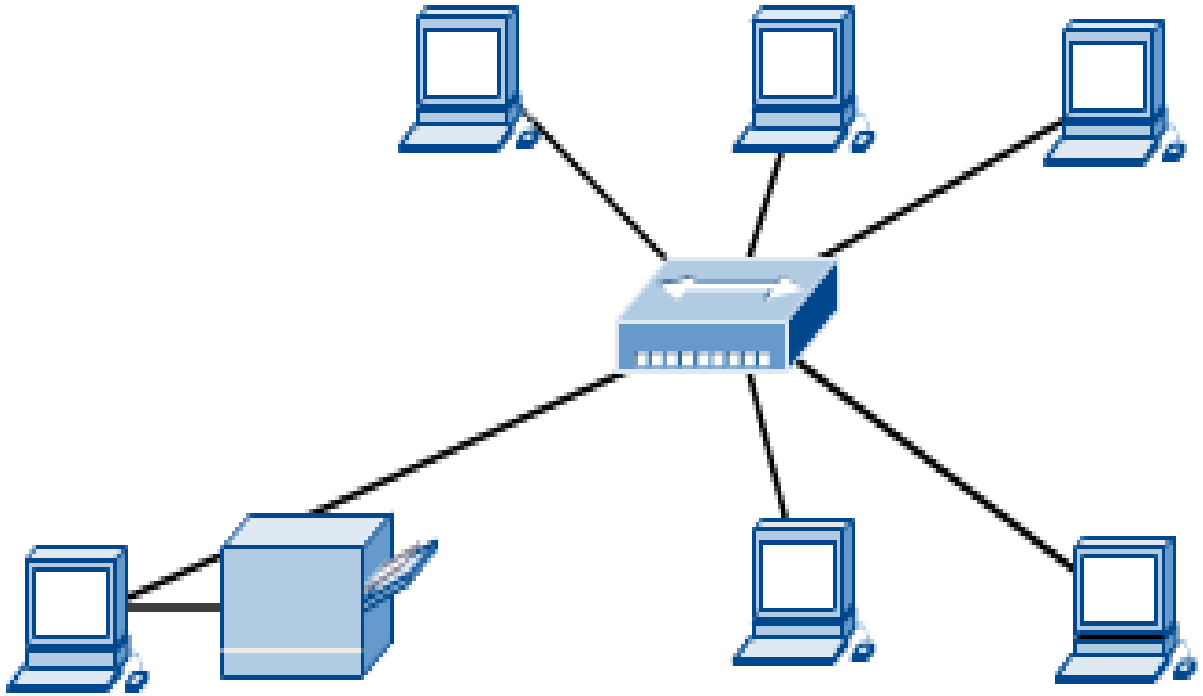
INTRODUCTION TO COMPUTER NETWORKS

Computer Networks



- **Computer network :** a collection of autonomous computers interconnected by a single technology.

- The computers can be geographically located anywhere.

- Two computers are said to be interconnected if they are able to exchange information.

- Networks come in many sizes, shapes and forms. Although it may sound strange to some people, neither the Internet nor the World Wide Web is a computer network.

- The ***Internet is not a single network but a network of networks*** and the Web is a distributed system that runs on top of the Internet.

CLASSIFICATION OF NETWORK

3 Broad categories:

LAN :

Network in small geographical Area (Room, Building or a Campus) is called LAN (Local Area Network)

MAN :

Network in a City is call MAN (Metropolitan Area Network)

WAN :

Network spread geographically (Country or across Globe) is called WAN (Wide Area Network)

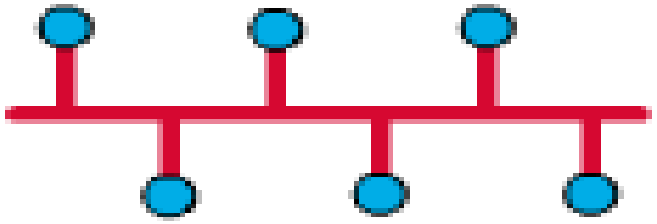
Applications of Networks:

1. **Resource Sharing**
   - Hardware (computing resources, disks, printers)
   - Software (application software)
2. **Information Sharing**
   - Easy accessibility from anywhere (files, databases)
   - Search Capability (WWW)
3. **Communication**
   - Email
   - Message broadcast
4. **Remote computing**
5. **Distributed processing (GRID Computing)**

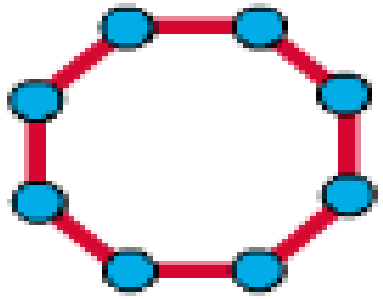
Network Topology

The network topology defines the way in which computers, printers, and other devices are connected. A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.

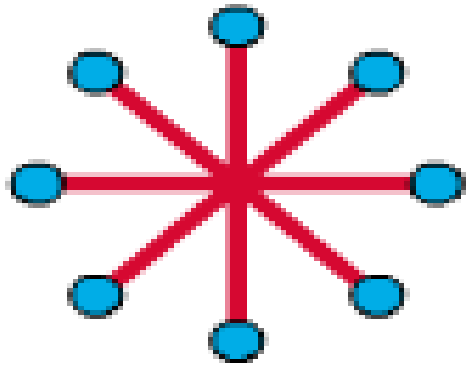
Topology:



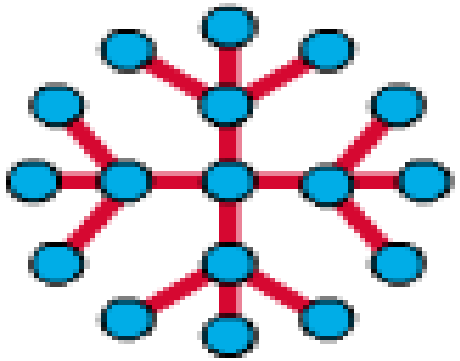
Bus Topology



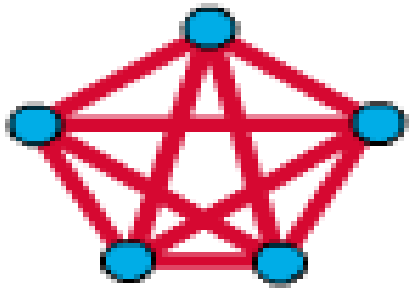
Ring Topology



Star Topology

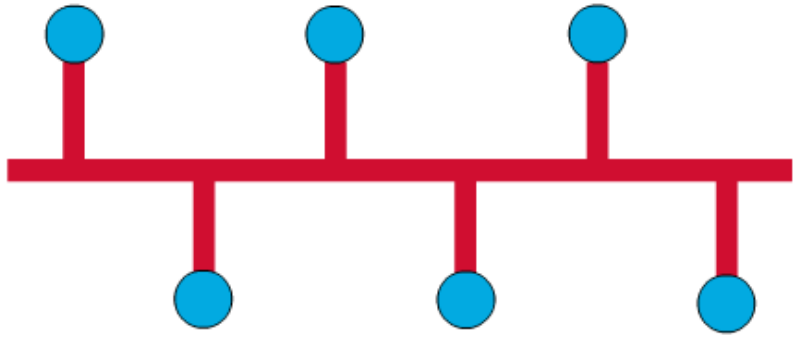


Extended Star Topology



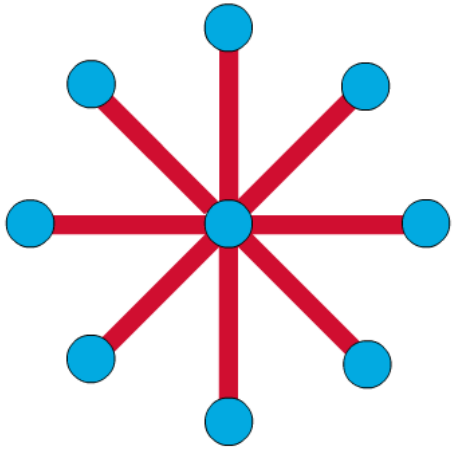
Mesh Topology

Bus Topology:



Commonly referred to as a linear bus, all the devices on a bus topology are connected by one single cable.

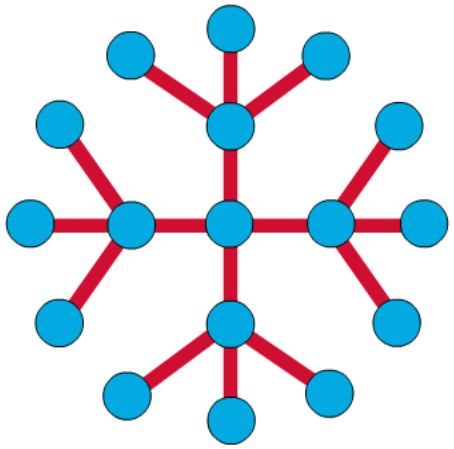
Star Topology:



The star topology is the most commonly used architecture in Ethernet LANs.

When installed, the star topology resembles spokes in a bicycle wheel.

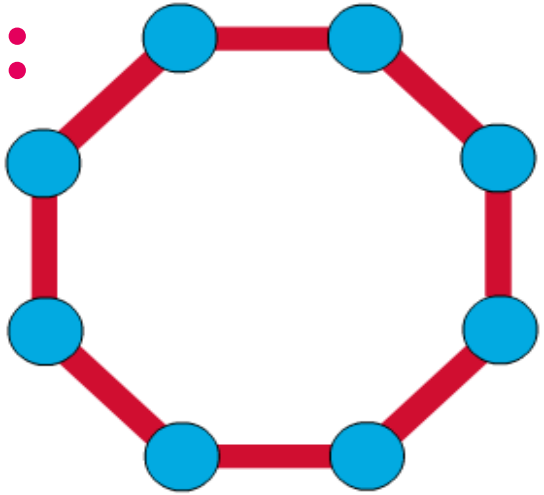
Tree Topology:

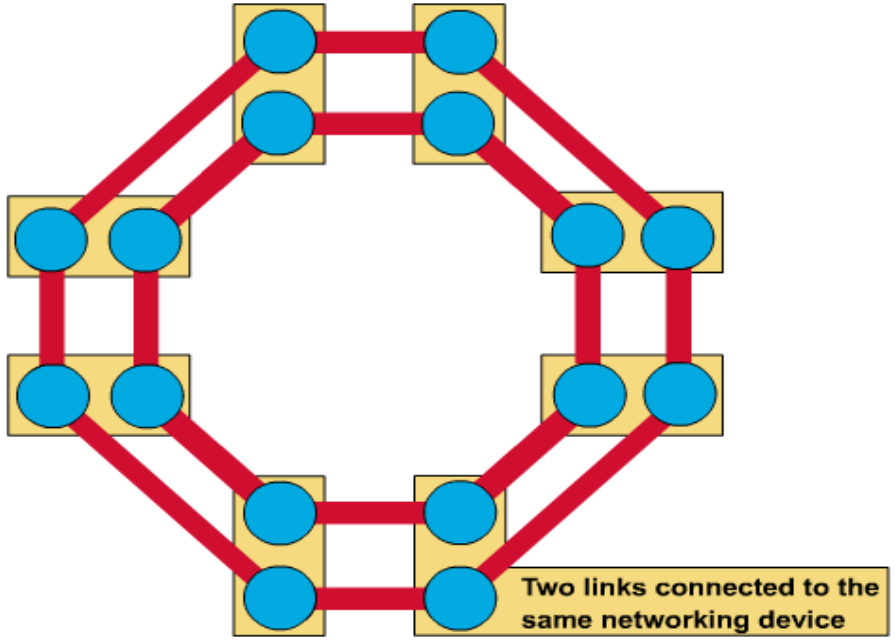


Larger networks use the extended star topology also called tree topology.

When it is used with network devices that filter frames or packets, like bridges, switches, and routers, this topology significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.

Ring Topology:





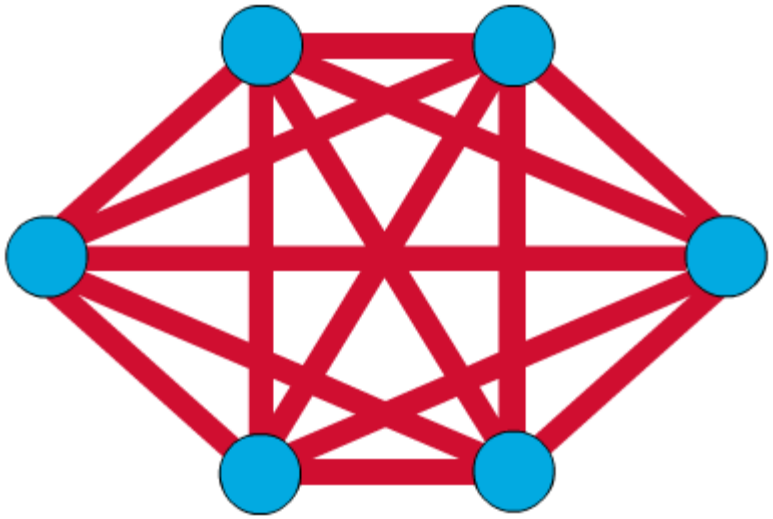
A frame travels around the ring, stopping at each node. If a node wants to transmit data, it adds the data as well as the destination address to the frame.

The frame then continues around the ring until it finds the destination node, which takes the data out of the frame.

Two types:

- Single ring – All the devices on the network share a single cable
- Dual ring – The dual ring topology allows data to be sent in both directions.

Mesh Topology:



The mesh topology connects all devices (nodes) to each other for redundancy and fault tolerance.

