate of 240 Tbps)

Wireless Transmission(cont.)

The Electromagnetic Spectrum

Types of transmissions with respect to bandwidth :

- Narrowband transmission
 - Efficient use of spectrum
 - Good quality transmission
- Wideband transmission
 - FHSS (Frequency hopping spread spectrum)
 - The transmitter hops from frequency to frequency hundreds of times per second.
 - Popular in military communications.
 - Makes transmissions hard to detect.
 - Impossible to jam.
 - Offers good resistance to multipath fading (avoids interference)
 - DSSS (Direct sequence spread spectrum)
 - Uses a code sequence to spread the signal over a wide frequency band (e.g. CDMA).
 - Spectrally efficient for multiple signal transmission sharing same channel.



Wireless Transmission(cont.)

Radio Transmission

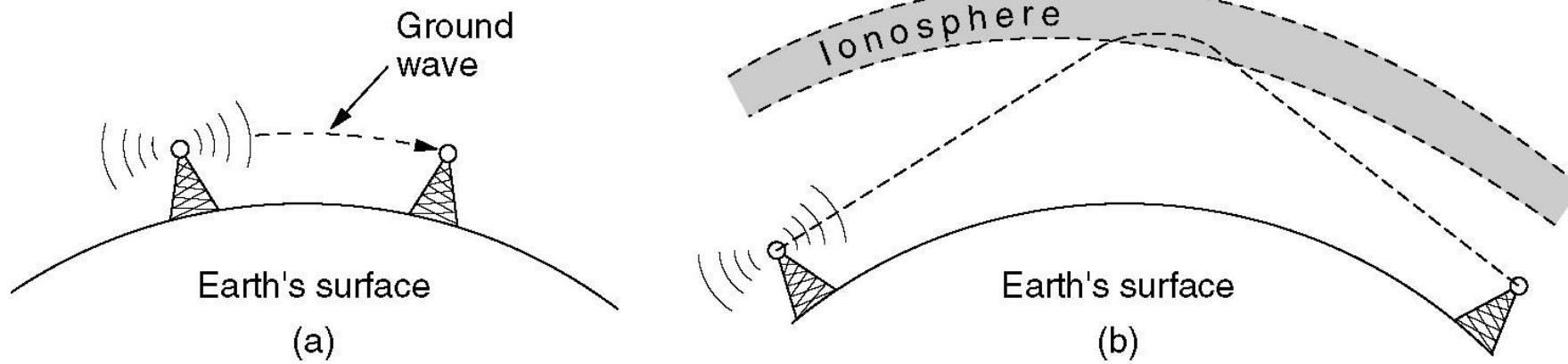
- Data transmits in the form of radio signals(or waves).
- Air/free space - medium of transmission
- RF waves are:
 - Easy to generate
 - Can travel a long distance
 - Penetrate buildings easily
 - Mostly **omnidirectional** (so, transmitter and receiver do not have to be carefully aligned physically)

Wireless Transmission(cont.)

Radio Transmission

Transmission property is frequency dependent.

- At low frequencies, radio waves pass through obstacles well, but the power falls off sharply with distance from the source, roughly as $1/r^2$ in air.
- At high frequencies, radio waves tend to travel in straight lines and bounce off obstacles.



(a) In the VLF, LF, and MF bands, radio waves follow the curvature of the earth.

(b) In the HF band, they bounce off the ionosphere.

Wireless Transmission(cont.)

Microwave Transmission

- The signals (or waves) above 100 MHz that travels in nearly straight line.
- Mostly uses parabolic antenna to achieve higher S/N ratio.
- Requires carefully alignment between transmission and Reception antennas.
- Before fiber optics, for decades these microwaves formed the heart of the long-distance telephone transmission system.
- Since the microwaves travel in a straight line, if the towers are too far apart, the earth will get in the way and thus requires repeater in between.
- Suffers from low penetration capability through buildings.
- Possibility of multipath fading due to reflected wave (delayed version of transmitted wave).

Wireless Transmission(cont.)

Infrared and Millimetre Waves

- Widely used for short-range communication(e.g. The remote controls used on televisions, VCRs, and stereos all use infrared communication.)
- Relatively directional, cheap and easy to build.
- Major drawback: they do not pass through solid objects, but can be treated as advantage (e.g. infrared transmission in one room never interferes to infrared transmission in other room.)
- No government license is needed to operate an infrared system.
- Mostly for indoor use.

Wireless vs. Wires/Fiber

Wireless:

- + Easy and inexpensive to deploy
- + Naturally supports mobility
- + Naturally supports broadcast
- Transmissions interfere and must be managed
- Signal strengths hence data rates vary greatly

Wires/Fiber:

- + Easy to engineer a fixed data rate over point-to-point links
- Can be expensive to deploy, esp. over distances
- Doesn't readily support mobility or broadcast

Public Switched Telephone Network (PSTN)

When the distances between computers are large or there are many computers to communicate with each other, the cables may have to pass through a public road or other public right of way.

Issues :

- Costs of running private cables are usually prohibitive.
- Stringing private transmission lines across (or underneath) public property is also illegal.

Solution to the issues :

- Rely on the existing telecommunication facilities (i.e. **PSTN**).

PSTN :

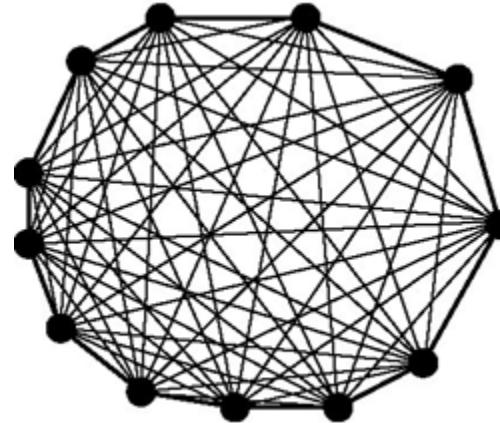
- Initially designed to provide voice communication service.
- Acceptable for data communication with lower magnitude of performance.
(e.g. A cable running between two computers can transfer data at 10^9 bps, In contrast, a dial-up line has a maximum data rate of 56 kbps)
- Trade off between speed and data communication services.

Note : In the due course of time with the use of advanced technology the performance w.r.t data communication through dial up service has also been enhanced.

Public Switched Telephone Network (cont.)

Structure of the Telephone System

- Soon after the commercialization of telephone instrument (in 1876), there was a high demand of interconnection between a pair of telephones in different houses in cities.
- Within a year, the cities were covered with wires (for making connections between a pair of phones) passing over houses and trees in a wild jumble.



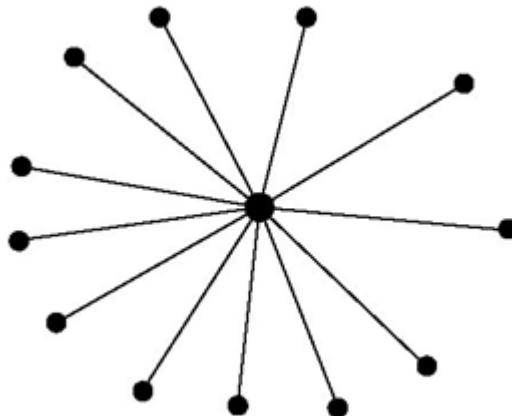
Fully-interconnected network.

- It became immediately obvious that the model of connecting every telephone to every other telephone, as shown in above figure, was not going to work.

Public Switched Telephone Network (cont.)

Structure of the Telephone System

- Formation of Bell Telephone Company, which opened its first switching office in 1878.
- The company ran a wire to each customer's house or office.
- Establishment of call between two customers takes place through the switching office.
(i.e. an operator makes the connection between caller and callee manually using a jumper wire.)



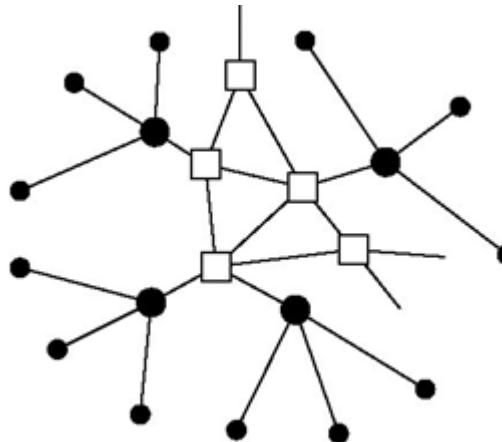
Centralized switch.

- A requirement of switching office in every city.

Public Switched Telephone Network (cont.)

Structure of the Telephone System

- People wanted to make long distance calls between cities, so the Bell system began to connect the switching offices.
- To connect every switching office to every other switching office by means of a wire between them quickly became unmanageable as happened in the beginning for connecting two telephones.
- Second-level switching offices were installed, and grew in number to fulfil the need.
- The system takes a look of hierarchical structure of offices.



Two-level hierarchy.

Public Switched Telephone Network (cont.)

Structure of the Telephone System

Three major parts of the telephone system to provide connection between two customers.

- The switching offices.
- The wires between the customers and the switching offices.
- The long-distance connections between the switching offices.

This basic Bell System model has remained essentially intact for over 100 years.

Concept of Local loop :

- Each telephone has two copper wires coming out of it that go directly to the telephone company's nearest end office situated at a distance between 1 to 10 km.
- The two-wire connections between each subscriber's telephone and the end office are known in the trade as the **local loop**.

Public Switched Telephone Network (cont.)

Structure of the Telephone System

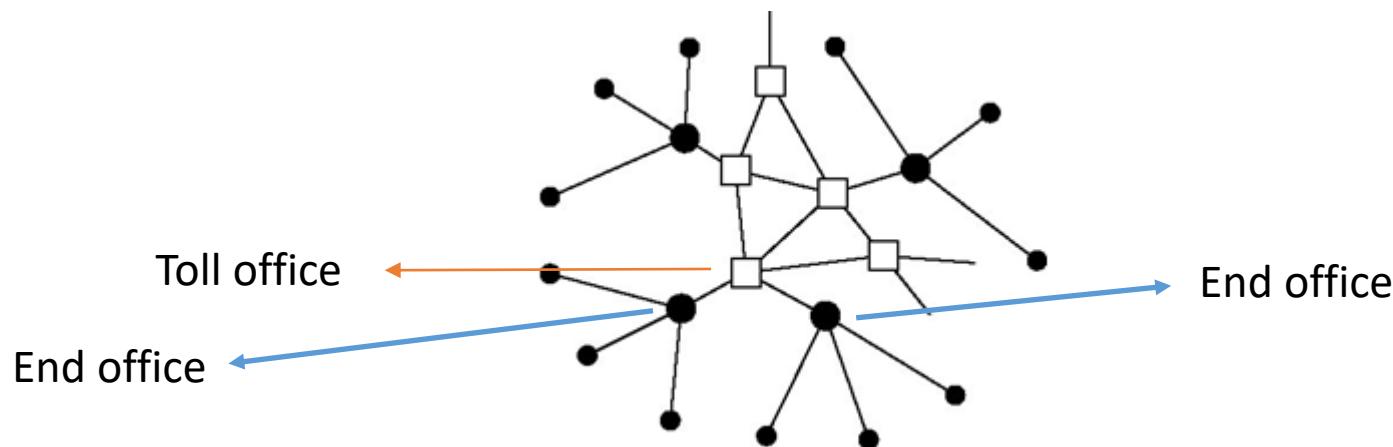
Communication process through telephone system:

Case 1 : Both subscribers attached to same end office.

- The switching mechanism within the office sets up a direct electrical connection between the two local loops.

Case 2 : Both subscribers attached to two different end office.

- Each end office has a number of outgoing lines(known as trunks) to one or more nearby switching centers, called toll offices.
- If both end offices are connected to same toll office, connection is limited within same toll office.

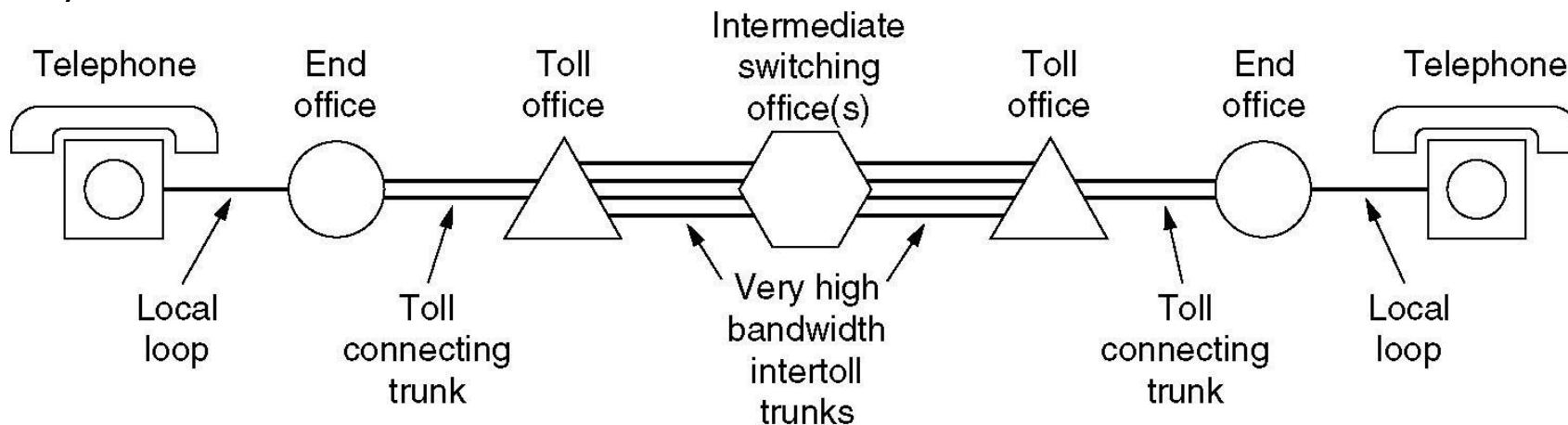


Public Switched Telephone Network (cont.)

Structure of the Telephone System

Case 3 : The caller and callee do not have a toll office in common.

- Communication established with the help of higher level in hierarchy (i.e. high bandwidth Inter toll trunks)



A typical circuit route for a medium-distance call.

Transmission media :

- Local loops consist of category 3 twisted pairs nowadays (early days, uninsulated wires spaced 25 cm apart on telephone poles).
- Between switching offices, coaxial cables, microwaves, and especially fiber optics are widely used.

Public Switched Telephone Network (cont.)

Structure of the Telephone System

Components in technical term in telephone system and their importance:

Three major components.

1. **Local loops** (analog twisted pairs going into houses and businesses).
 - Gives access to everyone into the whole system, so important.
2. **Trunks** (digital fiber optics connecting the switching offices).
 - For long haul trunks transmission of multiple calls together through single fiber(i.e. multiplexing) is an important issue.
3. **Switching offices** (where calls are moved from one trunk to another).
 - Switching can be done in different ways, so important.

The Local Loop: Modems, ADSL and Wireless

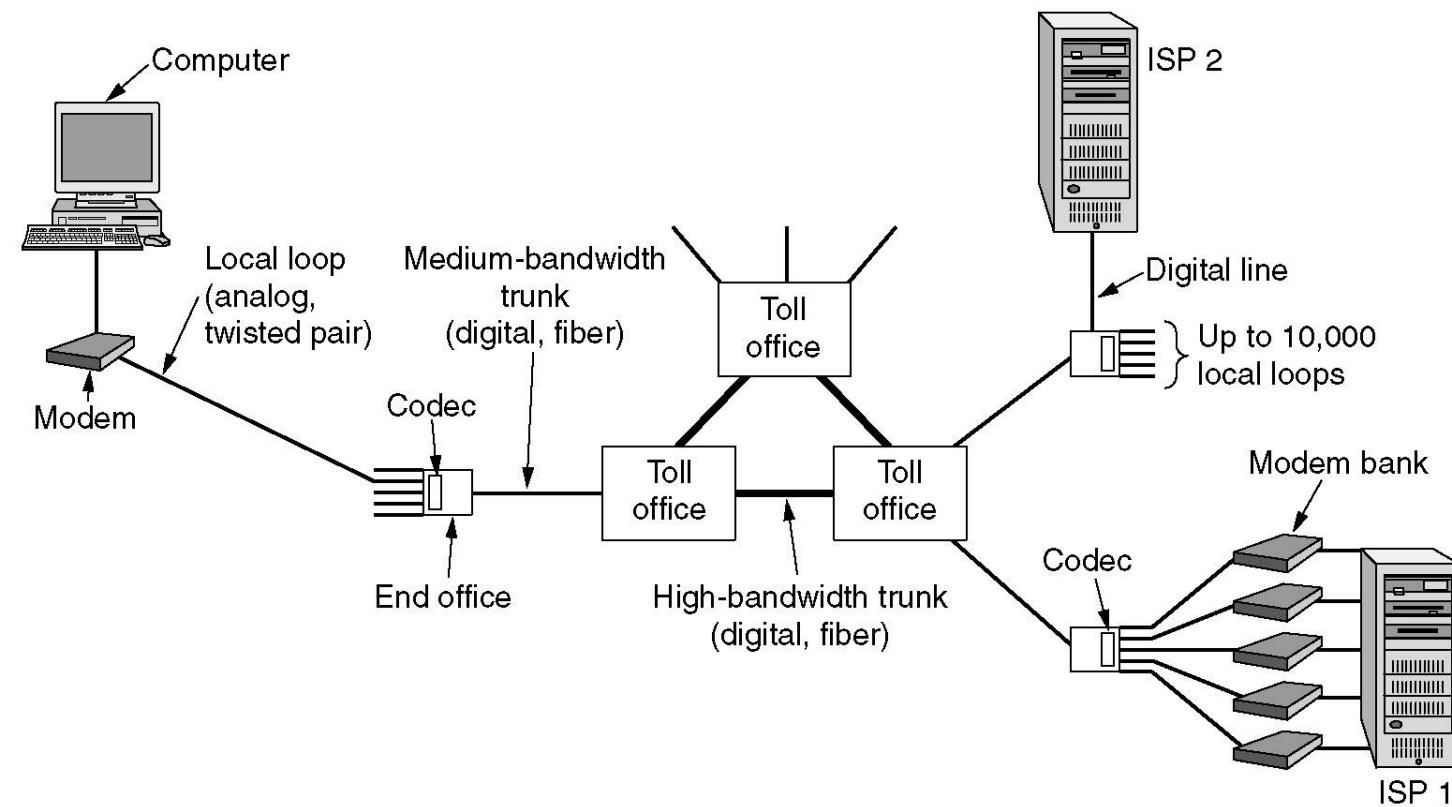
The computer to computer communication through telephone system involves both analog and digital transmission.

Local loop : Analog

End office – Toll office : Digital

Toll office – Toll office : Digital

Conversion between analog and digital done by modems and codecs.



The use of both analog and digital transmission for a computer to computer call.

The Local Loop: Modems, ADSL and Wireless(cont.)

- Though the computer works with digital data comprising of less error, due to the imperfection of transmission line the received signal in a telephone system may not be equal to the transmitted signal.
- Transmission lines suffer from three major problems: **attenuation**, **delay distortion**, and **noise**.

Attenuation:

- Loss of energy due to transmission over a distance (i.e. distance dependent).
- Loss of energy due to transmission of multiple frequency component in a signal (i.e. frequency dependent).
- Usually recovered by the use of amplifiers and equalizers.

Delay distortion:

- Caused due to transmission of multiple frequency component at different speeds.

Noise:

- Unwanted energy from sources other than transmitter (e.g. thermal noise, cross talk and impulse noise).
- **Thermal noise** : Caused by the random motion of the electrons in a wire and is unavoidable.
- **Crosstalk** : Caused by inductive coupling between two wires that are closed to each other.
- **Impulse noise** : Caused by spikes in the power line.

The Local Loop: Modems, ADSL and Wireless(cont.)

Modems

- Short form for Modulator-Demodulator.
- Modulation in transmitting end and demodulation in receiving end.

Why modulation ?

- Square waves used in digital signals have a wide frequency spectrum and thus are subject to strong attenuation and delay distortion.
- Baseband (DC) signalling found unsuitable except at slow speeds and over short distances.
- Solution : AC signalling (e.g. use of sine wave of 1-2 KHz to carry digital signal).
- Carrier signal changes its characteristics (i.e. amplitude, frequency or phase) according to baseband signal – Modulation.

The Local Loop: Modems, ADSL and Wireless(cont.)

Modems

Amplitude Modulation : ASK (Amplitude Shift Keying)

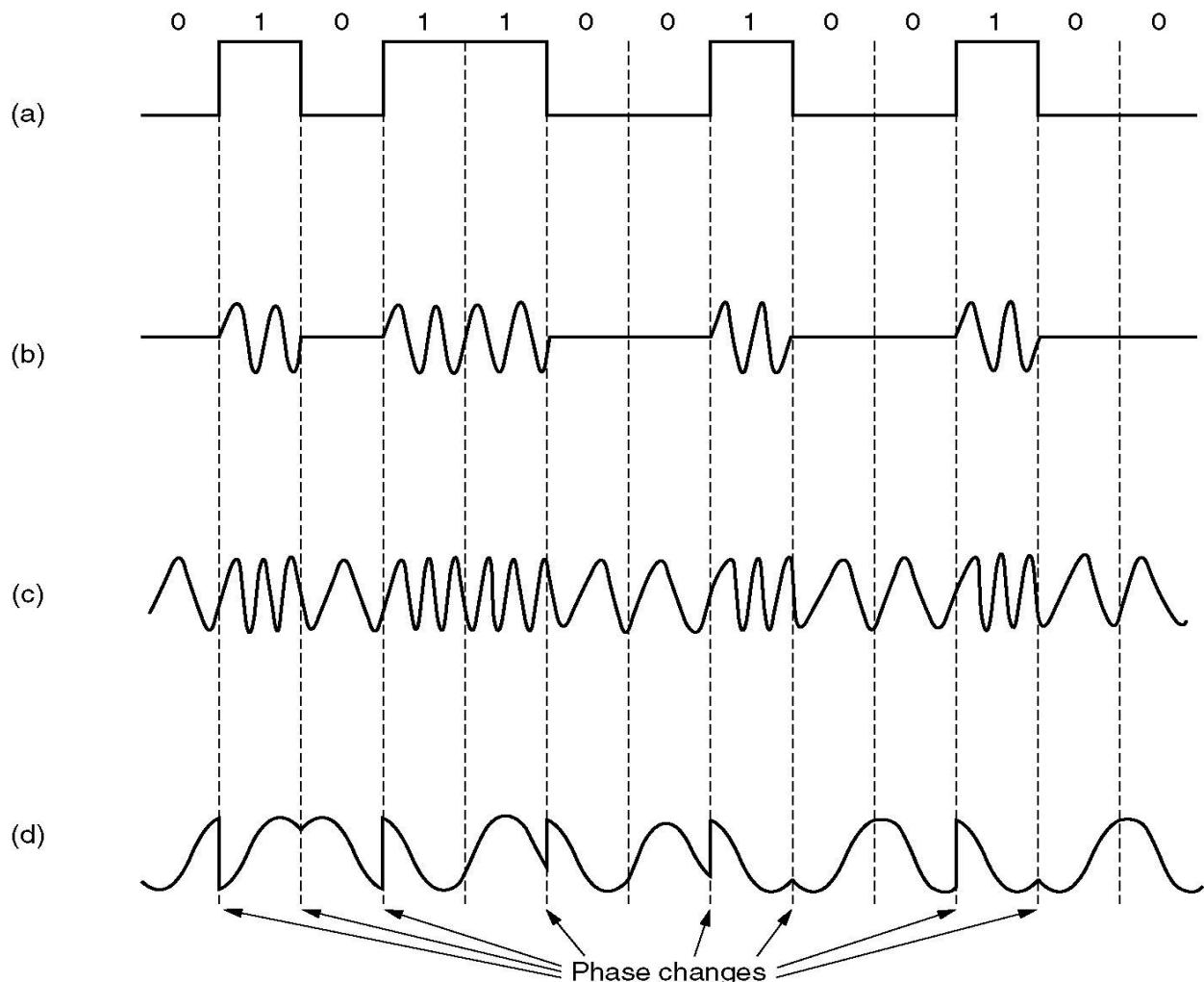
- Change in amplitude of carrier based on amplitude of baseband.
- For Binary signal two different amplitudes are used.

Frequency Modulation : FSK (Frequency Shift keying)

- Change in frequency of the carrier based on amplitude of baseband.
- For binary signal two different frequencies are used.

Phase Modulation : PSK (Phase shift Keying)

- Phase of the carrier changes based on amplitude of baseband signal.
- For binary signal two (0^0 and 180^0)/four phase angles (45^0 , 135^0 , 225^0 , or 315^0) are used depending on no. of bits transmitted per time interval.
- Ex : BPSK, QPSK



The Local Loop: Modems, ADSL and Wireless(cont.)

Modems

Concept of Bandwidth, Baud rate, Symbol rate, bit rate :

The data transmission rate in the channel can be associated with various terminologies such as **bandwidth**, **baud rate**, **symbol rate** and **bit rate**.

Bandwidth : Property of transmission medium which represents the range of frequencies that pass through it with minimum attenuation (measured in Hz).

Baud rate : The number of samples/sec made to be transmitted.

Symbol rate : The amount of information sample(i.e. symbol) transmitted per second.

(If each sample denotes one piece of information is a symbol, then baud rate is same as symbol rate)

Bit rate : Amount of information sent over the channel and is equal to the number of symbols/sec times the number of bits/symbol.

(Note : The modulation technique decides the no. of bits to be used to represent a symbol(e.g. in QPSK each symbol is represented by 2 bits))

Example :

If the baud rate is 2400 and each symbol is represented by 1 bit ('0' or '1'), then bit rate is 2400 bps.

If the baud rate is 2400 and each symbol is represented by 2 bits, then bit rate is 4800 bps.

The Local Loop: Modems, ADSL and Wireless(cont.)

Modems

- All advanced modems use a combination of modulation techniques to transmit multiple bits per baud.
- Often multiple amplitudes and multiple phase shifts are combined to transmit several bits/symbol.

QPSK (Quadrature PSK):

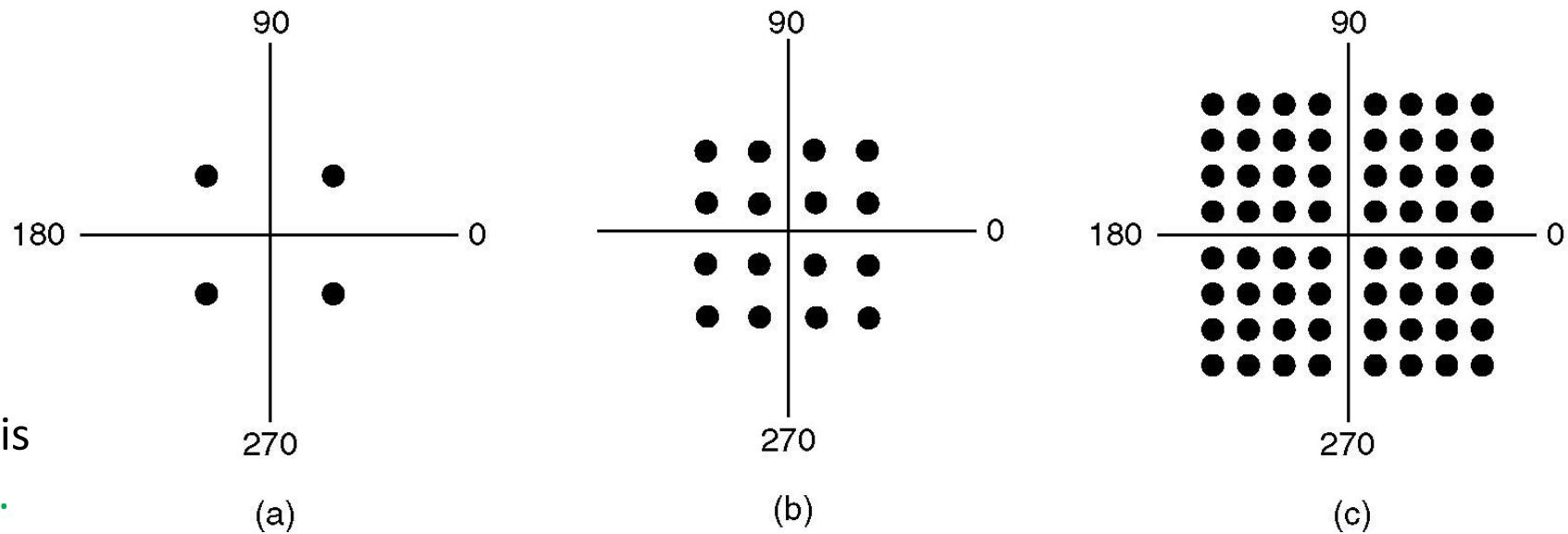
4 combinations, 2 bits/symbol.

QAM 16 :

16 combinations, 4 bits/symbol.

QAM 64 :

64 combinations, 6 bits/symbol.



- This kind of representation is known as **Constellation diagram**.
- Modems used at both ends must support same constellation pattern.

(a) QPSK. (b) QAM-16. (c) QAM-64.

The Local Loop: Modems, ADSL and Wireless(cont.)

Modems

Questions on data rate and modulation:

Question.

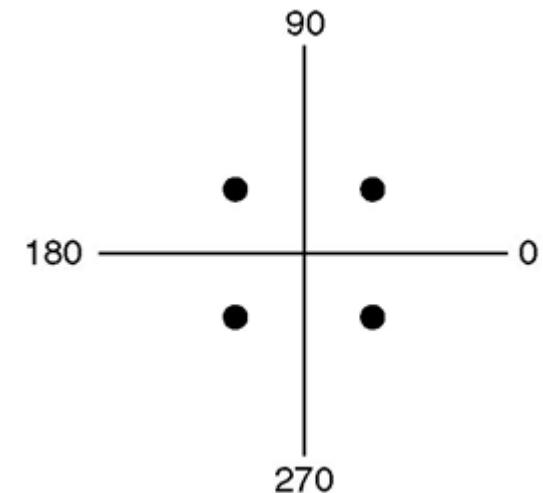
A modem constellation diagram has data points at the following coordinates: (1, 1), (1, -1), (-1, 1), and (-1, -1). How many bps can a modem with these parameters achieve at 1200 baud?

Answer :

4 combinations – 2 bits/symbol

Baud rate = Symbol rate = 1200

Bit rate = $1200 \times 2 = 2400$ bps



The Local Loop: Modems, ADSL and Wireless(cont.)

Modems

Questions on data rate and modulation:

Question 1.

A modem constellation diagram has data points at the following coordinates: (0, 1) and (0, 2). Does the modem use phase modulation or amplitude modulation?

Solution :

The two points indicates a phase shift of 0° with two different amplitudes. So the modulation used is only amplitude modulation.

Question 2.

In a constellation diagram, all the points lie on a circle centered on the origin. What kind of modulation is being used?

Solution :

All the points lie on the circle, which means all points are at equal distant from origin. However, the angle of each point with respect to +ve X axis drawn from origin are different, that means the points differs in phase. Since frequency modulation is not used in constellation diagram, the kind of modulation specified here is phase modulation.

The Local Loop: Modems, ADSL and Wireless(cont.)

Modems

Modulation supporting to error correction :

- Even a small amount of noise in the detected amplitude or phase can result in an error.
- Higher speeds modems do error correction by adding extra bits to each sample.
- Modulation process allows the data bits along with correction (say parity)bits : Ex- Trellis Coded Modulation

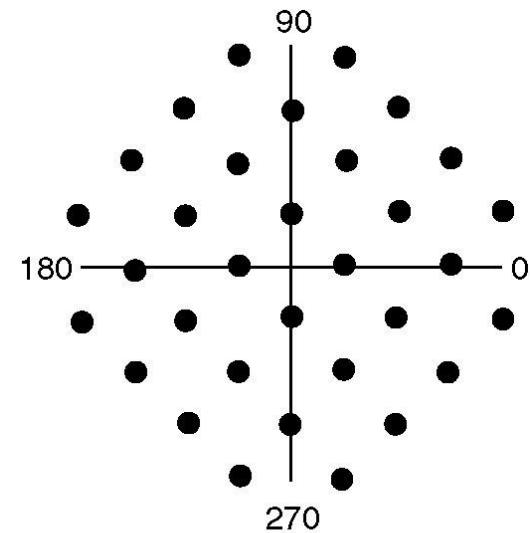
Modems using this type modulation :

V.32

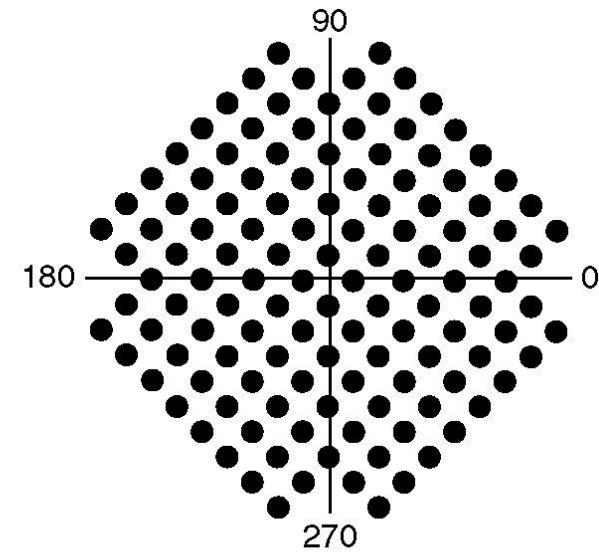
- 32 constellation points
- 4 data bits and 1 parity bit per symbol

V.32 bis

- 128 constellation points
- 6 data bits and 1 parity bit per symbol



(a)



(b)

(a) V.32 for 9600 bps.

(b) V.32 bis for 14,400 bps.

The Local Loop: Modems, ADSL and Wireless(cont.)

Modems

Some faster modems :

- V.90 offers 56kbps download and 33.6 kbps upload speeds.
- In uploading, the analog signal must be sampled at the switching stations which means the data rate for uploading is limited to 33.6 as earlier. But, there is no sampling in the downloading, hence no noise , hence no Shannon's limit (theoretically at least).
- Beyond V.90 is V.92 in which the upload speed can be at 48kbps.

The Local Loop: Modems, ADSL and Wireless(cont.)

Modems

All modern modems allow traffic in both directions at the same time (by using different frequencies for different directions).

Full duplex : A connection that allows traffic in both directions simultaneously.

Ex : A two lane road

Half duplex : A connection that allows traffic either way, but only one way at a time.

Ex : A single railroad

Simplex : A connection that allows traffic only one way.

Ex : (1) A one-way street

(2) An optical fiber with a laser on one end and a light detector on the other end

The Local Loop: Modems, ADSL and Wireless(cont.)

Modems

Questions :

Q1. Is an oil pipeline a simplex system, a half-duplex system, a full-duplex system, or none of these?

Ans : Oil can flow in either direction, but not both ways at once. So, half-duplex.

Q2. How many frequencies does a full-duplex QAM-64 modem use?

Ans : Two, one for upstream and one for downstream.

The Local Loop: Modems, ADSL and Wireless(cont.)

Digital Subscriber Lines (DSL)

- Demand for increased internet access speed among users.
- Cable TV industry supports a speed up to 10 Mbps.
- To compete with telephone industries offered digital services over local loop (i.e. **DSL**).
- Supports more bandwidth than standard telephone services (i.e. **broadband**)
- Most popular is **ADSL (Asymmetric DSL)**.

Technical justification of having more bandwidth :

Telephone systems used for voice

- The point where each local loop terminates in the end office, signal passes through a filter that attenuates all frequencies below 300 Hz and above 3400 Hz (i.e. bandwidth of 3100 Hz).

Telephone systems using DSL

- The incoming line coming through DSL is connected to a different switch, where the above said filter is absent, thus making the entire capacity of the local loop available.

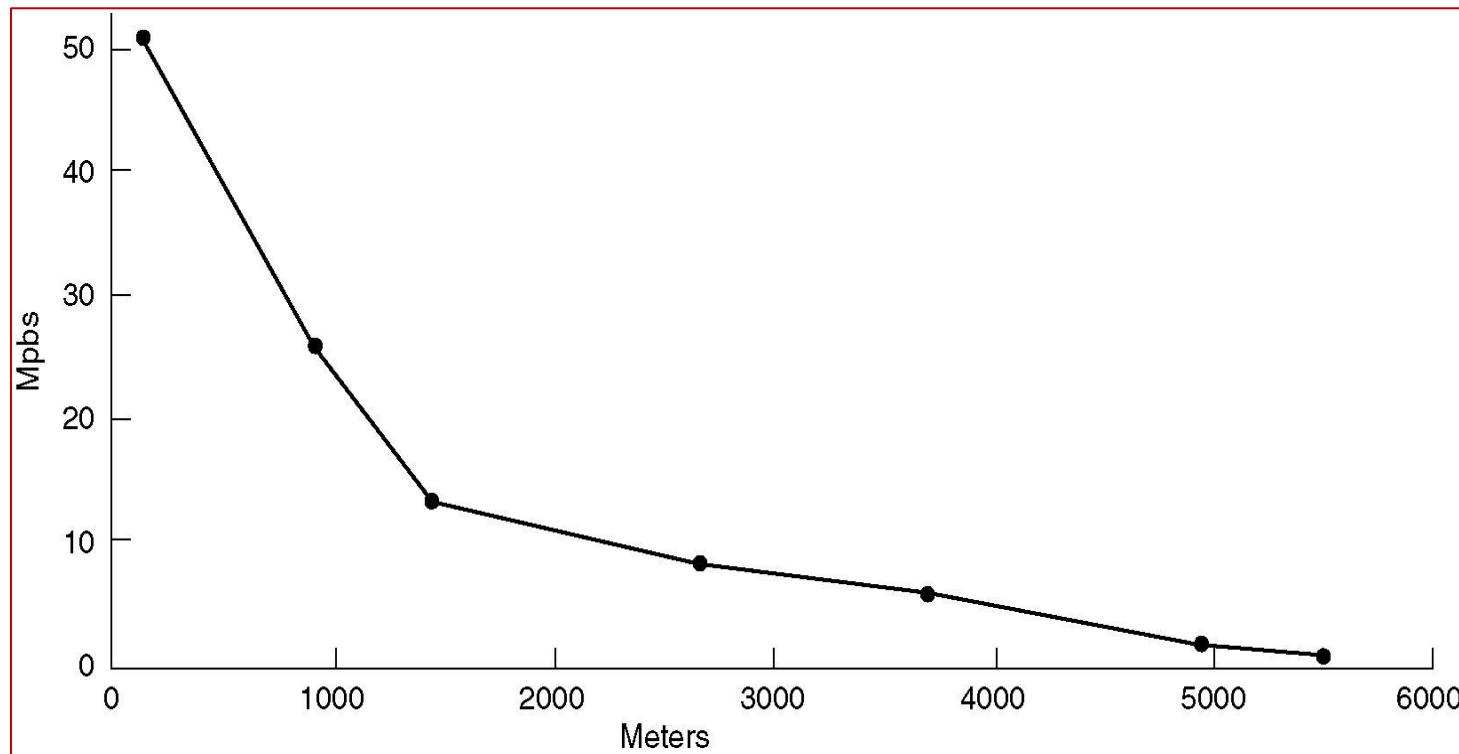
The Local Loop: Modems, ADSL and Wireless(cont.)

Digital Subscriber Lines (DSL)

The capacity of the local loop depends on several factors, including its length, thickness, and general quality.

DSL service is designed keeping 4 goals in mind.

- Services must work over the existing category 3 twisted pair local loops.
- They must not affect customers' existing telephones and fax machines.
- They must be much faster than 56 kbps.
- They should be always on, with just a monthly charge but no per-minute charge.



Bandwidth versus distance over category 3 UTP for DSL

The Local Loop: Modems, ADSL and Wireless(cont.)

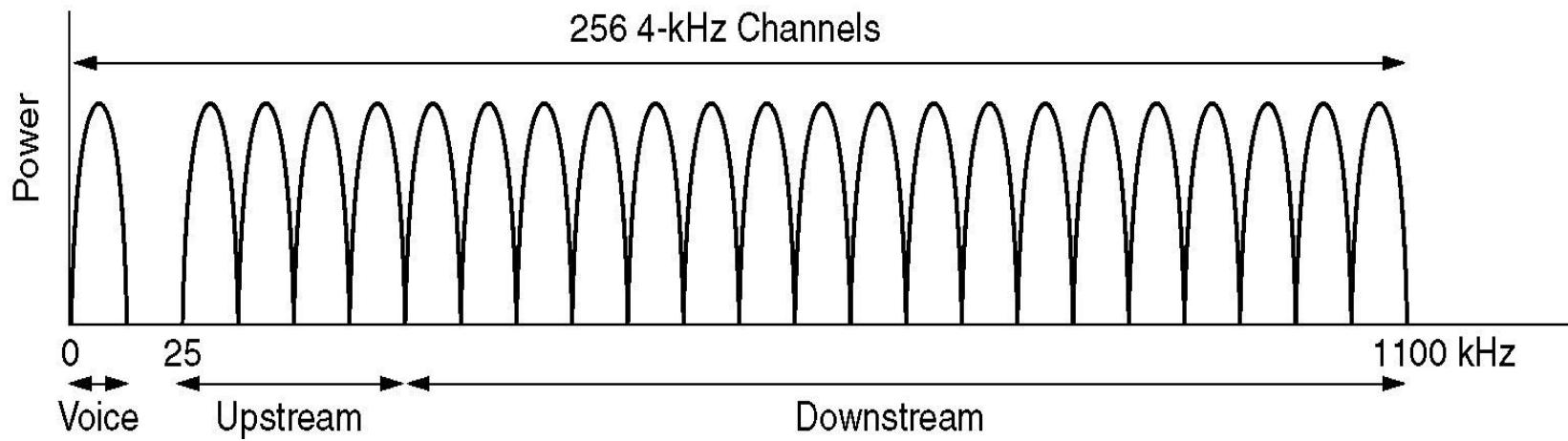
Digital Subscriber Lines (DSL)

Working of ADSL:

- Uses a spectrum of 1.1 MHz.
- Works through division of the allocated spectrum either of two ways.
 1. Divides the spectrum into three bands :
 - (i) POTS (Plain Old Telephone Service)
 - (ii) upstream (user to end office)
 - (iii) downstream (end office to user)
 2. Divides the spectrum into 256 channels each of size roughly 4312.5 Hz (Discrete Multi Tone).
 - Channel 0 : POTS
 - Channels 1-5 ; guard band between voice and data
 - Two for control channels, one for downstream and one for upstream
 - Remaining are partitioned between upstream and downstream for data : depends on the service provider; usually it is asymmetric giving 80-90% for download and remaining for upstream – hence the word Asymmetric

The Local Loop: Modems, ADSL and Wireless(cont.)