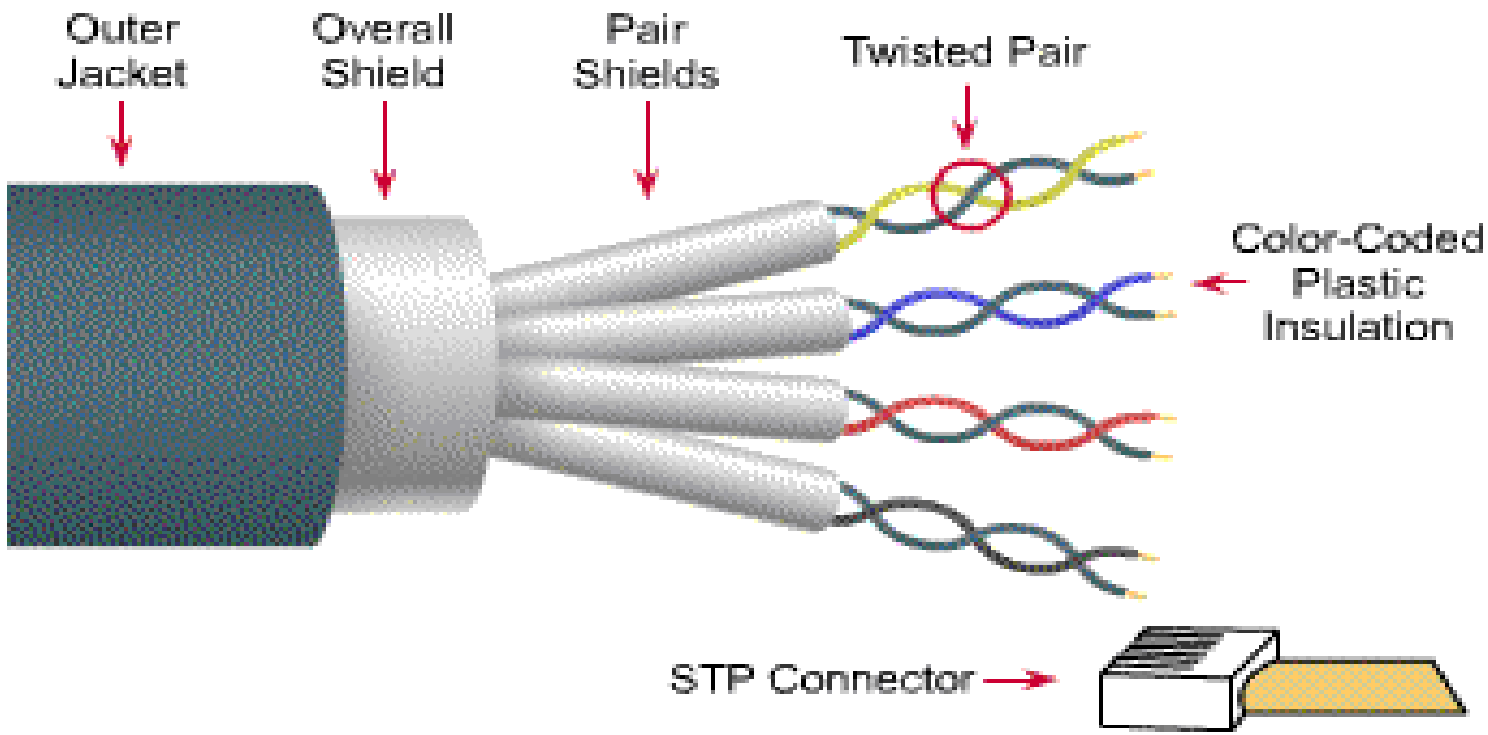
It is used in WANs to interconnect LANs and for mission critical networks like those used by banks and financial institutions.

Implementing the mesh topology is expensive and difficult.

Network Components:

- **Physical Media**
- **Interconnecting Devices**
- **Computers**
- **Networking Software**
- **Applications**

Network Physical Media:



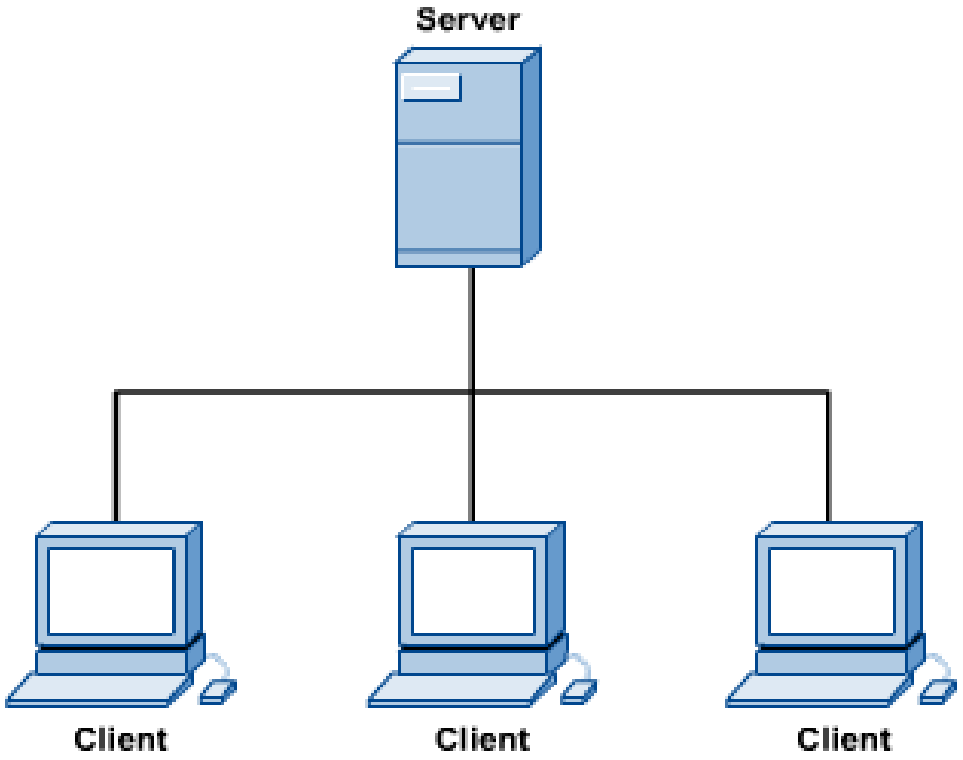
- Speed and throughput: 10-100 Mbps
- Cost per node: Moderately expensive
- Media and connector size: Medium to Large
- Maximum cable length: 100m (short)

Networking media can be defined simply as the means by which signals (data) are sent from one computer to another (either by cable or wireless means).

Networking Devices:

HUB, Switches, Routers, Wireless Access Points, Modems etc.

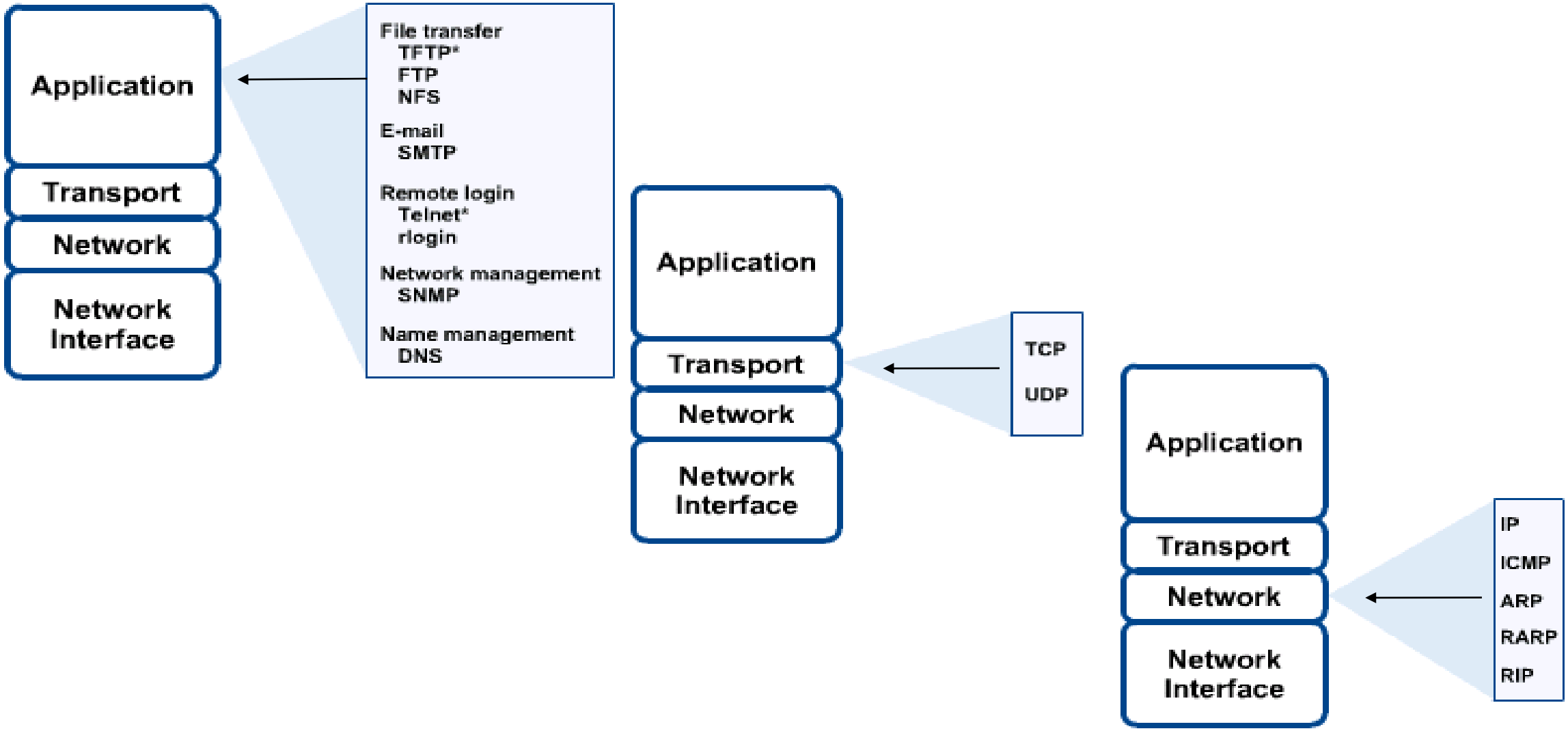
Computers: Clients and Servers



- In a client/server network arrangement, network services are located in a dedicated computer whose only function is to respond to the requests of clients.

- The server contains the file, print, application, security, and other services in a central computer that is continuously available to respond to client requests.

Networking Protocol: TCP/IP



Applications:

- E-mail
- Searchable Data (Web Sites)
- E-Commerce
- News Groups
- Internet Telephony (VoIP)
- Video Conferencing
- Chat Groups
- Instant Messengers
- Internet Radio

Uses of Computer Networks:

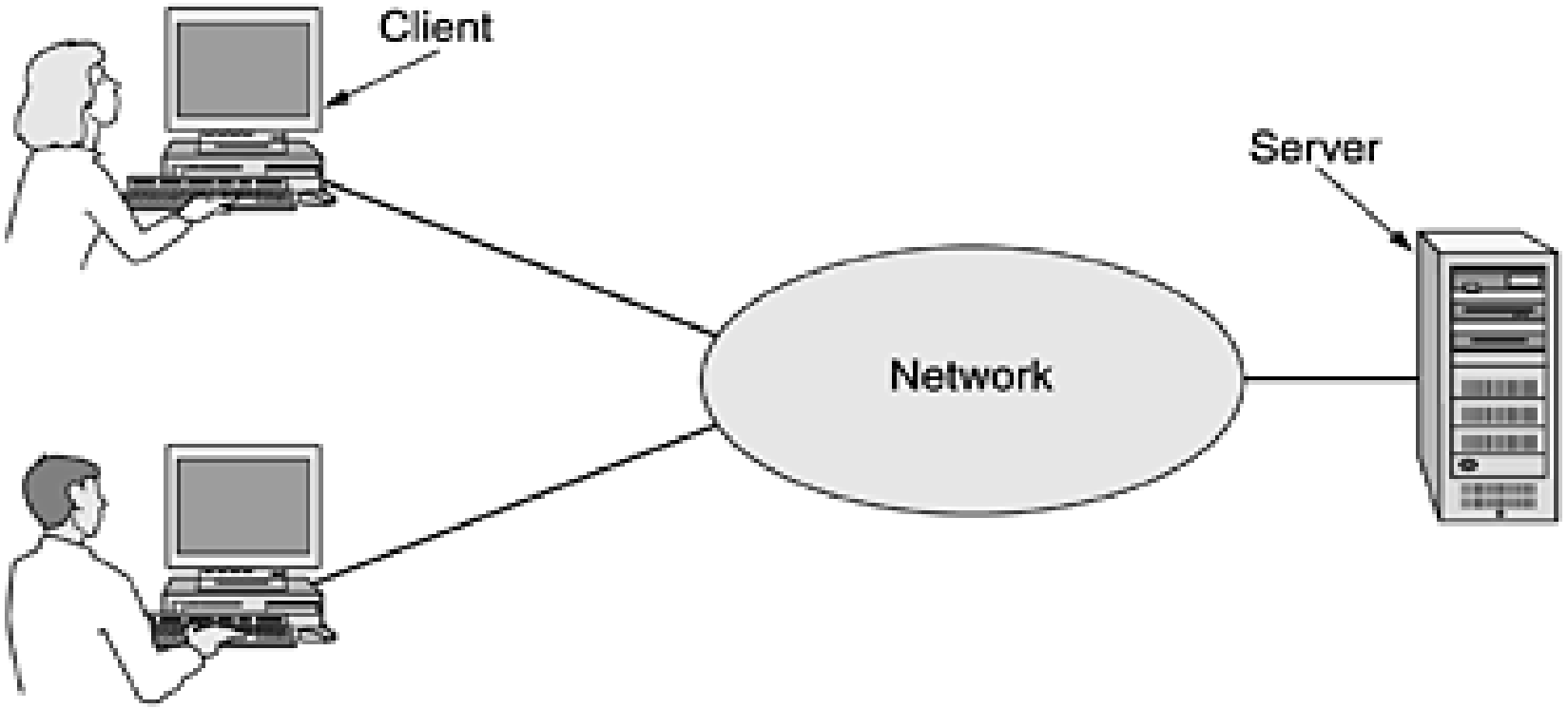
- Business Applications
- Home Applications
- Mobile Users
- Social Issues