Digital Subscriber Lines (DSL)



Operation of ADSL using discrete multi tone modulation.

The Local Loop: Modems, ADSL and Wireless(cont.)

Digital Subscriber Lines (DSL)

- Within each channel, modulation scheme similar to V.34 is used
- QAM with 15 bits per baud
- 4000 baud instead of 2400
- Depending on need and line quality the data rate is different for different channel.
- With 224 downstream channels, download speed 13.44 Mbps is theoretically possible
- In practice, S/N ratio is never good enough to achieve this rate, but 8 Mbps is possible on short runs over high quality local loops

The Local Loop: Modems, ADSL and Wireless(cont.)

Digital Subscriber Lines (DSL)

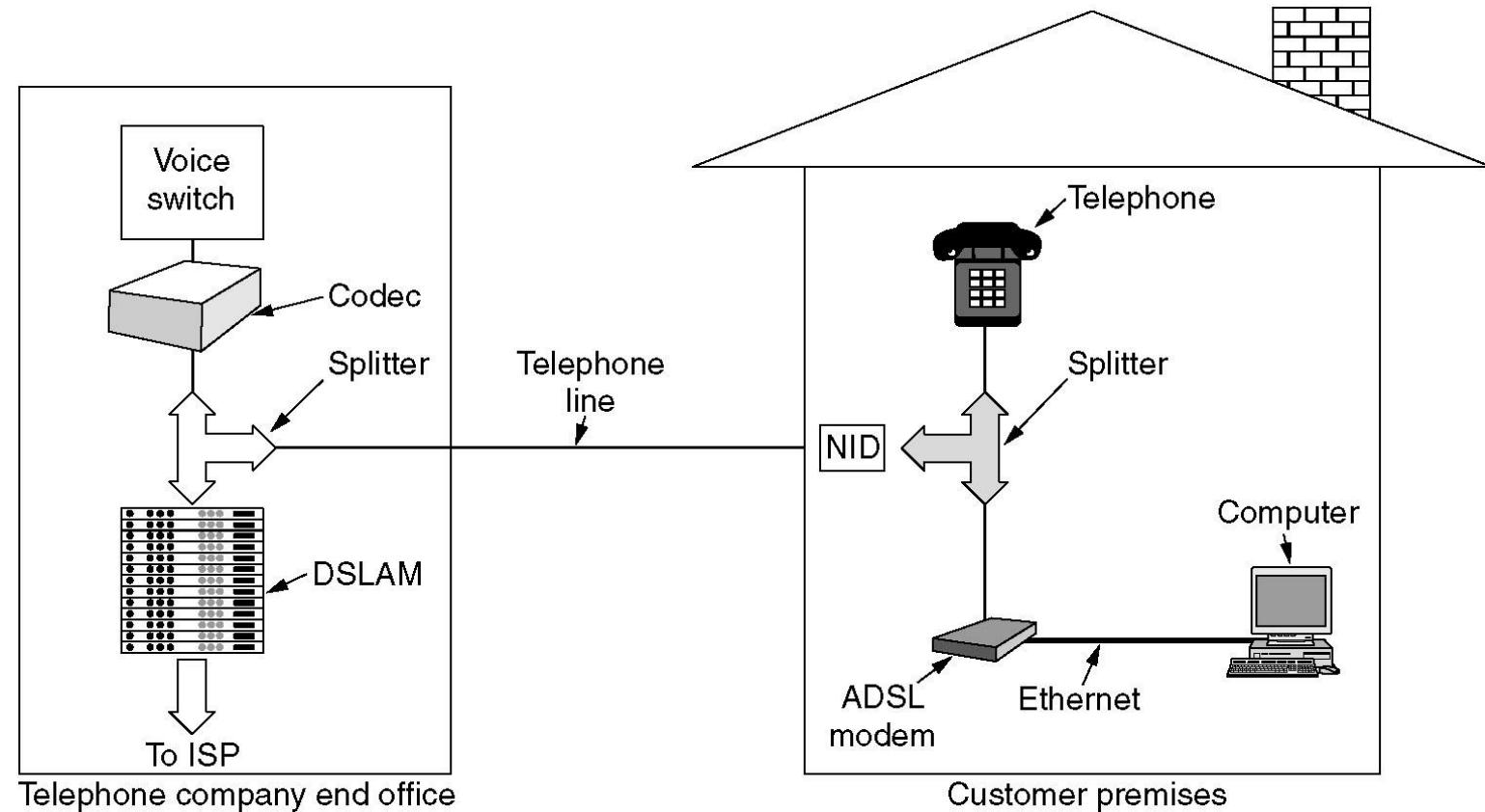
Installation requirement of ADSL

Customer premises :

- NID (Network Interface Device)
- Splitter
- ADSL modem

End office :

- Splitter
- DSLAM
(Digital Subscriber Line Access Multiplexer)



A typical ADSL equipment configuration

The Local Loop: Modems, ADSL and Wireless(cont.)

Digital Subscriber Lines (DSL)

Question :

An ADSL system using DMT allocates 3/4 of the available data channels to the downstream link. It uses QAM-64 modulation on each channel. What is the capacity of the downstream link?

Answer :

There are 256 channels in all, minus 6 for POTS and 2 for control, leaving 248 for data.

$\frac{3}{4}$ of 248 = 186 channels for downstream.

ADSL modulation uses 4000 baud rate.

With QAM-64 (i.e. 6 bits/baud) modulation the bit rate is 24,000 bps in each of the 186 channels. The capacity of downstream is

$$24,000 \times 186 = 4.464 \text{ Mbps}$$

The Local Loop: Modems, ADSL and Wireless(cont.)

Wireless Local Loop

- Started with an interest from private local companies to compete with existing monopolist telephone company.
- Objective : to provide better service at low price than existing monopolist telephone company.
- Uses a cheaper alternative to the traditional twisted pair local loop : **WLL (Wireless Local Loop)**
- A fixed telephone using a wireless local loop is a bit like a mobile phone, but there are three crucial technical differences.
 - High-speed Internet connectivity
 - Installation of a large directional antenna on customer roof pointed at the Company's end office
 - The user does not move, eliminating all the problems with mobility and cell handoff
- Popular in the term **fixed wireless**
- Used in two types of services
 - **MMDS (Multichannel Multipoint Distribution Service)**
 - **LMDS (Local Multipoint Distribution Service)**

The Local Loop: Modems, ADSL and Wireless(cont.)

Wireless Local Loop

MMDS(Multichannel Multipoint Distribution Service)

- Uses microwaves in 198 MHz band at 2.1 GHz frequency range
- Range of about 50km
- Advantage : Technology is well established and equipment readily available
- Disadvantage : Bandwidth available is not much and must be shared by several users

LMDS(Local Multipoint Distribution Service)

- Uses millimeter waves as an alternative to low bandwidth of MMDS (**Operative after arrival of gallium arsenide ICs because silicon ICs were difficult to operate**)
- Range of frequencies : 28-31 GHz in U.S & 40 GHz in Europe
- Covers 2-5 km range (Thus requires many towers to cover a city)
- Uses multiple directional antennas to cover different sectors in geographical area
- Uses asymmetric bandwidth like ADSL(say 36 Gbps for downstream and 1 Mbps for upstream)

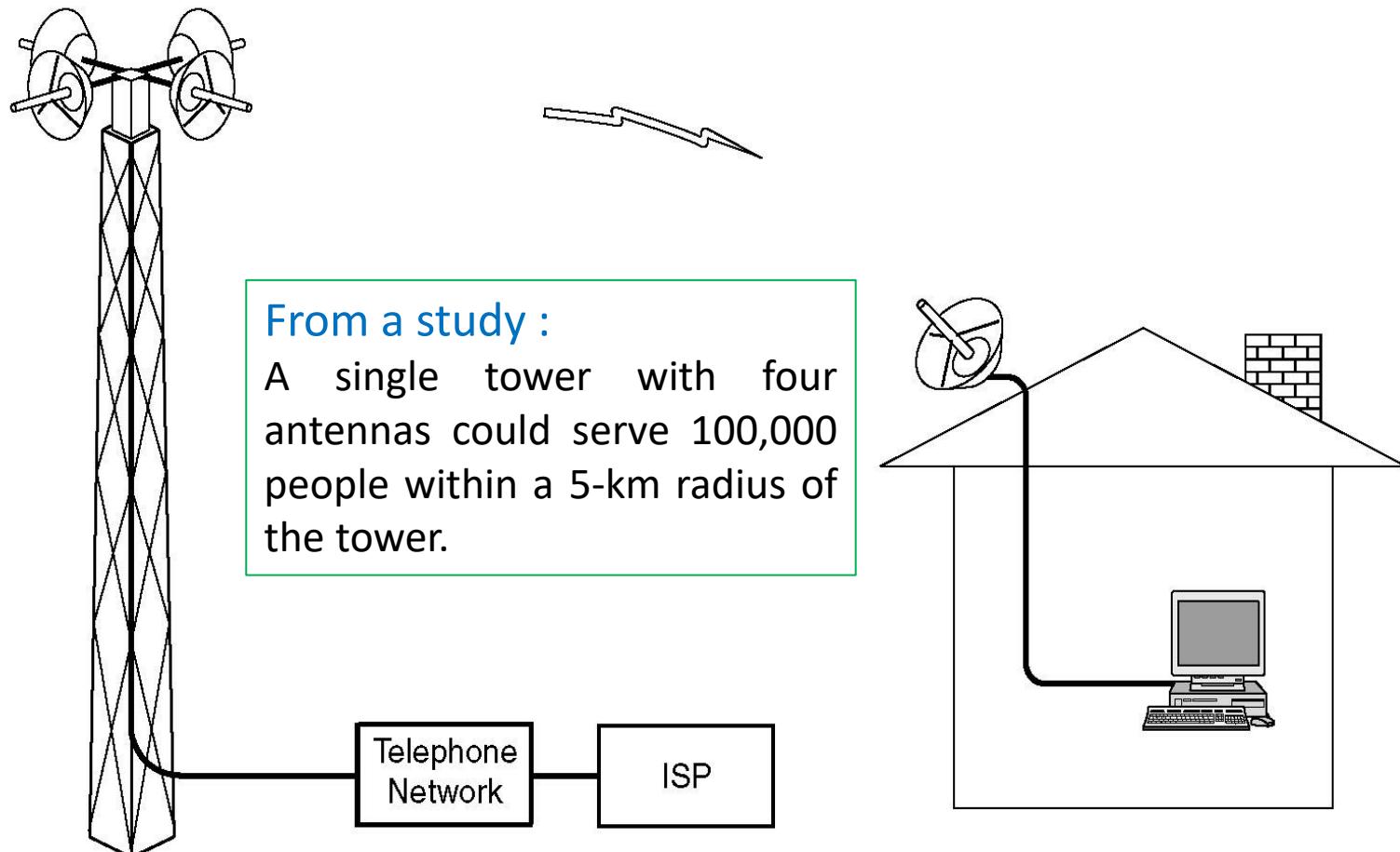
The Local Loop: Modems, ADSL and Wireless(cont.)

Wireless Local Loop

Problems with MM waves in LMDS:

- Highly directional : hence there must be a clear line of sight between the roof top antennas and the tower.
- Leaves absorb these waves well, so the tower must be high enough to avoid having trees in the line of sight.
- A clear line of sight in December may not be clear in July when the trees are full of leaves.
- Rain also absorbs these waves.

LMDS works with IEEE 802.16 standard.



Trunks and Multiplexing

- Keeping in view of economy, telephone companies have developed elaborate schemes for multiplexing many conversations over a single physical trunk.
- Two basic categories :
 - **FDM (Frequency Division Multiplexing)** :The frequency spectrum is divided into frequency bands, with each user having exclusive possession of some band.
(In fiber optics in the form of **WDM (Wavelength Division Multiplexing)**)
 - **TDM (Time Division Multiplexing)** : The users take turns (in a round-robin fashion), each one periodically getting the entire bandwidth for a little burst of time.

Example :

- AM radio broadcasting : Allocated spectrum is about 1MHz, roughly 500 to 1500 kHz.
- Different frequencies are allocated to different broadcasting stations.
(i.e. FDM)
- Individual stations can have music and advertising transmission alternate in time on the same frequency.
(i.e. TDM)

Trunks and Multiplexing (cont.)

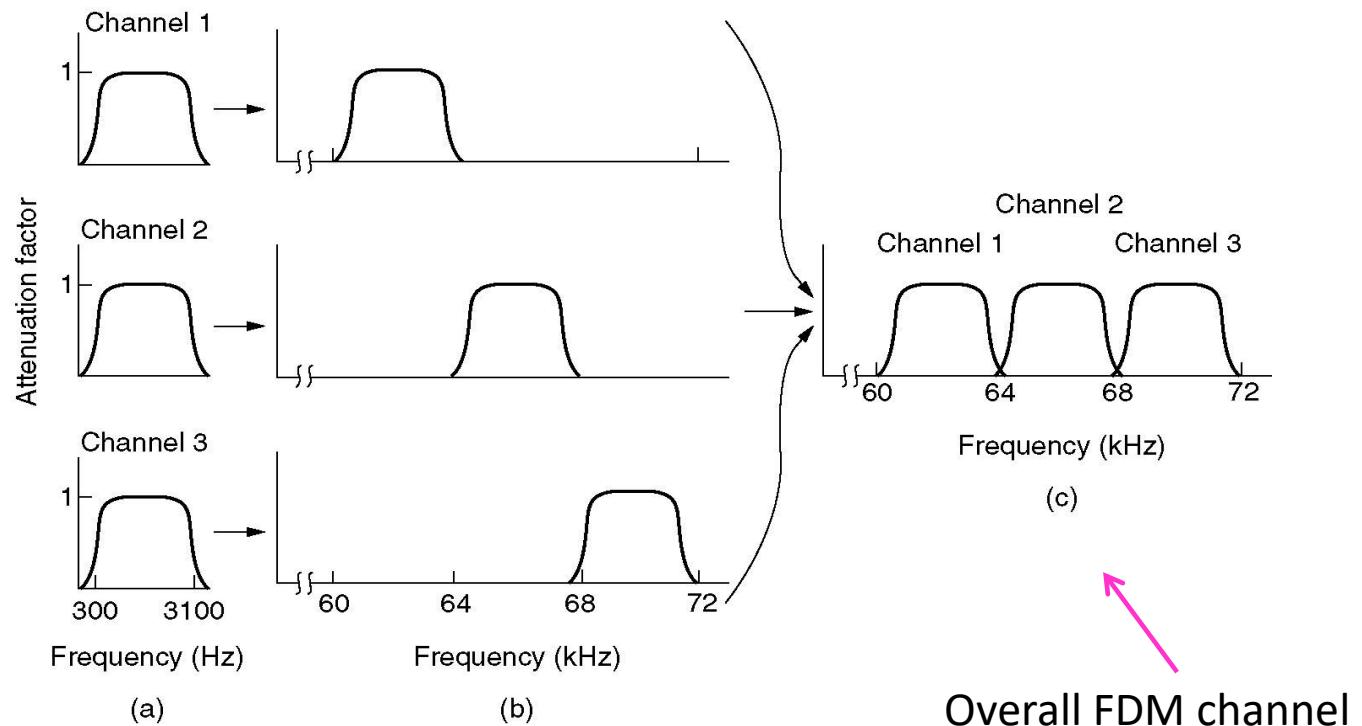
Frequency Division Multiplexing

Steps in FDM :

- First, the voice channels are raised in frequency, each by a different amount in the allocated spectrum.
- Second, they can be combined because no two channels now occupy the same portion of the spectrum.

Standard form of FDM :

- **Group** : Twelve 4000Hz voice channels multiplexed into a 48 KHz band (e.g. 12 – 60 KHz band & 60 – 108 KHz band).
- **Supergroup** : Combination of 5 groups.
- **Mastergroup** : Combination of 5/10 supergroups.



(a) The original bandwidths. (b) The bandwidths raised in frequency. (c) The multiplexed channel.

Trunks and Multiplexing (cont.)

Frequency Division Multiplexing

Question :

Ten signals, each requiring 4000 Hz, are multiplexed on to a single channel using FDM. How much minimum bandwidth is required for the multiplexed channel? Assume that the guard bands are 400 Hz wide.

Answer :

There are ten 4000 Hz signals to multiplexed.

Spectrum width = $10 \times 4000 = 40,000$ Hz

Each guard band = 400 Hz

No. of guard bands required to avoid interference in between 10 signals = 9

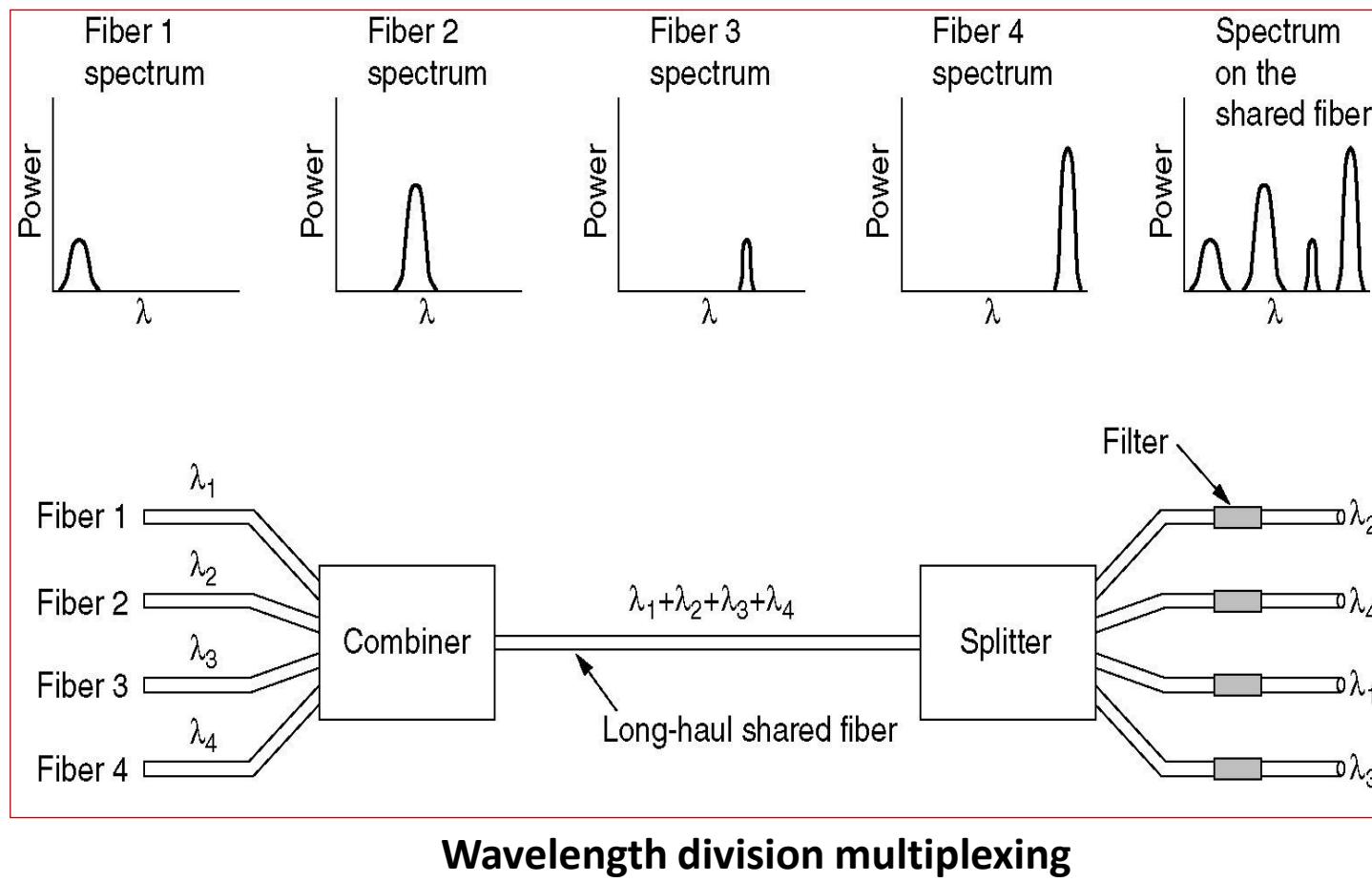
Spectrum used for guard band = $9 \times 400 = 3600$ Hz

Minimum bandwidth required for the multiplexed channel = $40,000 + 3,600 = 43,600$ Hz

Trunks and Multiplexing (cont.)

Wavelength Division Multiplexing

- Used in fiber optic channel.
- Signals with different wavelength coming through different fibers combined through optical combiner (here 4).
- Transmitted through a shared fiber over long distance.
- At the far end, the beam is split up over as many fibers as there were on the input side using specially-constructed core that filters out all but one wavelength.
- Just like FDM at high frequencies.
- Requires diffraction grating.



Trunks and Multiplexing (cont.)

Wavelength Division Multiplexing

Growth of WDM :

- 1990: 8 wavelengths X 2.5 Gbps → 20Gbps
- 1998: 40 X 2.5 Gbps → 100Gbps
- 2001: 96 X 10 Gbps → 960Gbps : enough to transmit 30 full-length movies per second.
- As more and more wavelengths are being discovered in a single fiber, WDM is getting denser and now the name DWDM (dense WDM) is being used.

Trunks and Multiplexing (cont.)

Time Division Multiplexing

- WDM : applicable only on optical fiber and not on copper, but a lot of copper is there and also analog.
- FDM : used on copper and microwave but requires analog circuitry and may not be suitable for computer.
- Solution : TDM : unfortunately, can be used only for digital data.
 - ❖ Requires A/D conversion at the end office (since local loops uses analog signaling) before being multiplexed and transmitted in the trunk.
 - ❖ Uses **Codecs**

Trunks and Multiplexing (cont.)

Time Division Multiplexing

CODEC : PCM (Pulse Code Modulation) :

- Uses 8000 samples/sec or one sample/125 μ sec.
(Satisfies Nyquist criteria as telephone channel bandwidth is 4000 Hz)
- All the time intervals (a pulse) within the telephone system are multiples of 125 μ sec.
- Technique is known as PCM.
- Each sample is represented in the form of a 8-bit number.

Different schemes incorporating PCM were used for implementing TDM.

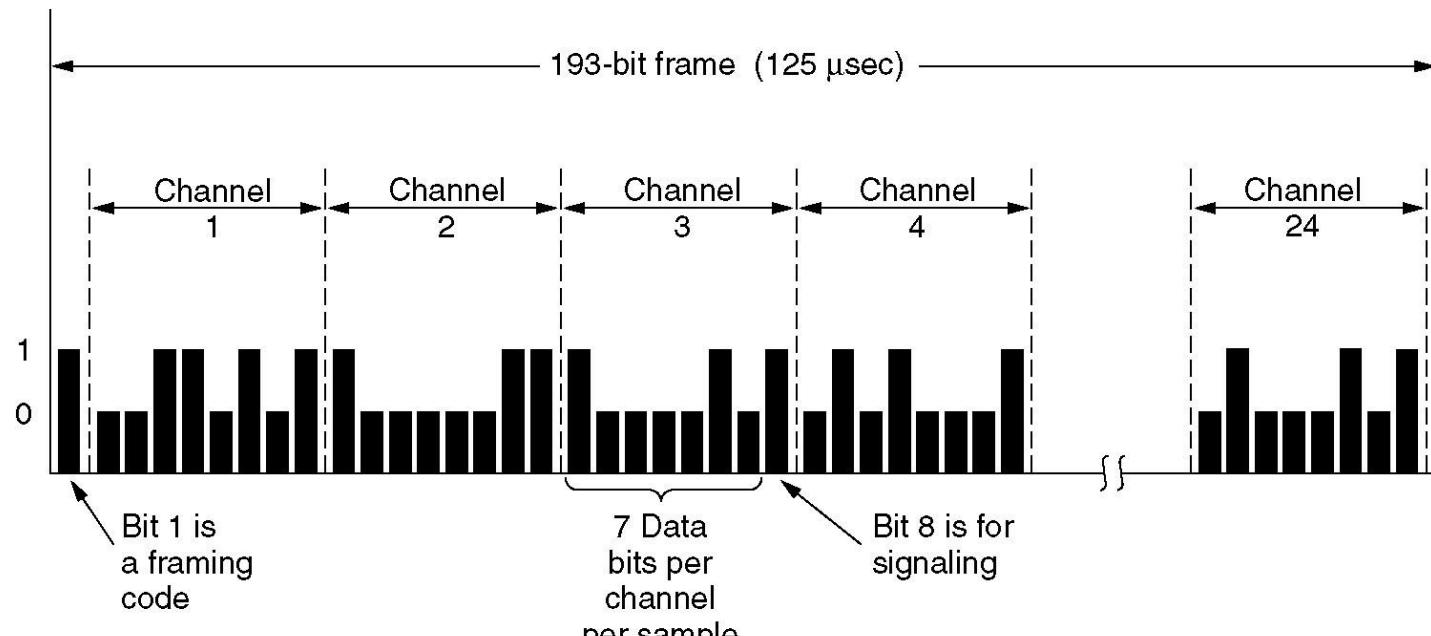
Example : **T1** carrier

Trunks and Multiplexing (cont.)

Time Division Multiplexing

T1 Carrier :

- Used for multiplexing 24 voice channels from local loops.
- Analog signals from these 24 channels are sampled on a round-robin basis with the resulting analog stream being fed to the codec rather than having 24 separate codecs.
- Each of these 24 channel insert 8 bits (7 data + 1 control) for each sample.
- Bits for each channel is $(7 \times 8000) = 56,000$ bps of data and $(1 \times 8000) = 8000$ bps of signaling information.
- Bits at codec w.r.t each sample from 24 channels is $24 \times 8 = 192$ bits along with one extra bit for synchronization (i.e. 193 bits).
- Data rate/sec is 1.544 Mbps



The T1 carrier (1.544 Mbps).

Trunks and Multiplexing (cont.)

Time Division Multiplexing

- The TDM using the PCM technique has been standardized with 1.544 Mbps with some variations in T1.
 - 8000 bps of signalling information is too much so no. of bits used to represent a data is 8 bit (instead of 7 bit).
 - Implemented with two possible approaches.

1. Common channel signalling :

The extra bit (which is attached onto the rear rather than the front of the 193-bit frame) takes on the data values in the odd frames and contains signaling information for all the channels in the even frames.

2. Channel-associated signaling :

- Each channel has its own private signaling subchannel
- Subchannel allocation : one of the eight user bits in every sixth frame is used for signaling (i.e. five out of six samples are 8 bits wide, and the other one is only 7 bits wide)

Trunks and Multiplexing (cont.)

Time Division Multiplexing

E1 Carrier :

- Another standard carrier besides T1 carrier used in TDM with PCM technique.
- 8000 samples/sec
- Accepts 32 channels with 8-bit data samples:
 - 30 channels for data + 2 channels for signaling
- Each group of four frames provides 64 bits of signaling :
 - Half for channel associated signaling + half for frame sync
- Capacity : $32 \times 8 \times 8000 = 2.04 \text{ Mbps}$

Trunks and Multiplexing (cont.)

Time Division Multiplexing

Differential Pulse Code Modulation and Delta Modulation :

- Objective : Reduction in no. of bits needed per channel without loosing information.
- Principle: Signal changes relatively slowly compared to the sampling frequency, so that much of the information in the 7- or 8-bit digital level is redundant.
- Appropriate for both speech encoding and digitization of analog signal.

In Differential Pulse Code Modulation :

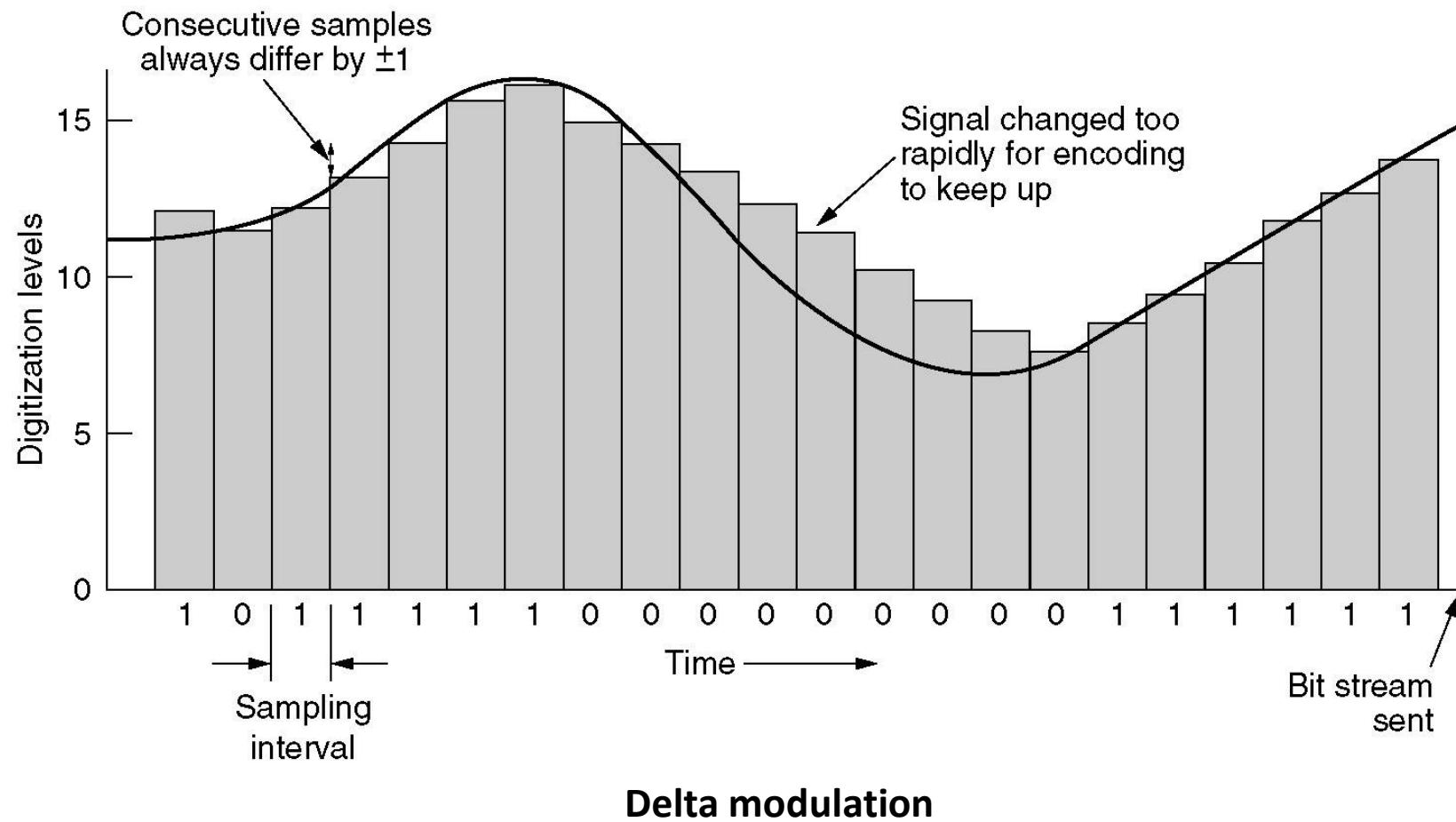
- Instead of digitized amplitude, difference between current value and previous one is digitized
- Jumps of magnitude ± 16 and more are rare in 128 levels. So 5 instead of 7 bits are sufficient.
- If the signal jumps occasionally widely, the information is lost

In Delta Modulation :

- Compare the current sample and previous one with a difference in ± 1 .
- For difference of +1, transmits 1 & for difference of -1 transmits 0.
- If signal changes too fast then information is lost.

Trunks and Multiplexing (cont.)

Time Division Multiplexing



Trunks and Multiplexing (cont.)

Time Division Multiplexing

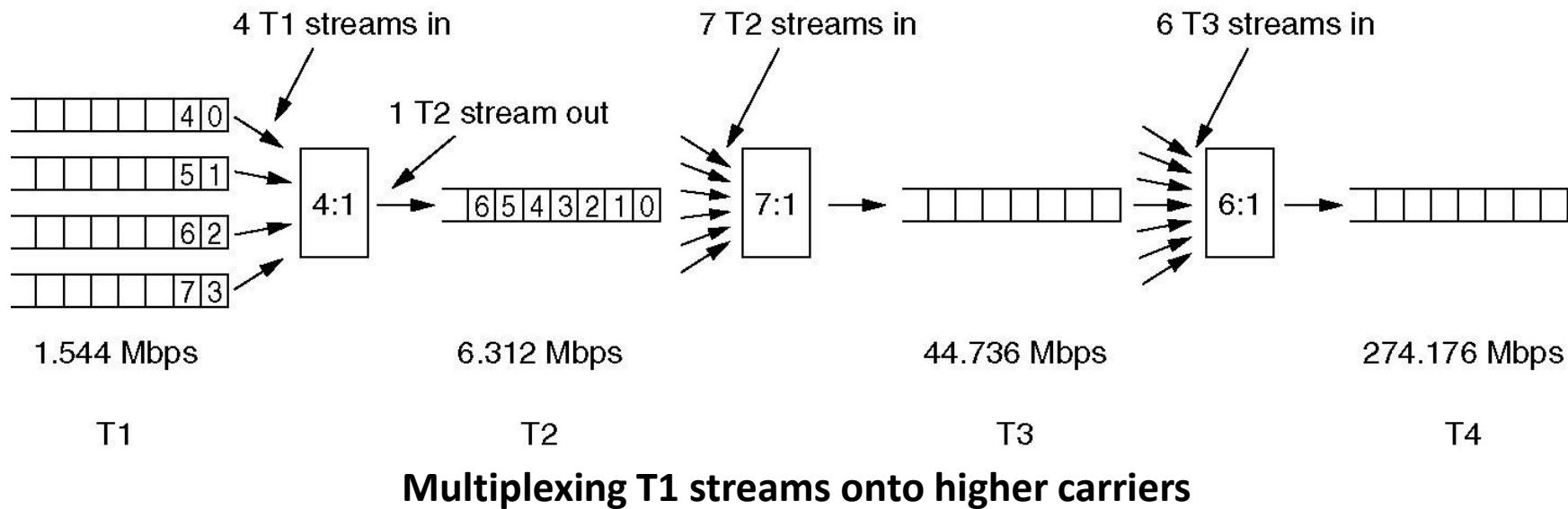
Predictive Encoding :

- Extrapolate the previous few values to predict the next value.
- Encode the difference between actual and the predicted signal
- Transmitter and receiver must have to use same prediction algorithm

Trunks and Multiplexing (cont.)

Time Division Multiplexing

- TDM allows carrier hierarchy.
 - Level 1 : Four T1 channels being multiplexed onto one T2 channel.
 - Level 2 : Seven T2 streams are combined bitwise to form a T3 stream.
 - Level 3 : Six T3 streams are joined to form a T4 stream.
- At each step a small amount of overhead is added for framing and recovery in case the synchronization between sender and receiver is lost.



Trunks and Multiplexing (cont.)

Time Division Multiplexing

Q. What signal-to-noise ratio is needed to put a T1 carrier on a 50-kHz line?

Answer :

To send a T1 signal we need $H \log_2(1 + S/N) = 1.544 \times 10^6$ with $H = 50,000$.

This yields $S/N = 2^{30} - 1$, which is about 93 dB.

Switching

From PSTN working point of view the structure can be seen as combination of two parts.

- Outside the plant (local loops and trunks).
- **Inside the plant (switching offices).**

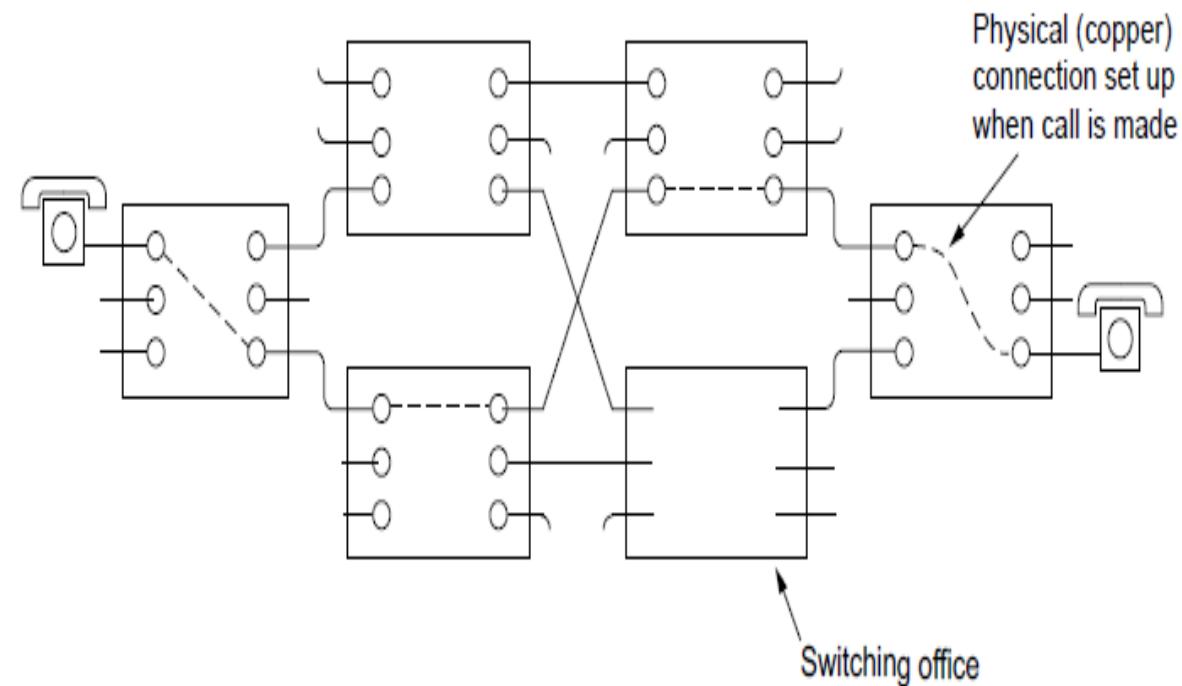
Two switching technologies used:

- Circuit switching
- Message switching (mostly obsolete now)
- Packet switching

Switching (cont.)

Circuit Switching

- When a telephone call is placed, the switching equipment within the telephone system seeks out a physical path all the way from transmitter's telephone to the receiver's telephone.
- The end office and toll office (here the six rectangles) in the physical path are called as switching offices.
- Each office has more than one (here three) incoming lines and more than one (here three) outgoing lines.
- When a call passes through a switching office, a physical connection is established between the line on which the call came in and one of the output lines, as shown by the dotted lines.
- In the early days of the telephone, the connection was made by the operator plugging a jumper cable into the input and output sockets.
- once a call has been set up, a dedicated path between both ends exists and will continue to exist until the call is finished.



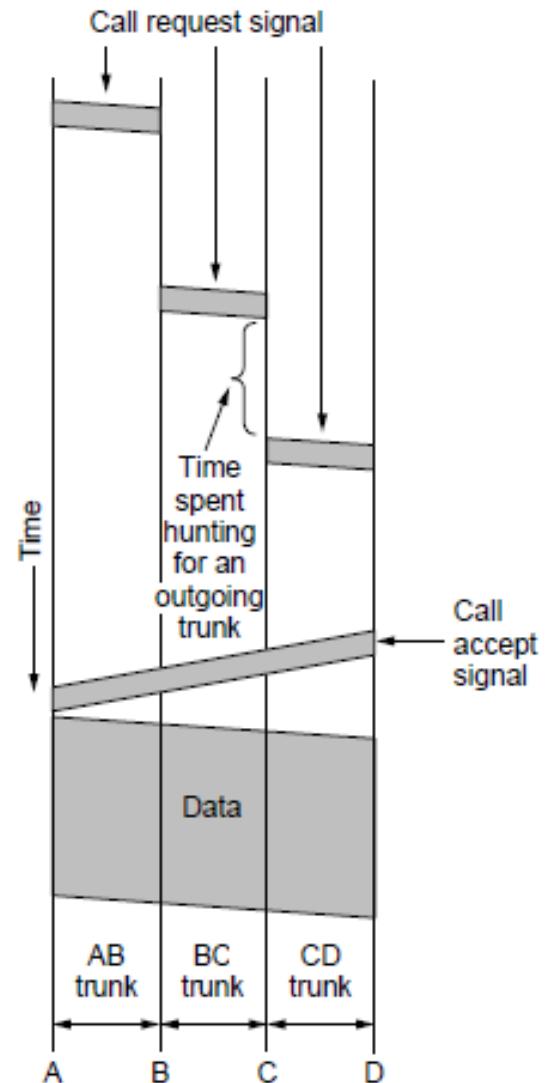
Circuit switching.

Switching (cont.)

Circuit Switching

Process of call progress in circuit switching :

- Set up an end-to-end path before any data can be sent (i.e. dialing at transmitting end and ringing at receiving end).
- The elapsed time between the end of dialing and the start of ringing can easily be 10 sec, more on long-distance or international calls.
- During the establishment of the direct path from two end users the system will hunt to find it.
- However, once the path is set-up
 - The only delay for data is the propagation time for the signal to travel to the destination: 5 msec per 1000 km.
 - There is no danger of congestion (i.e. once the call has been put through, you never get busy signals).
 - The busy signal might be heard before the connection has been established due to lack of switching or trunk capacity.