Business Applications:

- Resource sharing
- Information sharing

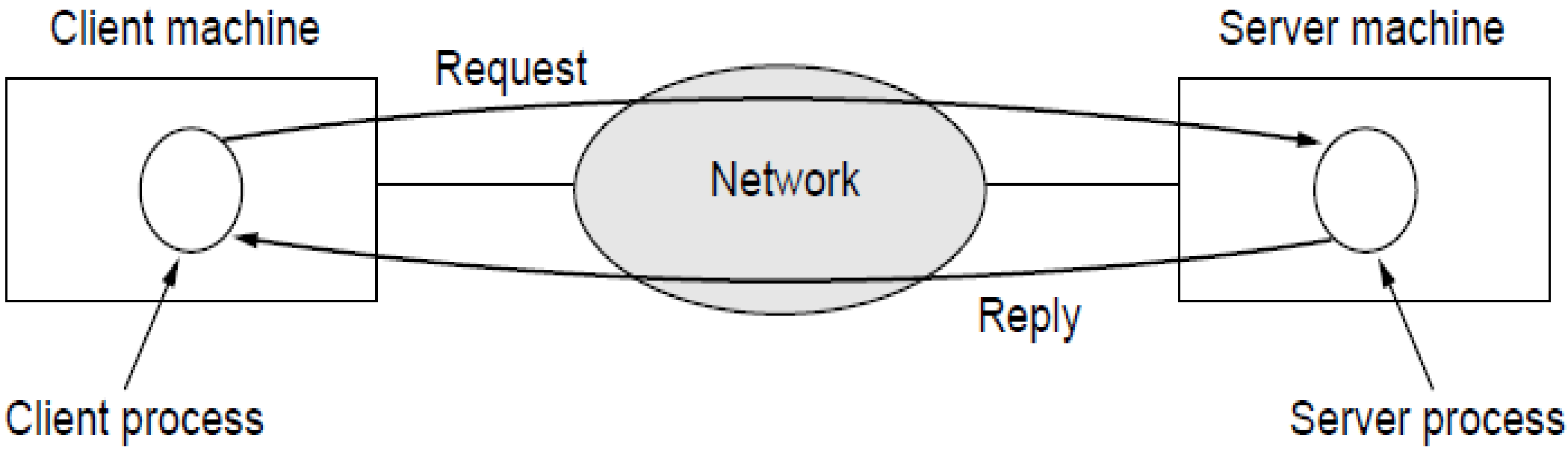
Client-server model

In client-server model , two processes are involved, one on the client machine and one on the server machine. Communication takes the form of the client process sending a message over the network to the server process.



The client-server model involves requests and replies

The client process then waits for a reply message. When the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply.



Business Applications

- **Second goal:**

A computer network has to do with people i;e. a computer network can provide a powerful communication medium among employees.

- **Third goal:**

Many companies is doing business electronically with other companies, especially suppliers and customers.

- **Fourth goal:**

Doing business with consumers over the Internet. It is called e-commerce (electronic commerce).

Home Applications:

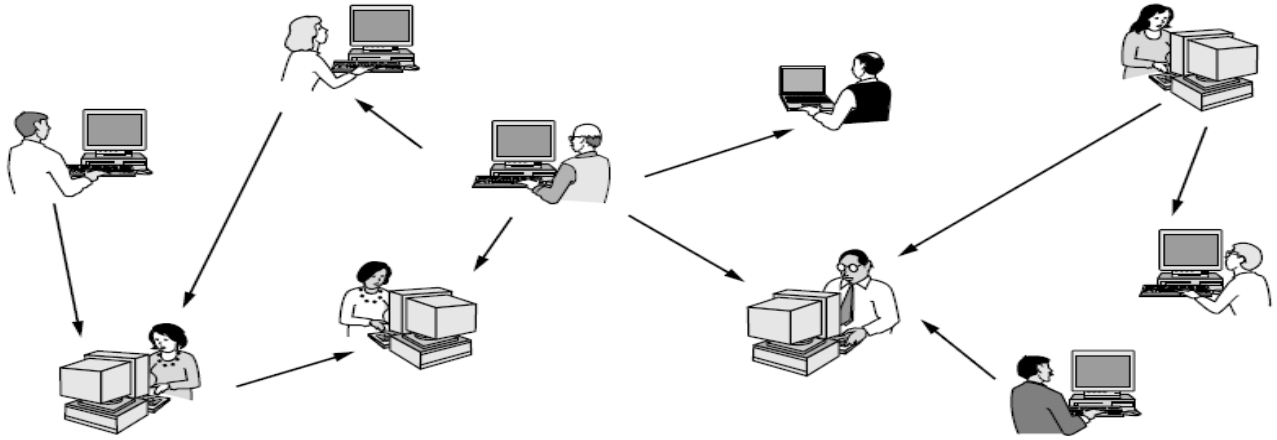
- Some of the more popular uses of the Internet for home users are as follows:

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

Access to remote information:

It comes in many forms. It can be surfing the World Wide Web for information or just for fun. Information available includes the arts, business, cooking, government, health, history, hobbies, recreation, science, sports, travel, and many others.

Person-to-Person communication:



- It is the **second broad category** of network use for person-to-person communication. E.g. ***E-mail***.

- Another name of this communication is peer-to-peer communication. E.g. ***client-server model*** where, every person can, in principle, communicate with one or more other people.

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

Interactive entertainment:

- It is a huge and growing industry.

  e.g. live gaming, live acting, dance, singing, exploration of hidden talents…etc

Electronic commerce:

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books online
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 online
P2P	Peer-to-peer	Music sharing

Mobile Users:

- Mobile computers, such as notebook computers and personal digital assistants (PDAs), are one of the fastest- growing segments of the computer industry.

- Many people love to access office desktop from home even when away from home via PDAs.

- Since having a wired connection is impossible in cars and airplanes, there is a lot of interest in wireless networks.

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

Network Hardware

There is no generally accepted taxonomy into which all computer networks fit, but two dimensions stand out as important:

a. **transmission technology.**
b. **scale**.

Transmission Technology:

Broadly two types.

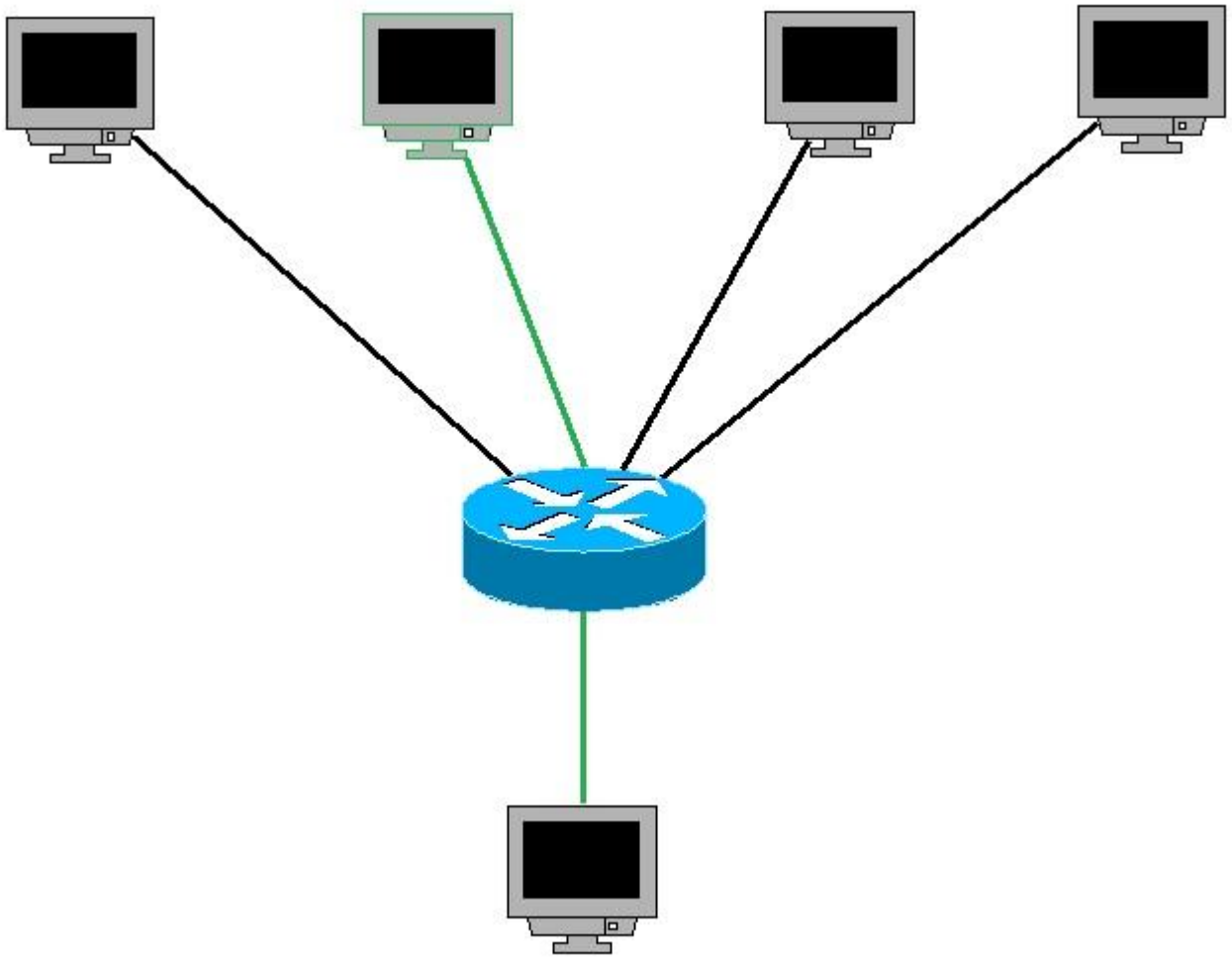
- **Broadcast links.**
- **Point-to-point links.**

Broadcast links:

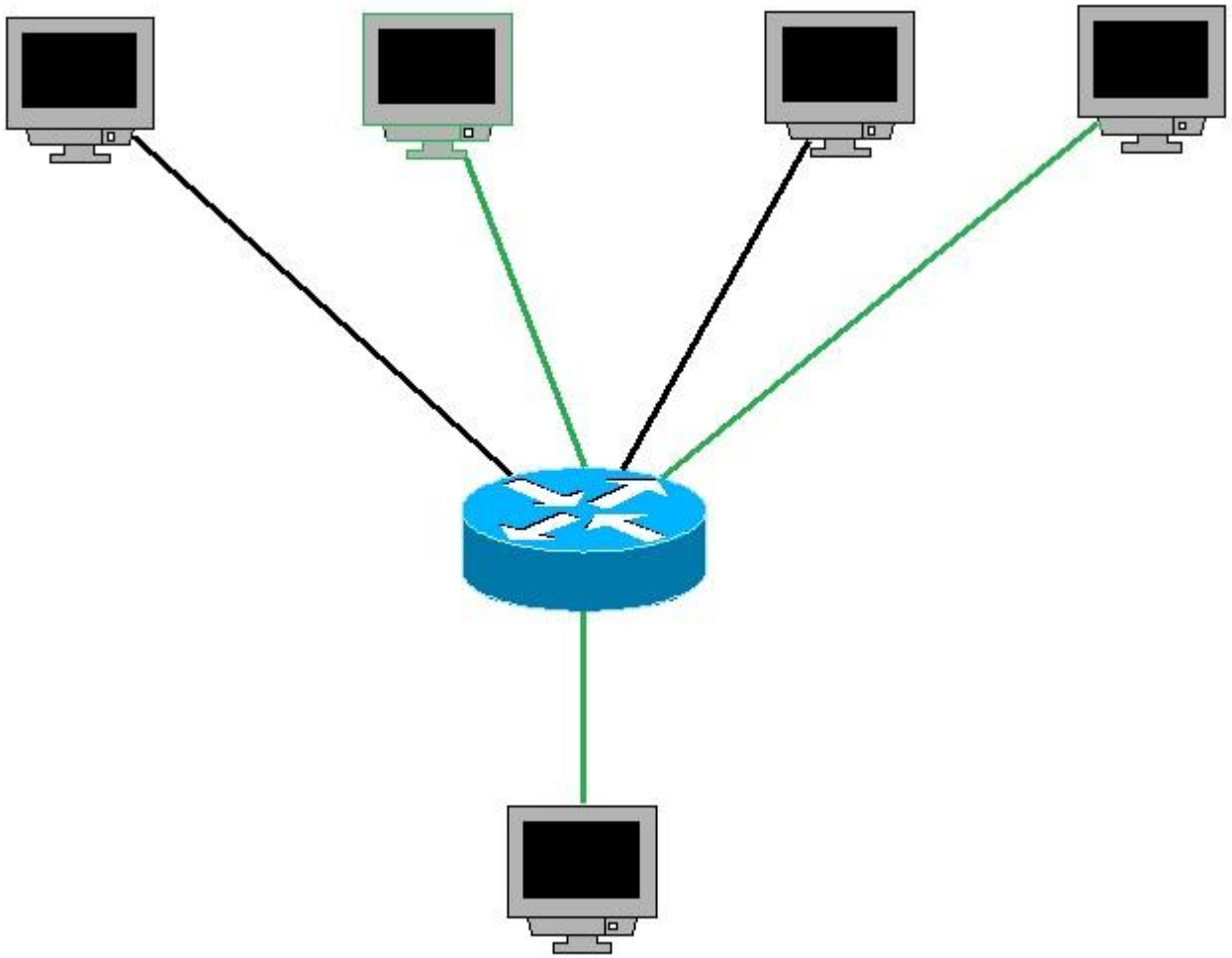
- Broadcast networks have a **single communication channel** that is shared by all the machines on the network.
- Short messages, called packets in certain contexts, sent by any machine are received by all the others. *An address field within the packet* specifies the intended recipient.
- Broadcast systems generally also allow the possibility of addressing a packet to all destinations by using a special code in the address field.
- When a packet with this code is transmitted, it is received and processed by every machine on the network. This ***mode of operation is called broadcasting.***
- Some broadcast systems also support transmission to a subset of the machines, known as ***multicasting.***