Timing of events in circuit switching

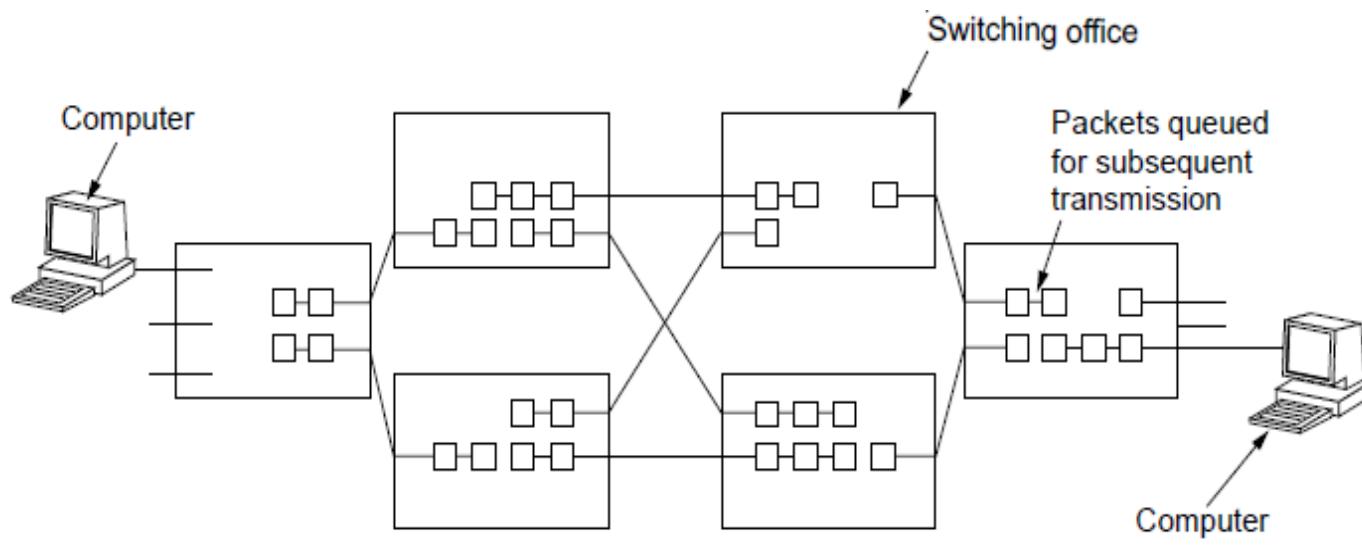
Switching (cont.)

Packet Switching

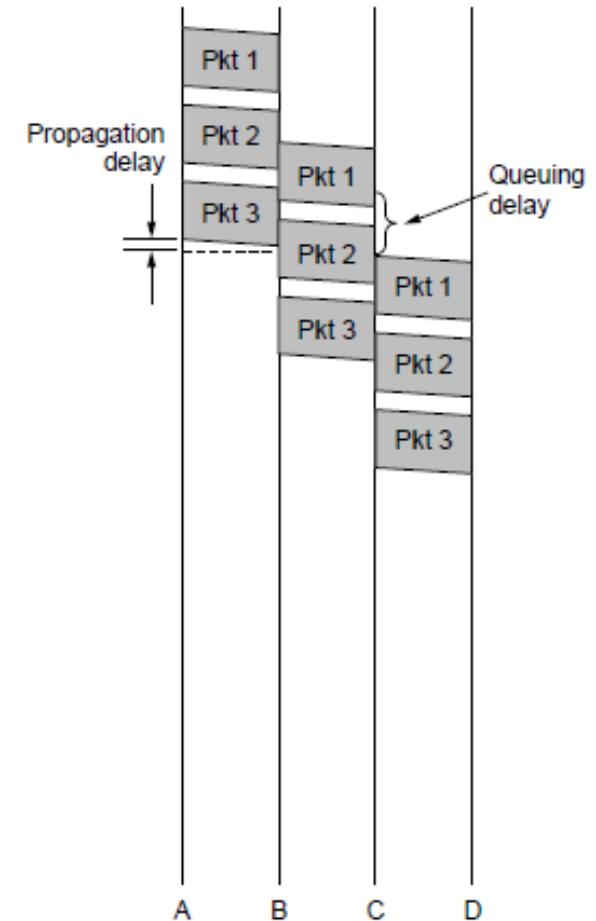
- Alternative to circuit switching.
- Individual packets are sent as need be, with no dedicated path being set up in advance.
- It is up to each packet to find its way to the destination on its own.
- Uses store and forward concept at the routers(i.e. at switching offices).
- Limitation in no. of packets through inclusion of fixed size buffer at the routers (i.e. no user can block a transmission line for longer time).
- In case of multi packet message, a packet is forwarded only if has been arrived as entirety before the arrival of second packet (arrival of packets may not be in order).
- Reduced delay and improved throughput in compare to message switching.

Switching (cont.)

Packet Switching



Packet switching



Timing of events in packet switching

Switching (cont.)

Circuit Vs. Packet Switching

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

A comparison of circuit-switched and packet-switched networks

Computer Network

(CSE 3034)

Text book: Computer Networks by Andrew S. Tanenbaum

Introduction to the course

Syllabus :

- Introduction(Chapter 1)
- The Physical Layer(Chapter 2)
- **The Data Link Layer(Chapter 3)**
- The Medium Access Control Sublayer(Chapter 4)
- The Network Layer(Chapter 5)
- The Transport layer(Chapter 6)
- The Application layer(Chapter 7)
- Network security(Chapter 8)

The Data Link Layer

The Data Link Layer

- Objective : To achieve reliable, efficient communication between two adjacent machines
- Communication circuits make errors during transmission of bits.
 - Requires error control
- Design issues with data link layer
- Protocols

Data Link Layer Design Issues

Functions of the Data Link Layer :

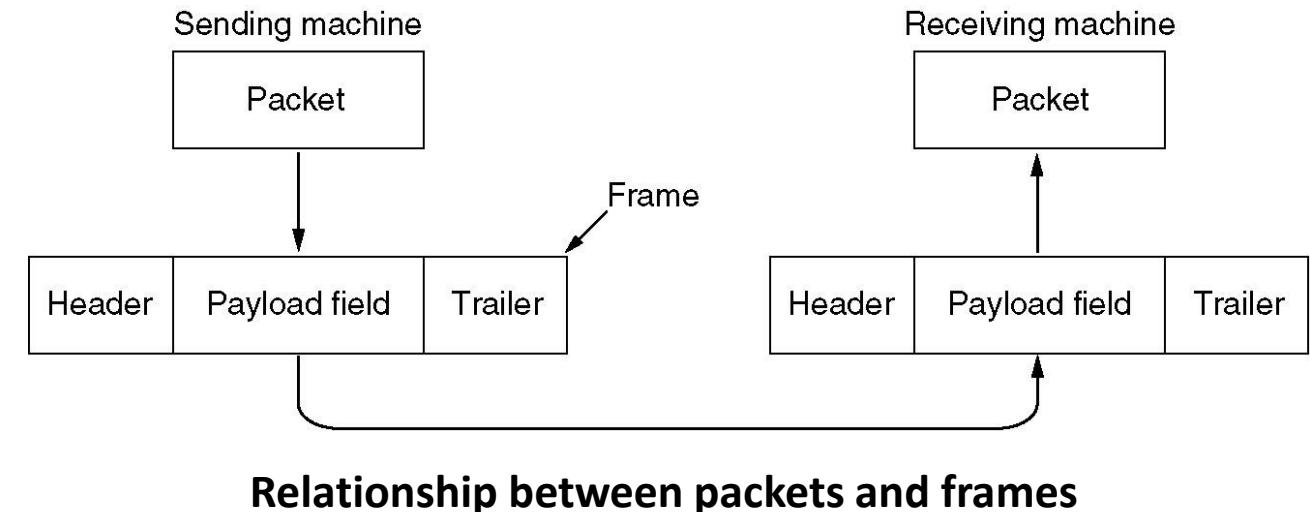
- Provide service interface to the network layer
- Dealing with transmission errors
- Regulating data flow so that slow receivers not swamped by fast senders

Data Link layer :

- Takes the packets from network layer, and encapsulates them into **frames** for transmission using physical layer (reverse process in reception).

Data frame :

1. A frame header
2. A payload field for holding the packet
3. A frame trailer



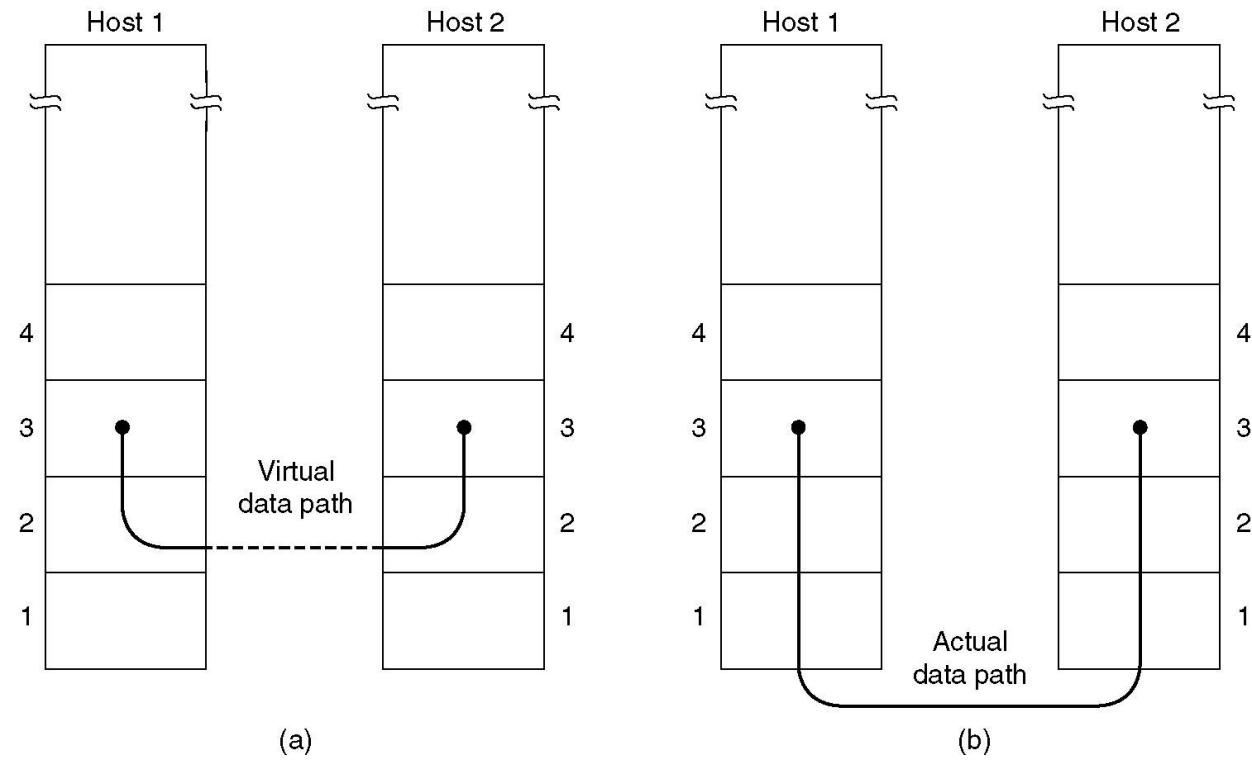
Data Link Layer Design Issues (cont.)

Services Provided to the Network Layer

The job of the data link layer is to transmit the bits obtained from network layer of source machine to the network layer of the destination machine.

Possible services offered by DLL (Data Link Layer) :

- Unacknowledged connectionless service.
- Acknowledged connectionless service.
- Acknowledged connection-oriented service.



(a) Virtual communication. (b) Actual communication.

Data Link Layer Design Issues (cont.)

Services Provided to the Network Layer

Unacknowledged connectionless service :

- Consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledge them.
- No logical connection is established beforehand or released afterward.
- If a frame is lost due to noise on the line, no attempt is made to detect the loss or recover from it in the data link layer.
- Service is appropriate when the error rate is very low so that recovery is left to higher layers.
- Acceptable for real-time traffic, such as voice, in which late data are worse than bad data
- Example: Ethernet, Voice over IP, etc.

Data Link Layer Design Issues (cont.)

Services Provided to the Network Layer

Acknowledged Connectionless Service :

- Each frame send by the Data Link layer is acknowledged and the sender knows if a specific frame has been received or lost.
- Typically the protocol uses a specific time period that if has passed without getting acknowledgment it will re-send the frame.
- This service is useful for commutation when an unreliable channel is being utilized (e.g., 802.11 WiFi).
- Network layer does not know frame size of the packets and other restriction of the data link layer. Hence it becomes necessary for data link layer to have some mechanism to optimize the transmission.

Data Link Layer Design Issues (cont.)

Services Provided to the Network Layer

Acknowledged Connection Oriented Service :

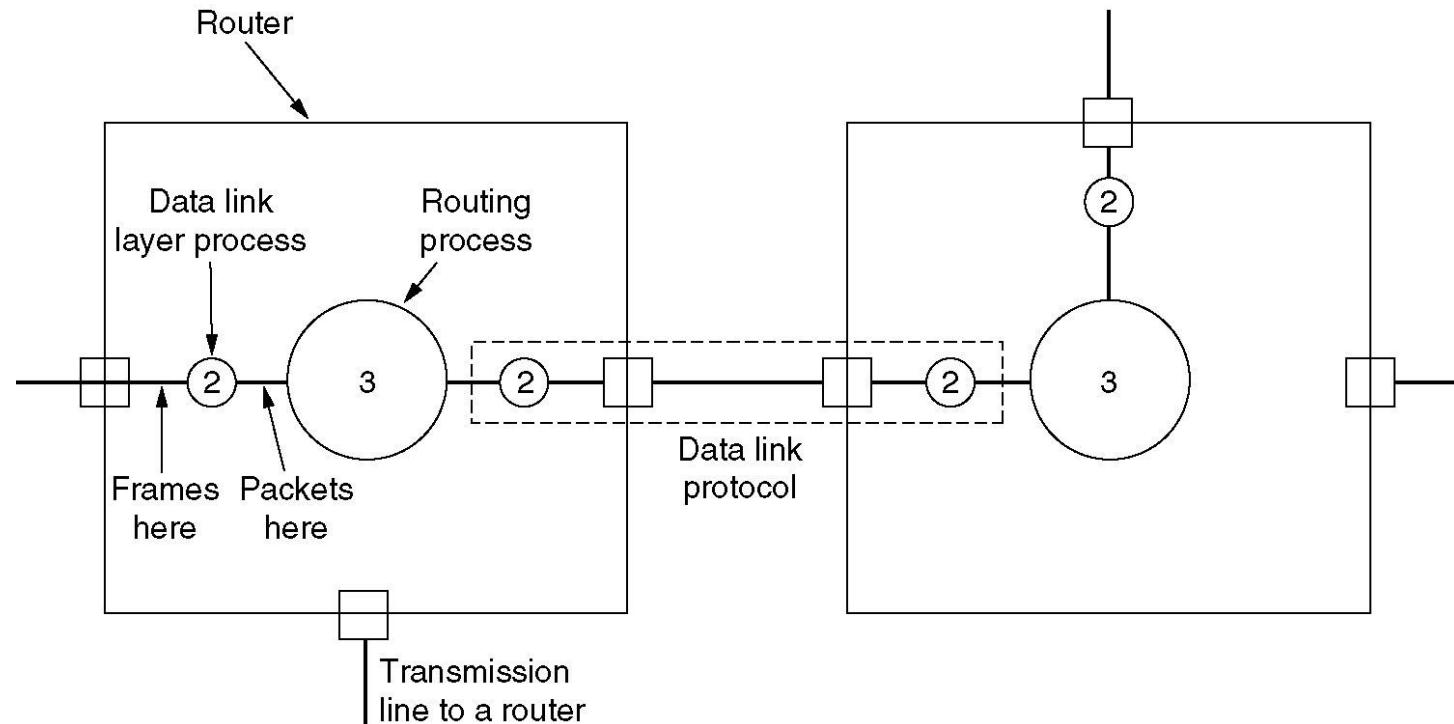
- Source and Destination establish a connection first.
- Each frame sent is numbered
 - Data link layer guarantees that each frame sent is indeed received.
 - It guarantees that each frame is received only once and that all frames are received in the correct order.
- Examples:
 - Satellite channel communication, Long-distance telephone communication, etc.
- Three distinct phases:
 1. Connection is established by having both side initialize variables and counters needed to keep track of which frames have been received and which ones have not.
 2. One or more frames are transmitted.
 3. Finally, the connection is released – freeing up the variables, buffers, and other resources used to maintain the connection.

Data Link Layer Design Issues (cont.)

Services Provided to the Network Layer

Flow over two routers : An example

- When a frame arrives at a router, the hardware checks it for errors, then passes the frame to the data link layer software.
- The data link layer software checks to see if this is the frame expected, and if so, gives the packet contained in the payload field to the routing software.
- The routing software then chooses the appropriate outgoing line and passes the packet back down to the data link layer software, which then transmits it.



Placement of the data link protocol.

Data Link Layer Design Issues (cont.)

Framing

- To provide service to the network layer, the data link layer must use the service provided to it by the physical layer.
- The physical layer deals with transmission of raw bit stream and doesn't give guarantee of error free transmission.
- Errors could be:
 - Number of received bits does not match number of transmitted bits (deletion or insertion)
 - Bit Value
- Data link layer takes the responsibility to detect errors and if possible, to correct errors.
 - It breaks up the bit stream into discrete frames and computes a checksum which it includes with each frame.
 - Braking up the bit stream into frames is more difficult than it seems.

Data Link Layer Design Issues (cont.)

Framing

Framing Methods :

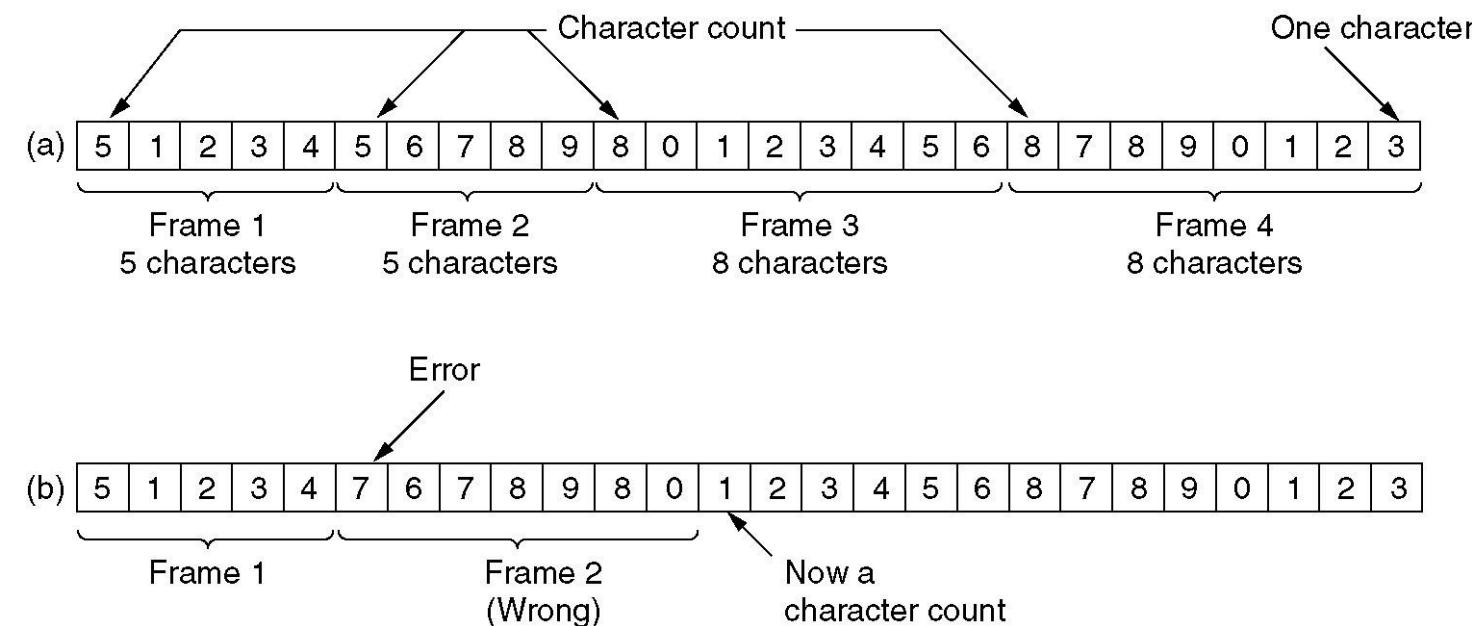
- Character count
- Flag bytes with byte stuffing
- Starting and ending flags with bit stuffing
- Physical layer coding violations

Data Link Layer Design Issues (cont.)

Framing

Character count :

- Uses the first field in the frame's header to indicate the length of the frame, so that the receiver knows how big the current frame is and can determine where does a frame ends.
- Trouble in the algorithm:
 - Receiver loses synchronization when the count become garbled due to transmission error.
 - The receiver will think that the frame contains fewer (or more) characters than it actually does.
- Although checksum will detect the frames are incorrect, the receiver will have difficulty in re-synchronizing to the start of a new frame.



A character stream. (a) Without errors. (b) With one error.

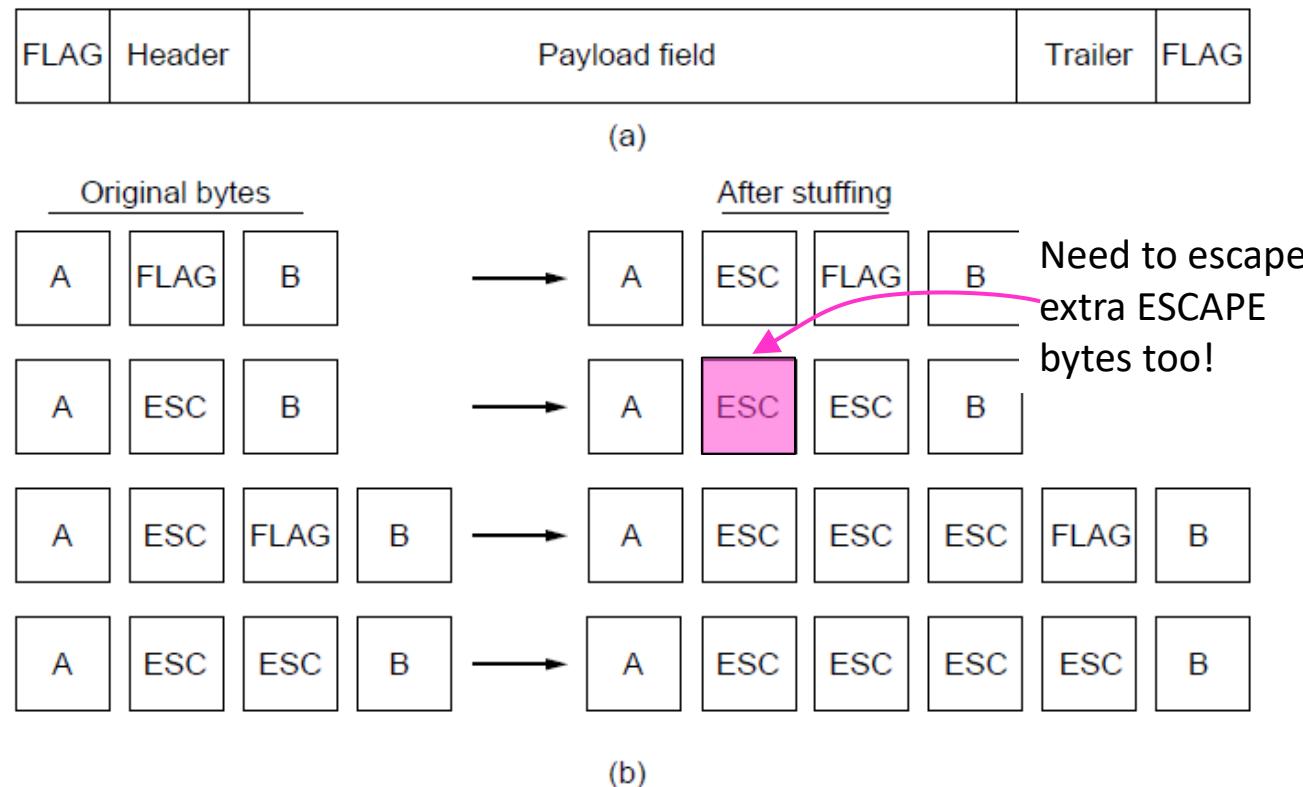
Data Link Layer Design Issues (cont.)

Framing

Flag bytes with byte stuffing :

- Uses frame boundary detection technique though appending of special byte just before and after each frame.
- Most protocols have used same bytes normally called as **flag bytes**.
- Problem occurs when the flag byte value matches a data value.
- Can be solved using an ESC character before flag bytes : known as **character/byte stuffing**.

Limitation : All character codes of 8 bit.



(a) A frame delimited by flag bytes.

(b) Four examples of byte sequences before and after byte stuffing.

Data Link Layer Design Issues (cont.)

Framing

Starting and ending flags with bit stuffing :

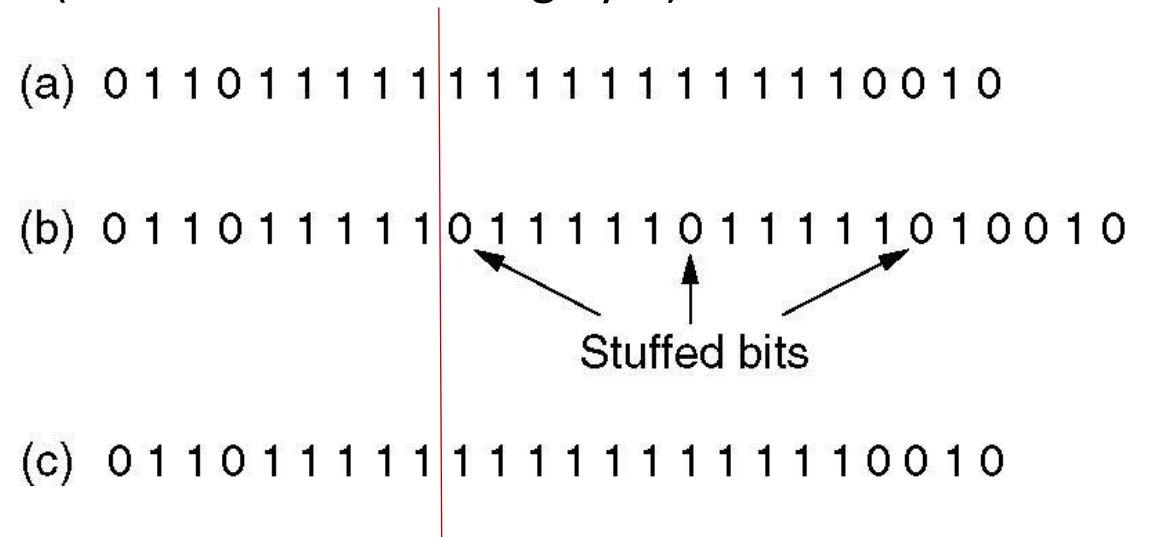
- Allows data frames to contain an arbitrary number of bits and allows character codes with an arbitrary number of bits per character.
 - This method achieves the same thing as Byte Stuffing method by using Bits (1) instead of Bytes (8 Bits).
 - Each frame begins and ends with a special bit pattern (i.e. 01111110 – a flag byte).
 - On transmit, after five consecutive 1s in the data, a 0 is added (i.e. **bit stuffing**).
 - On receive, a 0 after five 1s is deleted to get original data.
 - Flag bytes only occur at frame boundaries, not within the data (i.e. easy to recognize the frame if loses the track while receiving).
 - The side effect: the length of a frame depends on the contents of the data it carries.

(a) 011011111111111111110010

(b) 0110111110111110111110010
Stuffed bits

(c) 011011111111111111110010

(a) The original data.
(b) The data as they appear on the line.
(c) The data as they are stored in the receiver's memory after destuffing.



- (a) The original data.
 - (b) The data as they appear on the line.
 - (c) The data as they are stored in the receiver's memory after destuffing.

Data Link Layer Design Issues (cont.)

Framing

Physical layer coding violations :

- Applicable to networks in which the encoding on the physical medium contains some redundancy.
- Example : Some LANs encode 1 bit of data by using 2 physical bits.
 - Bit '1': high-low
 - Bit '0': low-high
 - (high-high and low-low are not used for data)

Note : Many data link protocols use a combination of a character count with one of the other methods for extra safety.

Data Link Layer Design Issues (cont.)

Framing

Q1. The following character encoding is used in a data link protocol:

A: 01000111; B: 11100011; FLAG: 01111110; ESC: 11100000

Show the bit sequence transmitted (in binary) for the four-character in a frame: A B ESC FLAG when each of the following framing methods are used:

- (a) Character count.
- (b) Flag bytes with byte stuffing.
- (c) Starting and ending flag bytes, with bit stuffing.

A1 : (a) 00000101 01000111 11100011 11100000 01111110
 5 A B ESC FLAG

(b) 01111110 01000111 11100011 11100000 11100000 11100000 01111110 01111110
 FLAG A B ESC ESC FLAG FLAG

(c) 01111110 01000111 110100011 111000000 011111010 01111110

Data Link Layer Design Issues (cont.)

Framing

Q2. A bit string, 0111101111101111110, needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing?

A2 : The bit string actually transmitted is 011110111110011111010.

Data Link Layer Design Issues (cont.)

Framing

Q3. The following data fragment occurs in the middle of a data stream for which the byte-stuffing algorithm is used: A B ESC C ESC FLAG FLAG D. What is the output after stuffing?

A3 : The output after stuffing is A B ESC ESC C ESC ESC FLAG ESC FLAG D.

Data Link Layer Design Issues (cont.)

Error control

- After solving the marking of the frame with start and end the data link layer must **handle eventual errors in transmission.**
 - ✓ Ensuring that all frames are delivered to the network layer at the destination and in proper order.
- Unacknowledged connectionless service: it is fine for the sender to output frames regardless of its reception.
- Reliable connection-oriented service: it is not fine.
- Usual way to ensure reliable delivery is to include **acknowledgement (i.e. special control frames)** to the sender.
 - Positive acknowledgement : frame has arrived safely.
 - Negative acknowledgement : something wrong during transmission, so need retransmission
 - I. A timer is required to be set so that if the data frame or the acknowledgement is lost then the sender is aware of the problem when the timer runs out.
 - II. Sequence numbers required to be associated with frames to ensure the passing of frames to the destination network layer, exactly once in the right order if frames are received more than once.

Data Link Layer Design Issues (cont.)

Flow control

- Important when the sender is running on a fast powerful computer and receiver is running on a slow low-end machine.
- Prevents a fast sender from out-pacing a slow receiver
- Two approaches:
 1. Feedback-based flow control : Can be taken care at the data link layer
 - Receiver gives feedback on the data it can accept and gives permission to send data
 2. Rate-based flow control : Mostly taken care at transport layer
 - Built in mechanism that limits the rate at which sender may transmit data, without the need for feedback from the receiver.

Error Detection and Correction

- Transmission errors: common on local loops (because of analog signalling), wireless links.
- Two basic strategies for dealing with errors.
 - **Error correction :** Include enough redundant information along with each block of data sent, to enable the receiver to deduce what the transmitted data must have been.
 - Applicable to wireless channel , where retransmission can be faulty.
 - Uses error correction codes.
Ex : Hamming code
 - **Error detection :** Include only enough redundancy to allow the receiver to deduce that an error occurred, but not which error, and have it request a retransmission.
 - Applicable to reliable transmission channel such as optical fiber (requires retransmission)
 - Uses error detection codes.
Ex : Cyclic Redundancy Code

Error Detection and Correction (cont.)

Handling the error :

A frame consists of m data (i.e., message) bits and r redundant, or check bits.

Total length be n (i.e., $n = m + r$) bits (normally known as **codeword**).

Example :

- Transmitted: 10001001
- Received: 10110001

XOR operation gives number of bits that are different.

- XOR: 00111000
- Number of bit positions in which two codewords differ is called **Hamming Distance**. It shows that two codes are d distance apart, and it will require d errors to convert one into the other.

Note :

- All 2^m possible data messages are legal.
- All 2^n possible codewords are not treated as legal as far as the hamming distance and check bits are concerned.

Error Detection and Correction(cont.)

Error correction code

Design of an error correction code requires a significant no. of check bits and has a lower limit defined by the relation

$$(m + r + 1) \leq 2^r, \text{ where 'r' indicates no. of check bits for } m \text{ message bits.}$$

Example : Hamming code (can be used to correct single error)

- Bits of the codeword : b₁ b₂ b₃ b₄
- Check bits: The bits that are powers of 2 (p₁, p₂, p₄, p₈, p₁₆, ...).
- The rest of bits (m₃, m₅, m₆, m₇, m₉, ...) are filled with **m** data bits.
- Check bits are considered as parity bits for subset(i.e. some collection of bits) of the codeword (e.g. p₁ is the parity bit for all data bits in positions whose binary representation includes a 1 in the least significant position excluding 1 (3, 5, 7, 9, 11 and so on))
- Data bits are checked by adding together parity bits for its position; e.g., 3 = 1 + 2, 5 = 1 + 4, 6 = 2 + 4, 7 = 1 + 2 + 4, 9 = 1 + 8, 10 = 2 + 8, 11 = 1 + 2 + 8, ...

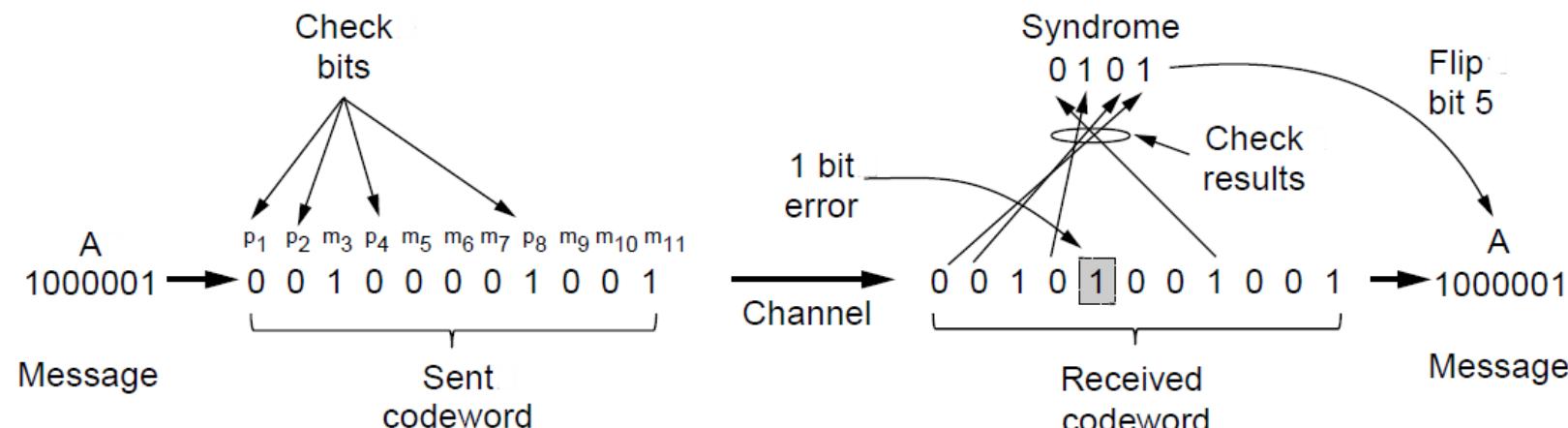
Error Detection and Correction(cont.)

Hamming code

Error correction :

- When a codeword arrives the receiver initializes a counter to '0'.
- After codeword arrives, it examines each check bit k for correct parity value.
 - If correct the codeword is accepted.
 - If incorrect, it adds k to the counter and after all check gives the no. of incorrect data bit.
(e.g. in a (11, 7) codeword, if check bits 1, 2, and 8 are in error, the inverted data bit is 11)
- Recomputing the parity sums (error syndrome) gives the position of the error to flip, or 0 if there is no error.

Example :



An (11, 7) Hamming code correcting a single-bit error

Error Detection and Correction(cont.)

Hamming code

Question :

An 8-bit byte with binary value 10101111 is to be encoded using an even-parity Hamming code. What is the binary value after encoding?

Answer :

Since, $(m + r + 1) \leq 2^r$, $r = 4$ (i.e. p1, p2, p4, p8)

1	2	3	4	5	6	7	8	9	10	11	12	
1	0	1	0	0	1	0	0	1	1	1	1	12-BIT CODEWORD
1	-	1	-	0	-	0	-	1	-	1	-	(EVEN PARITY)
-	0	1	-	-	1	0	-	-	1	1	-	(EVEN PARITY)
-	-	-	0	0	1	0	-	-	-	-	1	(EVEN PARITY)
-	-	-	-	-	-	-	0	1	1	1	1	(EVEN PARITY)

The binary value after encoding is 101001001111.

Error Detection and Correction(cont.)

Error detecting code

- Preferred to be used where the error rate associated with the transmission line is much lower (e.g. optical fiber, copper wire)
- Usually require retransmission if error is detected.

Say, it is required to transmit **1 megabit of data** in the form of data block each of size 1000 bit.

- Using error correction code each block requires 10 check bits for single bit error.
- Requires 10,000 bits to be transmitted for complete data.
- Using error detection code each block requires an extra bit(i.e. parity bit) for single bit error
- Requires an extra block of 1001 bits to be transmitted for complete data.

The total overhead for the error detection + retransmission method is only **2001 bits** per megabit of data, versus **10,000 bits** for a Hamming code.

Example : The polynomial code, also known as a CRC (Cyclic Redundancy Check)

Error Detection and Correction(cont.)

Polynomial (or CRC) code

- Bit strings are represented as polynomials with coefficients of 0 and 1(i.e. bit value) only.
- A k-bit frame is regarded as the coefficient list for a polynomial with k terms ranging from x^{k-1} to x^0 .

Example:

$$110001: 1x^5 + 1x^4 + 0x^3 + 0x^2 + 0x^1 + 1x^0$$

- Uses modulo 2 arithmetic(i.e. both addition and subtraction are equivalent to exclusive OR)
- The sender and receiver must agree upon a generator polynomial, $G(x)$, in advance.
- Both high- and low-order bits in the generator polynomial must be 1.
- CRC is computed for a frame of length m- bits (i.e. $M(x)$) using $G(x)$ known as check summed frame, such that $M(x)$ is longer than the $G(x)$.
- The resulting check summed frame must be divisible by $G(x)$.
- When the receiver gets a check summed frame it divides it by $G(x)$.
 - If the result is not equal to zero it means that there has been transmission error.

Error Detection and Correction(cont.)

Polynomial (or CRC) code

Algorithm for computing the checksum:

1. Let r be the degree of $G(x)$. Append r zero bits to the low-order end of the frame so it now contains $m+r$ bits and corresponds to the polynomial $x^r M(x)$

2. Divide the bit string corresponding to $G(x)$ into the bit string corresponding to $x^r M(x)$ using modulo 2 division.

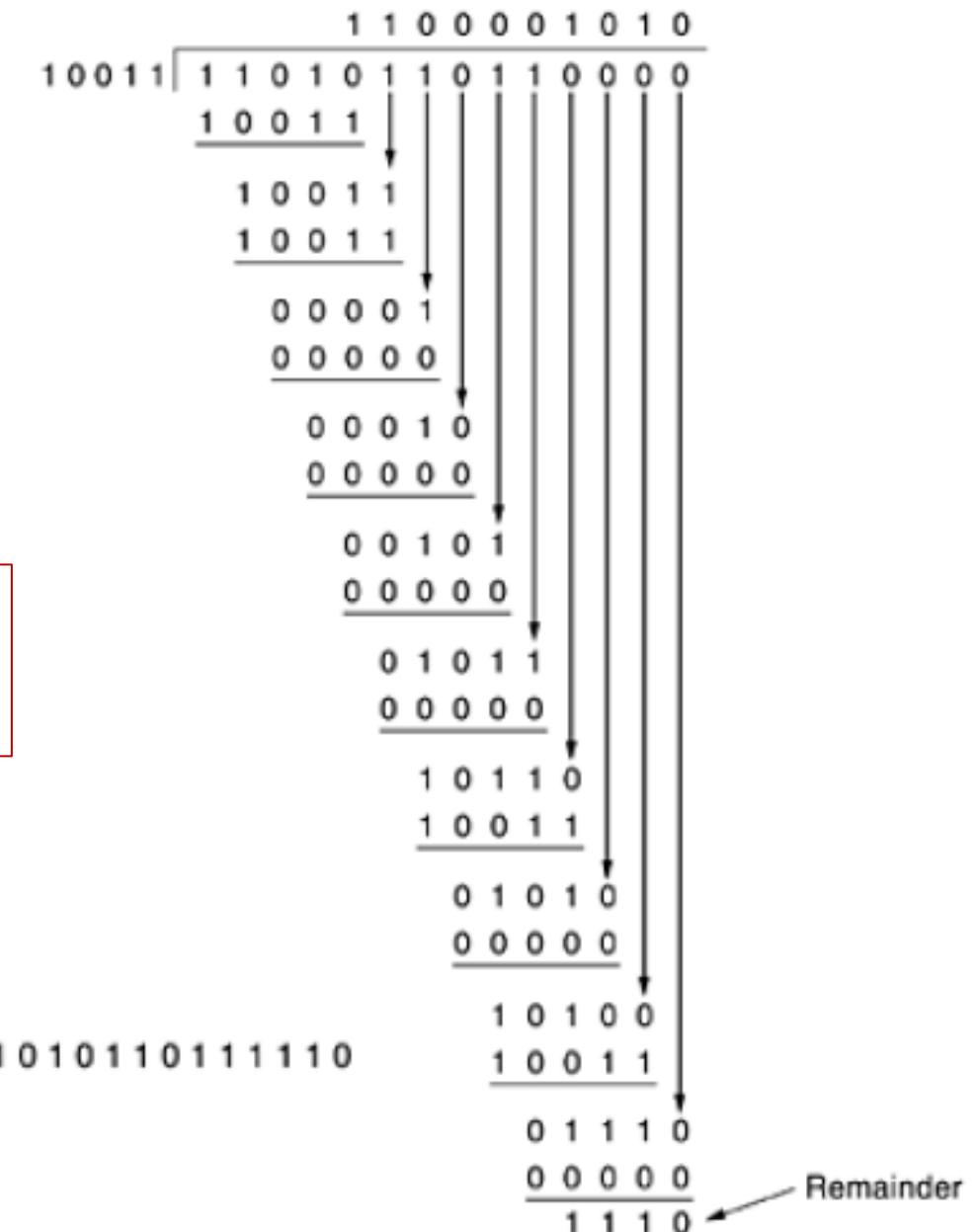
3. Subtract the remainder (which is always r or fewer bits) from the bit string corresponding to $x^r M(x)$ using module 2 subtraction. The result is the checksummed frame, $T(x)$, to be transmitted.

Example:

Frame: 1101011111

Generator: x^4+x+1

Transmitted frame: 11010110111110



Calculation of the polynomial code checksum

Elementary data link protocols

Assumptions:

- 1). DLL and Network layer are independent processes that communicate by passing messages back and forth through the physical layer.
- 2). Machine A wants to send a long stream of data to machine B, using a reliable, **connection-oriented service**.
- 3). Machines do not crash.

Channel: Noiseless

No frames are lost, duplicated, or corrupted.

Protocols :

- An Unrestricted Simplex Protocol
- A Simplex Stop-and-Wait Protocol

Elementary data link protocols (cont.)

Library procedures:

Group	Library Function	Description
Network layer	from_network_layer(&packet) to_network_layer(&packet) enable_network_layer() disable_network_layer()	Take a packet from network layer to send Deliver a received packet to network layer Let network cause “ready” events Prevent network “ready” events
Physical layer	from_physical_layer(&frame) to_physical_layer(&frame)	Get an incoming frame from physical layer Pass an outgoing frame to physical layer
Events & timers	wait_for_event(&event) start_timer(seq_nr) stop_timer(seq_nr) start_ack_timer() stop_ack_timer()	Wait for a packet / frame / timer event Start a countdown timer running Stop a countdown timer from running Start the ACK countdown timer Stop the ACK countdown timer

Note : Defined in a header file *protocol.h*

Elementary data link protocols (cont.)

Protocol definitions:

- Five data structures are defined : *boolean*, *seq_nr*, *packet*, *frame_kind*, and *frame*.
- Defined in *protocol.h*

```
#define MAX_PKT 1024                                /* determines packet size in bytes */

typedef enum {false, true} boolean;                  /* boolean type */
typedef unsigned int seq_nr;                         /* sequence or ack numbers */
typedef struct {unsigned char data[MAX_PKT];} packet; /* packet definition */
typedef enum {data, ack, nak} frame_kind;             /* frame_kind definition */

typedef struct {                                       /* frames are transported in this layer */
    frame_kind kind;                                /* what kind of a frame is it? */
    seq_nr seq;                                     /* sequence number */
    seq_nr ack;                                     /* acknowledgement number */
    packet info;                                    /* the network layer packet */
} frame;
```

Continued →

Elementary data link protocols (cont.)

```
/* Wait for an event to happen; return its type in event. */
void wait_for_event(event_type *event);

/* Fetch a packet from the network layer for transmission on the channel. */
void from_network_layer(packet *p);

/* Deliver information from an inbound frame to the network layer. */
void to_network_layer(packet *p);

/* Go get an inbound frame from the physical layer and copy it to r. */
void from_physical_layer(frame *r);

/* Pass the frame to the physical layer for transmission. */
void to_physical_layer(frame *s);

/* Start the clock running and enable the timeout event. */
void start_timer(seq_nr k);

/* Stop the clock and disable the timeout event. */
void stop_timer(seq_nr k);

/* Start an auxiliary timer and enable the ack_timeout event. */
void start_ack_timer(void);

/* Stop the auxiliary timer and disable the ack_timeout event. */
void stop_ack_timer(void);

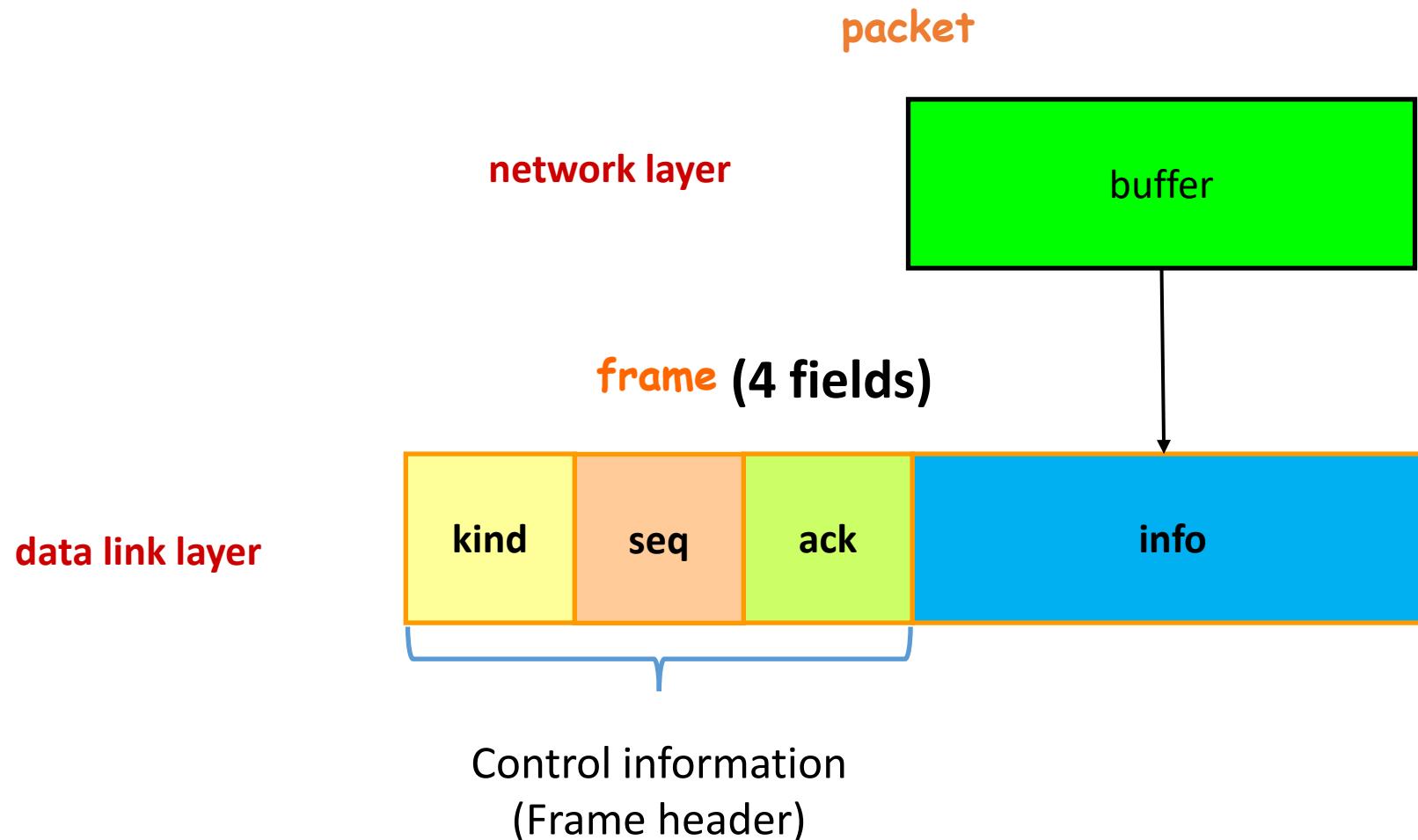
/* Allow the network layer to cause a network_layer_ready event. */
void enable_network_layer(void);

/* Forbid the network layer from causing a network_layer_ready event. */
void disable_network_layer(void);

/* Macro inc is expanded in-line: Increment k circularly. */
#define inc(k) if (k < MAX_SEQ) k = k + 1; else k = 0
```

Protocol Definitions (ctd.)

Elementary data link protocols (cont.)

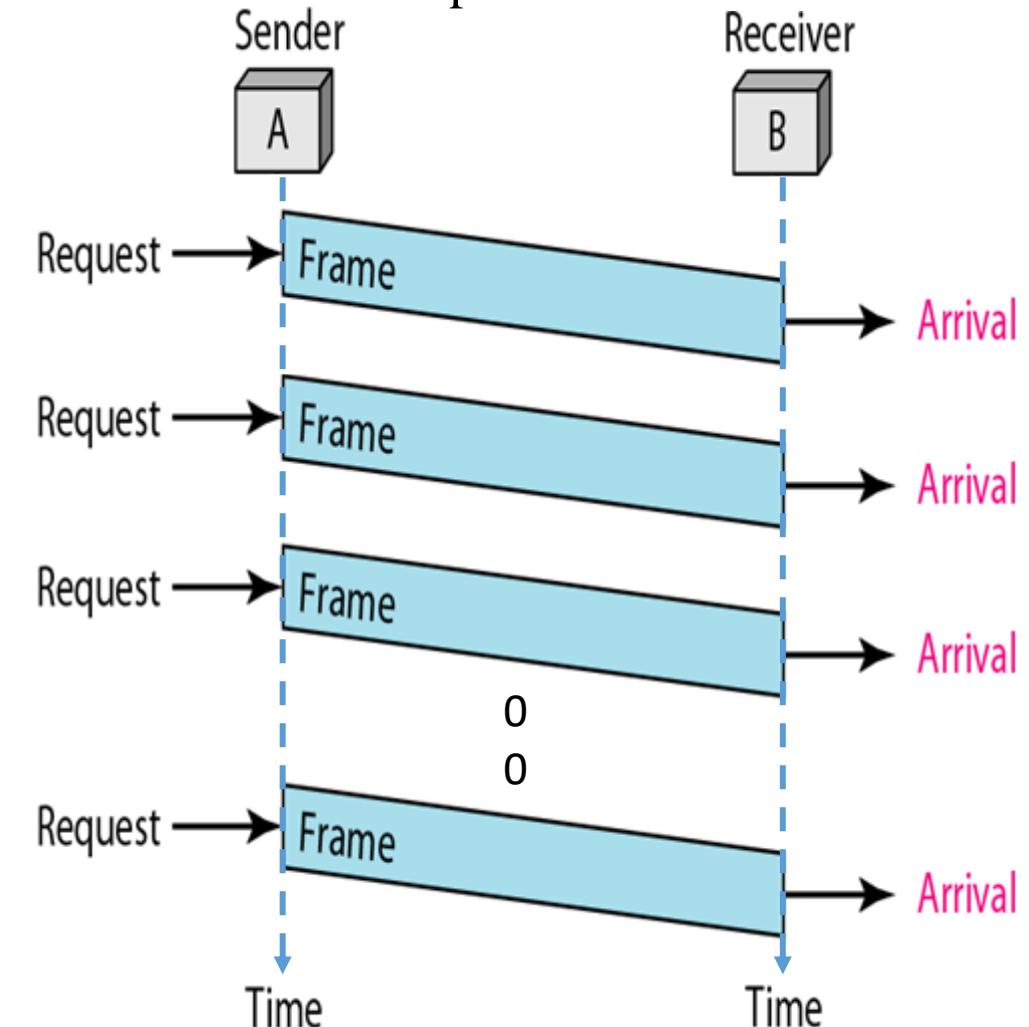


Elementary data link protocols (cont.)

An Unrestricted Simplex Protocol

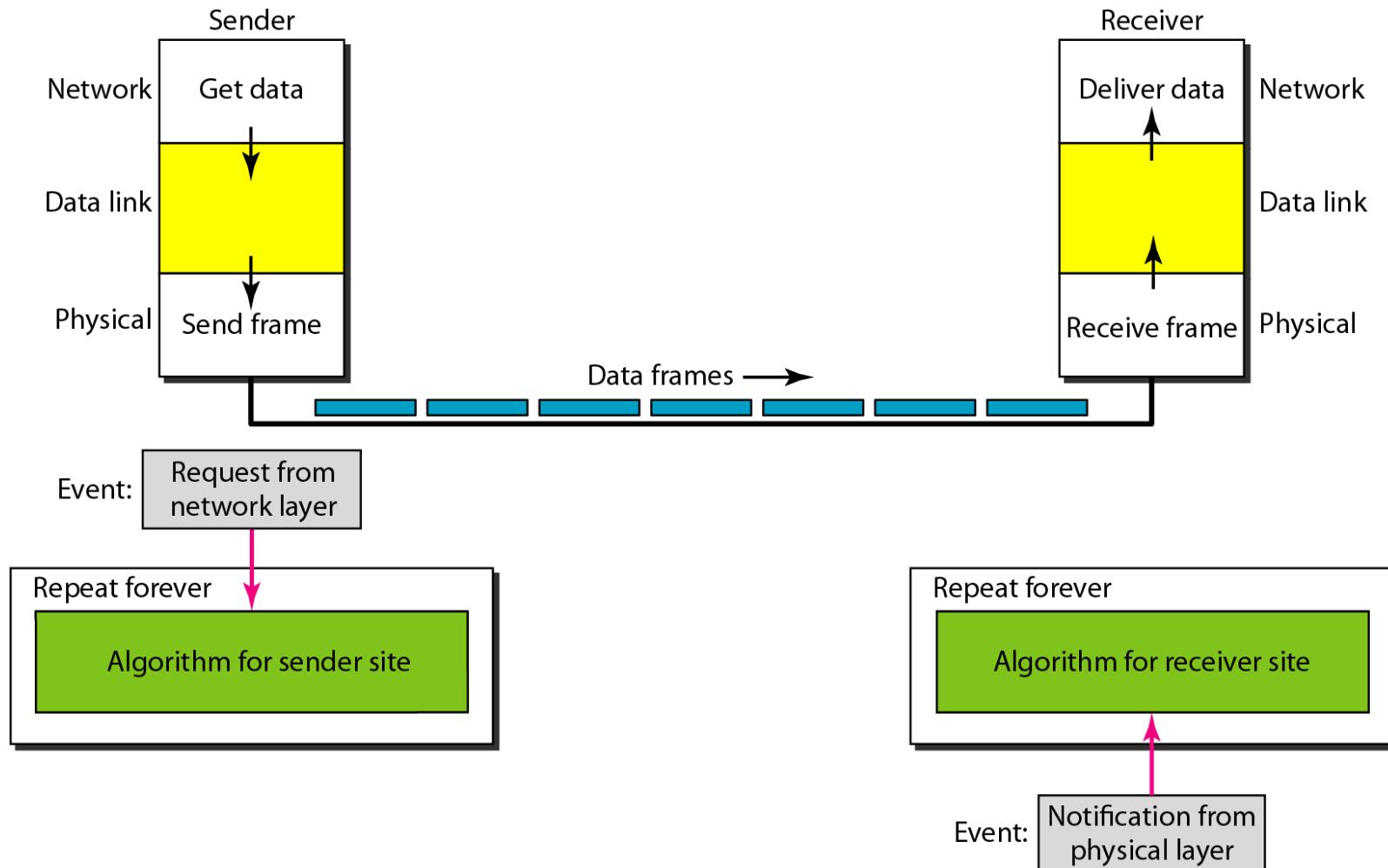
- Simplest Protocol (called as **utopia**)
- Unidirectional in which *data frames are traveling in only one direction*-from the sender to receiver.
- Both transmitting and receiving network layers are always ready.
- The receiver can immediately handle any frame it receives with a processing time that is small enough to be negligible.
- The data link layer of the receiver immediately removes the header from the frame and hands the data packet to network layer.
- In other words, the receiver can never be fill out with incoming frames.
- Unrealistic and resembles to connectionless
- Relies on higher layer for error handling

Communication using (Flow Diagram)
Simplest Protocol



Elementary data link protocols (cont.)

An Unrestricted Simplex Protocol



Design of the utopia protocol with no flow or error control

Elementary data link protocols (cont.)

An Unrestricted Simplex Protocol

```
/* Protocol 1 (utopia) provides for data transmission in one direction only, from
   sender to receiver. The communication channel is assumed to be error free,
   and the receiver is assumed to be able to process all the input infinitely quickly.
   Consequently, the sender just sits in a loop pumping data out onto the line as
   fast as it can. */
```

```
typedef enum {frame arrival} event type;
#include "protocol.h"

void sender1(void)
{
    frame s;                                /* buffer for an outbound frame */
    packet buffer;                          /* buffer for an outbound packet */

    while (true) {
        from_network_layer(&buffer); /* go get something to send */
        s.info = buffer;                /* copy it into s for transmission */
        to_physical_layer(&s);         /* send it on its way */
        /* Tomorrow, and tomorrow, and tomorrow,
           Creeps in this petty pace from day to day
           To the last syllable of recorded time
           - Macbeth, V, v */
    }
}

void receiver1(void)
{
    frame r;
    event_type event;

    while (true) {
        wait_for_event(&event);
        from_physical_layer(&r);
        to_network_layer(&r.info);
    }
}

/* filled in by wait, but not used here */

/* only possibility is frame_arrival */
/* go get the inbound frame */
/* pass the data to the network layer */
```

Runs at sender
machine



Runs at receiver
machine

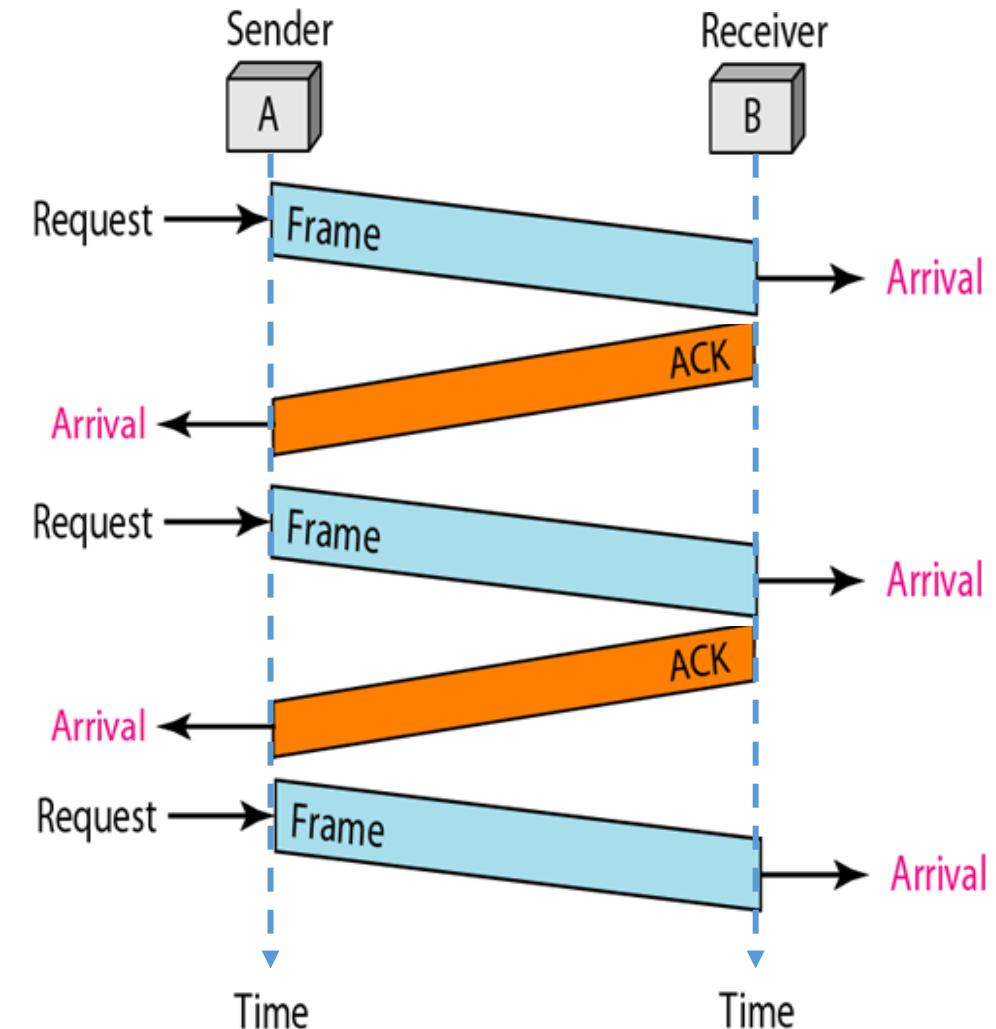


Elementary data link protocols (cont.)

A Simplex Stop-and-wait Protocol

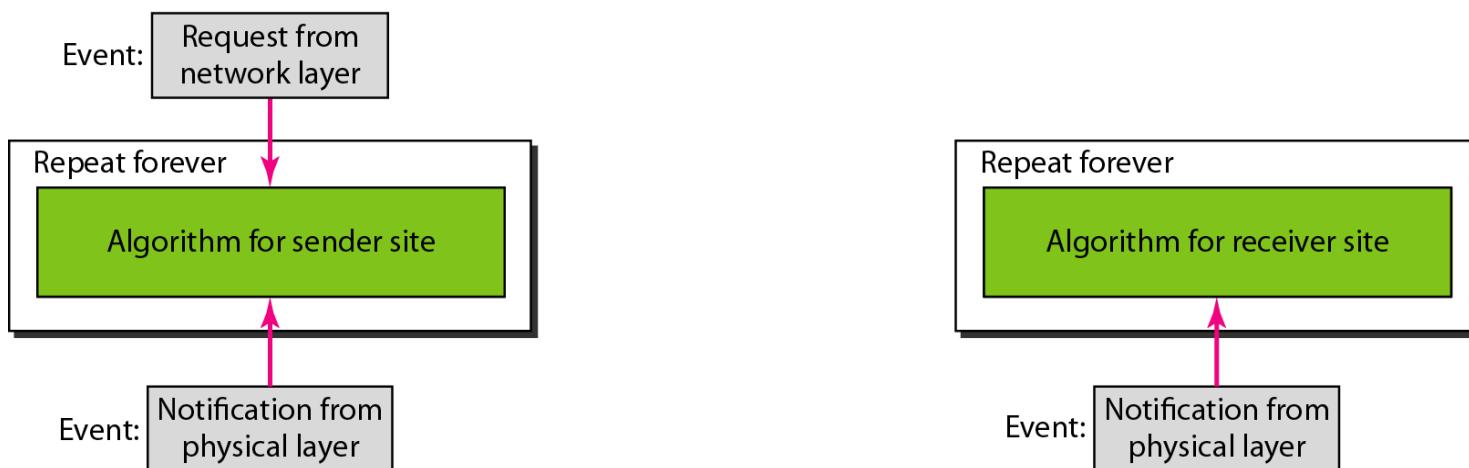
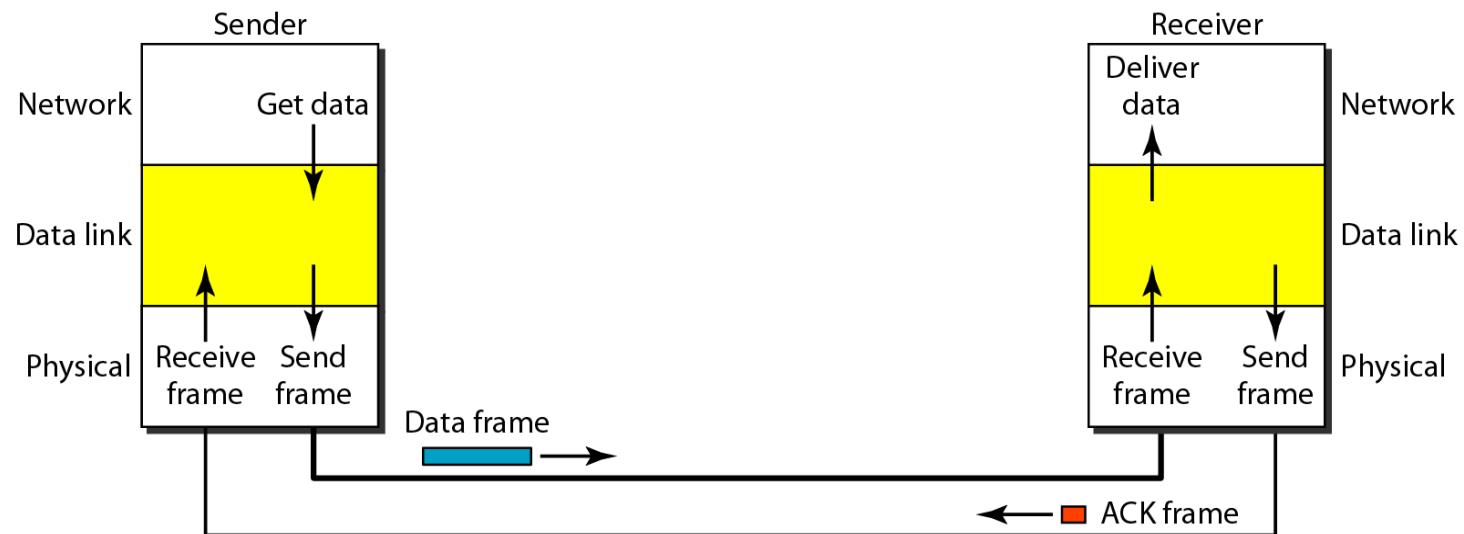
- If data frames arrive at the receiver site faster than they can be processed, the frames must be stored until their use.
- Normally, the receiver does not have enough storage space, especially if it is receiving data from many sources.
- Required to tell the sender to slow down.
- There must be feedback from the receiver to the sender.
- The sender sends one frame, stops until it receives agreement the receiver (okay to go ahead), and then sends the next frame.
- Still have unidirectional communication for data frames, but auxiliary ACK frames (simple tokens of acknowledgment) travel from the other direction.
- Includes flow control

Communication (Flow Diagram) using Stop-and-Wait Protocol



Elementary data link protocols (cont.)

A Simplex Stop-and-wait Protocol



Design of Stop-and-Wait Protocol

Elementary data link protocols (cont.)

A Simplex Stop-and-wait Protocol

/* Protocol 2 (stop-and-wait) also provides for a one-directional flow of data from sender to receiver. The communication channel is once again assumed to be error free, as in protocol 1. However, this time, the receiver has only a finite buffer capacity and a finite processing speed, so the protocol must explicitly prevent the sender from flooding the receiver with data faster than it can be handled. */

```

typedef enum {frame_arrival} event_type;
#include "protocol.h"

void sender2(void)
{
    frame s;                                /* buffer for an outbound frame */
    packet buffer;                          /* buffer for an outbound packet */
    event_type event;                      /* frame_arrival is the only possibility */

    while (true) {
        from_network_layer(&buffer);
        s.info = buffer;
        to_physical_layer(&s);
        wait_for_event(&event);
    }
}

void receiver2(void)
{
    frame r, s;                            /* buffers for frames */
    event_type event;                      /* frame_arrival is the only possibility */

    while (true) {
        wait_for_event(&event);
        from_physical_layer(&r);
        to_network_layer(&r.info);
        to_physical_layer(&s);
    }
}

```

Runs at sender
machine



Runs at receiver
machine



Sliding Window Protocols

- In most practical situations, there is a need for **transmitting data in both directions**.
- One way of **achieving full-duplex** data transmission is to have **two separate communication channels** and **use each one for simplex data traffic** (in different directions).
- If this is done, we have two separate physical circuits, each with a "forward" channel (for data) and a "reverse" channel (for acknowledgements).
- **In both cases the bandwidth of the reverse channel is almost entirely wasted.** In effect, the user is paying for two circuits but using only the capacity of one.

Sliding Window Protocols

Improvement...

- A better idea is to **use the same circuit for data in both directions**.
- In this model the **data frames from A to B are intermixed with the acknowledgement frames from A to B**.
- By looking at the **kind field** in the **header of an incoming frame**, the receiver can tell **whether the frame is data or acknowledgement**.

Sliding Window Protocols

Piggybacking

- When a data frame arrives, instead of immediately sending a separate control frame, the receiver restrains itself and waits until the network layer passes it the next packet.
- The acknowledgement is attached to the outgoing data frame (using the **ack field** in the frame header).
- In effect, the *acknowledgement gets a free ride on the next outgoing data frame*.
- The technique of temporarily delaying outgoing acknowledgements so that they can be hooked onto the next outgoing data frame is known as **piggybacking**.

Sliding Window Protocols

Piggybacking

- The principal **advantage** of using piggybacking over having distinct acknowledgement frames is a better use of the available channel bandwidth.
- The **ack field** in the frame header costs only a few bits, whereas **a separate frame would need a header, the acknowledgement, and a checksum**.
- However, **piggybacking introduces a complication not present with separate acknowledgements. How long should the data link layer wait for a packet onto which to piggyback the acknowledgement?**
- **If a new packet arrives quickly, the acknowledgement is piggybacked onto it; otherwise, if no new packet has arrived by the end of this time period, the data link layer just sends a separate acknowledgement frame.**

Sliding Window Protocols

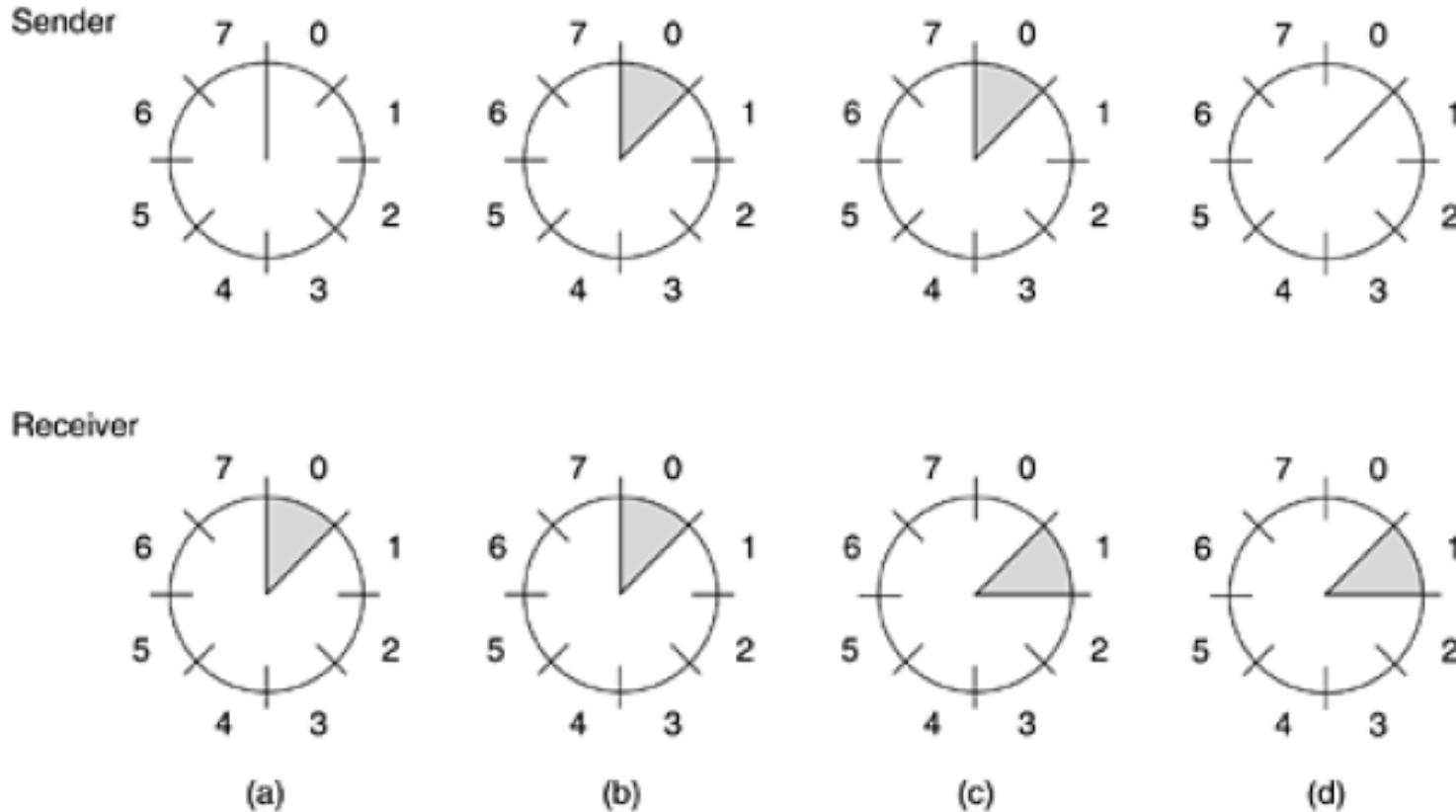
- All sliding window protocols, each **outbound frame** contains a **sequence number**, ranging from **0** up to some **maximum**.
- The **maximum** is usually $2^n - 1$ so the sequence number fits exactly in an n-bit field.
- The **stop-and-wait sliding window protocol** uses **n = 1**, **restricting the sequence numbers to 0 and 1**, but more sophisticated versions can use arbitrary n.

Sliding Window Protocols

- The essence of all sliding window protocols is that at any instant of time, the **sender maintains a set of sequence numbers corresponding to frames it is permitted to send**. These frames are said to fall within the sending window.
- Similarly, the receiver also maintains a receiving window corresponding to the set of frames it is permitted to accept.
- The sender's window and the receiver's window need not have the same lower and upper limits or even have the same size.
- In some protocols they are fixed in size, but in others they can grow or shrink over the course of time as frames are sent and received.

Sliding Window Protocols

Figure 3-13. A sliding window of size 1, with a 3-bit sequence number. (a) Initially. (b) After the first frame has been sent. (c) After the first frame has been received. (d) After the first acknowledgement has been received.



A One-Bit Sliding Window Protocol

Sliding Window Protocols

```
/* Protocol 4 (sliding window) is bidirectional. */

#define MAX_SEQ 1                      /* must be 1 for protocol 4 */
typedef enum {frame_arrival, cksum_err, timeout} event_type;
#include "protocol.h"

void protocol4 (void)
{
    seq_nr next_frame_to_send;          /* 0 or 1 only */
    seq_nr frame_expected;             /* 0 or 1 only */
    frame r, s;                       /* scratch variables */
    packet buffer;                   /* current packet being sent */
    event_type event;

    next_frame_to_send = 0;            /* next frame on the outbound stream */
    frame_expected = 0;              /* frame expected next */
    from_network_layer(&buffer);     /* fetch a packet from the network layer */
    s.info = buffer;                 /* prepare to send the initial frame */
    s.seq = next_frame_to_send;       /* insert sequence number into frame */
    s.ack = 1 - frame_expected;      /* piggybacked ack */
    to_physical_layer(&s);           /* transmit the frame */
    start_timer(s.seq);              /* start the timer running */
}
```

A One-Bit Sliding Window Protocol

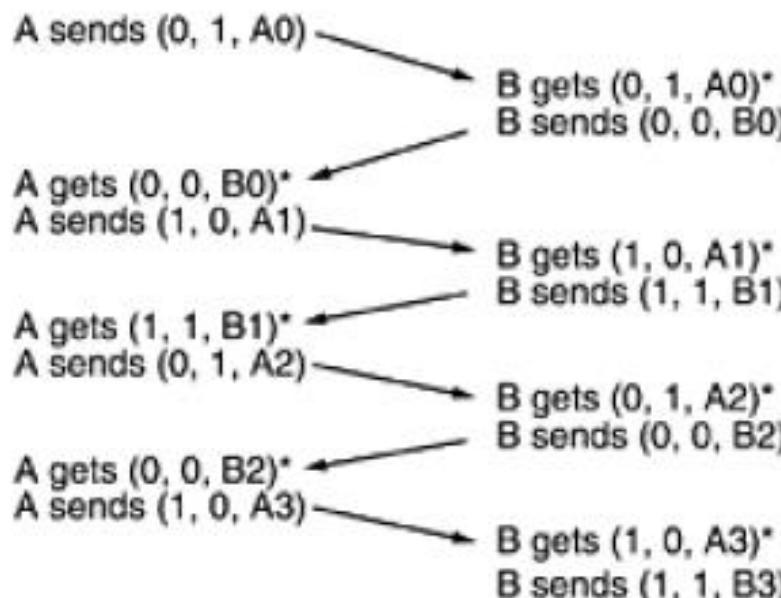
Sliding Window Protocols

```
while (true) {
    wait_for_event(&event);
    if (event == frame_arrival) {
        from_physical_layer(&r);
        if (r.seq == frame_expected) {
            to_network_layer(&r.info);
            inc(frame_expected);
        }
        if (r.ack == next_frame_to_send) { /* handle outbound frame stream. */
            stop_timer(r.ack);           /* turn the timer off */
            from_network_layer(&buffer); /* fetch new pkt from network layer */
            inc(next_frame_to_send);    /* invert sender's sequence number */
        }
    }
    s.info = buffer;                  /* construct outbound frame */
    s.seq = next_frame_to_send;       /* insert sequence number into it */
    s.ack = 1 - frame_expected;      /* seq number of last received frame */
    to_physical_layer(&s);          /* transmit a frame */
    start_timer(s.seq);              /* start the timer running */
}
```

A One-Bit Sliding Window Protocol

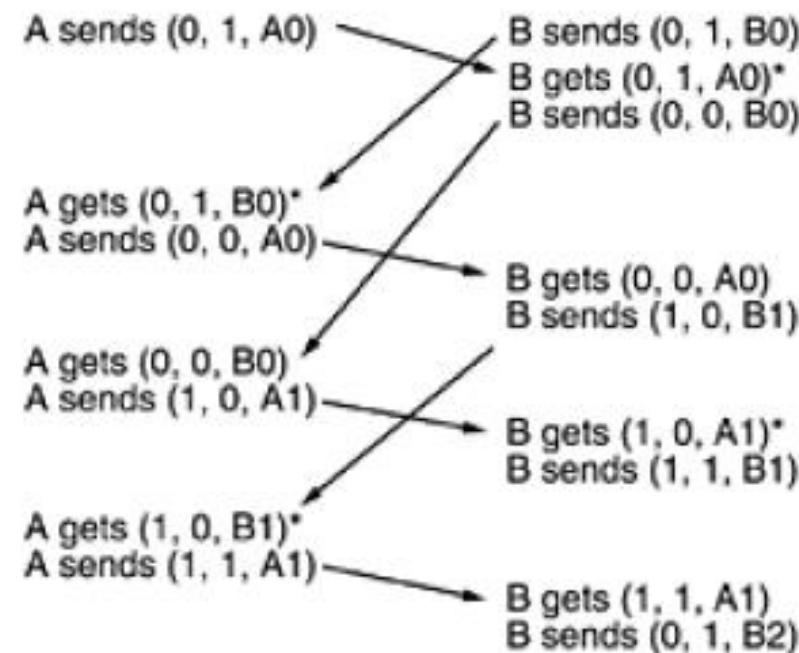
Sliding Window Protocols

Figure 3-15. Two scenarios for protocol 4. (a) Normal case. (b) Abnormal case. The notation is (seq, ack, packet number). An asterisk indicates where a network layer accepts a packet.



(a)

Time



(b)

A Protocol Using Go Back N

Sliding Window Protocols

- Until now we have made the tacit assumption that the transmission time required for a frame to arrive at the receiver plus the transmission time for the acknowledgement to come back is negligible.
- Sometimes this assumption is clearly false.
- In these situations, the long round-trip time can have important implications for the efficiency of the bandwidth utilization.

A Protocol Using Go Back N

Sliding Window Protocols

- As an example, consider a 50-kbps satellite channel with a 500-msec round-trip propagation delay. Let us imagine trying to use protocol 4 to send 1000-bit frames via the satellite. At $t = 0$ the sender starts sending the first frame. At $t = 20$ msec the frame has been completely sent.
- Not until $t = 270$ msec has the frame fully arrived at the receiver, and not until $t = 520$ msec has the acknowledgement arrived back at the sender, under the best of circumstances (no waiting in the receiver and a short acknowledgement frame).
- This means that the sender was blocked during $500/520$ or 96 percent of the time. In other words, only 4 percent of the available bandwidth was used. Clearly, the combination of a long transit time, high bandwidth, and short frame length is disastrous in terms of efficiency.

A Protocol Using Go Back N

Sliding Window Protocols

- The **problem** described above can be viewed because of **the rule requiring a sender to wait for an acknowledgement before sending another frame.**
- If we relax that restriction, much better efficiency can be achieved.
- Basically, the **solution** lies in **allowing the sender to transmit up to w frames before blocking, instead of just 1.**
- With an appropriate choice of w the **sender will be able to continuously transmit frames for a time equal to the round-trip transit time without filling up the window.**

A Protocol Using Go Back N

Sliding Window Protocols

- In the example above, w should be at least **26**.
- The sender begins sending frame 0 as before. By the time it has **finished sending 26 frames, at $t = 520$, the acknowledgement for frame 0 will have just arrived.**
- Thereafter, acknowledgements arrive every 20 msec, so the sender always gets permission to continue just when it needs it. At all times, 25 or 26 unacknowledged frames are outstanding. Put in other terms, the sender's maximum window size is 26.

A Protocol Using Go Back N

Sliding Window Protocols

- This technique is known as **pipelining**.