Point-to-point:

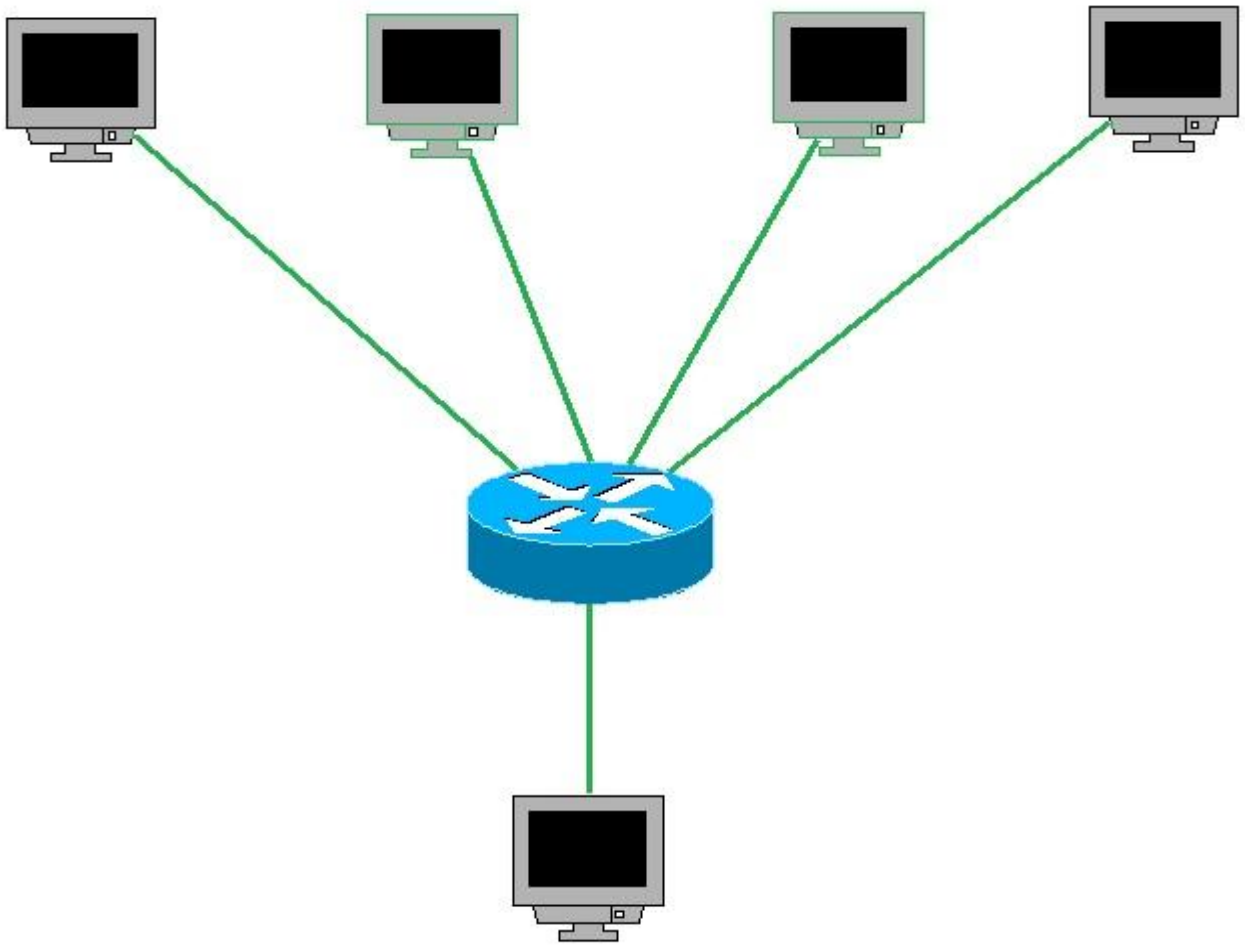
- Connect individual pairs of machines.
- Packets (short messages) may have to visit one or more intermediates machines.
- Multiple routes of different lengths are possible. But finding good ones is important.
- Unicasting – transmission with exactly one sender and exactly one receiver.



Unicast Network



MultiCast Network



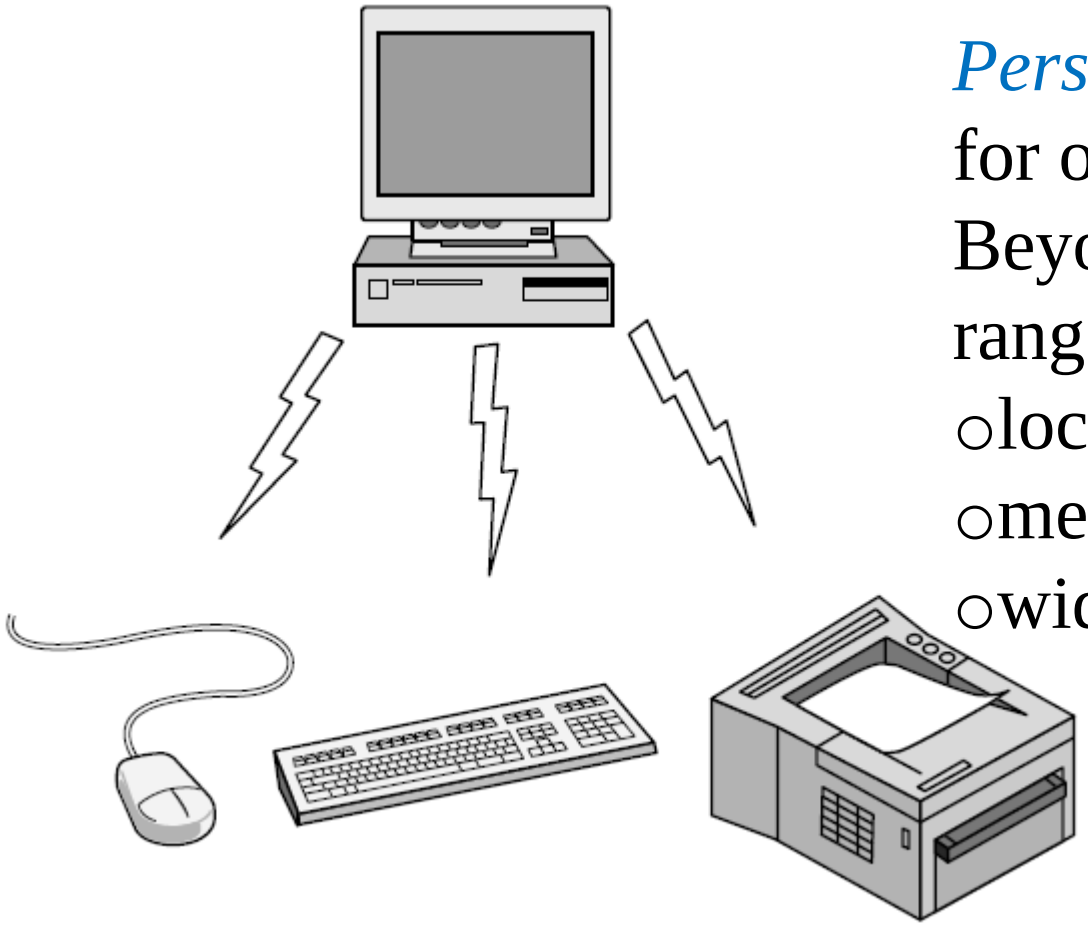
Broadcast Network

Classification by scale

- **Distance is important as a classification metric because different technologies are used at different scales.**

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	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Personal Area Network:



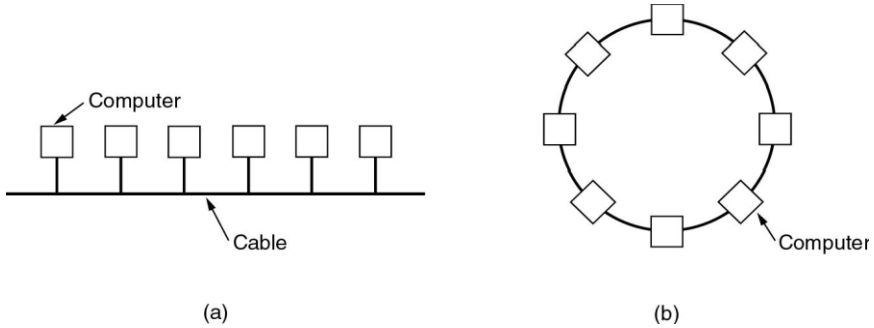
Bluetooth PAN configuration

Personal Area Network: networks that are meant for one person.

Beyond the personal area networks come longer-range networks. These can be divided into

- local
- metropolitan
- wide area networks.

Local Area Networks:



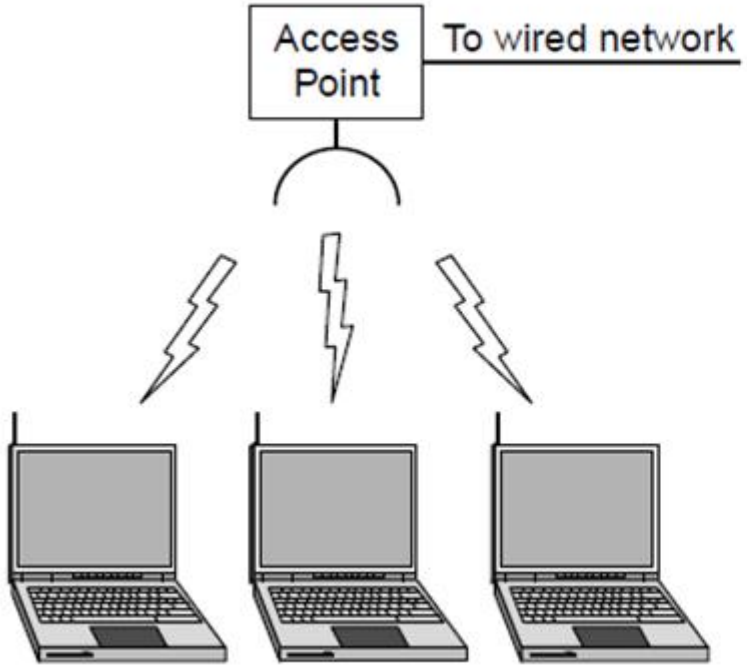
- Two broadcast networks
  - Bus
  - Ring

- LANs are distinguished from other kinds of networks by three characteristics:
  (1) their size,
  (2) their transmission technology
  (3) their topology.

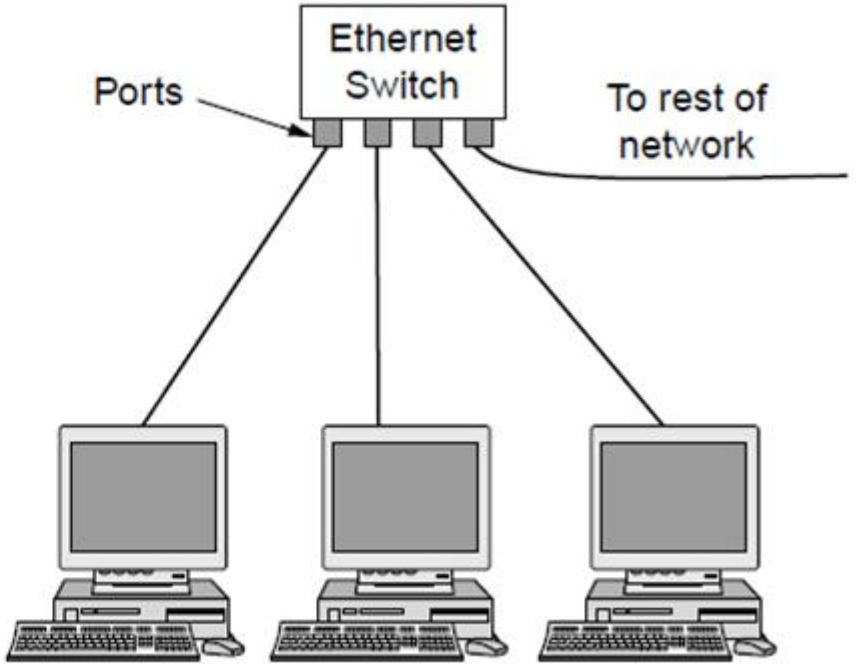
- Privately-owned networks within a single building or campus of up to a few kilometers in size.

- They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.

Cont…



(a) Wireless (802.11)



(b) wired LANs (Switched Ethernet.)