Channel capacity is ***b bits/sec***,

Frame size ***l bits***,

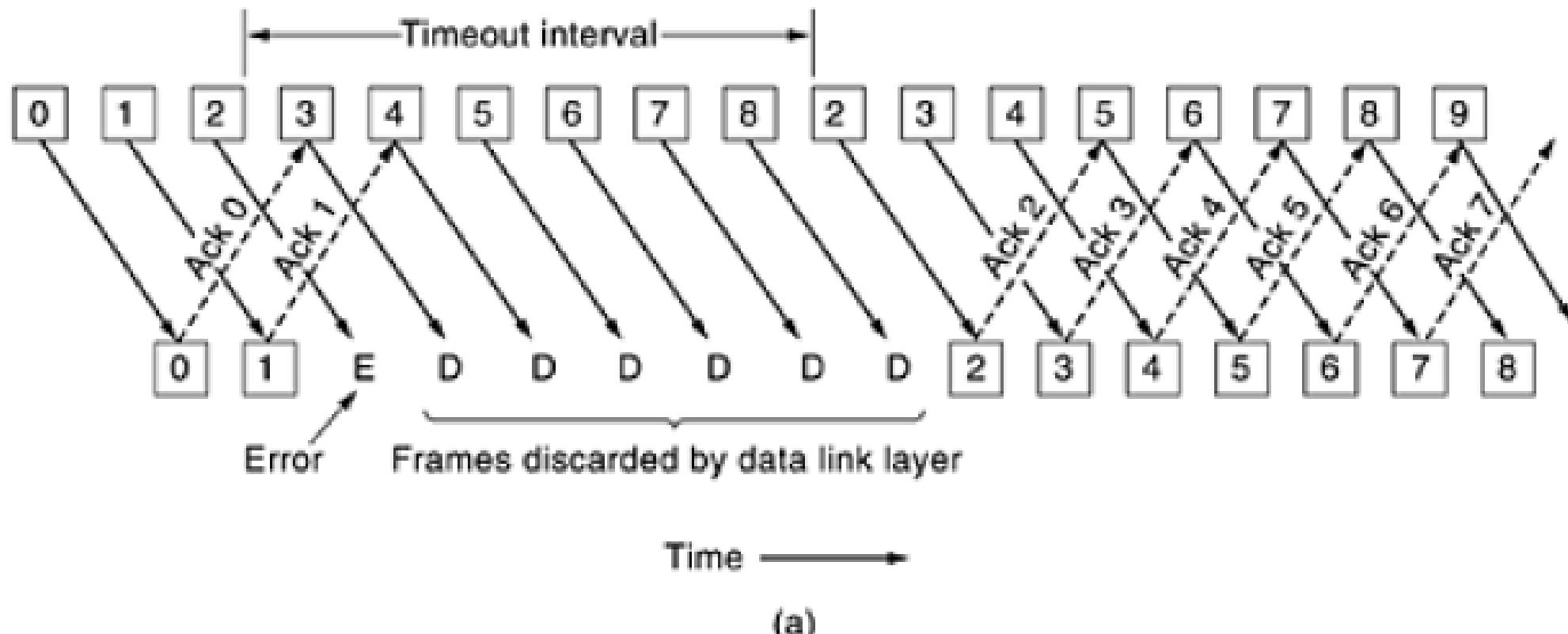
Roundtrip propagation time ***R sec***,

Then, the time required to transmit a single frame is ***l/b sec***.

$$\text{line utilization} = l/(l + bR)$$

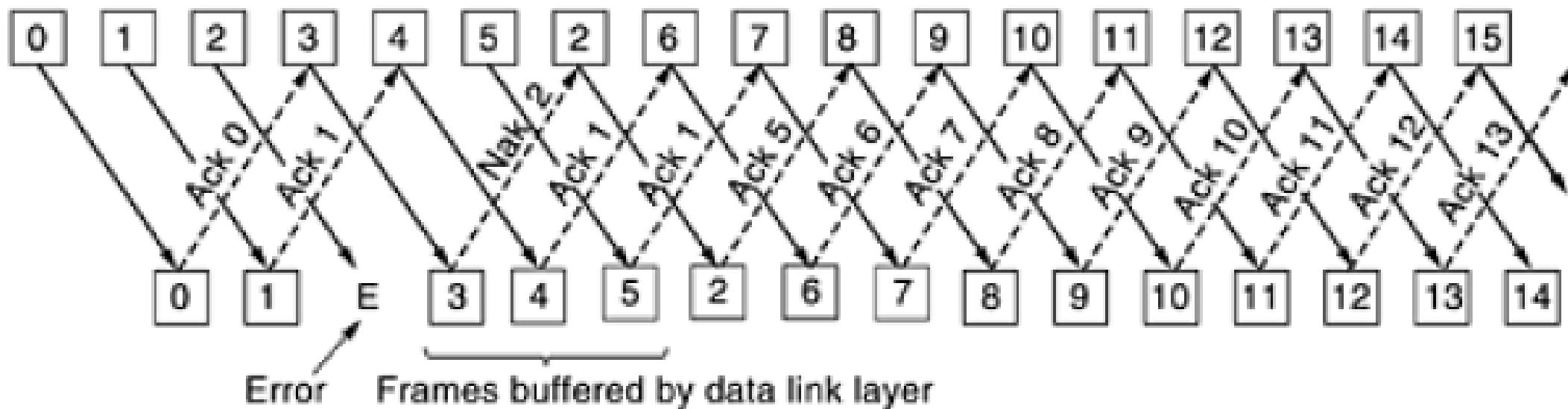
A Protocol Using Go Back N *Sliding Window Protocols*

- Pipelining and error recovery.
- Effect of an error when (a) receiver's window size is 1



A Protocol Using Go Back N *Sliding Window Protocols*

- Pipelining and error recovery.
- Effect of an error when (b) receiver's window size is large



(b)

A Protocol Using Selective Repeat *Sliding Window Protocols*

- **Go back N** works well if **errors** are **rare**, but if the *line is poor, it wastes a lot of bandwidth on retransmitted frames.*
- An alternative strategy for handling errors is to **allow the receiver to accept and buffer the frames following a damaged or lost one**. Such a protocol does not discard frames merely because an earlier frame was damaged or lost.
- In this protocol, **both sender and receiver maintain a window of acceptable sequence numbers**.
- The sender's window size starts out at 0 and grows to some predefined maximum, **MAX_SEQ**. The receiver's window, in contrast, is always fixed in size and equal to **MAX_SEQ**.

A Protocol Using Selective Repeat *Sliding Window Protocols*

- The receiver has a **buffer reserved** for each sequence number within its **fixed window**. Associated with each buffer is a bit (arrived) telling whether the **buffer is full or empty**.
- Whenever a **frame arrives**, its sequence number is checked by the **function between** to see if it falls within the **window**. If so and if it has not already been received, it is accepted and stored. This action is taken without regard to whether it contains the next packet expected by the network layer.
- It must be **kept within the data link layer** and not passed to the network layer until all the **lower-numbered frames** have already been delivered to the network layer in the **correct order**.

Error Detection and Correction(cont.)

The error-detecting and error-correcting properties of a code depend on this Hamming distance.

- To reliably detect d error, one would need a distance $d+1$ code.

Ex : Forming a code with adding a parity bit while transmitting can be used to detect single error even though it has a hamming distance of 2.

(when 1011010 transmitted with even parity the code will be 10110100. A single bit error produces a code word of odd parity)

- To correct d error, one would need a distance $2d+1$ code.

Ex : 4 valid codes: 000000000, 000001111, 111110000, 111111111

Minimal Distance of this code is 5 => can correct double errors.

(If the codeword 000000111 arrives, the receiver knows that the original must have been 000001111)

Error Detection and Correction(cont.)

Hamming code

Consider a message having four data bits (D) which is to be transmitted as a 7-bit codeword by adding three check bits. This would be called a (7,4) code. The three bits to be added are three EVEN Parity bits (P), where the parity of each is computed on different subsets of the message bits as shown below.

1	2	3	4	5	6	7	
P	P	D	P	D	D	D	7-BIT CODEWORD
P	-	D	-	D	-	D	(EVEN PARITY)
-	P	D	-	-	D	D	(EVEN PARITY)
-	-	-	P	D	D	D	(EVEN PARITY)

- For example, the message **1101** would be sent as **1010101**, since:

1	2	3	4	5	6	7	
1	0	1	0	1	0	1	7-BIT CODEWORD
1	-	1	-	1	-	1	(EVEN PARITY)
-	0	1	-	-	0	1	(EVEN PARITY)
-	-	-	0	1	0	1	(EVEN PARITY)

Problem

- Let us assume that $m = 3$ and $n = 4$. Find the list of valid data words and codewords assuming the check bit is used to indicate even parity in the code word.

Valid dataword	Valid codeword
000	0000
001	0011
010	0101
011	0110
100	1001
101	1010
110	1100
111	1111

Problem

What is the Hamming distance for each of the following codewords:

- a. (10000, 00000)
- b. (10101, 10000)
- c. (11111,11111)
- d. (000, 000)

Ans:

- a. 1
- b. 2
- c. 0
- d. 0

Problem

Find the minimum Hamming distance to be implemented in codeword for the following cases:

- a. Detection of two errors.
- b. Correction of two errors.
- c. Detection of 3 errors or correction of 2 errors.
- d. Detection of 6 errors or correction of 2 errors.

Problem

Find the minimum Hamming distance to be implemented in codeword for the following cases:

- a. Detection of two errors.
- b. Correction of two errors.
- c. Detection of 3 errors or correction of 2 errors.
- d. Detection of 6 errors or correction of 2 errors.

- a. For error detection \rightarrow Hamming distance = $d + 1 = 2 + 1 = 3$
- b. For error correction \rightarrow Hamming distance = $2d + 1 = 2 \times 2 + 1 = 5$
- c. For error detection \rightarrow Hamming distance = $d + 1 = 3 + 1 = 4$
For error correction \rightarrow Hamming distance = $2d + 1 = 2 \times 2 + 1 = 5$
Therefore, minimum Hamming distance should be 5.
- d. For error detection \rightarrow Hamming distance = $d + 1 = 6 + 1 = 7$
For error correction \rightarrow Hamming distance = $2d + 1 = 2 \times 2 + 1 = 5$
Therefore, minimum Hamming distance should be 7.

Problem

Given in the table a set of valid dataword and codeword.

What is the dataword transmitted for the following codewords received assuming there is 1 bit error?

- a. 01010
- b. 11010

Dataword	Codeword
00	00000
01	01011
10	10101
11	11110

Problem

Given in the table a set of valid dataword and codeword.

What is the dataword transmitted for the following codewords received assuming there is 1 bit error?

- a. 01010
- b. 11010

Answer:

- a. 01
- b. 11

Dataword	Codeword
00	00000
01	01011
10	10101
11	11110

Problem

- Sixteen-bit messages are transmitted using a Hamming code. How many check bits are needed to ensure that the receiver can detect and correct single bit errors? Show the bit pattern transmitted for the message 1101001100110101. Assume that even parity is used in the Hamming code.

Problem

- Sixteen-bit messages are transmitted using a Hamming code. How many check bits are needed to ensure that the receiver can detect and correct single bit errors? Show the bit pattern transmitted for the message 1101001100110101. Assume that even parity is used in the Hamming code.

Answer:

- 5 check bits are needed at positions 1, 2, 4, 8, and 16.
- The bit pattern transmitted for the message (first)1101001100110101 is 011010110011001110101

Problem

- An 8-bit message using even-parity Hamming code is received as 101001001111. Find the 8-bit message after getting decoded assuming no error during transmission?

Problem

- An 8-bit message using even-parity Hamming code is received as 101001001111. Find the 8-bit message after getting decoded assuming no error during transmission?
- Answer:
The 8-bit message after decoding is 10101111.

Problem

- A 12-bit Hamming code whose hexadecimal value is 0xE4F arrives at a receiver. What was the original value in hexadecimal? Assume that not more than 1 bit is in error.

Problem

- A 12-bit Hamming code whose hexadecimal value is 0xE4F arrives at a receiver. What was the original value in hexadecimal? Assume that not more than 1 bit is in error.

Answer:

- If we number the bits from left to right starting at bit 1, in this example bit 2 (a parity bit) is incorrect. The 12-bit value transmitted (after Hamming encoding) was 0xA4F. The original 8-bit data value was 0xAF.

Problem

- What is the remainder obtained by dividing x^7+x^5+1 by the generator polynomial x^3+1 ?

Problem

- What is the remainder obtained by dividing x^7+x^5+1 by the generator polynomial x^3+1 ?

Answer:

- The remainder is $x^2+x +1$.

Problem

- Given the dataword 101001111 and the divisor 10111. Show the generation of the CRC codeword at the sender site (using binary division).

Problem

- Given the dataword 101001111 and the divisor 10111. Show the generation of the CRC codeword at the sender site (using binary division).

Answer:

The codeword at the sender site is
1010011110101

Computer Network

(CSE 3034)

Text book: Computer Networks by Andrew S. Tanenbaum

Introduction to the course

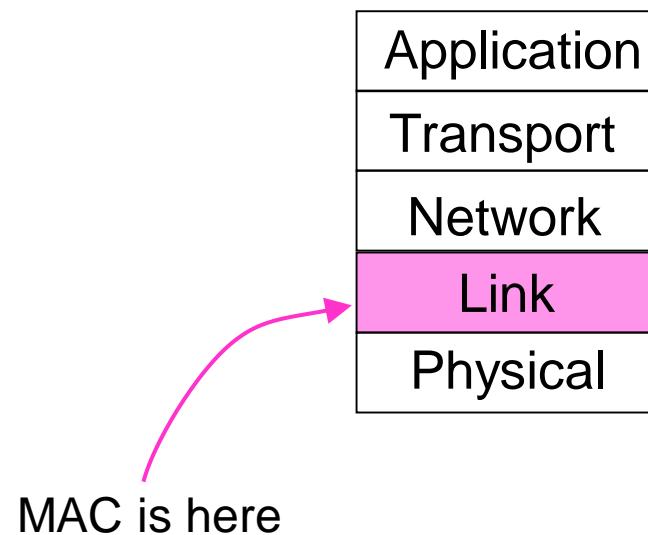
Syllabus :

- Introduction(Chapter 1)
- The Physical Layer(Chapter 2)
- The Data Link Layer(Chapter 3)
- **The Medium Access Control Sublayer(Chapter 4)**
- The Network Layer(Chapter 5)
- The Transport layer(Chapter 6)
- The Application layer(Chapter 7)
- Network security(Chapter 8)

The Medium access Control Sublayer

The MAC Sublayer

- Responsible for deciding who sends next on a multi-access link
- An important part of the link layer, especially for LANs



Multiple Access Protocols

- ALOHA »
- CSMA (Carrier Sense Multiple Access) »

Multiple Access Protocols (Cont.)

ALOHA

- In 1970 by Norman Abramson and colleagues at the University of Hawaii
- Used ground based radio broadcasting
- Applicable to any system in which uncoordinated users are competing for the use of a single shared channel
- Two versions of the protocol :
 - Pure ALOHA - time continuous
 - Slotted ALOHA - divided into discrete slots into which all frames must fit
- Basic idea – let users transmit whenever they have data to be sent. If there are collisions handle them.

Multiple Access Protocols(Cont.)

ALOHA

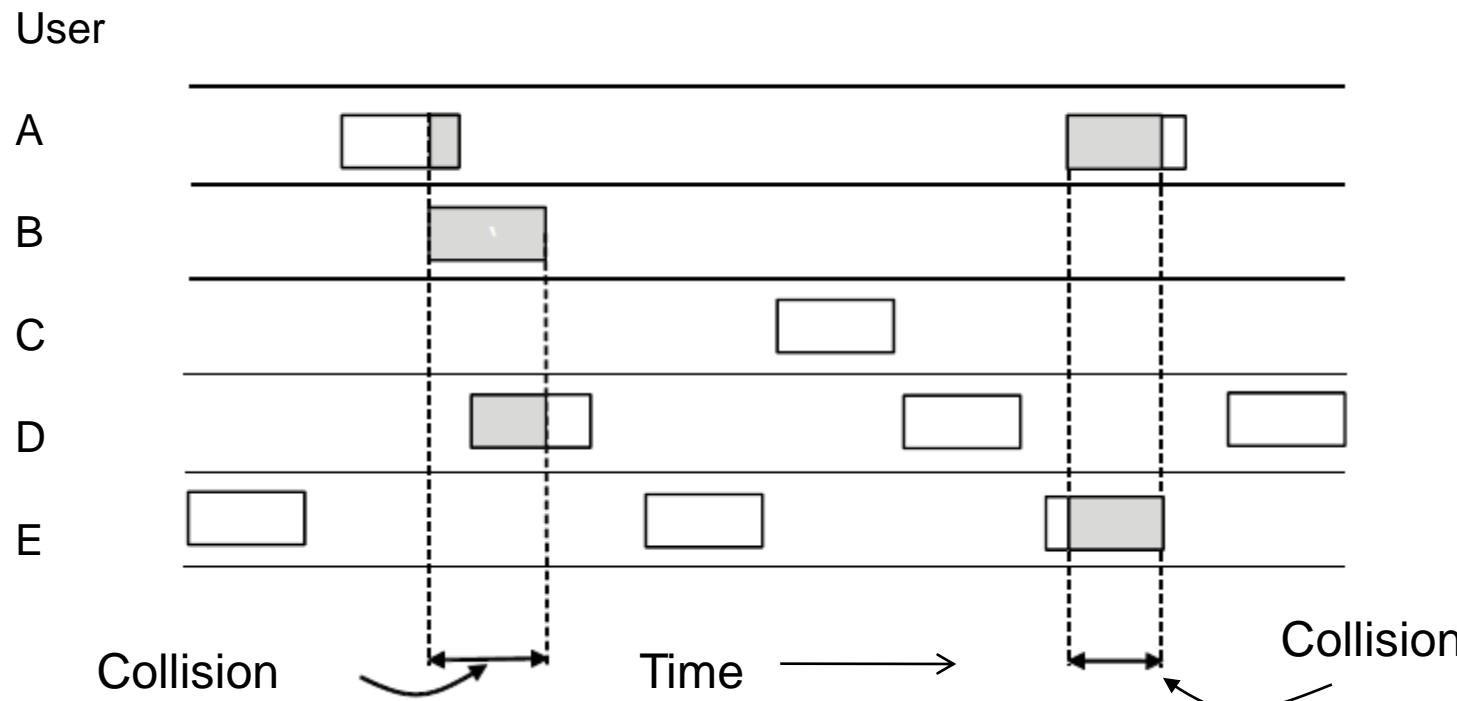
Pure ALOHA :

- Each user is free to transmit whenever they have data to be sent.
 - There will be collisions
 - Senders need some way to find out if this is the case.
 - Original sending station can listen to see if its frame has gone through.
 - If listening not possible, acknowledgments are alternative.
- If the frame is destroyed, the sender just waits a random amount of time and sends it again.
 - Waiting time must be random(usually doubles after each failure) or else the sending frames will collide over and over.
 - **Contention** systems: that use the same channel in the way that might lead to conflicts.
- Frames do not collide if no other frames are sent within one frame time of its start

Multiple Access Protocols(Cont.)

ALOHA

- When two frames try to occupy the same channel there is a collision.
- If the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed



In pure ALOHA, frames are transmitted
at completely arbitrary times

Multiple Access Protocols(Cont.)

ALOHA

Pure ALOHA :

What is the efficiency of an ALOHA channel?

- Infinite collection of users typing at their terminals (stations).
- User states: WAITING or TYPING.
- When a line is finished, the user stops typing waiting for response.
- The station then transmits a frame containing the line over the shared channel and checks the channel to see if it was successful.
- If so the user sees the reply and goes back to typing
- If not, the user continuously waits while the station retransmits the frame over and over until it has been successfully sent.

Multiple Access Protocols(Cont.)

Pure ALOHA :

ALOHA

- Frame Time – denotes the amount of time needed to transmit the standard, fixed-length frame.
- Each new frame is assumed to be generated by Poisson distribution with a mean of N frames per frame time.
 - If $N > 1$ the user community is generating frames at a higher rate than the channel can handle, and nearly every frame will suffer a collision.
 - For reasonable throughput we expect $0 < N < 1$.
- In addition to the new frames, the stations also generate retransmissions of frames that previously suffered collisions.
- Assume that the new and the old frames combined modeled by a Poisson distribution with mean G frames per frame time, so $G \geq N$.
 - Low load: $N \approx 0$, there will be few collisions, hence few retransmissions, $G \approx N$
 - High load: there will be many collisions, $G > N$.
- Under all loads the throughput S is just the offered load, G , times the probability P_0 of a transmission succeeding:

$$S = G P_0, \text{ where } P_0 \text{ is the probability of a frame not collided}$$

Multiple Access Protocols(Cont.)

Pure ALOHA :

- How to find P_0 ? Can be computed making an assumption that collisions happen only when other users transmit during a vulnerable period.
- Vulnerable period = $2*t$, $t \Rightarrow$ Frame period
- The probability that k frames generated during a given frame time, in which G frames are expected, is given by the Poisson distribution:

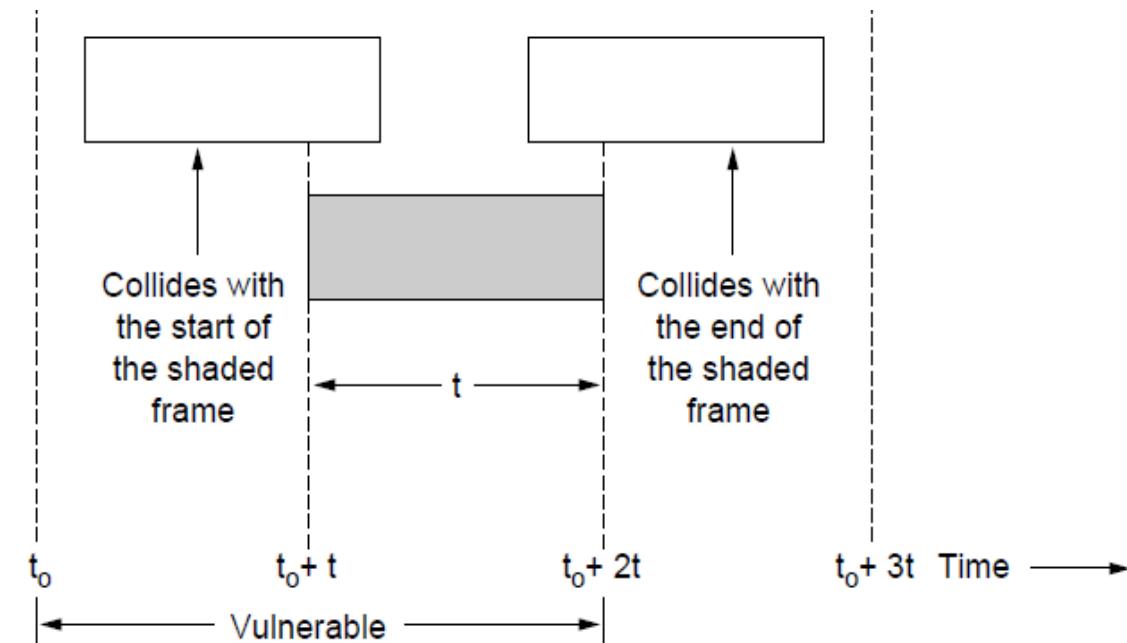
$$\Pr[k] = \frac{G^k e^{-G}}{k!}$$

- Probability of zero frames: e^{-G}
- In an interval two frame times long, the mean number of frames generated is $2G$.
- Probability of no frames being initiated during the entire vulnerable period is given by $P_0 = e^{-2G}$.

Thus, $S = G e^{-2G}$

- S will be maximum when $G = 0.5$ and is found to be 0.184(i.e. 18.4 %)

ALOHA



Vulnerable period for the shaded frame

Multiple Access Protocols(Cont.)

Slotted ALOHA :

ALOHA

- Roberts in 1972 published a method for doubling the capacity of an ALOHA system.
- Divide time into discrete intervals called **slots**.
- Each interval/slot corresponds to one frame time.
- Users will have to agree on slot boundaries.
- A station is not permitted to send whenever the user types a carriage return.
- User waits for the beginning of the next slot.
- Continuous time ALOHA is turned into a discrete time one.
- Synchronization is required:
 - One special station emit a pip at the start of each interval, like clock.

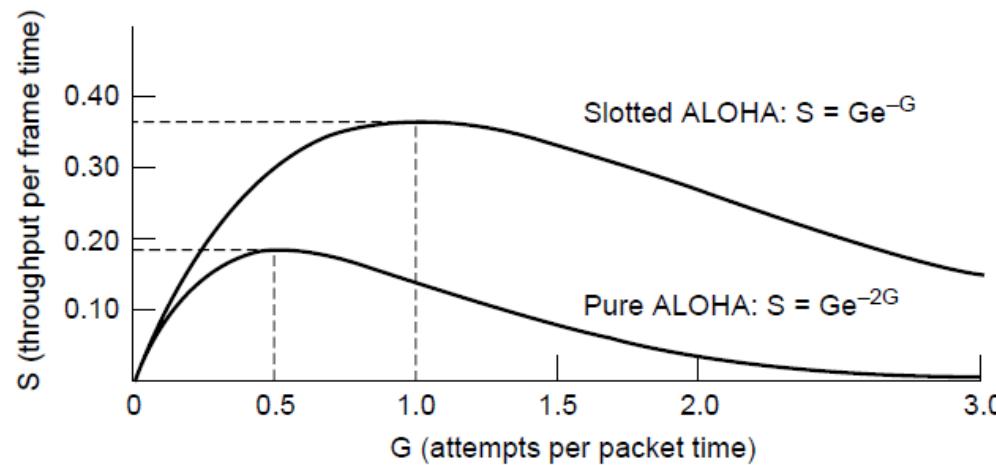
Multiple Access Protocols(Cont.)

Slotted ALOHA :

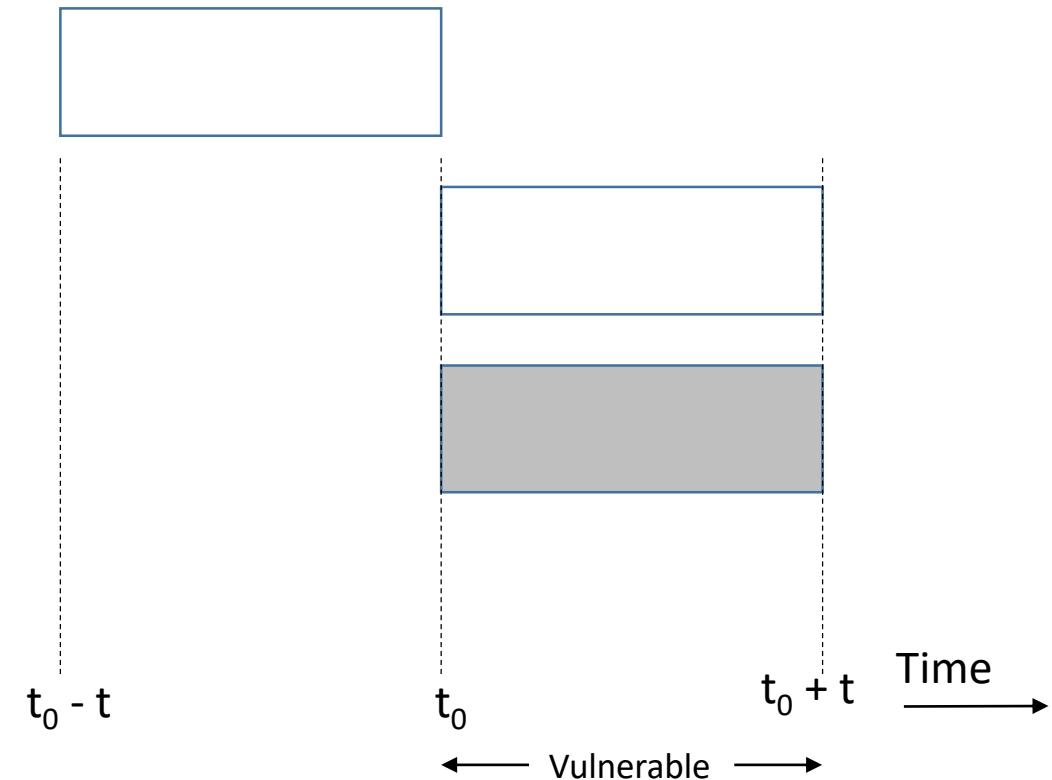
- Vulnerable period = t , ($t \Rightarrow$ Frame period)
- Probability of no frames being initiated during the entire vulnerable period is given by $P_0 = e^{-G}$.

$$\text{Thus, } S = Ge^{-G}$$

- S will be maximum when $G = 1$ and is found to be 0.368(i.e. 36.8 %)



ALOHA



Throughput versus offered traffic for ALOHA systems

Multiple Access Protocols(Cont.)

Carrier Sense Multiple Access (CSMA) Protocols

- CSMA improves on ALOHA by sensing the channel.
- Protocols in which stations listen for a carrier (i.e., transmission) and act accordingly are called **carrier sense** protocols.
- User doesn't send if it senses someone else.
- Versions of these protocols :
 - Persistent and Nonpersistent CSMA
 - 1-persistent
 - Nonpersistent
 - p-persistent
 - CSMA with Collision Detection

Multiple Access Protocols(Cont.)

Carrier Sense Multiple Access (CSMA) Protocols

Persistent and Nonpersistent CSMA

- **1-Persistent** is the simplest scheme.
 - When station has data to send, it listens to channel to see if anyone else is transmitting
 - If channel is idle, it sends its data, otherwise it waits until the channel is idle.
 - When channel becomes idle it transmits.
 - If a collision occurs, it waits a random amount of time and starts again.
- Called 1-persistent because the station transmits with a probability of 1 when the channel is idle.
- Collisions may occur when two patiently waiting stations will start transmitting at the same time if the channel becomes idle and propagation delay increases.
- Still better than ALOHA because both stations have the decency of interfering with third station's frame.

Multiple Access Protocols(Cont.)

Carrier Sense Multiple Access (CSMA) Protocols

Persistent and Nonpersistent CSMA

- **Nonpersistent:** Conscious attempt is made to sense the channel and less greedy.
- Station listens for an idle signal and if no one else is transmitting it sends its data.
- If channel is in use it does not keep sensing; instead it waits a random amount of time before it tries sensing again.
- This leads to a better channel utilization but longer delays than 1-Persistent CSMA.

Multiple Access Protocols(Cont.)

Carrier Sense Multiple Access (CSMA) Protocols

Persistent and Nonpersistent CSMA

- **p – persistent:** Transmission with probability p
- Protocol is applied to slotted channels
- When a station is ready to send, it senses the channel
- If the channel is idle, it sends with a probability p.
- With a probability $q = 1-p$, it defers until the next slot.
- If that slot is idle, it either transmits or defers again with probabilities p and q.
- This continues until the frame is transmitted or until another station begins transmitting.

Multiple Access Protocols(Cont.)

Carrier Sense Multiple Access (CSMA) Protocols

CSMA with Collision Detection

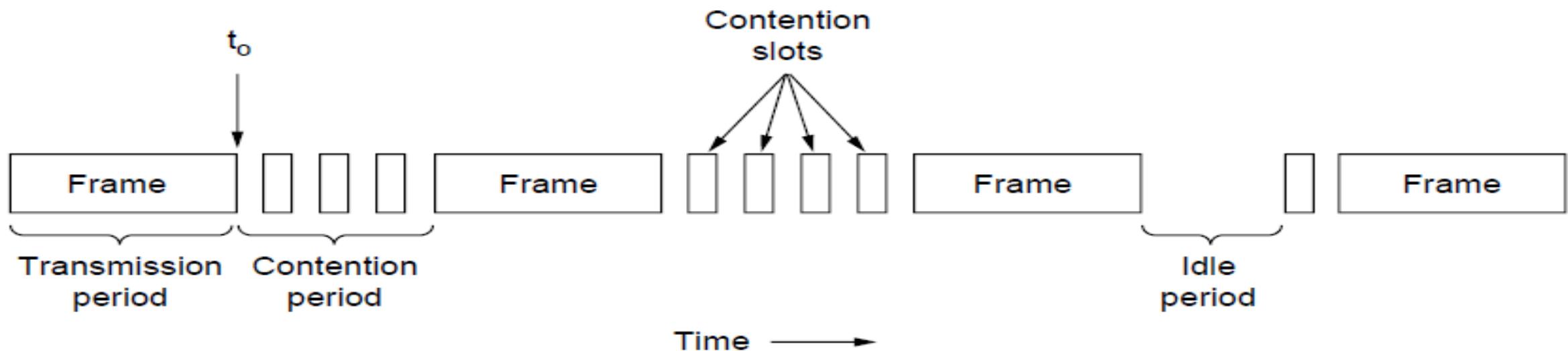
- CSMA protocols are an improvement over ALOHA because they ensure that no station transmits while the channel is busy.
- If two stations sense the channel to be idle and both start transmitting simultaneously, collisions occur.
- An improvement is for the station to quickly detect the busy channel and to stop transmitting since the frame will be garbled and lost anyway.
- This is known as **CSMA/CD** (**Carrier Sense Multiple Access with Collision Detection**) and it saves time and bandwidth.
- Forms the basis of Ethernet LAN protocol.

Multiple Access Protocols(Cont.)

Carrier Sense Multiple Access (CSMA) Protocols

CSMA with Collision Detection

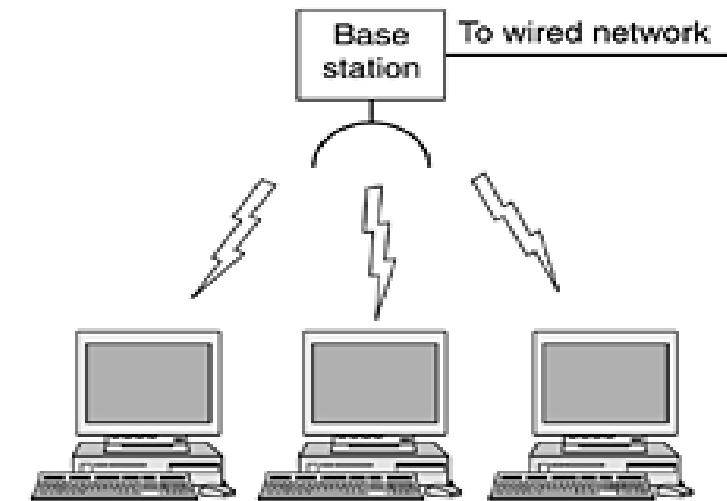
- Consists of alternate contention and transmission periods with idle periods when all stations are quiet.



Multiple Access Protocols(Cont.)

Wireless LAN Protocols

- System of laptops/notebook computers that communicate by radio can be regarded as a **wireless LAN**.
- Require **special MAC sub layer protocols** since different from conventional **LAN** in structure.
- Common configuration of wireless LAN:
 - Office Building with **Access Points (APs)**(also called as base stations)
 - APs Strategically placed
 - APs are wired together (copper or fiber)
 - APs provide connectivity
- A geographical area/room covered by an AP can be treated as a **cell like in cellular telephony system**.
- All radio transmitters have some **fixed range**.
- Receiver within the transmission range can only receive the signal form transmitter.
- In wireless LANs **not all stations are within range of one another**(so complicity develops during communication).



Multiple Access Protocols(Cont.)

Wireless LAN Protocols

Can CSMA be used in Wireless LAN for transmission ?

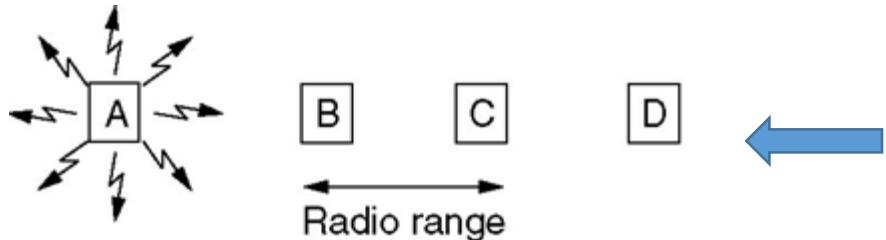
- Not really appropriate because what matters is interference at the receiver, not at the sender.

Example scenario : 4 stations *A, B, C* and *D*.

Assumption :

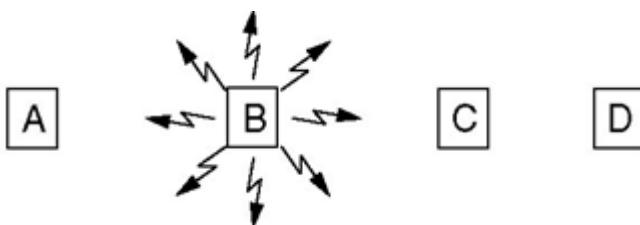
- *A* and *B* are within each other's range and can potentially interfere with one another.
- *C* can also potentially interfere with both *B* and *D*, but not with *A*.

Case I : Hidden node problem - Senders that cannot sense each other but nonetheless collide at intended receiver



- *A* starts sending to *B*.
- *C* senses and finds the channel is free so starts sending to *B*.
- *A* and *C* are hidden to each other so can't sense each other's status.
- Both of their data's gets interfered at *B*.

Case II : Exposed node problem - Senders who can sense each other but still transmit safely (to different receivers)



- There is an ongoing transmission from *B* to *A*.
- *C* can sense it since it is in the range of *B* and so thinks not to transmit.
- Absolutely not face any problem if *C* transmits to *D* since *B* and *D* are not in either's range.
- *B* and *C* are exposed terminals when transmitting to *A* and *D*.

Multiple Access Protocols(Cont.)

Wireless LAN Protocols

Problems to note :

- Before starting a transmission, a station really wants to know whether there is activity around the receiver.
- With a wire, **only one transmission can take place at once** anywhere in the system though all signals can propagate to all stations.
- In a system based on short-range radio waves, **multiple transmissions can occur simultaneously** if they all have different destinations and these destinations are out of range of one another.

Two protocols :

1. MACA
2. MACAW

Multiple Access Protocols(Cont.)

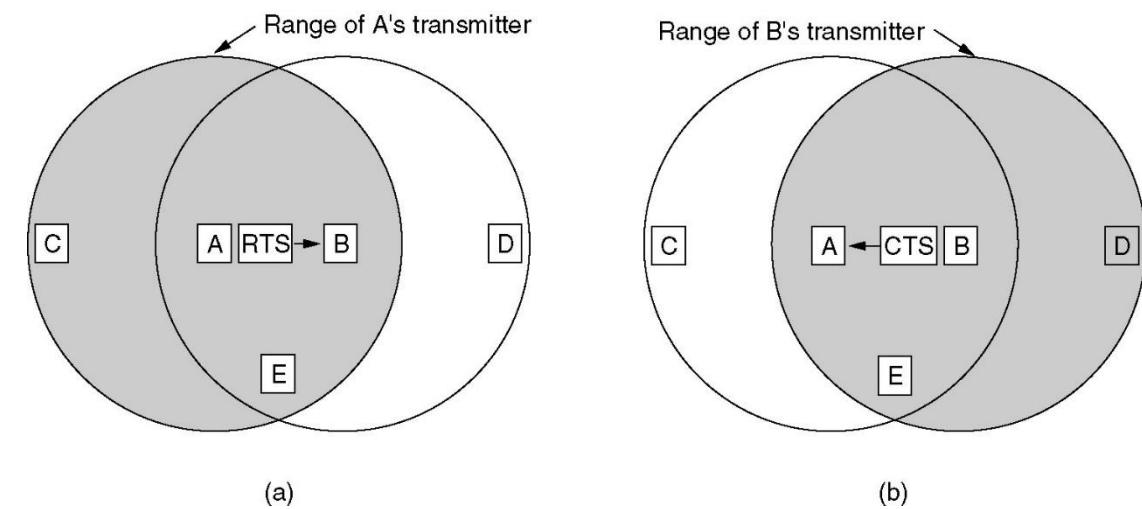
Wireless LAN Protocols

MACA (Multiple Access with Collision Avoidance)

- An early protocol designed for wireless LANs .
- Basic idea :
 - Sender to simulate the receiver into outputting a short frame.
 - Nearby stations can detect this transmission and avoid transmitting for the duration of the upcoming (larger) data frame.

Example :

- A initiates by sending **Request To Send (RTS)** (a short frame say of 30 bytes indicating the data length) to station B.
- B replies with a **Clear To Send (CTS)** (contains the data length being copied from RTS) frame.
- After reception of the CTS frame A begins transmission.
- Any station hearing the RTS from A (*i.e. C and E*) must remain silent long enough for the CTS to be transmitted back to A without conflict.
- Any station hearing the CTS from B(*i.e. D and E*) must remain silent during the upcoming data transmission.
- Still collisions are possible (e.g C and B sends RTS to A simultaneously). Requires random waiting time for retransmission following to collision.



(a) A sending an RTS to B. (b) B responding with a CTS to A.

Multiple Access Protocols(Cont.)

Wireless LAN Protocols

MACAW (MACA for Wireless)

- Fine tuned MACA to improve its performance.
- Introduces an ACK frame after each successful data frame.
- Includes CSMA to sense any nearby station has transmitted RTS to the destined node of itself.
- Runs the back off algorithm separately for each data stream (source-destination pair), rather than for each station.
- Adds a mechanism for stations to exchange information about congestion.

Ethernet

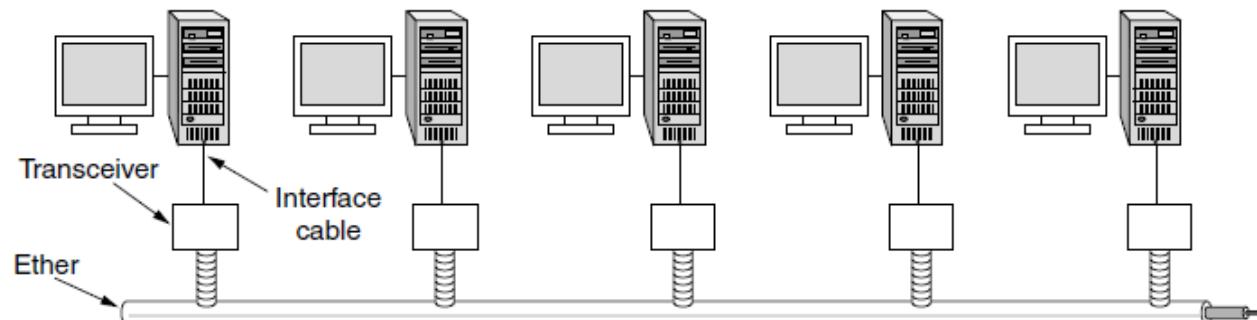
- Many of the designs for personal, local, and metropolitan area networks have been standardized under the name of **IEEE 802**.
- A few have survived but many have not.
- The most important of the survivors are **802.3 (Ethernet)** and **802.11 (wireless LAN)**.
- Two kinds of Ethernet exist:
 1. **Classic Ethernet**, which solves the multiple access problem using the techniques such as CSMA.
 - Original form and ran at rates from 3 to 10 Mbps.
 2. **Switched Ethernet**, in which devices called **switches** are used to connect different computers.
 - The today's Ethernet runs at
 - **100 Mbps (fast Ethernet)**
 - **1000 Mbps (gigabit Ethernet)**
 - **10,000 Mbps (10 gigabit Ethernet)**

Ethernet(Cont.)