Switched Ethernet:

- **Switch; Hardware that connects two devices point-to-point**
- **A Switch has multiple ports**

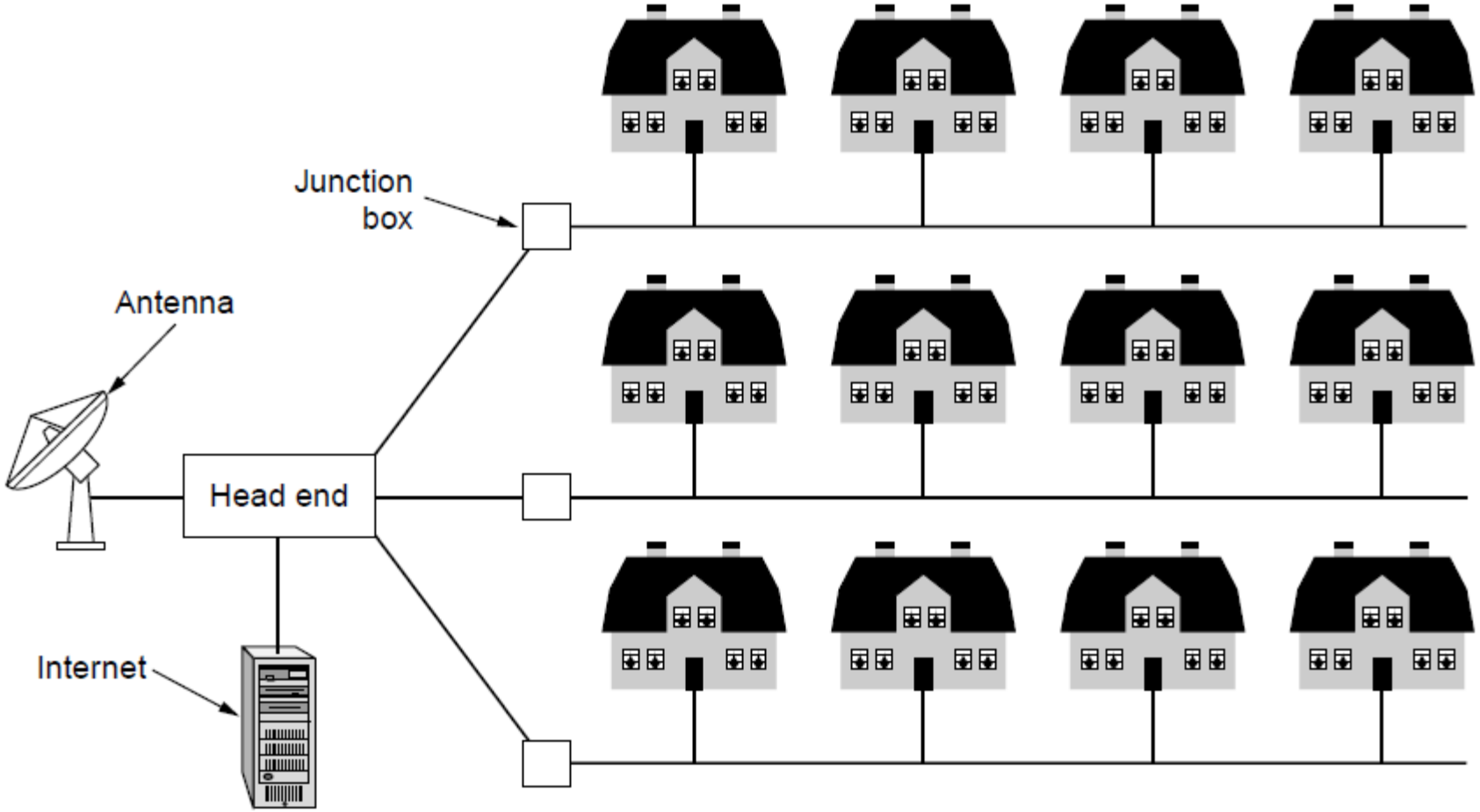
- Broadcast networks can be further divided into **static and dynamic**, depending on how the channel is allocated.

- **A typical static allocation** would be to divide time into discrete intervals and use a round-robin algorithm, allowing each machine to broadcast only when its time slot comes up.

- **Static allocation wastes channel capacity** when a machine has nothing to say during its allocated slot, so most systems attempt to allocate the channel dynamically (i.e., on demand).

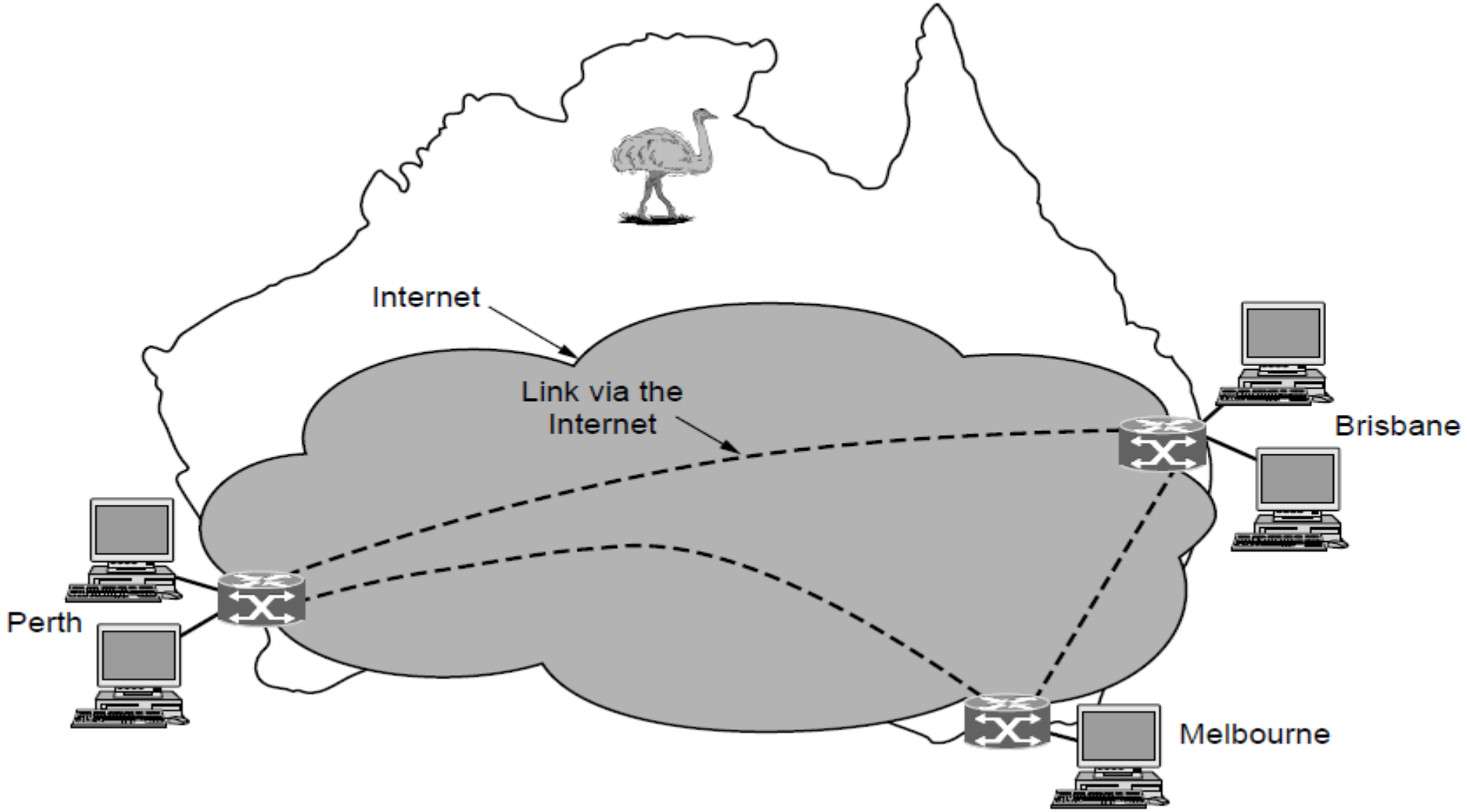
Metropolitan Area Networks (MAN):

- A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the **cable television network** available in many cities.



Wide Area Networks (WAN):

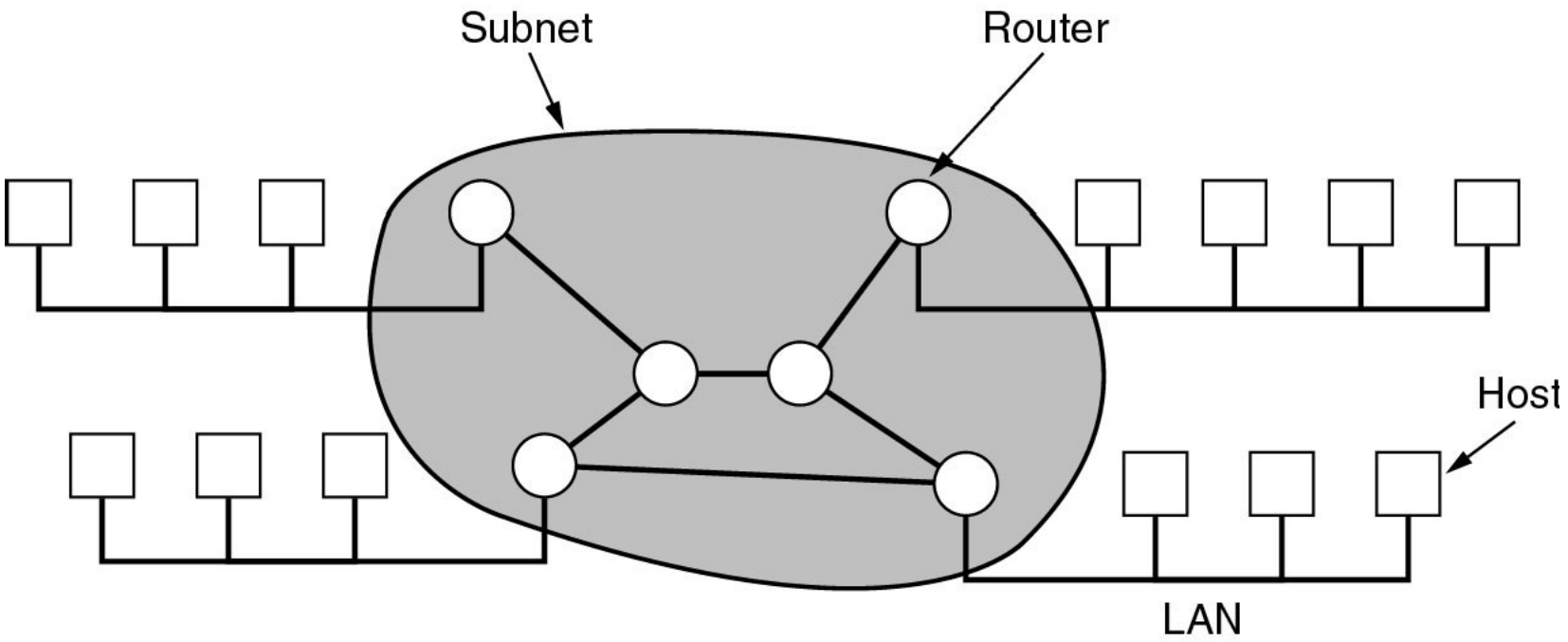
- A wide area network, or WAN, spans a large geographical area, a country or continent.



- It contains a collection of machines intended for running user (i.e., application) programs and call these machines hosts.

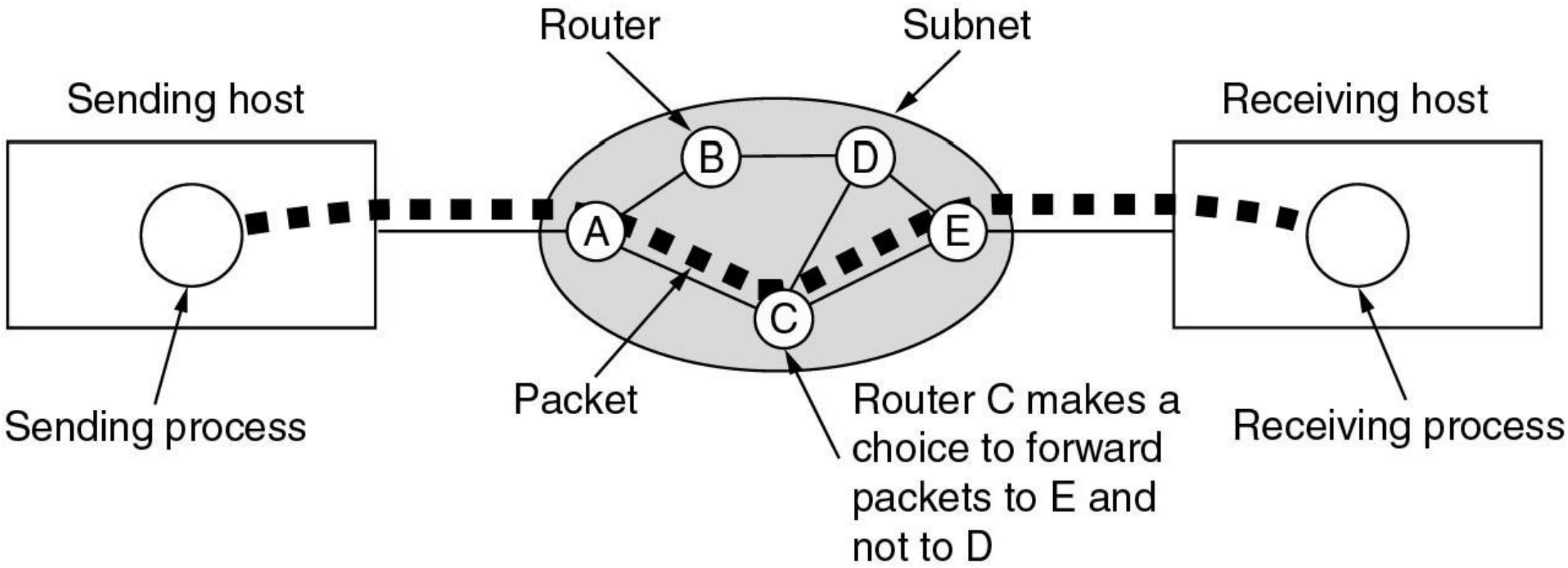
- The hosts are connected by a communication subnet, or just subnet for short. **The hosts are owned by the customers** (e.g., people's personal computers)

- The communication subnet is typically owned and operated by a telephone company or Internet service provider.



- In most wide area networks, the subnet consists of two distinct components: **transmission lines and switching elements.**

- The job of the subnet is to carry messages from host to host.