Classical Ethernet physical layer

History and standard :

- Bob Metcalfe with David Boggs designed and implemented the first local area network in 1976 in Xerox Palo Alto Lab.
- It used a single long thick coaxial cable.
- Speed **3 Mbps**.
- **Named this as Ethernet.**
- Successfully designed and later drafted as **DIX standard** in 1978 by Xerox, DEC, Intel with a **10 Mbps**.
- With a minor change, the DIX standard became the **IEEE 802.3 standard in 1983**.



Architecture of classic Ethernet

Ethernet(Cont.)

Classical Ethernet physical layer

Structure :Two varieties

➤ Thick Ethernet:

- Uses a thick cable with markings every 2.5 meters to show where to attach computers.
- Segment could be as long as 500 m.
- Could be used to connect up to 100 computers.

➤ Thin Ethernet:

- Cables bent more easily and connections made using BNC connectors.
- Segment could be no longer than 185 m.
- Could be used to connect up to 30 computers.

- Each version of Ethernet has a maximum cable length per segment (i.e. unamplified length) over which the signal will propagate.
- For a large length connectivity the cables could be connected by **repeaters**.
 - Repeater is a physical layer device that receives, amplifies, and retransmits signals in both directions.
- Over each of those cables the signal was coded using **Manchester encoding**.
- Other restriction was that no two transceivers could be more than 2.5 km apart and no path between any two transceivers could traverse more than four repeaters.

Ethernet(Cont.)

Classic Ethernet MAC Sublayer Protocol

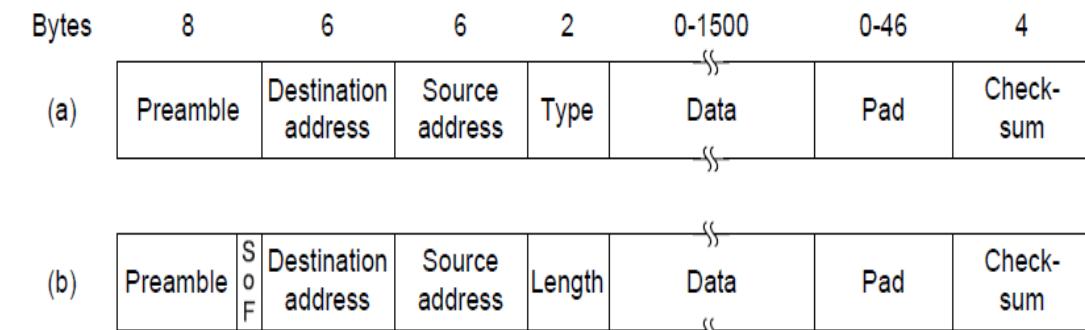
Frame format :

➤ Preamble (8 bytes)

- Contains the bit pattern 10101010 (with the exception of the last byte, in which the last 2 bits are set to 11).
- This last byte is called the *Start of Frame delimiter for 802.3*.
- *The Manchester encoding of this pattern produces a 10-MHz square wave for 6.4 µsec to allow the receiver's clock to synchronize with the sender's.*
- The last two 1 bits tell the receiver that the rest of the frame is about to start.

➤ Source and destination address (6 bytes)

- First bit of the destination address is 0 for ordinary addresses and 1 for group addresses.
- Group address allow multiple destinations to listen to a single address – **Multicasting**.
- Special address consisting of all 1 is reserved for **broadcasting**.
- Uniqueness of the addresses:
 - First 3 bytes are used for (**Organizationally Unique Identifier**)
 - Blocks of 2^{24} addresses are assigned to a manufacturer.
 - Manufacturer assigns the last 3 bytes of the address and programs the complete address into the NIC.



(a) Ethernet (DIX). (b) IEEE 802.3.

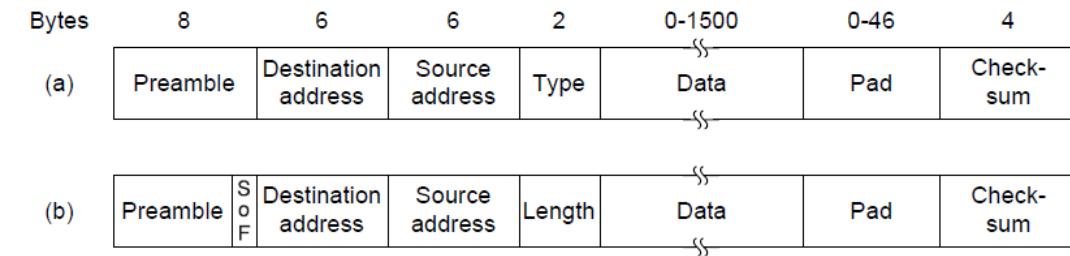
Ethernet(Cont.)

Classic Ethernet MAC Sublayer Protocol

Frame format :

➤ Type / length (2 bytes- depending on Ethernet/IEEE 802.3)

- Ethernet uses a Type field to tell the receiver what to do with the frame.
 - For example, a type code of 0x0800 means that the data contains an IPv4 packet
- Now the rule is that any number there **less than or equal to 0x600 (1536)** can be interpreted as **Length**, and any number **greater than 0x600** can be interpreted as **Type**.



(a) Ethernet (DIX). (b) IEEE 802.3.

➤ Data, Pad & Checksum

- Data field is up to 1500 bytes.
- Minimum frame length – valid frames must be at least 64 bytes long – from destination address to checksum, including both.
- If data portion is less than 46 bytes the Pad field is used to fill out the frame to the minimum size.
- Checksum field uses 32 bit CRC.

Ethernet(Cont.)

Ethernet Performance

- Performance of Ethernet can be analysed through the evaluation of **channel efficiency**.
- Assumptions :
 - k stations always ready to transmit.
 - Constant retransmission probability in each slot following to collision.
- If each station transmits during a contention slot with probability p , the probability A that some station acquires the channel :

$$A = kp(1 - p)^{k-1} \quad \text{Max } A \text{ for } p=1/k \text{ with } A \rightarrow 1/e \text{ as } k \rightarrow \infty.$$

- The probability that contention interval has exactly j slots in it is $A(1-A)^{j-1}$.
- Mean number of slots per contention is:

$$\sum_{j=0}^{\infty} jA(1 - A)^{j-1} = \frac{1}{A}$$

- Duration of each slot is 2τ , the mean contention interval $w = 2\tau/A$ (**Max $w=2\tau e$ with p optimum**)

Ethernet(Cont.)

Ethernet Performance

channel efficiency:

- If the mean frame takes P sec to transmit, when many stations have frames to send channel efficiency (E) can be expressed as

$$E = \frac{P}{P + 2\tau/A}$$

- The longer the cable the longer the contention interval; This is why the Ethernet standard specifies the maximum cable length.

- Thus, considering

- Frame length F
- Network bandwidth B
- The cable length L
- Speed of signal propagation c

For the optimal case e contention slots per frame and using $P = F/B$

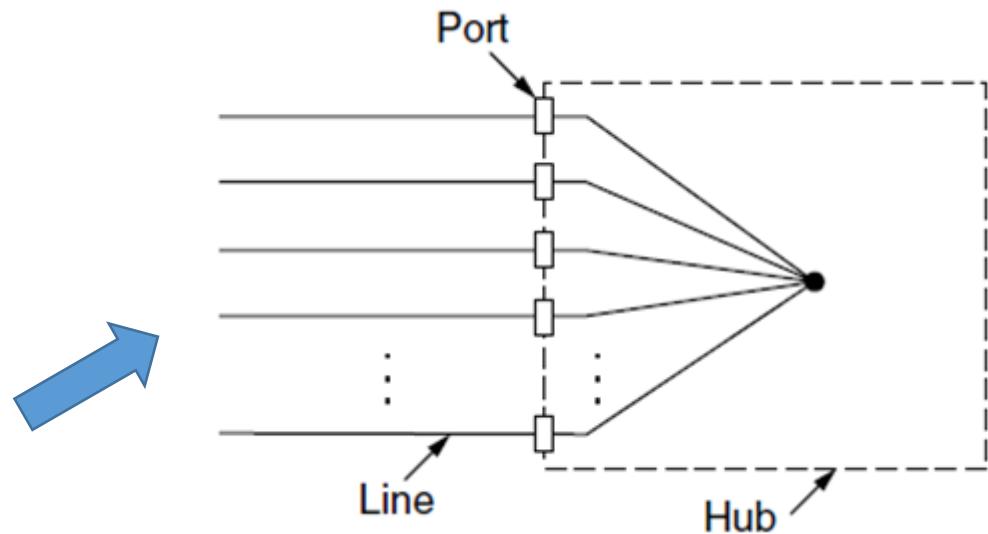
$$E = \frac{1}{1 + 2BLe/cF}$$

- When the term $2BLe/cF \gg 0$ the network efficiency becomes very low.
- Increasing BL ; Bandwidth and/or Length of the cable reduces the efficiency.
 - This is contrary to the design criteria to have largest possible bandwidth and longest connections.
 - Classic Ethernet implemented in this manner is not the best system for these applications

Ethernet(Cont.)

Switched Ethernet

- Long cable architecture of classic Ethernet often suffers from problems associated with finding breaks or loose connections.
- Replaced with a different kind of wiring pattern in which each station has a dedicated cable running to a central **hub**.
- A hub simply connects all the attached wires electrically, as if they were soldered together.
- Advantage :
 - Reuse of spare twisted pair cable.
 - Cable breaks can be detected easily.
 - Adding or removing a station is simpler.
- Limitation :
 - Maximum cable run from hub is upto 100m or **200m(high quality cat 5 cable)**
 - Do not increase capacity. As more and more stations are added, each station gets a decreasing share of the fixed capacity.



} Maintenance becomes easier

Leads to development and use of switched Ethernet

Ethernet(Cont.)

Switched Ethernet

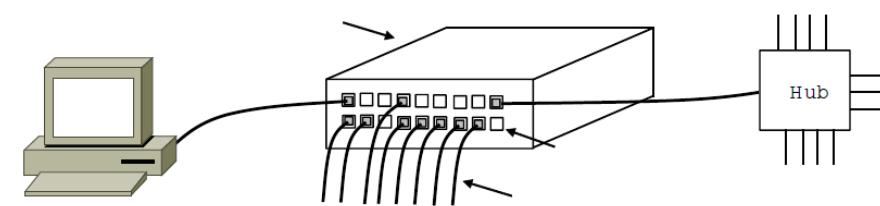
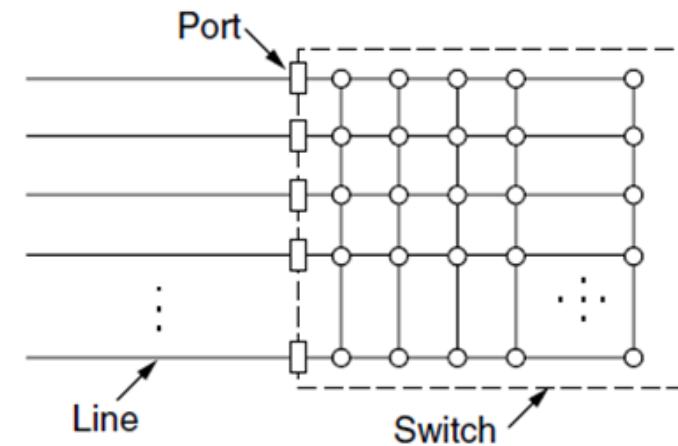
➤ Looks appropriate to handle the increased load in LAN efficiently as compared to hub.

➤ Switch :

- From outside looks like a hub typically with 4 to 48 ports each with a standard RJ-45 connector for a twisted-pair cable.
- Ports are interconnected through a high speed backplane.
- **Similarity with hub :**
 - Easy to add or remove a new station by plugging or unplugging a wire.
 - Easy to find most faults since a flaky cable or port will usually affect just one station.

➤ Operation of switch:

- After receiving data frame through a port output frames to the ports for which those frames are destined.
- The destination port then transmits the frame on the wire so that it reaches the intended station.
- None of the other ports even knows the frame exists.



Ethernet(Cont.)

Switched Ethernet

Handling collision in switch and hub

➤ Hub :

- All stations are in the same collision domain.
- Uses CSMA/CD for scheduling transmission.

➤ Switch :

- Each port has its own independent collision domain.
- Doesn't effect other port's transmission if occurs at the same time.
- Full duplex transmission possible without the use of CSMA/CD.
- Only half duplex transmission requires CSMA/CD.

Important to note :

➤ A switch **improves performance** over a hub.

- Since there are **no collisions, the capacity is used more efficiently.**
- **Multiple frames can be sent simultaneously(by different stations).**
- **Includes buffering to handle multiple frames reaching at the same output port simultaneously.**

➤ A switch also gives **security benefits** to the traffic.

- With a hub, every computer that is attached can see the traffic sent between all of the other computers.
- With a switch, traffic is forwarded only to the ports where it is destined.

Ethernet(Cont.)

Fast Ethernet

- With time it seemed that data expanded to fill the bandwidth available for their transmission.
- In Ethernet switches, the maximum bandwidth of a single computer was limited by the cable that connected it to the switch port.
- **Data rate of switched Ethernet required to increase.**
- The work was done quickly (by standards committees' norms), and the result, **802.3u**, was approved by IEEE in June 1995.
- Technically, 802.3u is not a new standard, but an addendum to the existing 802.3 standard (to emphasize its backward compatibility).
- This strategy is used a lot. Since practically everyone calls it **fast Ethernet**, rather than 802.3u.

Basic Idea :

- *Keep all the old frame formats, interfaces, and procedural rules, but reduce the bit time from 100 nsec to 10 nsec.*
- Still detect collisions on time by just reducing the maximum cable length by a factor of 10.

Ethernet(Cont.)

Fast Ethernet

Structure :

- All fast Ethernet systems use hubs and switches with a specific choice of cables as per requirement.

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps (Cat 5 UTP)
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

The original fast Ethernet cabling.

Ethernet(Cont.)

Gigabit Ethernet

After the standard for Fast Ethernet was adopted the work for yet even faster standard started:

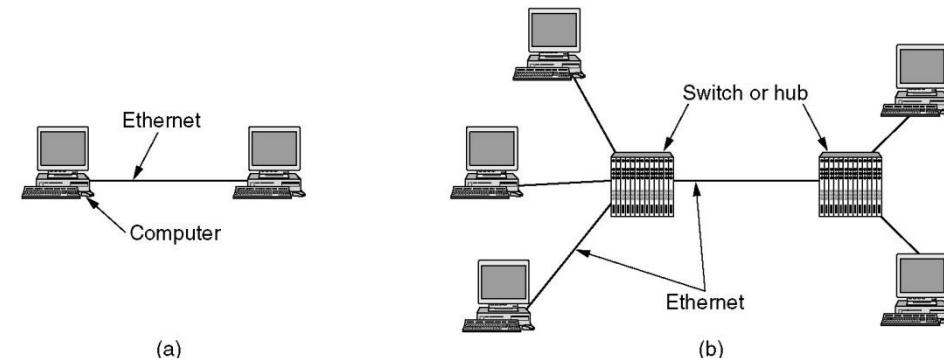
GigaBit Ethernet

➤ Goals:

- Increase performance ten fold over Fast Ethernet while maintaining compatibility with all existing Ethernet standards.
- Offer unacknowledged datagram service with both unicast and broadcast.
- Use the same 48-bit addressing scheme already in use.
- Maintain the same frame format including minimum and maximum sizes.

➤ Similar to fast Ethernet :

- Uses point to point link in all types of configuration.
- Supports both modes of operation
 - Full duplex (normal mode):- when there is a central switch connected to computers (or other switches) on the periphery.
 - Half duplex :- when the computers are connected to a hub rather than a switch.



(a) A two-station Ethernet (b) A multistation Ethernet

Ethernet(Cont.)

Gigabit Ethernet

Issue raised initially and its solution

- Suffers from length restriction to support high speed (i.e. 100 times faster than classic Ethernet).
- Length restriction seems not supportive by the users.
- **To overcome length restriction and increase maximum cable length to 200m (enough for office buildings) two noticeable features are added.**
 - ***Carrier extension :***
 - Tells the hardware to add its own padding after the normal frame to extend the frame to 512 bytes.
 - Software modification is not required since it is unaware of it.
 - ***Frame bursting :***
 - Allows a sender to transmit a concatenated sequence of multiple frames in a single transmission.
 - If the total burst is less than 512 bytes, the hardware pads it again.

Structure :

- Gigabit Ethernet supports fast Ethernet structure with a specific choice of cables as per requirement.

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

Wireless LANS

- Quite popular in the current scenario.
- Homes, offices, cafes, libraries, airports, zoos, and other public places are being outfitted with them to connect computers, PDAs, and smart phones to the Internet.
- Lets two or more nearby computers communicate without using the Internet with the help of local wireless access point.
- The main wireless LAN standard is **802.11**.
 - 802.11 architecture and protocol stack
 - 802.11 physical layer
 - 802.11 MAC sublayer protocol
 - 802.11 frame structure

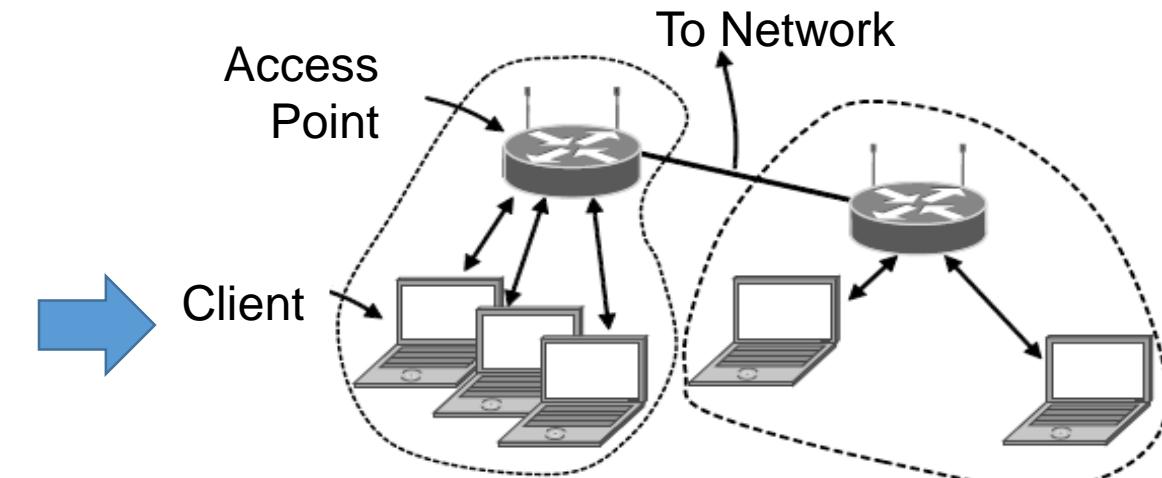
Wireless LANs(Cont.)

The 802.11 Architecture and Protocol Stack

➤ 802.11 networks can be used in two modes:

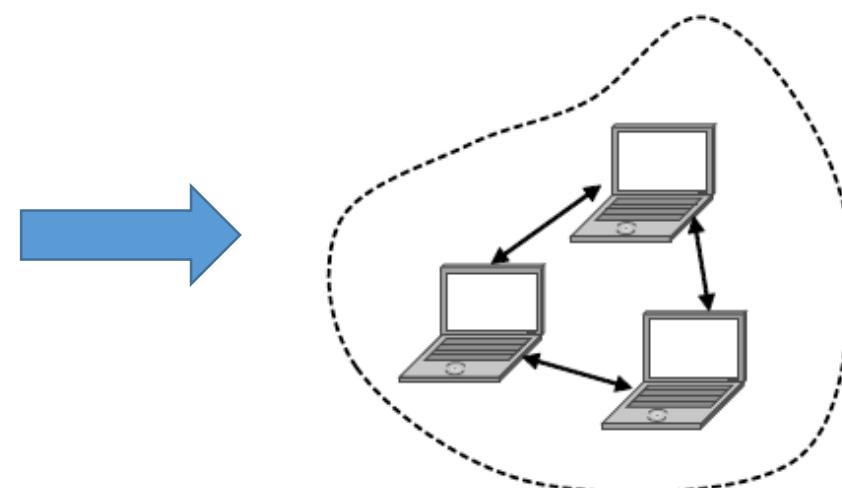
▪ Infrastructure mode

- Each client (i.e. smart phones, laptops) is associated with an **AP (Access Point)** that is in turn connected to the other network (intranet/internet).
- The client sends and receives its packets via the AP.
- Several access points may be connected, typically by a wired network called a **distribution system**, to form an extended 802.11 network.



▪ Ad-hoc mode

- In this mode a collection of computing systems are associated so that they can directly send frames to each other **without the help of an access point**.



Wireless LANS(Cont.)

The 802.11 Architecture and Protocol Stack

➤ The 802.11 protocol stack is same for clients and APs.

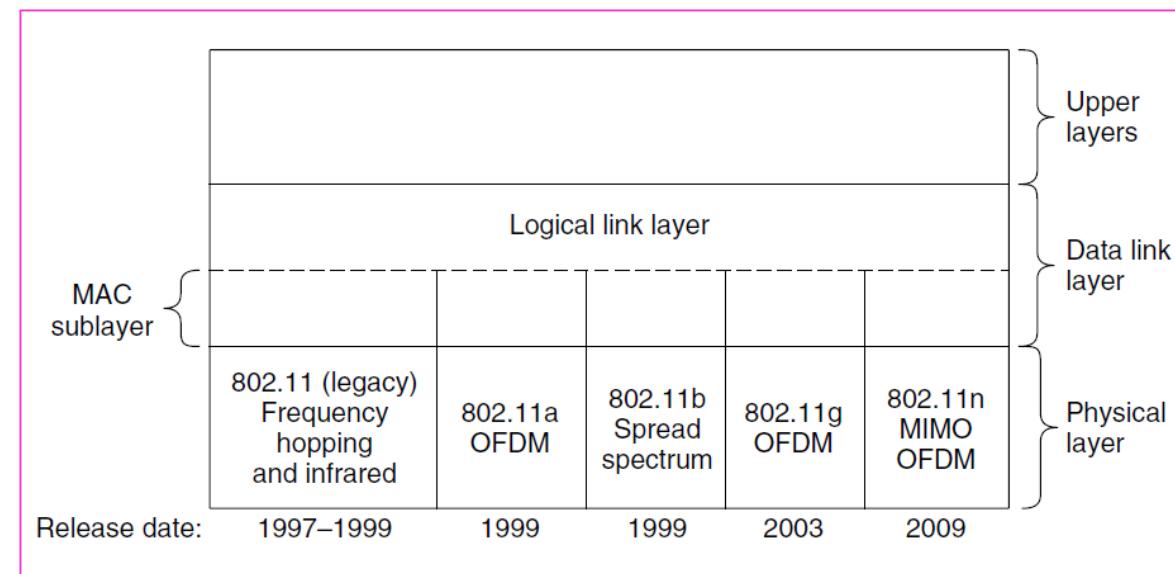
□ The **physical layer** corresponds fairly well to the OSI physical layer.

- Several transmission techniques are adopted with evolution as time grows from initial use leading to higher data rates.

(e.g. initially of 1 or 2 Mbps to currently of 54 Mbps through different techniques)

□ The **data link layer** splits into two parts.

- **MAC sub layer** does its specified job (i.e. channel allocation).
- **LLC sub layer** hides the differences between the different 802 variants and make them indistinguishable as far as the network layer is concerned.
- These days the LLC layer also identifies the protocol (e.g. IP) that is carried within an 802.11 frame.



Part of the 802.11 protocol stack

Wireless LANs(Cont.)

The 802.11 Physical Layer

- All of the 802.11 techniques use short-range radios to transmit signals in either the **2.4-GHz or the 5-GHz ISM frequency bands** license free.
- Signals may get **interfered** with the use of devices such as **microwave oven, cordless phones** and many more mostly in 2.4 GHz band.
- 5 GHz can be better for short range applications due to the higher frequency.
- All of the transmission methods also define multiple rates and uses rate adaptation based on current conditions.

(i.e. If the wireless signal is weak, a low rate can be used. If the signal is clear, the highest rate can be used)

Wireless LANS(Cont.)

The 802.11 Physical Layer

More on transmission techniques :

➤ [802.11b :](#)

- uses spread spectrum method and supports rates of 1, 2, 5.5, and 11 Mbps. (Initially 1 to 2 Mbps but later it enhanced to 11 Mbps)
- Uses **barker sequence** (since of less autocorrelation between spectrum sequences) with BPSK and QPSK modulation for lower speed (i.e. 1 and 2 Mbps respectively).
- Uses **CCK (Complementary Code Keying)** technique to construct code representing each baud as 4 bit/8 bit to enhance data rate (i.e. 5.5/11 Mbps respectively).

➤ [802.11a :](#)

- Supports rates up to 54 Mbps in the 5-GHz ISM band.
- Uses OFDM technique with 52 subcarriers (i.e. 48 against data and 4 against synchronization) for transmission.
- Bits undergoes binary convolutional coding for error correction.
- Can run at eight different rates, ranging from 6 to 54 Mbps.

➤ [802.11g :](#)

- Comes after the lifting of rule in U.S. (i.e. 2.4 GHz ISM band transmission can't use techniques other than spread spectrum) in 2002 and **approved by IEEE in 2003**.
- Copies the OFDM modulation methods of [802.11a](#) but operates in the narrow 2.4-GHz ISM band along with [802.11b](#).

➤ [802.11n :](#)

- Ratified in **2009** and employs **MIMO (Multiple Input Multiple Output)** communication technique.
- Uses up to four antennas to transmit up to four streams of information at the same time and separated at the receiver through multiple antennas.

Wireless LANs(Cont.)

The 802.11 MAC Sublayer Protocol

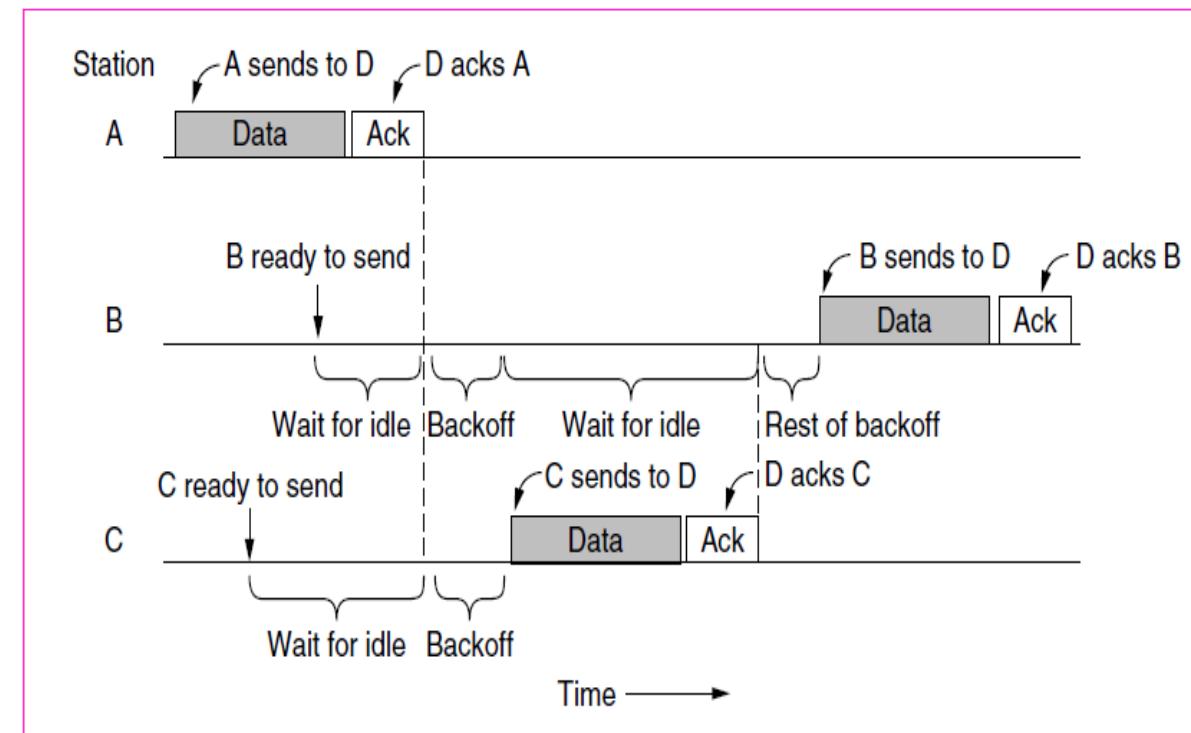
- 802.11 tries to avoid collisions with a protocol called **CSMA/CA (CSMA with Collision Avoidance)**.
- **CSMA/CA** conceptually same as CSMA/CD meant for Ethernet as far as a station wants to transmit (i.e. channel sensing before sending and exponential back off to avoid collisions).
 - A station that has a frame to send, starts with a random backoff (except in the case that it has not used the channel recently and the channel is idle).
 - The station waits until the channel is idle, by sensing that there is no signal for a short period of time and counts down idle slots, pausing when frames are sent.
 - It sends its frame when the counter reaches 0. If the frame gets through, the destination immediately sends a short acknowledgement.
 - Lack of an acknowledgement is inferred to indicate an error, whether a collision or otherwise.
 - In this case, the sender doubles the backoff period and tries again, continuing with exponential backoff as in Ethernet until the frame has been successfully transmitted or the maximum number of retransmissions has been reached.

Wireless LANs(Cont.)

The 802.11 MAC Sublayer Protocol

Example:

- Station A is the first to send a frame.
- While A is sending, stations B and C become ready to send.
- They see that the channel is busy and wait for it to become idle.
- Shortly after A receives an acknowledgement, the channel goes idle.
- However, rather than sending a frame right away and colliding, B and C both perform a back off.
- C picks a short back off, and thus sends first.
- B pauses its countdown while it senses that C is using the channel, and resumes after C has received an acknowledgement.
- B soon completes its back off and sends its frame.



Sending a frame with CSMA/CA.

Wireless LANs(Cont.)

The 802.11 MAC Sublayer Protocol

Difference from Ethernet :

- Starting backoffs early helps to avoid collisions.
 - Avoidance is worthwhile because collisions are expensive, as the entire frame is transmitted even if one occurs.
- Acknowledgements are used to infer collisions because collisions cannot be detected.

Mode of operation:

- **DCF (Distributed Coordination Function) :**
 - Each station acts independently, without any kind of central control.
- **PCF (Point Coordination Function) :**
 - The access point controls all activity in its cell, just like a cellular base station.

Wireless LANs(Cont.)

The 802.11 MAC Sublayer Protocol

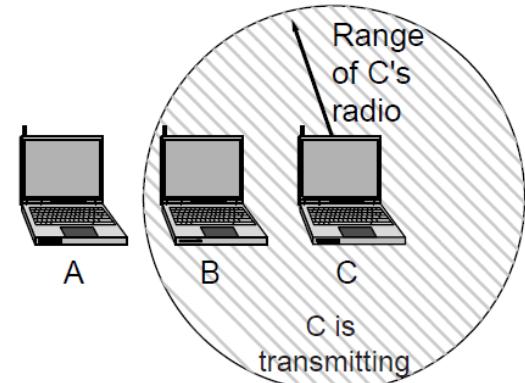
Handling the hidden & exposed node problem :

- Source : Incapability of channel sensing due to limited Transmission range
- To reduce ambiguities about which station is sending, 802.11 defines channel sensing to consist of both **physical sensing** and **virtual sensing**.
- **Physical sensing** : Simply checks the medium to see if there is a valid signal.
- **Virtual sensing** : Each station keeps a logical record of when the channel is in use by tracking the **NAV (Network Allocation Vector)**.

- **NAV :**

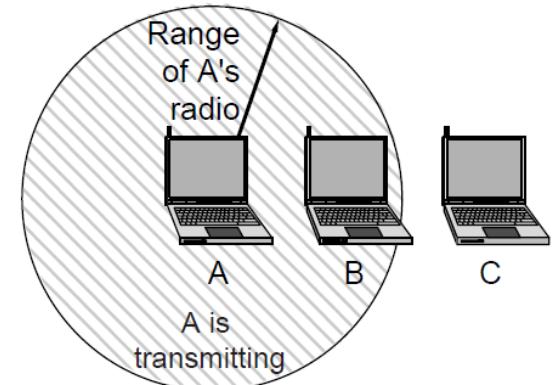
- Each frame carries a NAV field that says how long the sequence of which this frame is part will take to complete.
- Stations that overhear this frame know that the channel will be busy for the period indicated by the NAV, regardless of whether they can sense a physical signal.
- *For example, the NAV of a data frame includes the time needed to send an acknowledgement. All stations that hear the data frame will defer during the acknowledgement period, whether or not they can hear the acknowledgement.*

A wants to send to B
but cannot hear that
B is busy



The hidden terminal problem

B wants to send to C
but mistakenly thinks
the transmission will fail



The exposed terminal problem

Wireless LANs(Cont.)

The 802.11 MAC Sublayer Protocol

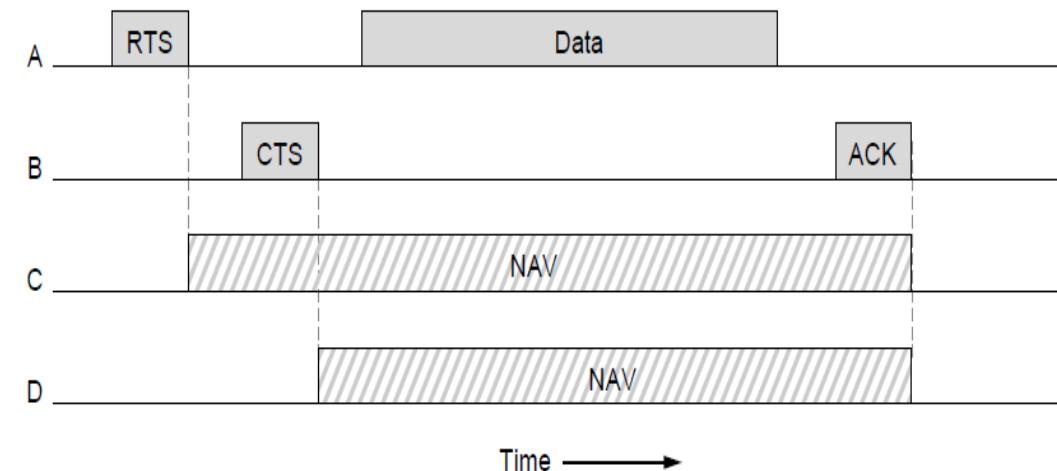
- An optional RTS/CTS mechanism uses the NAV to prevent terminals from sending frames at the same time as hidden terminals.

Example: Transmission of data from A to B

Assumptions : (i) C is within range of A (and possibly within range of B) (ii) D is a station within range of B but not within range of A.

Protocol operation :

1. A begins by sending a RTS frame to B.
2. Upon receipt of RTS, B answers A with a CTS frame.
3. Upon receipt of CTS, A sends its frame and starts an ACK timer.
4. Upon correct receipt of the data frame, B sends an ACK frame.
5. If A's ACK timer expires before the ACK gets back to it, it is treated as a collision and the whole protocol is run again after a backoff.



Virtual channel sensing using CSMA/CA

Role of NAV :

- C is within range of A, so it may receive the RTS frame.
- From the information provided in the RTS request, it can estimate how long the sequence will take, including the final ACK and so it desists from transmitting anything until the exchange is completed.
- It does so by updating its record of the NAV to indicate that the channel is busy.
- D does not hear the RTS, but it does hear the CTS since within range of B and so it also updates its NAV.

Wireless LANs(Cont.)

The 802.11 MAC Sublayer Protocol

- Depending on needs of real operation several other mechanisms are included.

1. Reliability :

- In contrast to wired networks, wireless networks are noisy and unreliable due to interference from other devices in ISM band.
- Use of acknowledgements and retransmissions is of little help if the probability of getting a frame through is small.

Possible strategies to improve successful transmission :

- Lower the transmission rate -- If too many frames are lost, a station can lower the rate.
- Send shorter frames -- If the probability of any bit being in error is p , the probability of an n -bit frame being received entirely correctly is $(1 - p)^n$.

Ex : Assume $p = 10^{-4}$

- If the frame length is of 12,144 bits, then probability of receiving a full Ethernet frame correctly is less than 30%.
- if the frames are only a third as long (4048 bits) two thirds of them will be received correctly.

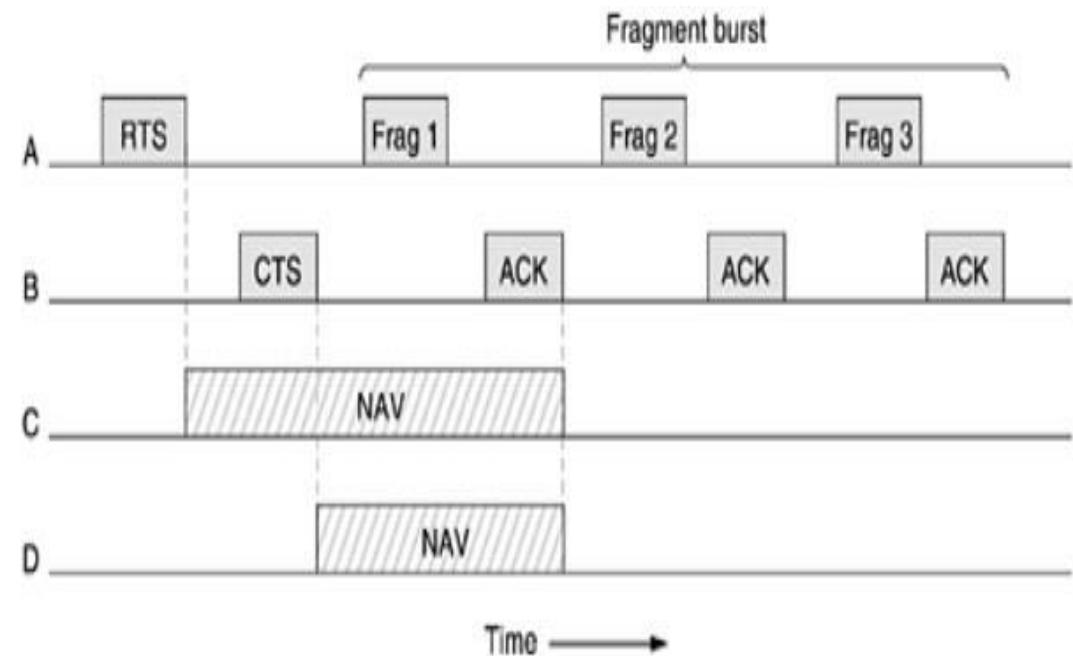
- In summary, *if a frame is too long, it has very little chance of getting through undamaged and will probably have to be retransmitted.*

Wireless LANs(Cont.)

The 802.11 MAC Sublayer Protocol

Fragment burst :

- To deal with the problem of noisy channels, 802.11 allows frames to be fragmented into smaller pieces, called **fragments**, each with its own checksum.
- The fragments are individually numbered and acknowledged using a stop-and-wait protocol (i.e., the sender may not transmit fragment $k + 1$ until it has received the acknowledgement for fragment k).
- Once the channel has been acquired using RTS and CTS, multiple fragments can be sent in a row, as shown in Fig. sequence of fragments is called a **fragment burst**.
- The NAV mechanism keeps other stations quiet only until the next acknowledgement.
- Fragmentation **increases the throughput** by restricting retransmissions to the bad fragments rather than the entire frame.
- All of the above discussion applies to the 802.11 **DCF** mode.



Wireless LANS(Cont.)

The 802.11 MAC Sublayer Protocol

2. Power saving :

- Battery life is always an issue with mobile wireless devices.
- To deal with this issue 802.11 supports power management while operating in **PCF mode**.
- Goal : Clients need not waste power when they have neither information to send nor to receive.
- Basic mechanism : Use of **beacon frame** and **polling** by AP.
- Beacons are periodically broadcasted by the AP (e.g. every 100 or 1000msec) indicating its presence.
- Also contains system parameters and the time, how long until the next beacon.
- Besides, AP also does polling from clients to know whether it has the data to transmit/receive.
- If client has data to transmit then responds to poll and transmit to AP following which goes to sleep mode.
- Receive Process :
 - Clients can intimate AP when it enters to **power-save mode**.
 - In this mode, the client can doze and the AP will buffer traffic intended for it.
 - To check for incoming traffic, the client wakes up for every beacon, and checks a traffic map that is sent as part of the beacon.
 - This map tells the client if there is buffered traffic for it.
 - If so, the client sends a poll message to the AP, which then sends the buffered traffic.
 - The client can then go back to sleep until the next beacon is sent.

Wireless LANs(Cont.)