Wireless Networks:

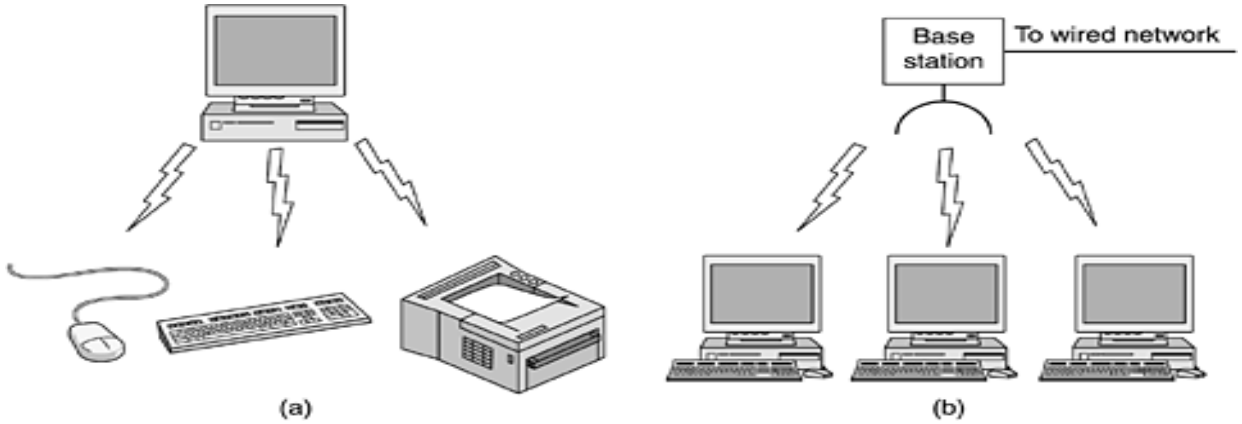
wireless networks can be divided into **three main categories**:

- ***System interconnection.***
- ***Wireless LANs.***
- ***Wireless WANs.***

System interconnection: It is all about interconnecting the components of a computer using short-range radio.

Wireless LANs: These are systems in which every computer has a radio modem and antenna with which it can communicate with other systems.

(a) Bluetooth configuration. (b) Wireless LAN.



Wireless WANs : The radio network used for cellular telephones is an example of a low-bandwidth wireless system.

Home Networks:

- This kind of network though properly not categorized under computer network but looking at the current technology (i.e. IoT and smart homes) it is possible to establish such type of network.

- The fundamental idea is that in the future most homes will be set up for networking. ***Every device in the home will be capable of communicating with every other device, and all of them will be accessible over the Internet.***

- Some of the categories (with examples) are as follows:

    - Computers (desktop PC, notebook PC, PDA, shared peripherals).
    - Entertainment (TV, DVD, VCR, camcorder, camera, stereo, MP3).
    - Telecommunications (telephone, mobile telephone, intercom, fax).
    - Appliances (microwave, refrigerator, clock, furnace, AC, lights).
    - Telemetry (utility meter, smoke/burglar alarm, thermostat, baby cam).

Internetworks:

1. ***A collection of interconnected networks is called an internetwork or internet.***

2. ***A common form of internet is a collection of LANs connected by a WAN.***

3. ***Subnets, networks, and internetworks are often confused.***

   - subnet makes the most sense in the context of a wide area network, where it refers to the collection of routers and communication lines owned by the network operator.
   - The combination of a subnet and its hosts forms a network.
   - An internetwork is formed when distinct networks are interconnected.

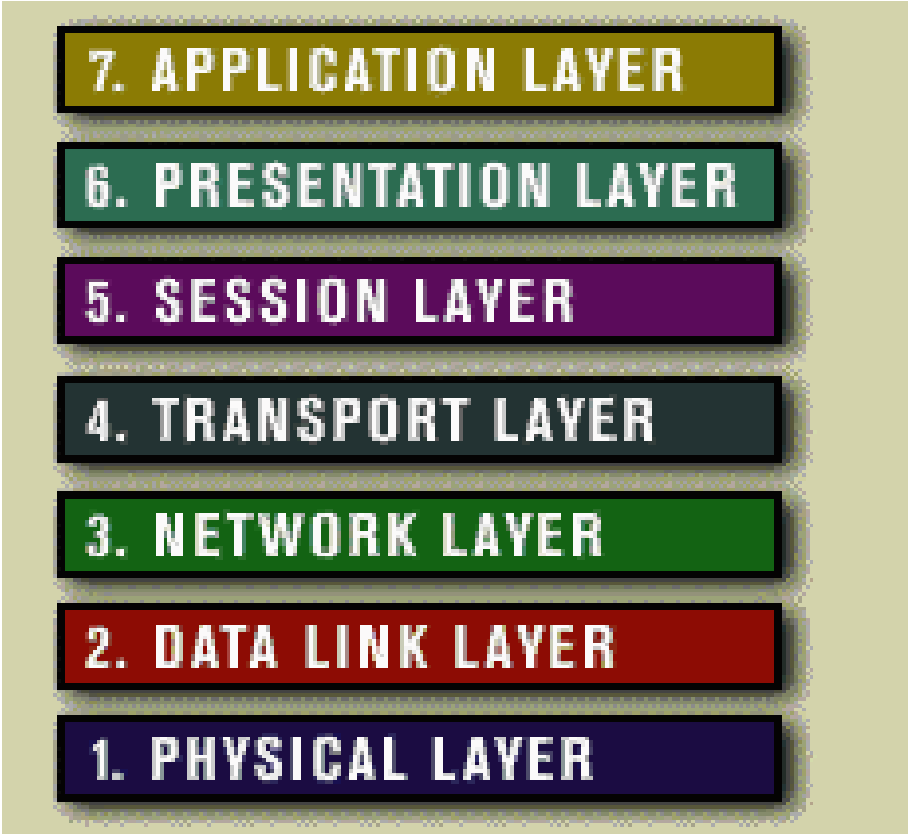
Network Software:

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

Protocol Hierarchies:

- ***A protocol*** *is a standard set of rules that allow electronic devices to communicate with each other. More precisely, It is an agreement between the communicating parties on how communication is to proceed.*

- To reduce the design complexity, most **networks are organized as a stack of layers** or levels. E.g. *OSI-7-Layer model*.



- *The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.*

- *The purpose of each layer is to offer certain services to the higher layers and concerned about how the offered services are actually implemented.*

- Layer n on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are collectively known as the ***layer n protocol.***

- Violating the protocol will make communication more difficult.

❑***OSI (Open Systems Interconnection) reference model.***

❑***TCP/IP (Transmission Control Protocol/Internet Protocol) reference model.***

- The OSI model is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology.

- *The **OSI Model** is a conceptual framework used to describe the functions of a networking system.*

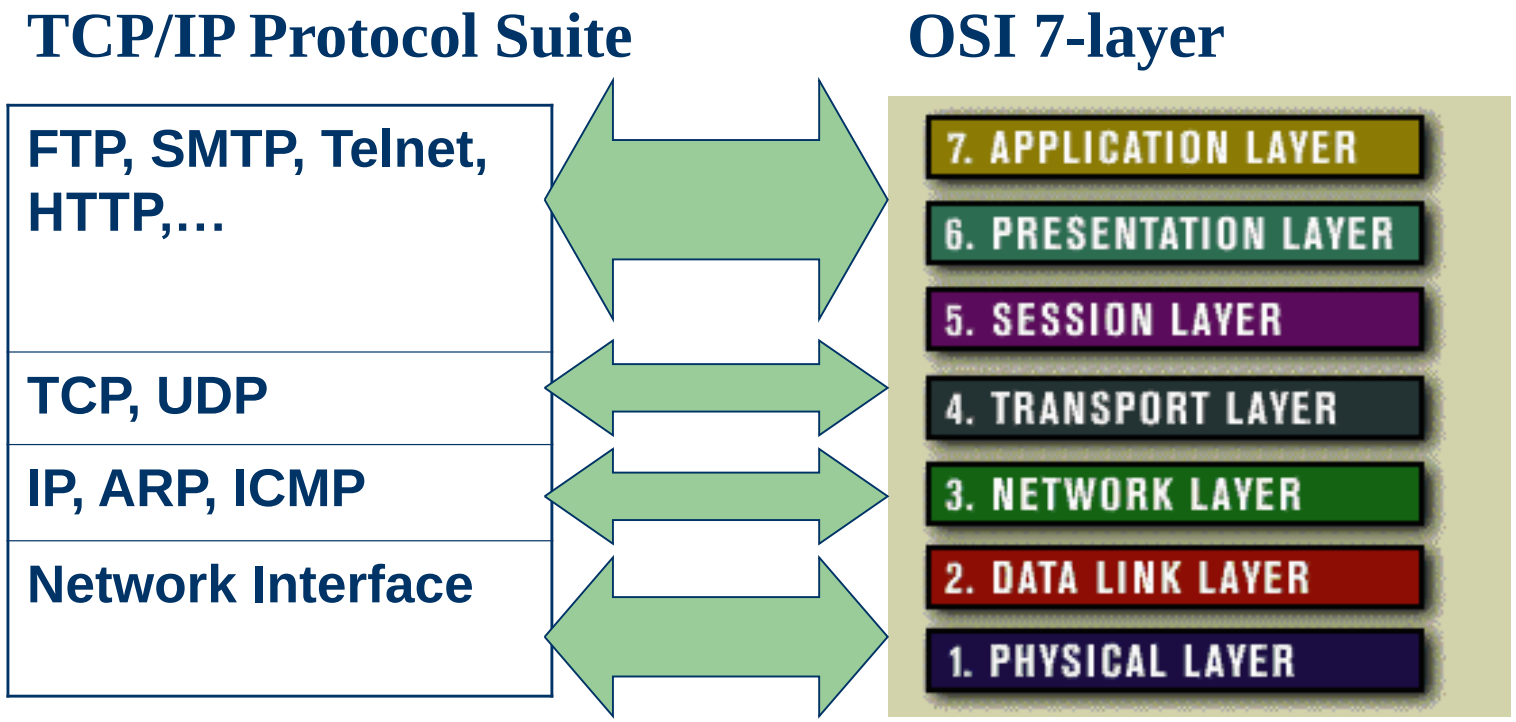
- ***TCP/IP Model** is a suite of communication protocols used to interconnect network devices on the internet.*

Why TCP/IP is so popular?

- **TCP/IP was developed very early**
- **Technologies were widely discussed and circulated in documents called "Request for Comments" (RFC) – free of charge**

TCP/IP Model

- **Because TCP/IP was developed earlier than the OSI 7-layer mode, it does not have 7 layers but only 4 layers**



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 prtocols fit perfectly.

Application layer protocols: It defines the rules when implementing specific network applications.

- 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

- **TCP/IP is built on "connectionless" technology, each datagram finds its own way to its destination**

Transport Layer protocols: **It defines the rules of**

- **Dividing a chunk of data into segments**
- **Reassemble segments into the original chunk**

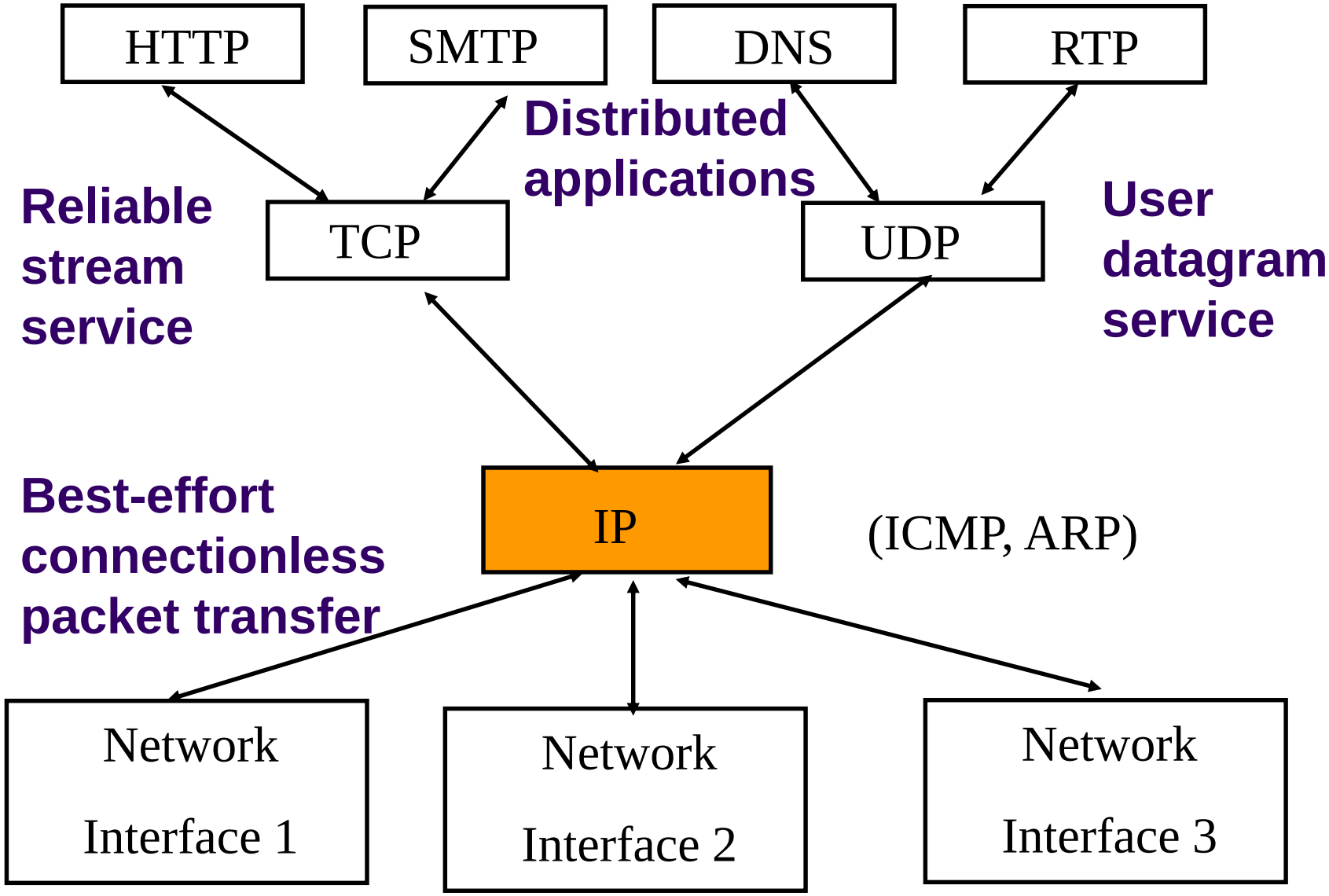
- **Typical protocols:**
  - **TCP – Transmission Control Protocol**
    - **Provide further the functions such as reordering and data resend**
  - **UDP – User Datagram Service**
    - **Use when the message to be sent fit exactly into a datagram**
    - **Use also when a more simplified data format is required**

Network layer protocols:

It defines the rules of how to find the routes for a packet to the destination.

- It only gives best effort delivery. Packets can be delayed, corrupted, lost, duplicated, out-of-order
-
- Typical protocols:
  - IP – Internet Protocol
    - Provide packet delivery
  - ARP – Address Resolution Protocol
    - Define the procedures of network address / MAC address translation
  - ICMP – Internet Control Message Protocol
    - Define the procedures of error message transfer

TCP/IP Protocol Suite

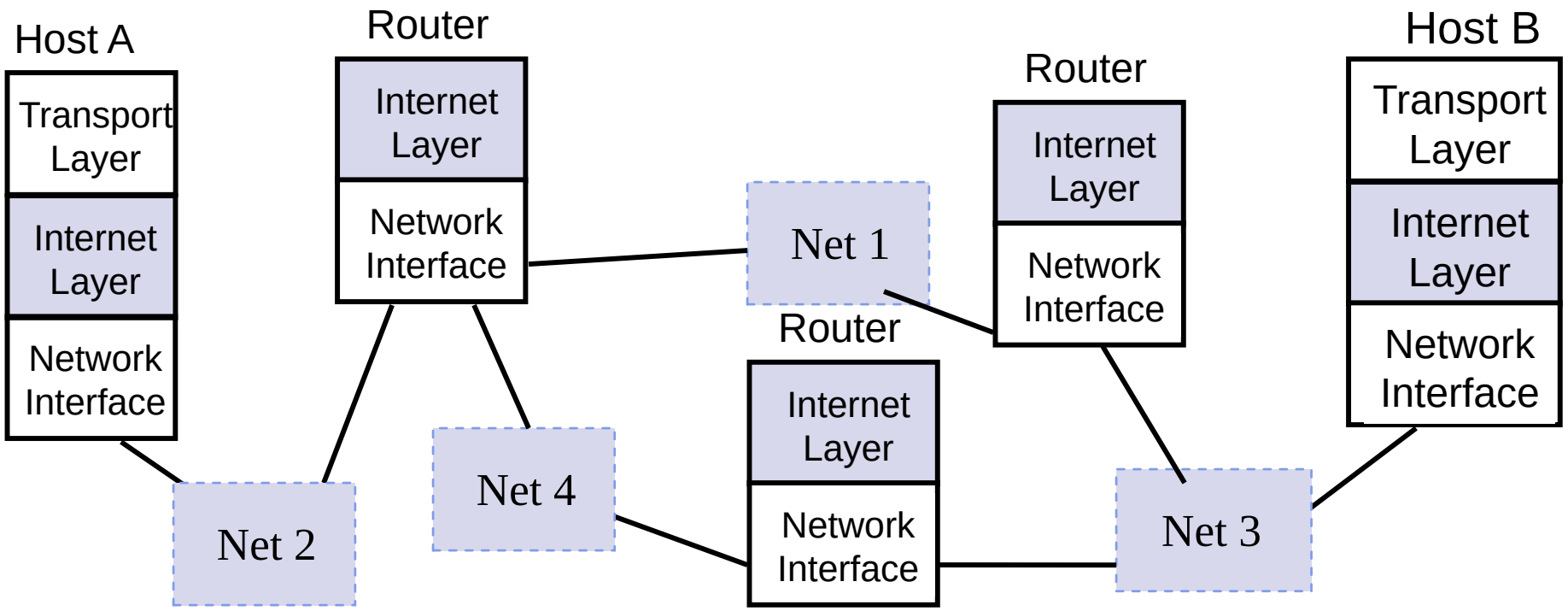


Internet Protocol Approach

- IP packets transfer information across Internet

  Host A IP → router→ router…→ router→ Host B IP

- IP layer in each router determines next hop (router)
- Network interfaces transfer IP packets across networks



- The entities comprising the corresponding layers on different machines are called **peers.**

- *The peers may be processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol.*

- *In reality, no data are directly transferred from layer n on one machine to layer n on another machine. Instead, 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.

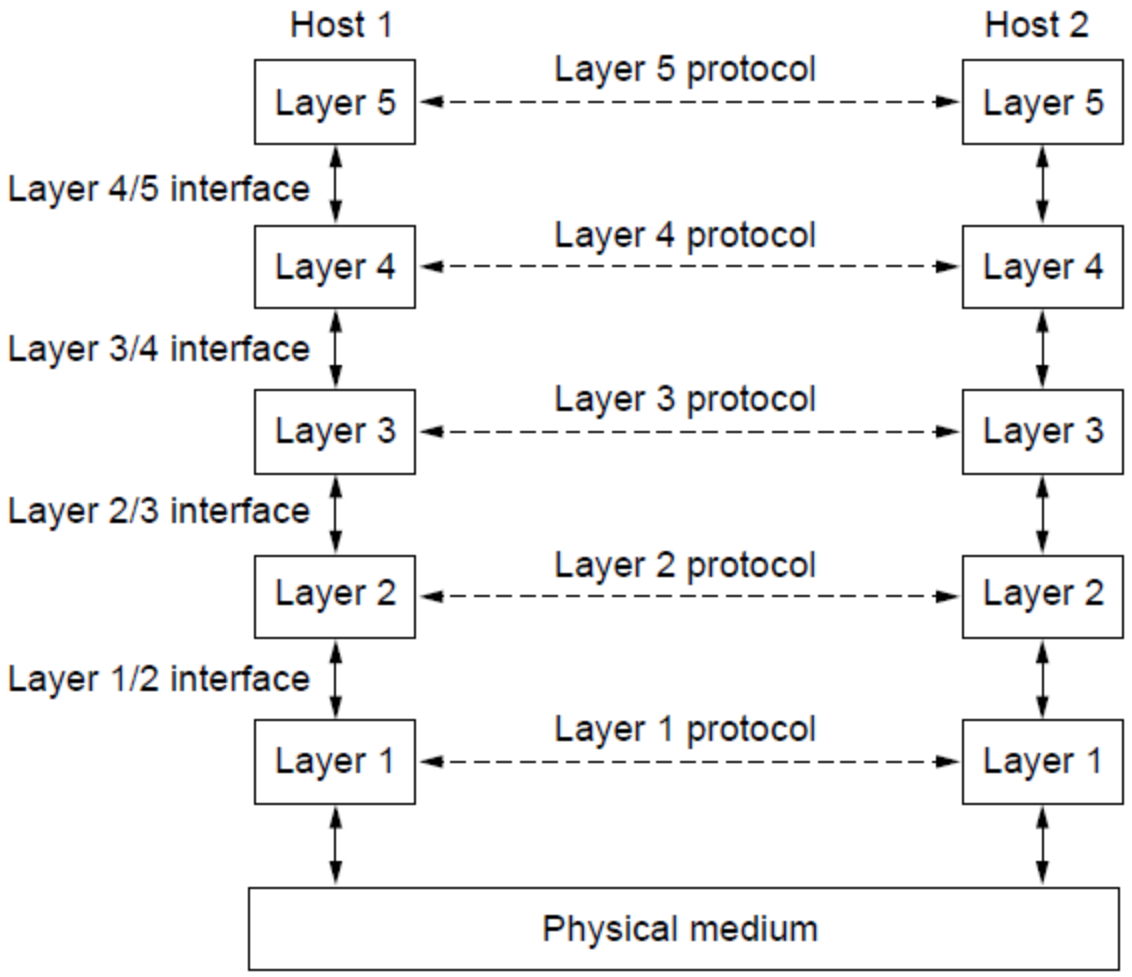
- Between each pair of adjacent layers is an interface. The interface defines which primitive operations and services the lower layer makes available to the upper one.

- **A set of layers and protocols is called a network architecture.** The specification of an architecture must contain enough information to allow an implementer to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol.

- A list of protocols used by a certain system, one protocol per layer, is called a ***protocol stack.***

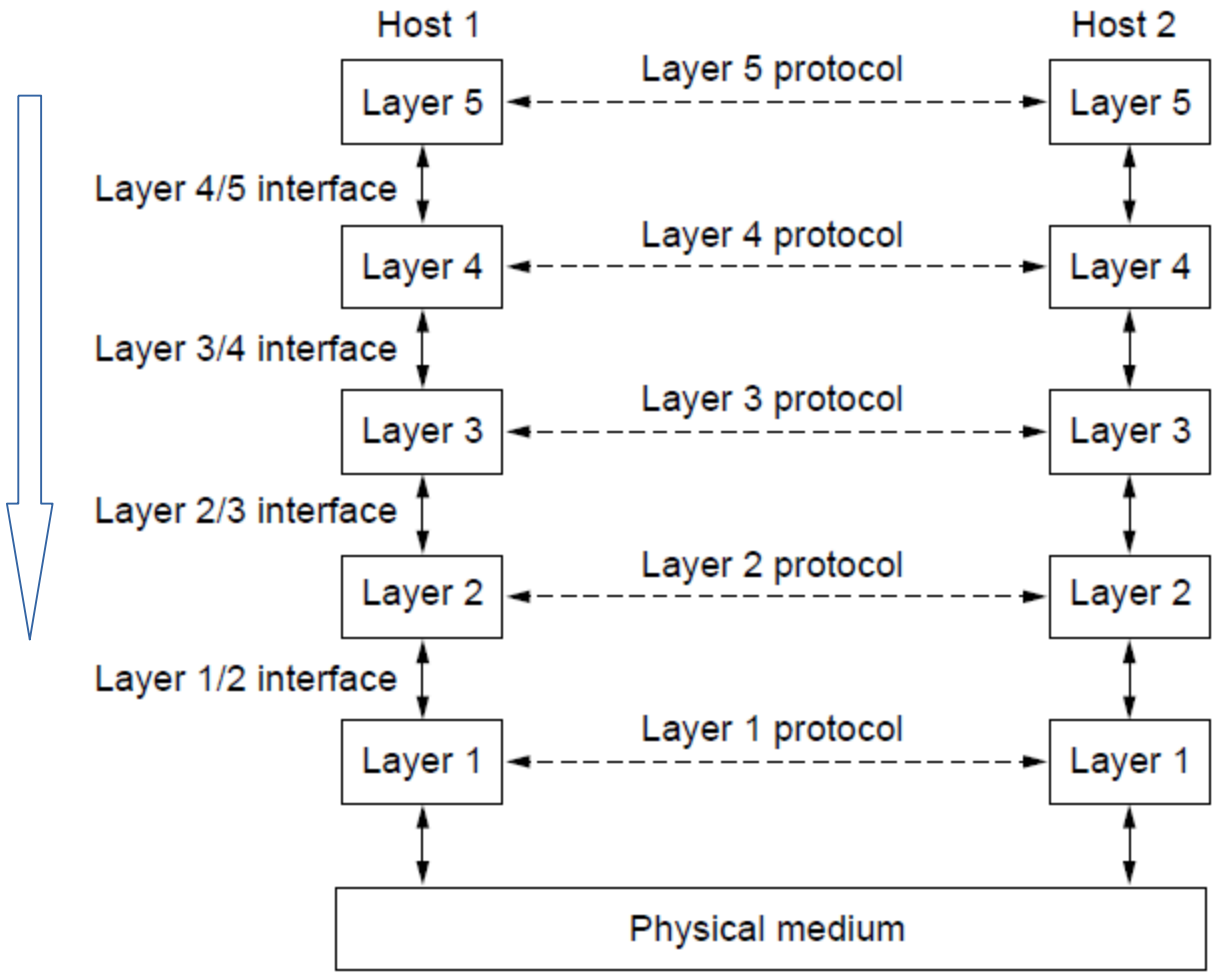
- Virtual communication is shown by dotted lines and physical communication by solid lines in the example below.