The 802.11 MAC Sublayer Protocol

3. Quality of service:

- Applications such as VoIP takes the attention of 802.11 to focus on quality of service by giving different priority to different traffics.
- 802.11 supports coexistence of DCF and PCF for such kind of need.
- Works by extending CSMA/CA with carefully defined intervals between frames.
- After a frame has been sent, a certain amount of idle time is required before any station may send a frame.
- Different time intervals are defined for different kinds of frames.
 - **DIFS (DCF Inter Frame Spacing) : Meant for regular DCF data frames**
 - **SIFS (Short Inter Frame Spacing) : Meant for short frames such as RTS, CTS, fragments.**
 - **AIFS (Arbitration Inter Frame Spacing) : Meant for different priority frames**
 - **EIFS (Extended Inter Frame Spacing) : Meant for unknown/bad frame**

Wireless LANs(Cont.)

The 802.11 MAC Sublayer Protocol

More on inter frame spacing:

➤ **DIFS (DCF Inter Frame Spacing) :**

- Interval between regular data frame.
- Any station may attempt to acquire the channel to send a new data frame after the medium has been idle for DIFS.

➤ **SIFS (Short Inter Frame Spacing) :**

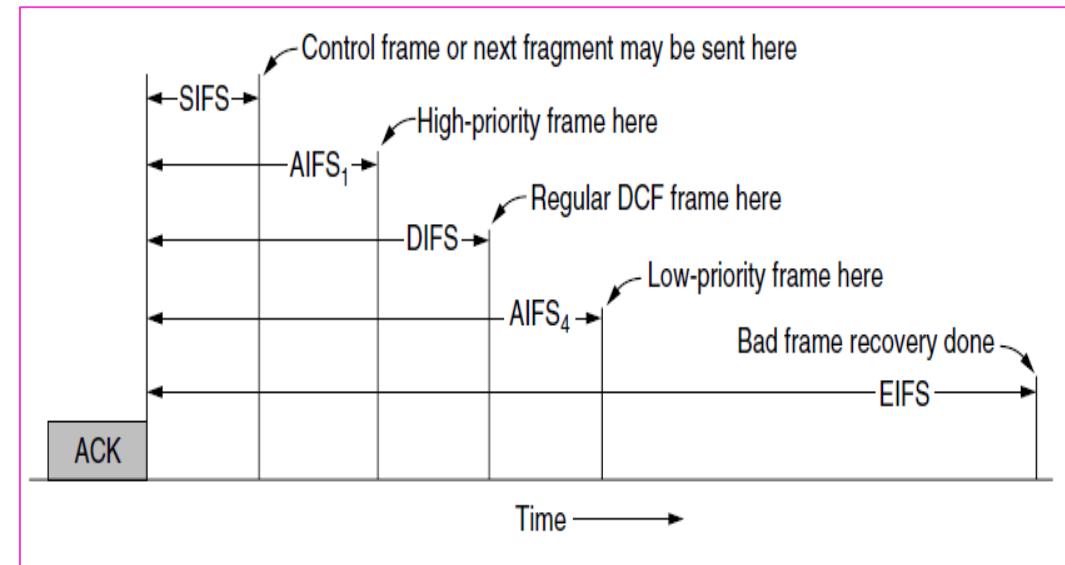
- The shortest interval among all.
- Allows the parties in a single dialog the chance to go first.
- Examples : ACK, RTS, CTS, Fragments

➤ **AIFS (Arbitration Inter Frame Spacing) :**

- Used by AP for sending priority based traffic.
- EX :
 - AIFS₁: AP will wait for a shorter interval before it sends the voice traffic, and thus send it before regular traffic.
 - AIFS₄: AP will wait for a longer interval before it sends regular traffic the opportunity to transmit first.

➤ **EIFS (Extended Inter Frame Spacing) :**

- Used only by a station that has just received a bad or unknown frame, to report the problem.



Inter frame spacing in 802.11

Wireless LANs(Cont.)

The 802.11 Frame Structure

► 802.11 standard defines three different classes of frames in the air: **data**, **control**, and **management**.

Data frame :

Frame control : Size **2 bytes** and made up of **11 subfields**

- *Protocol version* : Set to '**00**' - allow two versions of 802.11 protocol to operate at the same time in the same cell.
- *Type* : Indicates (data, control, management)
- *Subtype* : (e.g. RTS or CTS).
- *To DS and From DS* : '**1**' - Indicate whether the frame is going to or coming from the network using APs (i.e. distribution system)
- *More fragments* : '**1**' – Means more fragments will follow after it
- *Retry* : '**1**' - Retransmission of a frame sent earlier
- *Power management* : '**1**' - Sender is going into power-save mode
- *More data* : '**1**' – More data frames to come for receiver
- *Protected* : '**1**' – Encrypted frame body
- *Order* : '**1**' – Higher layer to expect frame to arrive in sequence

Bytes	2	2	6	6	6	2	0-2312	4
Frame control	Duration	Address 1 (recipient)	Address 2 (transmitter)	Address 3	Sequence	Data	Check sequence	
Version = 00	Type = 10	Subtype = 0000	To DS	From DS	More frag.	Retry	Pwr. mgt.	More data

Bits 2 2 4 1 1 1 1 1 1 1

Format of the 802.11 data frame

Wireless LANs(Cont.)

The 802.11 Frame Structure

Data frame :

➤ Duration :

- Tells how long the frame and its acknowledgement will occupy the channel(in microseconds).
- *Present in other frames (i.e. control and management)*
 - *In management indicates the NAV.*

➤ Address :

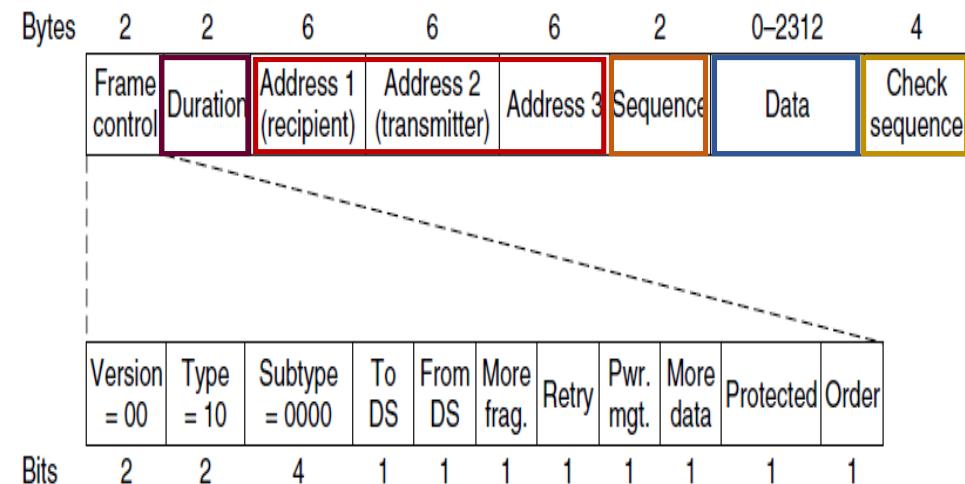
- *Data frames involving AP uses all 3 fields.*
- *1st address – Receiver (AP /station)*
- *2nd address – Sender (AP/station)*
- *3rd address – Distant point/station for which AP acts as relay.*

➤ Sequence :

- A number associated with frames to check duplicity.
- Of the 16 bits available
 - *4 identify the fragment*
 - *12 carry a number that is advanced with each new transmission*

➤ Data : Contains the payload, up to **2312 bytes**.

➤ Check sequence : 32-bit CRC



Format of the 802.11 data frame

Wireless LANs(Cont.)

The 802.11 Frame Structure

Control frame :

- Short in size.
- Contains the *Frame control, Duration, and Frame check sequence fields*.
- May have only *one address and no data portion*.
- Most of the key information is conveyed with the *Subtype field* (e.g., ACK, RTS and CTS).

Management frame :

- Similar to that of data frames, except without one of the base station addresses, because management frames are restricted to a single cell.

Wireless LANS(Cont.)

Data Link Layer Switching

- Many organizations have multiple LANs and wish to connect them.
- Requires the use of **Repeaters, Hubs, Bridges, Switches, Routers, and Gateways**

Possible reasons why a single organization may end up with multiple LANs.

- **First**, many university and corporate departments have their own LANs, primarily to connect their own personal computers, workstations, and servers. Since the *goals of the various departments differ, different departments choose different LANs, without regard to what other departments are doing.*
- **Second**, the organization may be *geographically spread over several buildings* separated by considerable distances.
- **Third**, it may be necessary to split what is logically a single LAN into separate LANs to *accommodate the load*.
- **Fourth**, in some situations, a single LAN would be adequate in terms of the load, but the *physical distance* between the most distant machines is too great (e.g., more than 2.5 km for Ethernet).
- **Fifth**, there is the matter of *reliability*. On a single LAN, a defective node that keeps outputting a continuous stream of garbage can cripple the LAN.
- **Sixth**, bridges can contribute to the organization's *security*. Most LAN interfaces have a promiscuous mode, in which all frames are given to the computer, not just those addressed to it. Spies and busybodies love this feature.

Wireless LANs(Cont.)

Data Link Layer Switching

Repeaters, Hubs, Bridges, Switches, Routers, and Gateways :

- All of these devices are in common use.
- Operate in different layers. Why? 

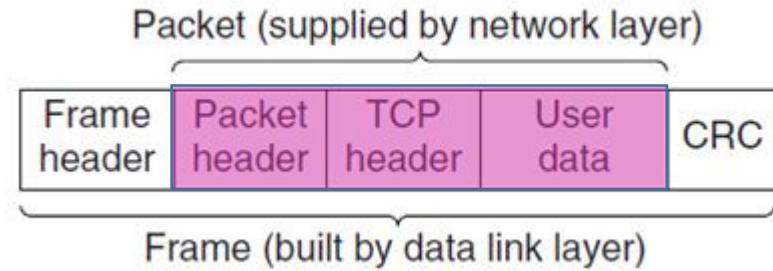
- Different devices use different pieces of information to decide how to switch.

A typical scenario :

- The user generates some data to be sent to a remote machine.
- Those data are passed to the transport layer, which then adds a header (for example, a TCP header) and passes the resulting unit down to the network layer. The network layer adds its own header to form a network layer packet (e.g., an IP packet).
- Then the packet goes to the data link layer, which adds its own header and checksum (CRC) and gives the resulting frame to the physical layer for transmission, for example, over a LAN.

Application layer	Application gateway
Transport layer	Transport gateway
Network layer	Router
Data link layer	Bridge, switch
Physical layer	Repeater, hub

Which device is in which layer



Frames, packets, and headers

Wireless LANs(Cont.)

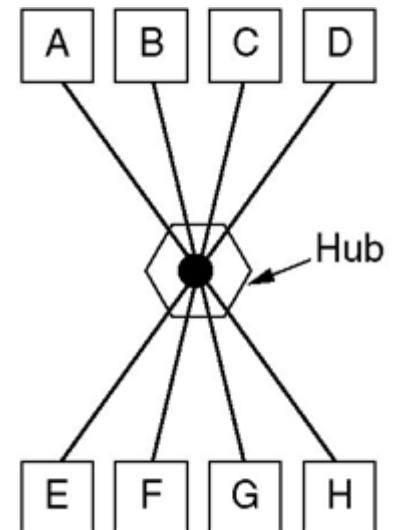
Data Link Layer Switching

Repeaters

- These are **analog devices** that work with signals on the cables to which they are connected.
- A signal appearing on one cable is cleaned up, amplified, and put out on another cable.
- Repeaters **do not understand frames, packets, or headers**.
- They **understand the symbols that encode bits as volts**.
- Example :
 - In classic Ethernet four repeaters are used for boosting the signal to extend the maximum cable length from 500 meters to 2500 meters.

Hubs

- A hub has *several input lines that it joins electrically*.
- Frames arriving on any of the lines are sent out on all the others.
 - **If two frames arrive at the same time, they will collide.**
- All the lines coming into a hub must operate at the same speed.
- Differ from repeaters in that they **do not** (usually) amplify the incoming **signals** and are designed for multiple input lines.
- Like repeaters, hubs are physical layer devices that do not examine the link layer addresses or use them in any way.

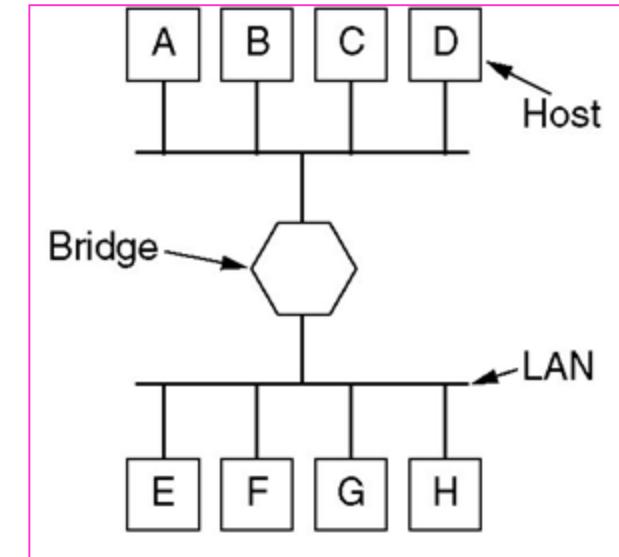


Wireless LANs(Cont.)

Data Link Layer Switching

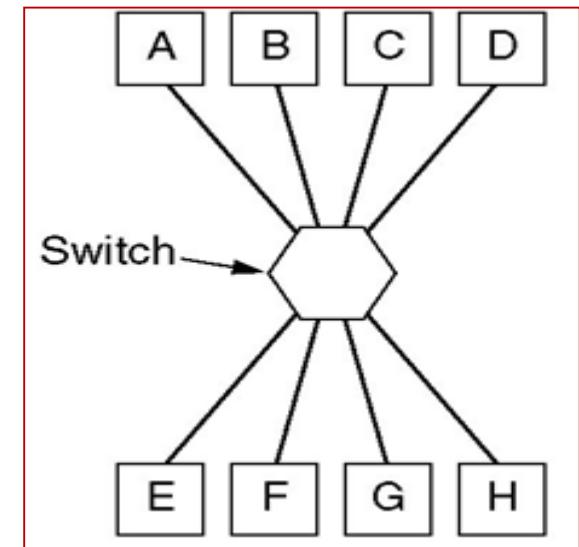
Bridge

- Connects two or more LANs.
- When a frame arrives, the bridge *extracts the destination address* from the frame header and looks it up in a table to see where to send the frame.
- The bridge only outputs the frame on the port where it is needed and can forward multiple frames at the same time.
- It also offer the input lines may run at different speeds, possibly even with different network types using a buffer.
- Limitation -- Used for connection between same kind of LAN.



Switches

- Switches are modern bridges by another name with more ports.
- Most often used to connect individual computers.



Wireless LANs(Cont.)

Data Link Layer Switching

Router

- When a packet comes into a router, the **frame header and trailer are stripped off** and *the packet located in the frame's payload field is passed to the routing software.*
- This software uses the *packet header to choose an output line.*
- For an IP packet, the packet header will contain a 32-bit (IPv4) or 128-bit (IPv6) address.
- Used for connection between different kinds of LAN.

Transport gateways

- These *connect* two computers that use *different connection-oriented transport protocols.*
- For example, suppose a computer using the connection-oriented TCP/IP protocol needs to talk to a computer using a different connection-oriented transport protocol called SCTP.
- The transport gateway can copy the packets from one connection to the other, *reformatting* them as need be.

Application gateways

- It understand the format and contents of the data and can translate messages from one format to another.
 - An email gateway could translate Internet messages into SMS messages for mobile phones.

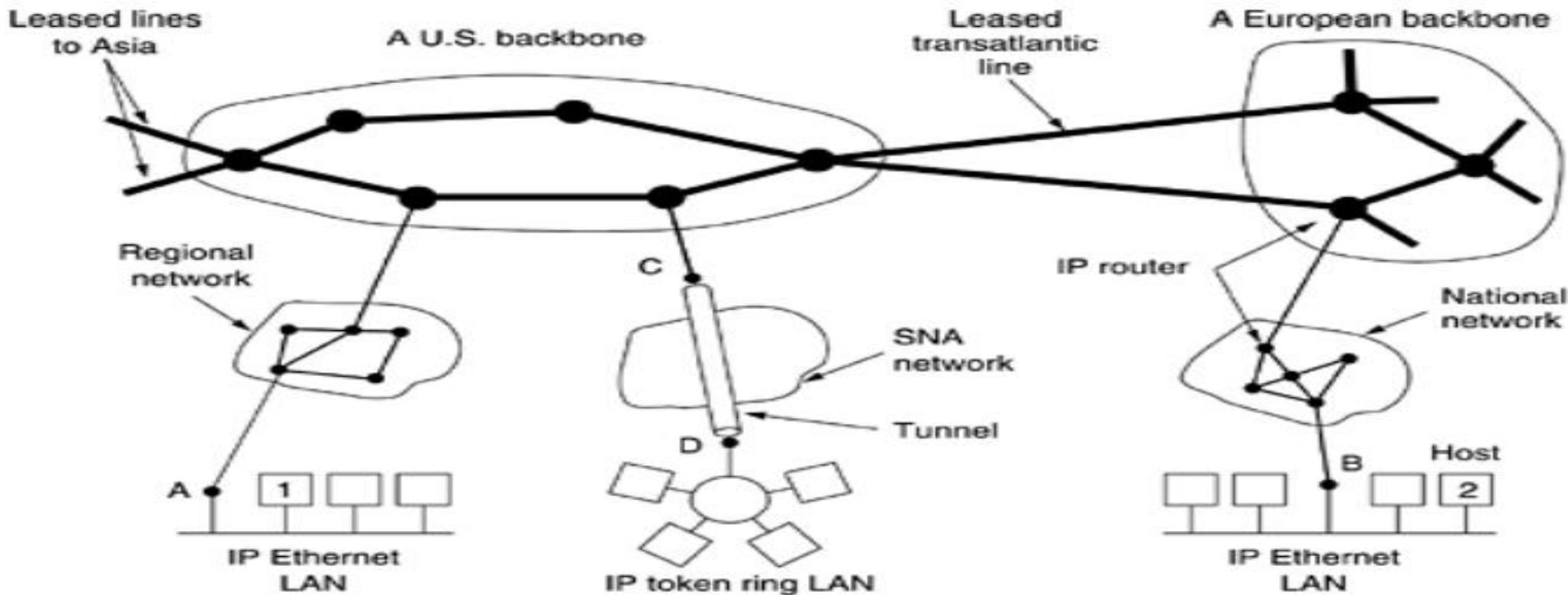
The Network Layer in the Internet(CH-5)

- 10 Basic principles behind the network layer in the internet

1. **Make sure it works.** Do not finalize the design or standard until multiple prototypes have successfully communicated with each other. All too often designers first write a 327 1000-page standard, get it approved, then discover it is deeply flawed and does not work. Then they write version 1.1 of the standard. This is not the way to go.
2. **Keep it simple.** When in doubt, use the simplest solution. William of Occam stated this principle (Occam's razor) in the 14th century. Put in modern terms: fight features. If a feature is not absolutely essential, leave it out, especially if the same effect can be achieved by combining other features.
3. **Make clear choices.** If there are several ways of doing the same thing, choose one. Having two or more ways to do the same thing is looking for trouble. Standards often have multiple options or modes or parameters because several powerful parties insist that their way is best. Designers should strongly resist this tendency. Just say no.
4. **Exploit modularity.** This principle leads directly to the idea of having protocol stacks, each of whose layers is independent of all the other ones. In this way, if circumstances that require one module or layer to be changed, the other ones will not be affected.

- 5. **Expect heterogeneity.** Different types of hardware, transmission facilities, and applications will occur on any large network. To handle them, the network design must be simple, general, and flexible.
- 6. **Avoid static options and parameters.** If parameters are unavoidable (e.g., maximum packet size), it is best to have the sender and receiver negotiate a value than defining fixed choices.
- 7. **Look for a good design; it need not be perfect.** Often the designers have a good design but it cannot handle some weird special case. Rather than messing up the design, the designers should go with the good design and put the burden of working around it on the people with the strange requirements.
- 8. **Be strict when sending and tolerant when receiving.** In other words, only send packets that rigorously comply with the standards, but expect incoming packets that may not be fully conformant and try to deal with them.
- 9. **Think about scalability.** If the system is to handle millions of hosts and billions of users effectively, no centralized databases of any kind are tolerable and load must be spread as evenly as possible over the available resources.
- 10. **Consider performance and cost.** If a network has poor performance or outrageous costs, nobody will use it.

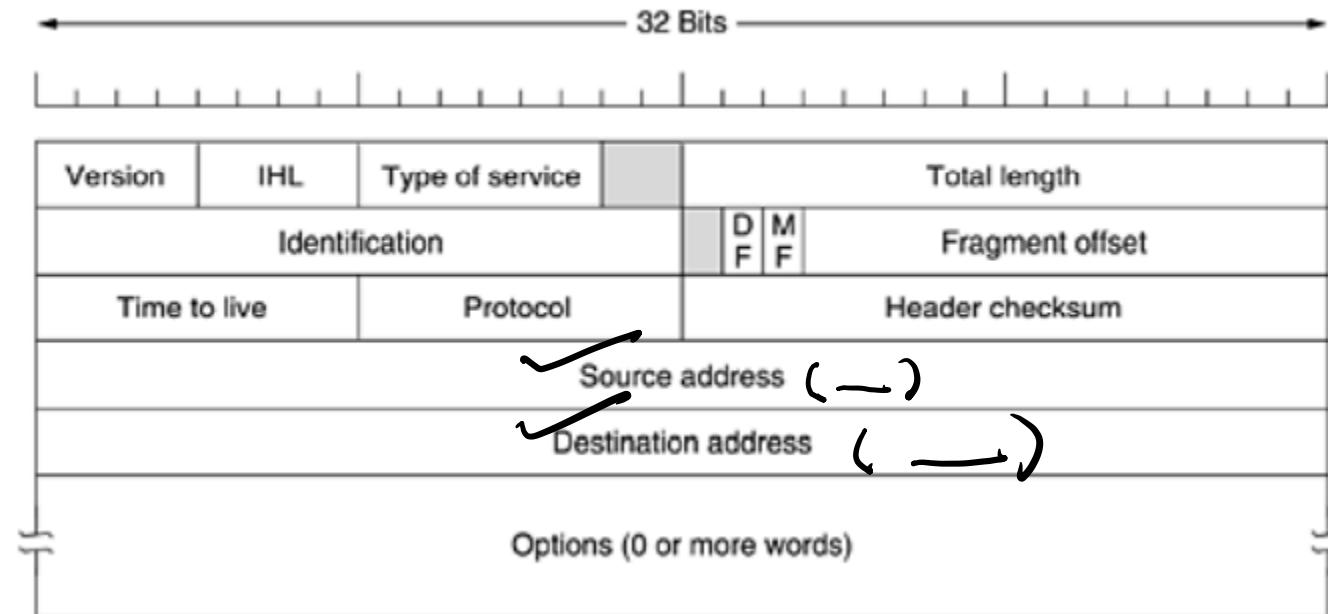
The Internet is an interconnected collection of many networks.



- The job of the network layer protocols is to provide a best-efforts (i.e., not guaranteed) way to transport datagrams from source to destination, without regard to whether these machines are on the same network or whether there are other networks in between them.
- Communication in the Internet works as follows.
 1. The transport layer takes data streams and breaks them up into datagrams. In theory, datagrams can be up to 64 Kbytes each, but in practice they are usually not more than 1500 bytes (so they fit in one Ethernet frame).
 2. Each datagram is transmitted through the Internet, possibly being fragmented into smaller units as it goes.
 3. When all the pieces finally get to the destination machine, they are reassembled by the network layer into the original datagram.
 4. This datagram is then handed to the transport layer, which inserts it into the receiving process' input stream.

The IP Protocol

The IPv4 (Internet Protocol) header.



- An IP datagram consists of a header part and a text part.
- The header has a 20-byte fixed part and a variable length optional part.
- It is transmitted in big-endian order: from left to right, with the high-order bit of the Version field going first. (The SPARC is big endian; the Pentium is little-endian.) On little endian machines, software conversion is required on both transmission and reception.
- **Version** field keeps track of which version of the protocol the datagram belongs to. Currently a transition between IPv4 and IPv6 is going on.
- Since the header length is not constant, a field in the header, **IHL**, is provided to tell how long the header is, in 32-bit words. The minimum value is 5, which applies when no options are present. The maximum value of this 4-bit field is 15, which limits the header to 60 bytes, and thus the **Options** field to 40 bytes. For some options, such as one that records the route a packet has taken, 40 bytes is far too small, making that option useless.

- The **Type of service** field is one of the few fields that has changed its meaning (slightly) over the years. It was and is still intended to distinguish between different classes of service. Various combinations of reliability and speed are possible. For digitized voice, fast delivery beats accurate delivery. For file transfer, error-free transmission is more important than fast transmission.
- the 6-bit field contained (from left to right), a three-bit Precedence field and three flags, D, T, and R. The Precedence field was a priority, from 0 (normal) to 7 (network control packet). The three flag bits allowed the host to specify what it cared most about from the set {Delay, Throughput, Reliability}. In theory, these fields allow routers to make choices between, for example, a satellite link with high throughput and high delay or a leased line with low throughput and low delay. In practice, current routers often ignore the Type of service field altogether.
- The Total length includes everything in the datagram—both header and data. The maximum length is 65,535 bytes. At present, this upper limit is tolerable, but with future gigabit networks, larger datagrams may be needed. The Identification field is needed to allow the destination host to determine which datagram a newly arrived fragment belongs to. All the fragments of a datagram contain the same Identification value.

- DF stands for Don't Fragment. It is an order to the routers not to fragment the datagram because the destination is incapable of putting the pieces back together again. By marking the datagram with the DF bit, the sender knows it will arrive in one piece, even if this means that the datagram must avoid a small-packet network on the best path and take a suboptimal route. All machines are required to accept fragments of 576 bytes or less.
- MF stands for More Fragments. All fragments except the last one have this bit set. It is needed to know when all fragments of a datagram have arrived.
- The Fragment offset tells where in the current datagram this fragment belongs. All fragments except the last one in a datagram must be a multiple of 8 bytes, the elementary fragment unit. Since 13 bits are provided, there is a maximum of 8192 fragments per datagram, giving a maximum datagram length of 65,536 bytes, one more than the Total length field.
- The Time to live field is a counter used to limit packet lifetimes. It is supposed to count time in seconds, allowing a maximum lifetime of 255 sec. It must be decremented on each hop and is supposed to be decremented multiple times when queued for a long time in a router. In practice, it just counts hops. When it hits zero, the packet is discarded and a warning packet is sent back to the source host. This feature prevents datagrams from wandering around forever, something that otherwise might happen if the routing tables ever become corrupted.

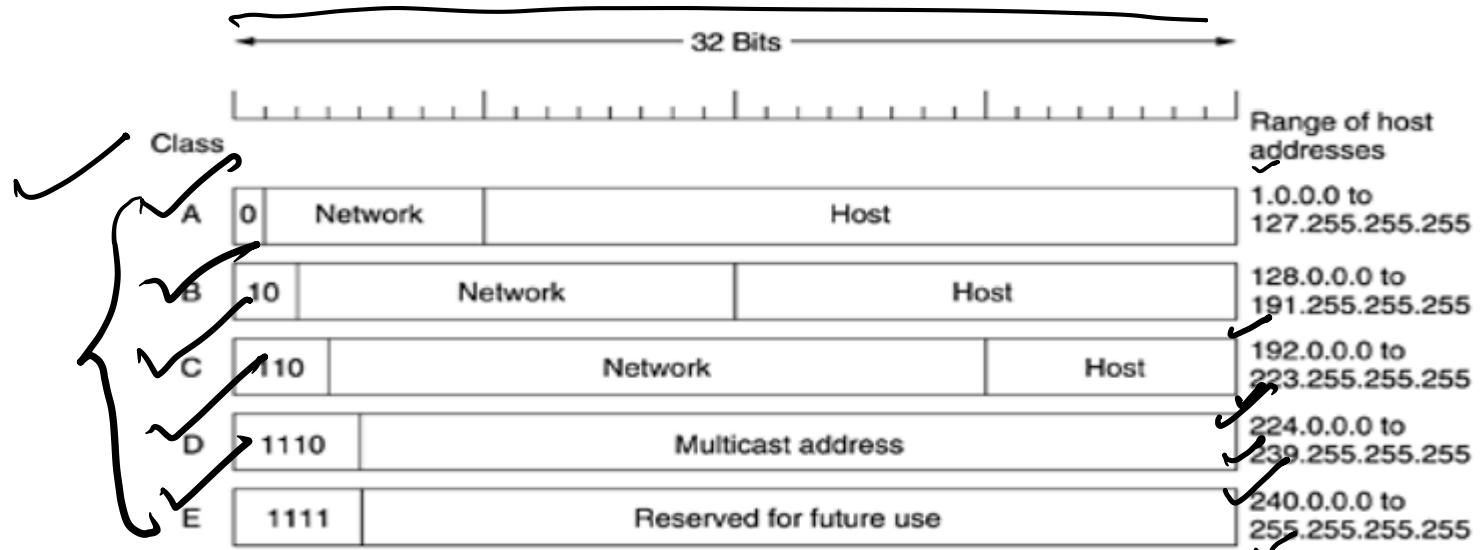
- When the network layer has assembled a complete datagram, it needs to know what to do with it. The **Protocol field** tells it which transport process to give it to. TCP is one possibility, but so are UDP and some others. The numbering of protocols is global across the entire Internet. Protocols and other assigned numbers were formerly listed in RFC 1700, but nowadays they are contained in an on-line data base located at www.iana.org.
- The **Header checksum** verifies the header only. Such a checksum is useful for detecting errors generated by bad memory words inside a router. The algorithm is to add up all the 16-bit half words as they arrive, using one's complement arithmetic and then take the one's complement of the result. For purposes of this algorithm, the Header checksum is assumed to be zero upon arrival. This algorithm is more robust than using a normal add. Note that the Header checksum must be recomputed at each hop because at least one field always changes (the Time to live field), but tricks can be used to speed up the computation.
- The **Source address and Destination address** indicate the network number and host number. We will discuss Internet addresses in the next section. The Options field was designed to provide an escape to allow subsequent versions of the protocol to include information not present in the original design, to permit experimenters to try out new ideas, and to avoid allocating header bits to information that is rarely needed. The options are variable length. Each begins with a 1-byte code identifying the option. Some options are followed by a 1-byte option length field, and then one or more data bytes. The Options field is padded out to a multiple of four bytes.

- The Security option tells how secret the information is. In theory, a military router might use this field to specify not to route through certain countries the military considers to be "bad guys." In practice, all routers ignore it, so its only practical function is to help spies find the good stuff more easily.
- The Strict source routing option gives the complete path from source to destination as a sequence of IP addresses. The datagram is required to follow that exact route. It is most useful for system managers to send emergency packets when the routing tables are corrupted, or for making timing measurements.
- The Loose source routing option requires the packet to traverse the list of routers specified, and in the order specified, but it is allowed to pass through other routers on the way.
- The Record route option tells the routers along the path to append their IP address to the option field. This allows system managers to track down bugs in the routing algorithms.
- The Timestamp option is like the Record route option, except that in addition to recording its 32-bit IP address, each router also records a 32-bit timestamp. This option, too, is mostly for debugging routing algorithms.

IP Addresses

27.12.25.47 → IP address

- Every host and router on the Internet has an IP address, which encodes its network number and host number.
- The combination is unique: in principle, no two machines on the Internet have the same IP address. All IP addresses are 32 bits long and are used in the Source address and Destination address fields of IP packets.
- It is important to note that an IP address does not actually refer to a host. It really refers to a network interface, so if a host is on two networks, it must have two IP addresses. However, in practice, most hosts are on one network and thus have one IP address.
- For several decades, IP addresses were divided into the five categories. This allocation has come to be called classful addressing



1.

The class A, B, C, and D formats allow for up to 128 networks with 16 million hosts each, 16,384 networks with up to 64K hosts, and 2 million networks (e.g., LANs) with up to 256 hosts each (although a few of these are special).

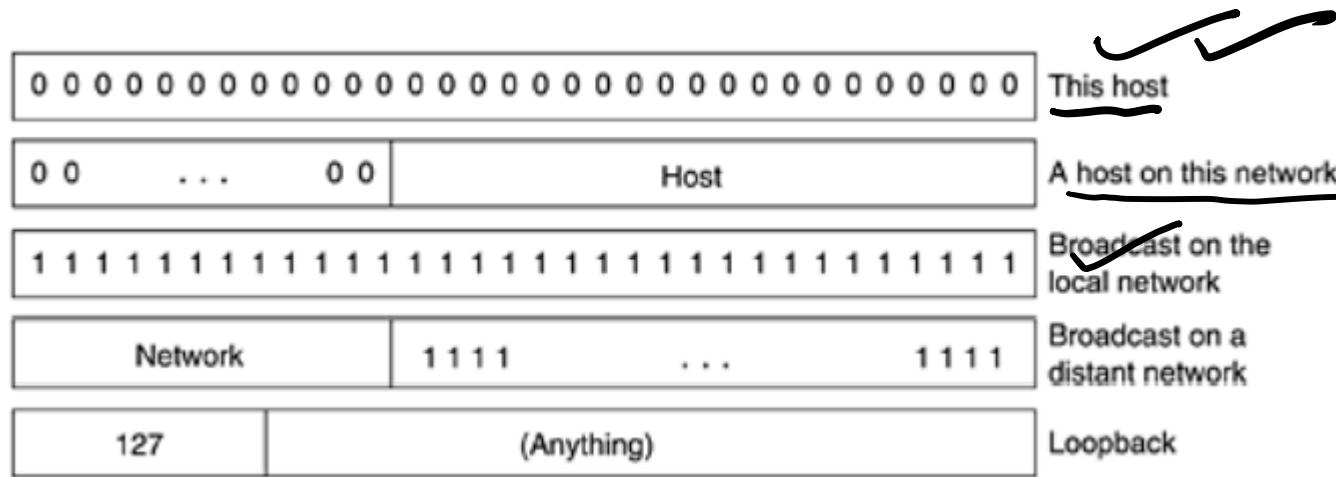
- Also supported is multicast, in which a datagram is directed to multiple hosts. Addresses beginning with 1111 are reserved for future use.
- Over 500,000 networks are now connected to the Internet, and the number grows every year. Network numbers are managed by a nonprofit corporation called ICANN (Internet Corporation for Assigned Names and Numbers) to avoid conflicts.

2.

Network addresses, which are 32-bit numbers, are usually written in dotted decimal notation. In this format, each of the 4 bytes is written in decimal, from 0 to 255. For example, the 32-bit hexadecimal address C0290614 is written as 192.41.6.20. The lowest IP address is 0.0.0.0 and the highest is 255.255.255.255.

2

The value 0 means this network or this host. The value of -1 is used as a broadcast address to mean all hosts on the indicated network.



Special IP addresses.

- The IP address 0.0.0.0 is used by hosts when they are being booted.
- IP addresses with 0 as network number refer to the current network. These addresses allow machines to refer to their own network without knowing its number (but they have to know its class to know how many 0s to include).
- The address consisting of all 1s allows broadcasting on the local network, typically a LAN.
- The addresses with a proper network number and all 1s in the host field allow machines to send broadcast packets to distant LANs anywhere in the Internet (although many network administrators disable this feature).
- Finally, all addresses of the form 127.xx.yy.zz are reserved for loopback testing.
- Packets sent to that address are not put out onto the wire; they are processed locally and treated as incoming packets. This allows packets to be sent to the local network without the sender knowing its number.

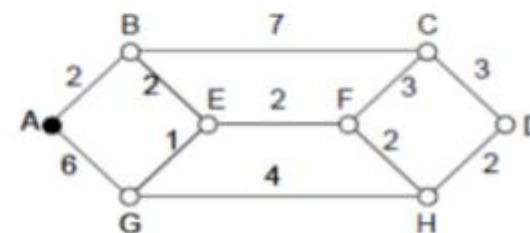
Q. 4

A | B | C | D | E

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

- a. 114.34.2.8
- b. 129.14.6.8
- c. 208.34.54.12
- d. 238.34.2.1

Q. 1. Consider the following network, but ignore the weights on the lines. Suppose that it uses flooding as the routing algorithm. If a packet sent by A to D has a maximum hop count of 3, list all the routes it will take. Also tell how many hops worth of bandwidth it consumes.



Q. 6 Convert the IP address whose hexadecimal representation is C22F1582 to dotted decimal notation.

Internet Control Protocols

- Internet has several control protocols used in the network layer i.e ICMP, ARP, RARP, BOOTP, and DHCP
- ICMP
 - When something unexpected occurs, the event is reported by the ICMP (Internet Control Message Protocol), which is also used to test the Internet.
 - The DESTINATION UNREACHABLE message is used when the subnet or a router cannot locate the destination or when a packet with the DF bit cannot be delivered because a "small-packet" network stands in the way.
 - The TIME EXCEEDED message is sent when a packet is dropped because its counter has reached zero. This event is a symptom that packets are looping, that there is enormous congestion, or that the timer values are being set too low.

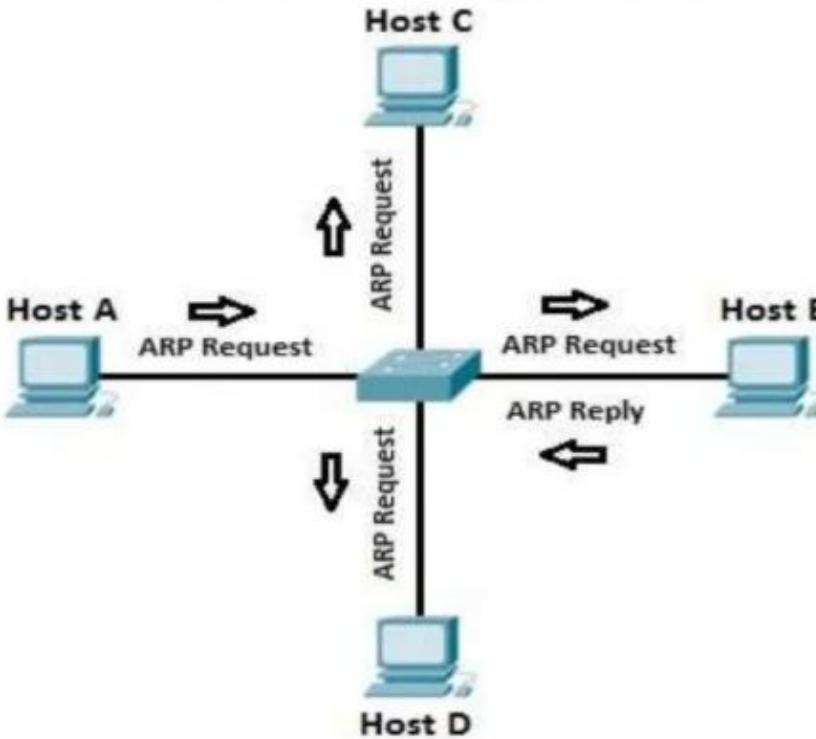
- The PARAMETER PROBLEM message indicates that an illegal value has been detected in a header field. This problem indicates a bug in the sending host'sIP software or possibly in the software of a router transited.
- The SOURCE QUENCH message was formerly used to throttle hosts that were sending too many packets. When a host received this message, it was expected to slow down. It is rarely used any more because when congestion occurs, these packets tend to add more fuel to the fire. Congestion control in the Internet is now done largely in the transport layer; we will study it in detail in
- The REDIRECT message is used when a router notices that a packet seems to be routed wrong. It is used by the router to tell the sending host about the probable error.
- The ECHO and ECHO REPLY messages are used to see if a given destination is reachable and alive. Upon receiving the ECHO message, the destination is expected to send an ECHO REPLY message back. The TIMESTAMP REQUEST and TIMESTAMP REPLY messages are similar, except that the arrival time of the message and the departure time of the reply are recorded in the reply. This facility is used to measure network performance.

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

ARP(Address Resolution Protocol)

- ARP (Address Resolution Protocol) is a network protocol used to find out the hardware (MAC) address of a device from an IP address.
- It is used when a device wants to communicate with some other device on a local network (for example on an Ethernet network that requires physical addresses to be known before sending packets).
- The sending device uses ARP to translate IP addresses to MAC addresses.
- The device sends an ARP request message containing the IP address of the receiving device.
- All devices on a local network segment see the message, but only the device that has that IP address responds with the ARP reply message containing its MAC address.
- The sending device now has enough information to send the packet to the receiving device.
- ARP request packets are sent to the broadcast addresses (FF:FF:FF:FF:FF for the Ethernet broadcasts and 255.255.255.255 for the IP broadcast).

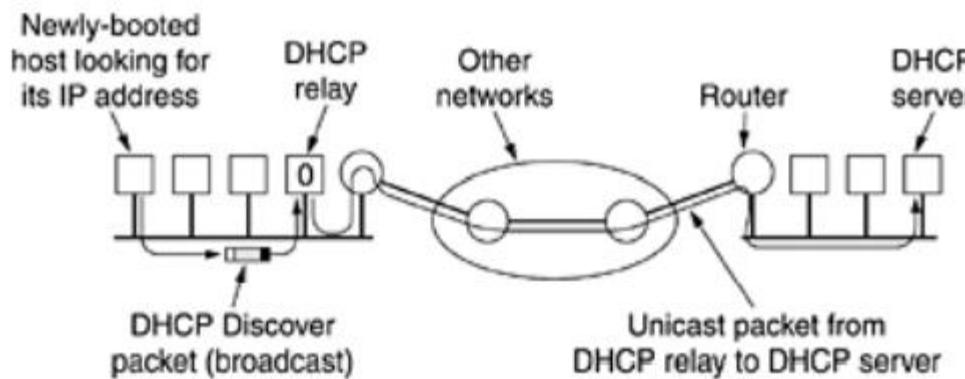
ARP broadcast explained:



- Let's say that Host A wants to communicate with host B.
- Host A knows the IP address of host B, but it doesn't know the host B's MAC address.
- In order to find out the MAC address of host B, host A sends an ARP request, listing the host B's IP address as the destination IP address and the MAC address of FF:FF:FF:FF:FF:FF (Ethernet broadcast).
- Switch will forward the frame out all interfaces (except the incoming interface).
- Each device on the segment will receive the packet, but because the destination IP address is host B's IP address, only host B will reply with the ARP reply packet, listing its MAC address.
- Host A now has enough information to send the traffic to host B.

DHCP

- DHCP (Dynamic Host Configuration Protocol). DHCP allows both manual IP address assignment and automatic assignment. It is described in RFCs 2131 and 2132. In most systems, it has largely replaced RARP and BOOTP.
- Like RARP and BOOTP, DHCP is based on the idea of a special server that assigns IP addresses to hosts asking for one. This server need not be on the same LAN as the requesting host. Since the DHCP server may not be reachable by broadcasting, a DHCP relay agent is needed on each LAN.

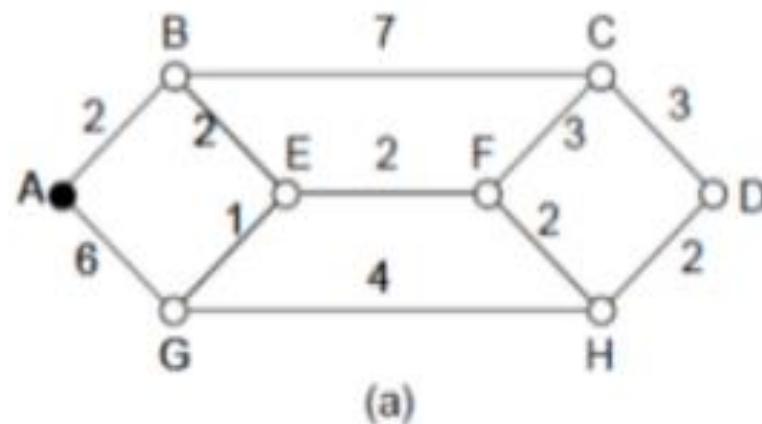


To find its IP address, a newly-booted machine broadcasts a DHCP DISCOVER packet. The DHCP relay agent on its LAN intercepts all DHCP broadcasts. When it finds a DHCP DISCOVER packet, it sends the packet as a unicast packet to the DHCP server, possibly on a distant network. The only piece of information the relay agent needs is the IP address of the DHCP server.

DHCP

- An issue that arises with automatic assignment of IP addresses from a pool is how long an IP address should be allocated. If a host leaves the network and does not return its IP address to the DHCP server, that address will be permanently lost. After a period of time, many addresses may be lost. To prevent that from happening, IP address assignment may be for a fixed period of time, a technique called leasing. Just before the lease expires, the host must ask the DHCP for a renewal. If it fails to make a request or the request is denied, the host may no longer use the IP address it was given earlier.

Q. 1. Consider the following network, but ignore the weights on the lines. Suppose that it uses flooding as the routing algorithm. If a packet sent by A to D has a maximum hop count of 3, list all the routes it will take. Also tell how many hops worth of bandwidth it consumes.



CHAPTER-6

TRANSPORT LAYER

Transport Layer

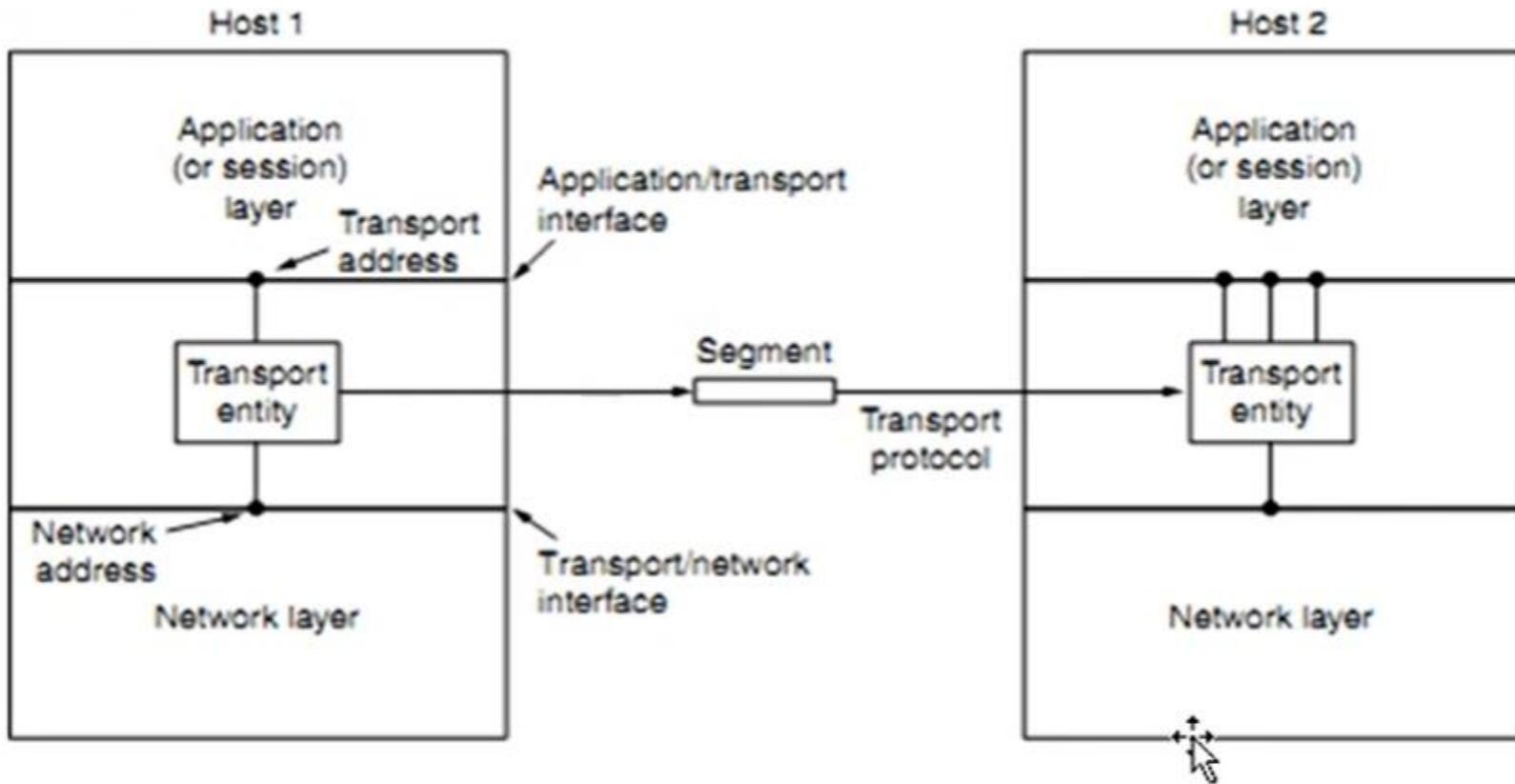
- The network layer provides end-to-end packet delivery using data-grams or virtual circuits.
- **TPDU (Transport Protocol Data Unit):** Transmissions of message between 2 transport entities are carried out by TPDU.

- The transport entity carries out the transport service primitives and send a packet the service.
- Encapsulated in the payload of this packet is a transport layer message for the server's transport entity.
- The task of the transport layer is to provide reliable, cost-effective data transport from the source machine to the destination machine.

Transport Services

1. Services Provided to the Upper Layers

- The ultimate goal of the transport layer is to provide efficient, reliable, and cost-effective data transmission
- software and/or hardware within the transport layer that does the work is called the **transport entity**.
- The transport entity can be located in the operating system kernel, in a library package bound into network applications, in a separate user process, or even on the network interface card.



There are two types of transport services

- Connection-oriented
- Connectionless

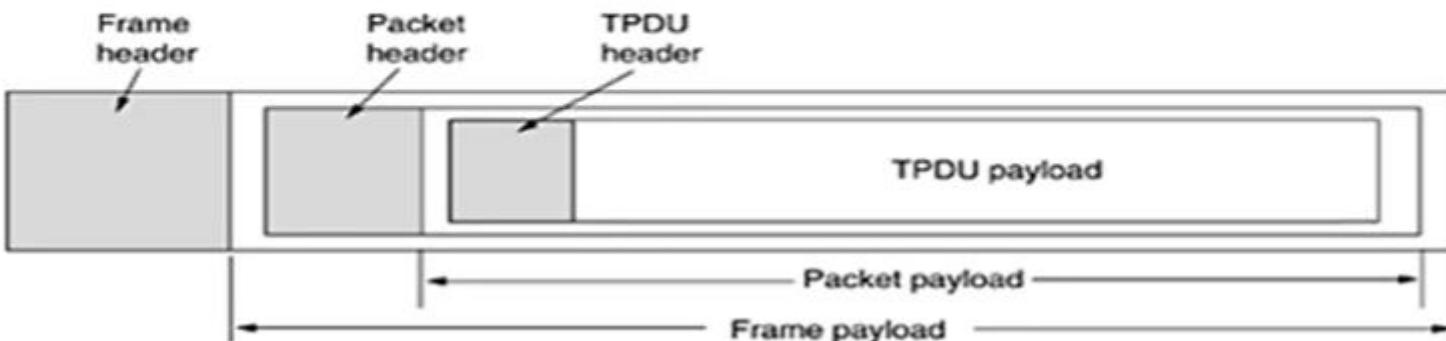
- In both cases, connections have three phases:
- Establishment
- Data transfer
- Release.

2.Transport Service Primitives

Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	This side wants to release the connection

- The server executes a “LISTEN” primitive by calling a library procedure that makes a System call to block the server until a client is found.
- When a client wants to talk to the server, it executes a “CONNECT” primitive, with “CONNECTION REQUEST” TPDU sent to the server.
- When it arrives, the TE unblocks the server and sends a “CONNECTION ACCEPTED” TPDU back to the client.
- When it arrives, the client is unblocked and the connection is established. Data can now be exchanged using “SEND” and “RECEIVE” primitives.
- When a connection is no longer needed, it must be released to free up table space within the 2 transport entries, which is done with “DISCONNECT” primitive by sending “DISCONNECTION REQUEST”

Nesting of TPDUs, packets, and frames



- The term segment for messages sent from transport entity to transport entity.
- TCP, UDP and other Internet protocols use this term. Segments (exchanged by the transport layer) are contained in packets (exchanged by the network layer).

- These packets are contained in frames(exchanged by the data link layer).When a frame arrives, the data link layer processes the frame header and, if the destination address matches for local delivery, passes the contents of the frame payload field up to the network entity.
- The network entity similarly processes the packet header and then^I passes the contents of the packet payload up to the transport entity.

- **BERKLEY SOCKETS**

- These primitives are socket primitives used in Berkley UNIX for TCP.
- The first four primitives in the list are executed in that order by servers last four by client

Primitive	Meaning
SOCKET	Create a new communication end point
BIND	Attach a local address to a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Block the caller until a connection attempt arrives
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

- The **SOCKET** primitive creates a new endpoint and allocates table space for it within the transport entity.
- The **BIND** primitive is used to **connect the newly created sockets to an address**. Once a server has bound an address to a socket, remote clients can connect to it.
- The **LISTEN** call, which allocates space to queue incoming calls for the case that several clients try to connect at the same time. [
- The server executes an **ACCEPT** primitive to block waiting for an incoming connection

- The **CONNECT** primitive blocks the caller and actively starts the connection process. When it completes, the client process is unblocked and the connection is established.
- Both sides can now use **SEND** and **RECEIVE** to transmit and receive data over the full-duplex connection.
- Connection release with sockets is symmetric. When both sides have executed a **CLOSE** primitive, the connection is released.

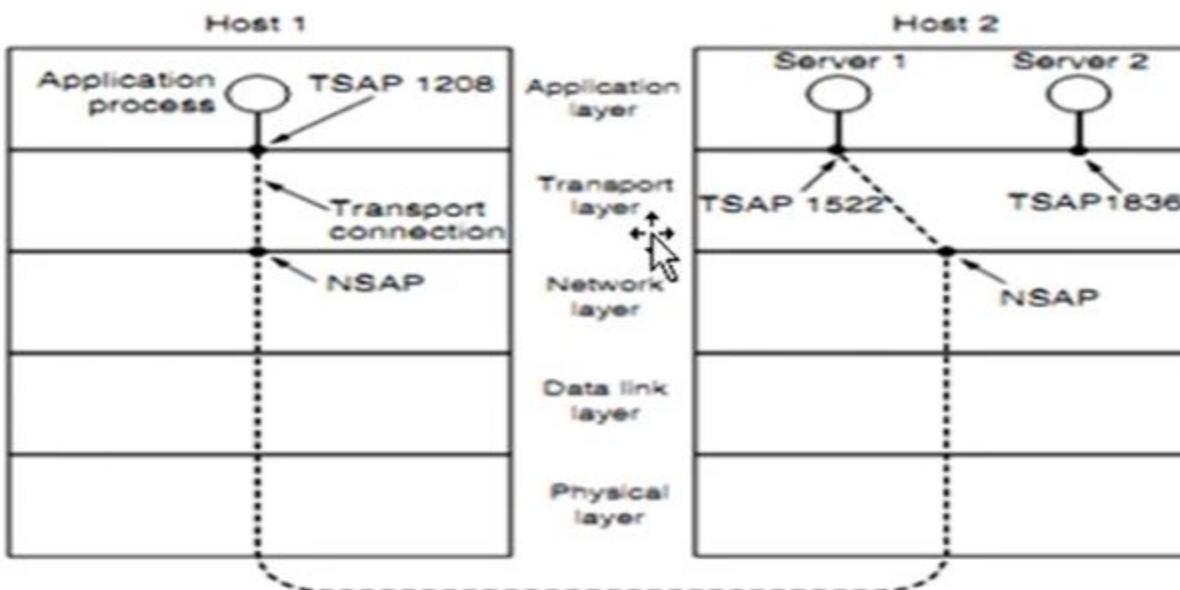
Elements Of Transport Protocols

- The elements of transport protocols are:
 - 1.ADDRESSING
 - 2.Connection Establishment.
 - 3.Connection Release.
 - 4.Error control and flow control
 - 5.Multiplexing.

I

- ADDRESSING
- When an application process wishes to set up a connection to a remote application process, it must specify which one to connect to
- The method normally used is to define transport addresses to which processes can listen for connection requests.
- In the Internet, these endpoints are called **ports**.

- There are two types of access points.
- **TSAP (Transport Service Access Point)** to mean a specific endpoint in the transport layer.
- **NSAPs (Network Service Access Points)**. IP addresses are examples of NSAPs(in the network layer)



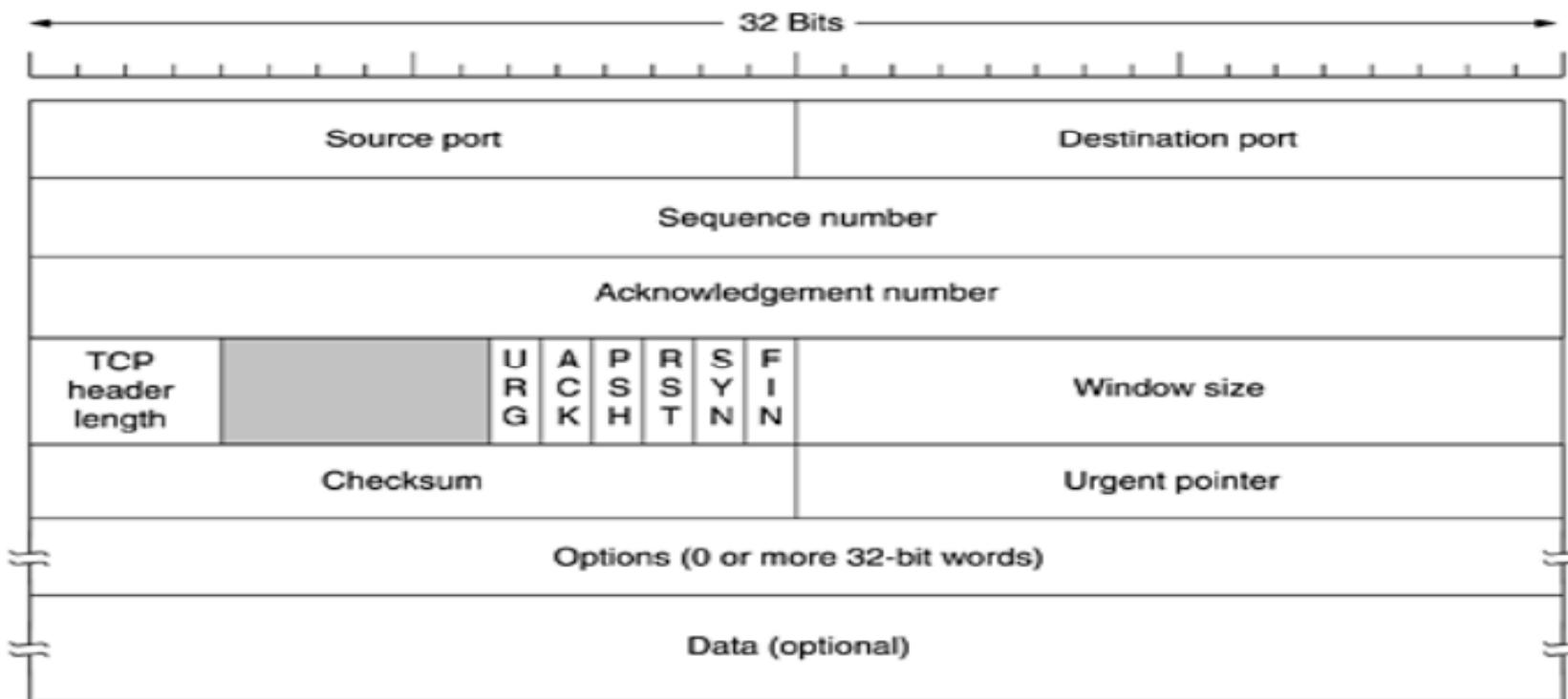
1. A mail server process attaches itself to TSAP 1522 on host 2 to wait for an incoming call.
2. An application process on host 1 wants to send an email message, so it attaches itself to TSAP 1208 and issues a CONNECT request.
3. The request specifies TSAP 1208 on host 1 as the source and TSAP 1522 on host 2 as the destination.
4. This action ultimately results in a transport connection being established between the application process and the server.
5. The application process sends over the mail message.
6. The mail server responds to say that it will deliver the message.
7. The transport connection is released.

TCP(Transmission Control Protocol)

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

The TCP segment Header

The TCP header.



- Every segment begins with a fixed-format, 20-byte header. The fixed header may be followed by header options.
- After the options, if any, up to $65,535 - 20 - 20 = 65,495$ data bytes may follow, where the first 20 refer to the IP header and the second to the TCP header. Segments without any data are legal and are commonly used for acknowledgements and control messages.
- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.

- **Flags (1-bit each)**
 - **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
 - **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
 - **ECE** - It has two meanings:
 - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
 - If SYN bit is set to 1, ECE means that the device is ECT capable.
 - **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
 - **ACK** - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
 - **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
 - **RST** - Reset flag has the following features:
 - It is used to refuse an incoming connection.
 - It is used to reject a segment.
 - It is used to restart a connection.
 - **SYN** - This flag is used to set up a connection between hosts.
 - **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.

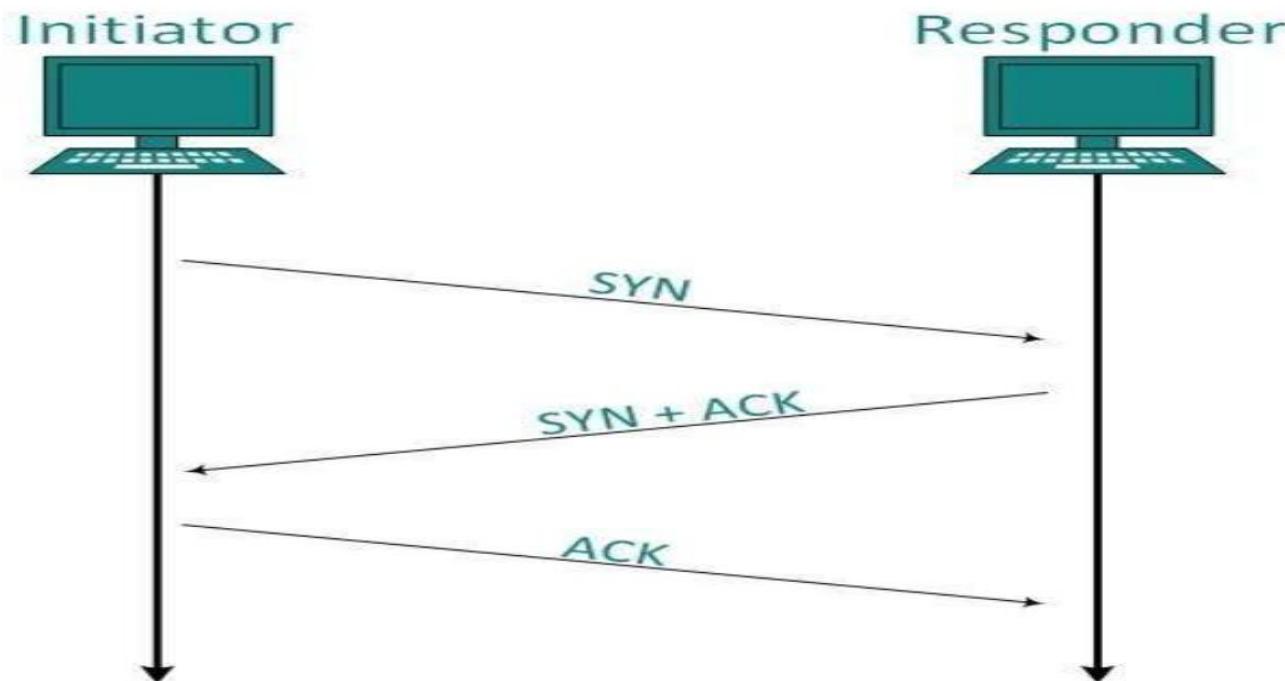
- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.
- **Options** - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

- Addressing
- TCP communication between two remote hosts is done by means of port numbers (TSAPs). Ports numbers can range from 0 – 65535 which are divided as:
 - System Ports (0 – 1023)
 - User Ports (1024 – 49151)
 - Private/Dynamic Ports (49152 – 65535)

UDP(User Datagram Protocol)

- The User Datagram Protocol (UDP) is simplest Transport Layer communication protocol. It involves minimum amount of communication mechanism. UDP is said to be an unreliable transport protocol but it uses IP services which provides best effort delivery mechanism.

- Connection Management
- TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.



- Establishment

Client initiates the connection and sends the segment with a Sequence number. Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number. Client after receiving ACK of its segment sends an acknowledgement of Server's response.

- Release

Either of server and client can send TCP segment with FIN flag set to 1. When the receiving end responds it back by ACKnowledging FIN, that direction of TCP communication is closed and connection is released.

- Bandwidth Management
- TCP uses the concept of window size to accommodate the need of Bandwidth management. Window size tells the sender at the remote end, the number of data byte segments the receiver at this end can receive. TCP uses slow start phase by using window size 1 and increases the window size exponentially after each successful communication.
- For example, the client uses windows size 2 and sends 2 bytes of data. When the acknowledgement of this segment received the windows size is doubled to 4 and next sent the segment sent will be 4 data bytes long. When the acknowledgement of 4-byte data segment is received, the client sets windows size to 8 and so on.
- If an acknowledgement is missed, i.e. data lost in transit network or it received NACK, then the window size is reduced to half and slow start phase starts again.

- **Error Control &and Flow Control**
- TCP uses port numbers to know what application process it needs to handover the data segment. Along with that, it uses sequence numbers to synchronize itself with the remote host. All data segments are sent and received with sequence numbers. The Sender knows which last data segment was received by the Receiver when it gets ACK. The Receiver knows about the last segment sent by the Sender by referring to the sequence number of recently received packet.
- If the sequence number of a segment recently received does not match with the sequence number the receiver was expecting, then it is discarded and NACK is sent back. If two segments arrive with the same sequence number, the TCP timestamp value is compared to make a decision.
- **Multiplexing**
- The technique to combine two or more data streams in one session is called Multiplexing. When a TCP client initializes a connection with Server, it always refers to a well-defined port number which indicates the application process. The client itself uses a randomly generated port number from private port number pools.
- Using TCP Multiplexing, a client can communicate with a number of different application process in a single session. For example, a client requests a web page which in turn contains different types of data (HTTP, SMTP, FTP etc.) the TCP session timeout is increased and the session is kept open for longer time so that the three-way handshake overhead can be avoided.
- This enables the client system to receive multiple connection over single virtual connection. These virtual connections are not good for Servers if the timeout is too long.

- Congestion Control
- When large amount of data is fed to system which is not capable of handling it, congestion occurs. TCP controls congestion by means of Window mechanism. TCP sets a window size telling the other end how much data segment to send. TCP may use three algorithms for congestion control:
 - Additive increase, Multiplicative Decrease
 - Slow Start
 - Timeout React

- Timer Management
- TCP uses different types of timer to control and management various tasks:
- Keep-alive timer:
 - This timer is used to check the integrity and validity of a connection.
 - When keep-alive time expires, the host sends a probe to check if the connection still exists.
- Retransmission timer:
 - This timer maintains stateful session of data sent.
 - If the acknowledgement of sent data does not receive within the Retransmission time, the data segment is sent again.
- Persist timer:
 - TCP session can be paused by either host by sending Window Size 0.
 - To resume the session a host needs to send Window Size with some larger value.
 - If this segment never reaches the other end, both ends may wait for each other for infinite time.
 - When the Persist timer expires, the host re-sends its window size to let the other end know.
 - Persist Timer helps avoid deadlocks in communication.

- Timed-Wait:
 - After releasing a connection, either of the hosts waits for a Timed-Wait time to terminate the connection completely.
 - This is in order to make sure that the other end has received the acknowledgement of its connection termination request.
 - Timed-out can be a maximum of 240 seconds (4 minutes).
- Crash Recovery
 - TCP is very reliable protocol. It provides sequence number to each of byte sent in segment. It provides the feedback mechanism i.e. when a host receives a packet, it is bound to ACK that packet having the next sequence number expected (if it is not the last segment).
 - When a TCP Server crashes mid-way communication and re-starts its process it sends TPDU broadcast to all its hosts. The hosts can then send the last data segment which was never unacknowledged and carry onwards.

Computer Network

(CSE 3034)

Text book: Computer Networks by Andrew S. Tanenbaum

Introduction to the course

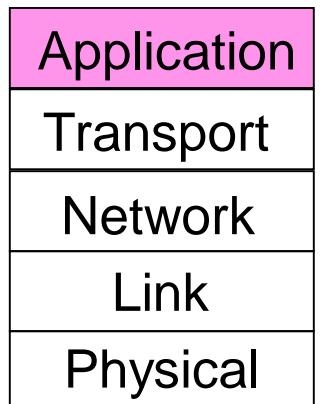
Syllabus :

- Introduction(Chapter 1)
- The Physical Layer(Chapter 2)
- The Data Link Layer(Chapter 3)
- The Medium Access Control Sublayer(Chapter 4)
- The Network Layer(Chapter 5)
- The Transport layer(Chapter 6)
- **The Application layer(Chapter 7)**
- Network security(Chapter 8)

The Application Layer

The application Layer

- Layers below the application layer are there to provide reliable transport, but they do not do real work for users.
- Even in the application layer there is a need for support protocols, to allow the applications to function.
- One popular term for network users : **DNS (Domain Name system)**
 - **DNS** : Resolves high-level human readable names for computers to low-level IP addresses.
 - DNS name space
 - Domain Resource records
 - Name servers



The application Layer

DNS—The Domain Name System

Why do we need DNS?

- Network addresses (e.g., IP) are hard for people to remember.
- Also, sending e-mail to tana@128.111.24.41 means that if Tana's ISP moves the mail server to a different machine with different IP address, her e-mail address has to change.
- Consequently, **ASCII names** were introduced to decouple machine names from machine addresses.
- In this way, Tana's address might be something like tana@art.ucsb.edu.
- However, network itself understand only numerical addresses, so some mechanism is required to convert the ASCII strings to network addresses.
- Originally one file with names and IP addresses – became too large with increase in no. of hosts
- Host name conflicts began to occur
- **Solution : DNS** An Example : telnet [134.58.42.36](telnet://134.58.42.36)
telnet [nix.cs.kuleuven.ac.be](telnet://nix.cs.kuleuven.ac.be)

The application Layer

DNS—The Domain Name System

- Hierarchical domain based naming scheme.
- Uses a distributed database system for implementing it.
- Primarily for mapping host names and e-mail destinations to IP addresses.

Mapping a name to an IP address:

- Application program calls a library procedure called a **resolver**, for example *gethostname*, passing it the name as a parameter.
- The resolver sends a query with the name to a local DNS server, which looks up the name and returns the IP address.
- The query and response are sent as UDP packets.
- Once it has the IP address the host can now establish a TCP connection or send UDP packets.

The application Layer

DNS—The Domain Name System

The DNS Name Space :

- Internet is divided into over **200 top- level domains**, where each domain covers many hosts.
- Each domain is partitioned into **subdomains**, and these are further partitioned, and so on.
- All these domains can be represented by a tree.

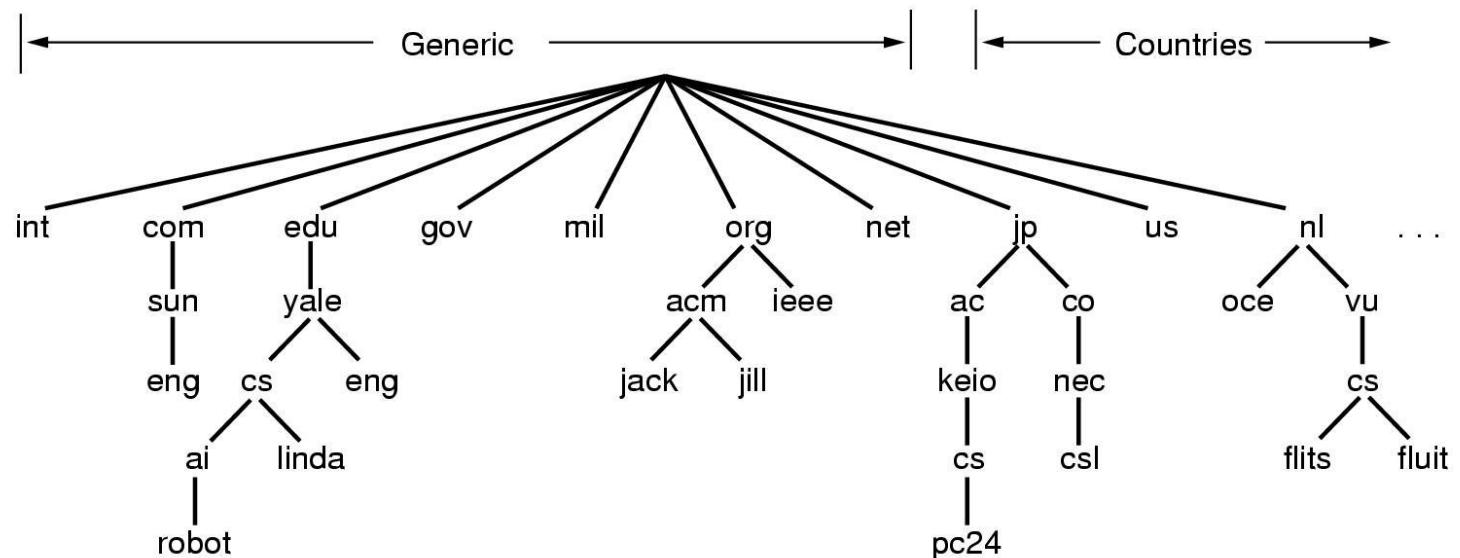
Top level domains in two groups :

Generic

- com commercial organisations
- org non-commercial organisations
- int international organisations
- net companies offering network services
- edu universities
- gov US government
- mil US army
- **NEW:** name, biz, info,...

Countries (entry for every countries)

- jp Japan
- us USA
- nl Netherland



A portion of the Internet domain name space.

The application Layer

DNS—The Domain Name System

The DNS Name Space :

- Getting a second-level domain, such as **name-of-company.com**, is easy.
- It requires going to a registrar for the corresponding top-level domain (e.g. **.com**) to check if the desired name is available and not somebody's trademark.
- If there are no problems, the register pays a small annual fee and gets the name.
- Each domain is named by the path upward from it to the root.
- The components are separated by periods (pronounced “dot”).
- ***eng.sun.com*** is the engineering department at Sun Microsystems.
- Domain names are case insensitive, (e.g. **edu**, **Edu**, and **EDU** mean the same thing).
- Component names can be up to 63 characters long, and full path names must not exceed 255 characters.

The application Layer

DNS—The Domain Name System

The DNS Name Space :

- Domains can be inserted into the tree in two different ways.
 - *cs.yale.edu* and *cs.yale.ct.us* both are form of domains.
- Each domain controls how it allocates the domains under it.
 - For example, Japan has domains **ac.jp** and **co.jp** that mirror **edu** and **com**
 - The Netherlands does not make this distinction and puts all organization directly under **nl**
- Thus, all three of the following are university computer science departments:
 - **cs.yale.edu** (Yale University, in the US)
 - **cs.vu.nl** (Vrije University, in the Netherl)
 - **cs.keio.ac.jp** (Keio University, in Japan)
- To create a new domain, permission is required of the domain in which it will be included.
- Naming follows organizational boundaries, not physical networks.

The application Layer

DNS—The Domain Name System

Resource Records:

- Every domain, whether it is a single host or a top-level domain, can have a set of **resource records** associated with it.
- For a single host, the most common resource record is just its IP address, but many other kinds of resource records also exist.
- When a resolver gives a domain name to DNS, what it gets back are the resource records associated with that name.
- A resource record is of five field.
- Resource records are presented as ASCII text, one line per resource record.

Domain_name	Time_to_live	Class	Type	Value
-------------	--------------	-------	------	-------

The application Layer

DNS—The Domain Name System

Resource Records:

Domain_name

- It tells the domain to which this record applies (normally, many records exist for each domain and each copy of the database holds information about multiple domains).
- Primary search key used to satisfy queries.

Time_to_live

- It gives an indication of how stable the record is.
 - Large value = 86400 (the number of seconds in 1 day) , highly stable.
 - Small value = 60 (1 minute), highly volatile.

Class

- For Internet information, it is always *IN* and for non internet information other code.

Type

- It tells what kind of record this is (e.g. IP address, primary e mail address, name server etc.)

Value

- This field can be a number, a domain name, or an ASCII string.
- The semantics depend on the record type.

The application Layer

DNS—The Domain Name System

Resource Records:

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IP address of host	32-bit integer
NS	Name Server	Name of name server for this domain
MX	Mail exchange	Priority, domain willing to accept email
CNAME	Canonical Name	Domain Name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ascii
TXT	Text	Uninterpreted ascii text

The principal DNS resource record types for IPv4

The application Layer

DNS—The Domain Name System

Resource Records:

```
; Authoritative data for cs.vu.nl
cs.vu.nl.      86400  IN  SOA   star boss (952771,7200,7200,2419200,86400)
cs.vu.nl.      86400  IN  TXT   "Divisie Wiskunde en Informatica."
cs.vu.nl.      86400  IN  TXT   "Vrije Universiteit Amsterdam."
cs.vu.nl.      86400  IN  MX    1 zephyr.cs.vu.nl.
cs.vu.nl.      86400  IN  MX    2 top.cs.vu.nl.

flits.cs.vu.nl. 86400  IN  HINFO Sun Unix
flits.cs.vu.nl. 86400  IN  A    130.37.16.112
flits.cs.vu.nl. 86400  IN  A    192.31.231.165
flits.cs.vu.nl. 86400  IN  MX   1 flits.cs.vu.nl.
flits.cs.vu.nl. 86400  IN  MX   2 zephyr.cs.vu.nl.
flits.cs.vu.nl. 86400  IN  MX   3 top.cs.vu.nl.
www.cs.vu.nl.   86400  IN  CNAME star.cs.vu.nl
ftp.cs.vu.nl.   86400  IN  CNAME zephyr.cs.vu.nl

rowboat          IN  A    130.37.56.201
                  IN  MX   1 rowboat
                  IN  MX   2 zephyr
                  IN  HINFO Sun Unix

little-sister    IN  A    130.37.62.23
                  IN  HINFO Mac MacOS

laserjet         IN  A    192.31.231.216
                  IN  HINFO "HP Laserjet IISi" Proprietary
```

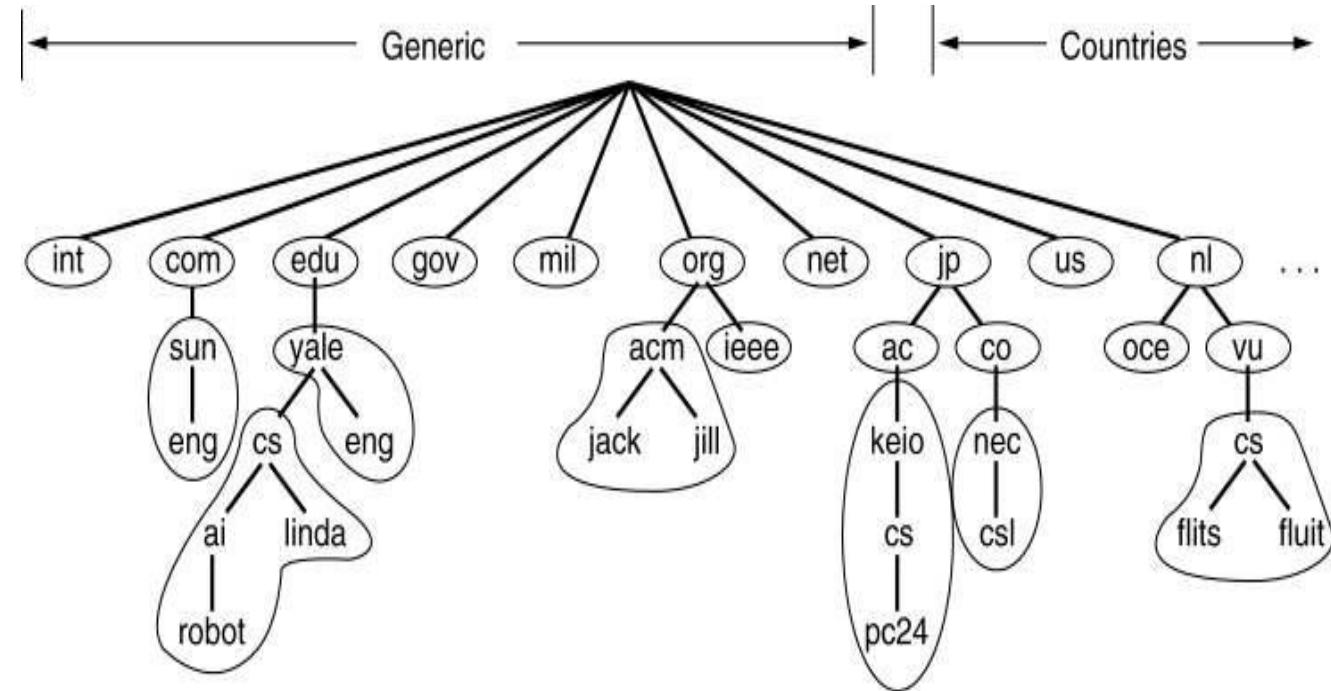
A portion of a possible DNS database for cs.vu.nl

The application Layer

DNS—The Domain Name System

Name Servers :

- In theory at least, a single name server could contain the entire DNS database and respond to all queries about it.
- In practice, this server would be so overloaded as to be useless.
- Furthermore, if it ever went down, the entire Internet would be crippled.
- To avoid the problems associated with having only a single source of information, the DNS name space is divided into nonoverlapping **zones**.

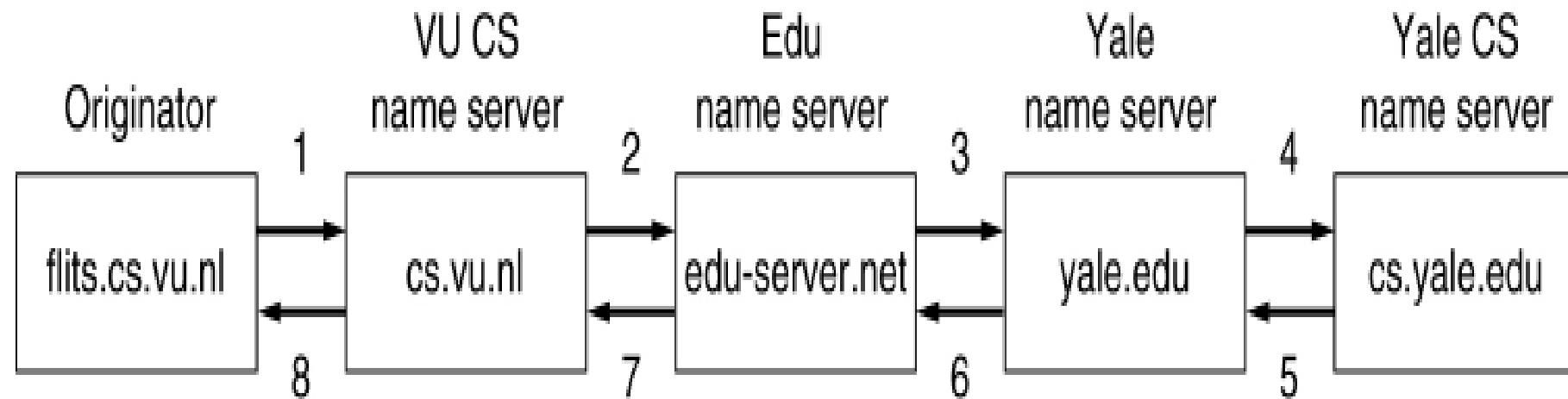


Part of the DNS name space showing the division into zones.

The application Layer

DNS—The Domain Name System

Name Servers :



How a resolver looks up a remote name in eight steps