Protocol Hierarchies



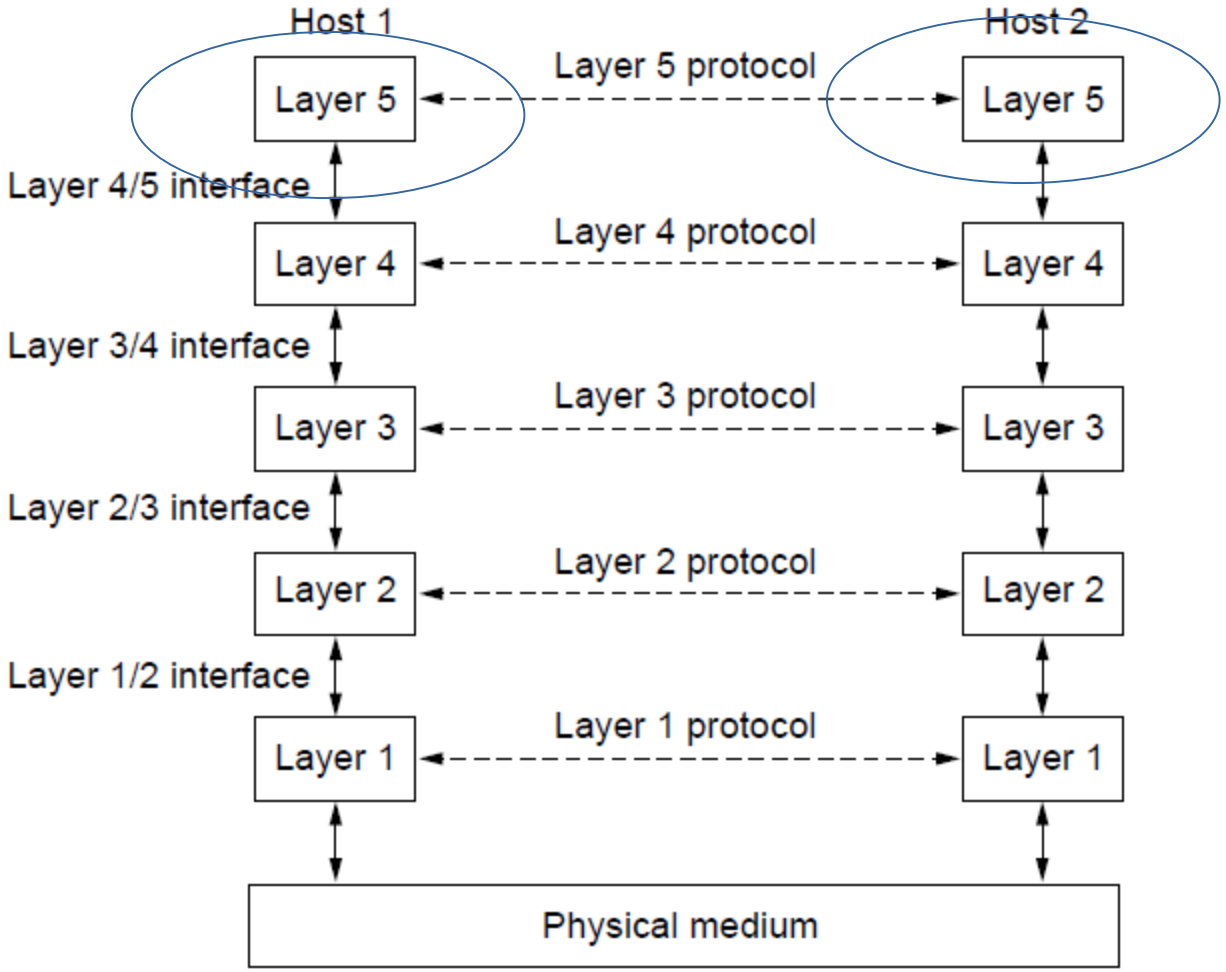
Layers, protocols, and interfaces.

Protocol Hierarchies



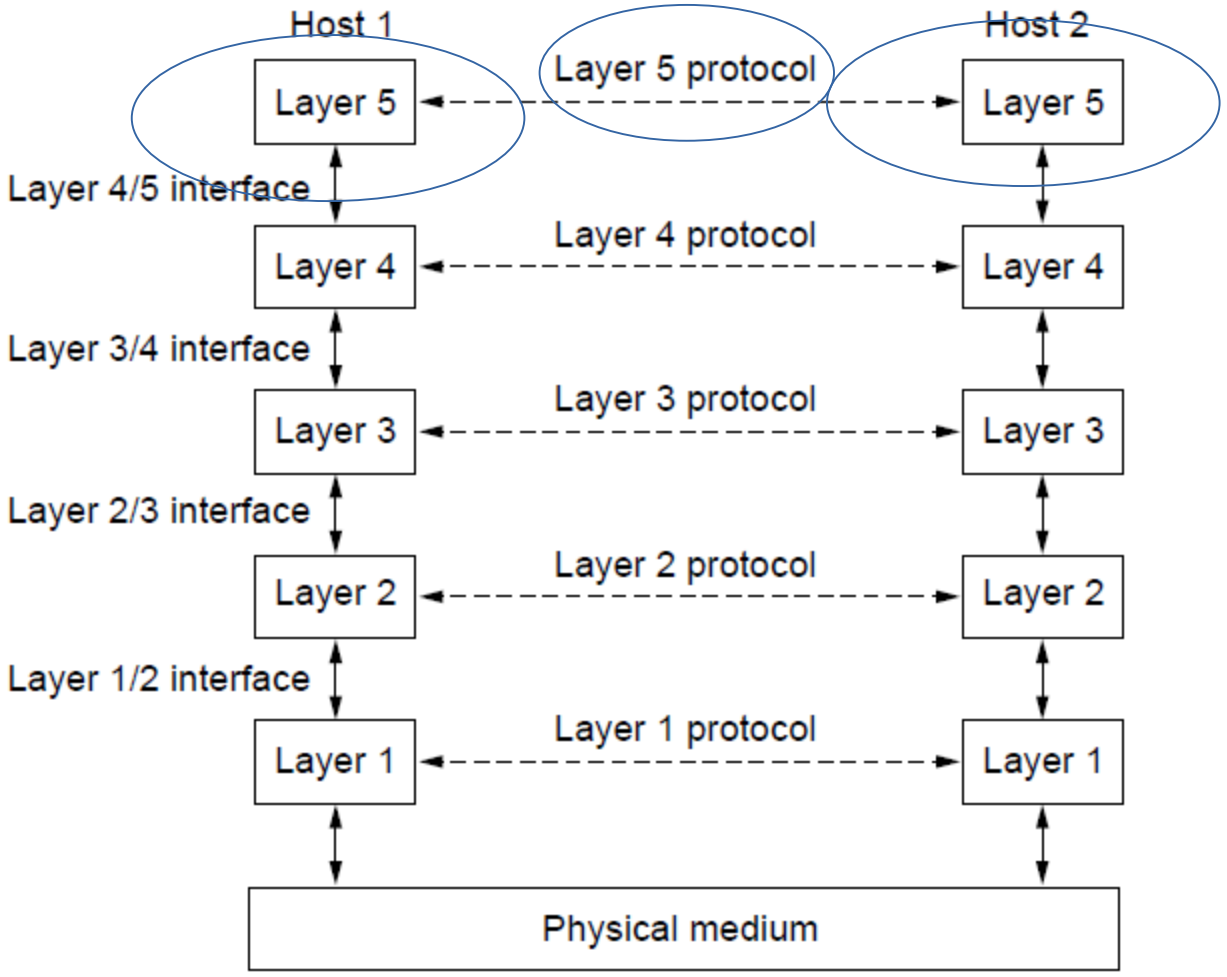
Layers, protocols, and interfaces.

Protocol Hierarchies



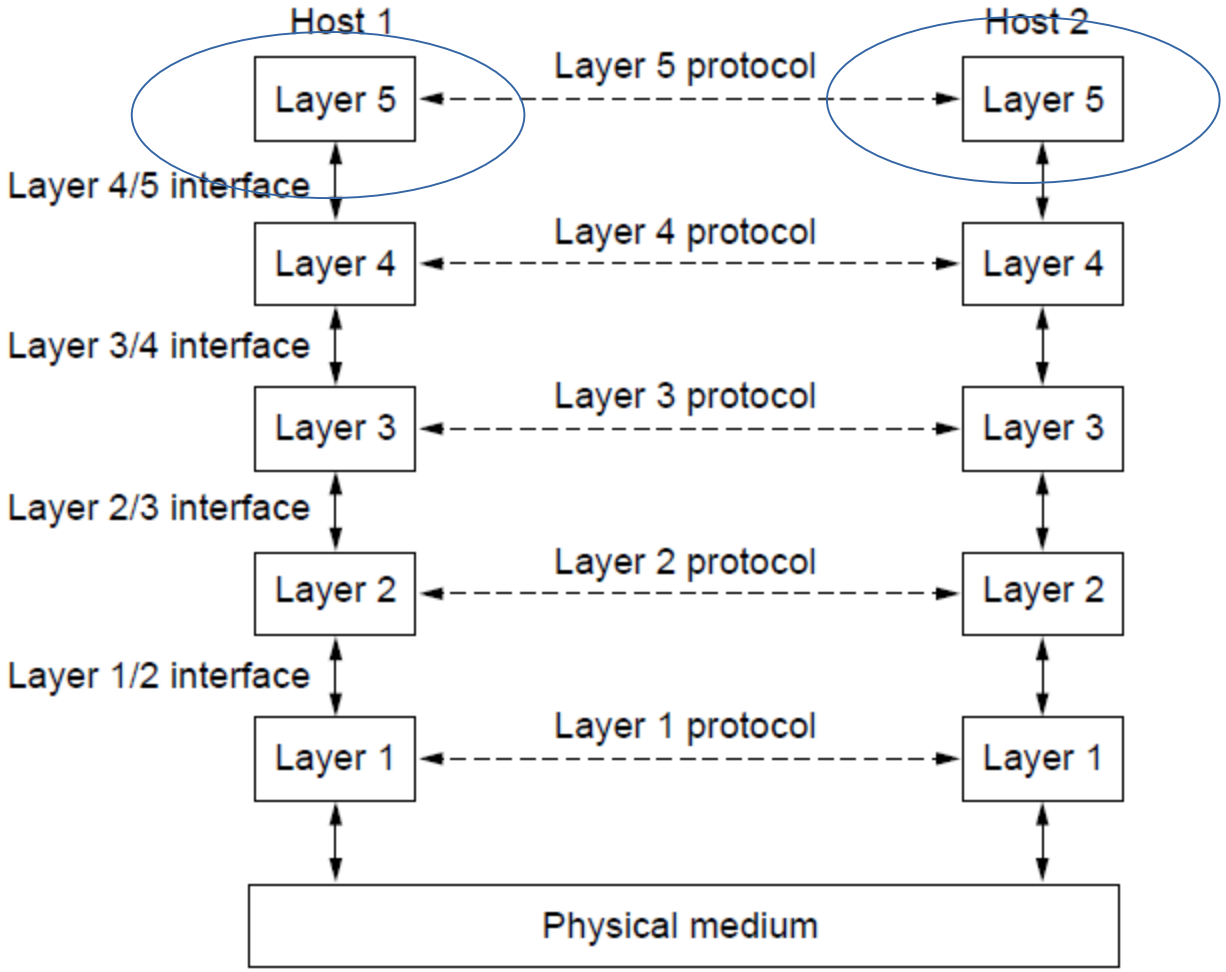
Layers, protocols, and interfaces.

Protocol Hierarchies



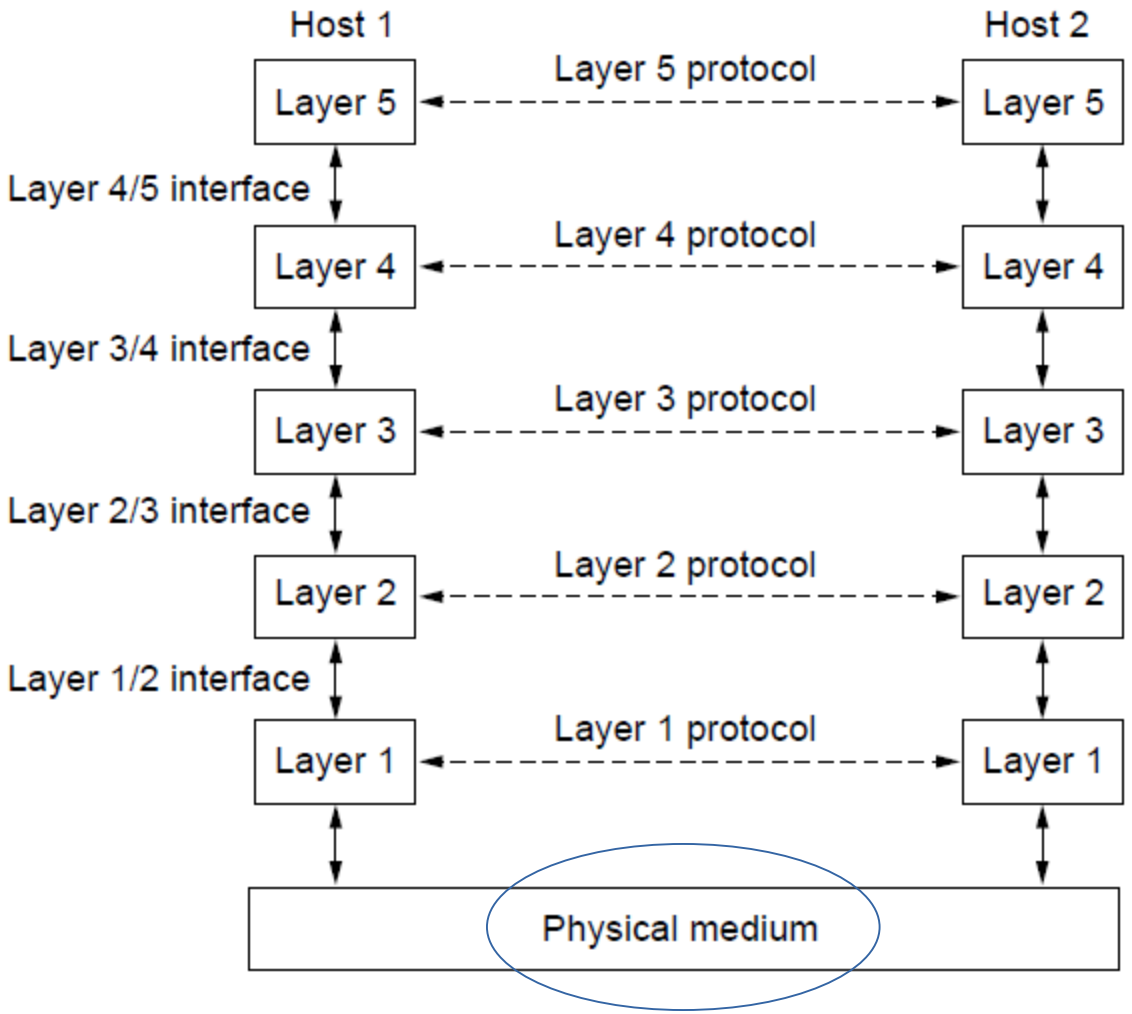
Layers, protocols, and interfaces.

Protocol Hierarchies



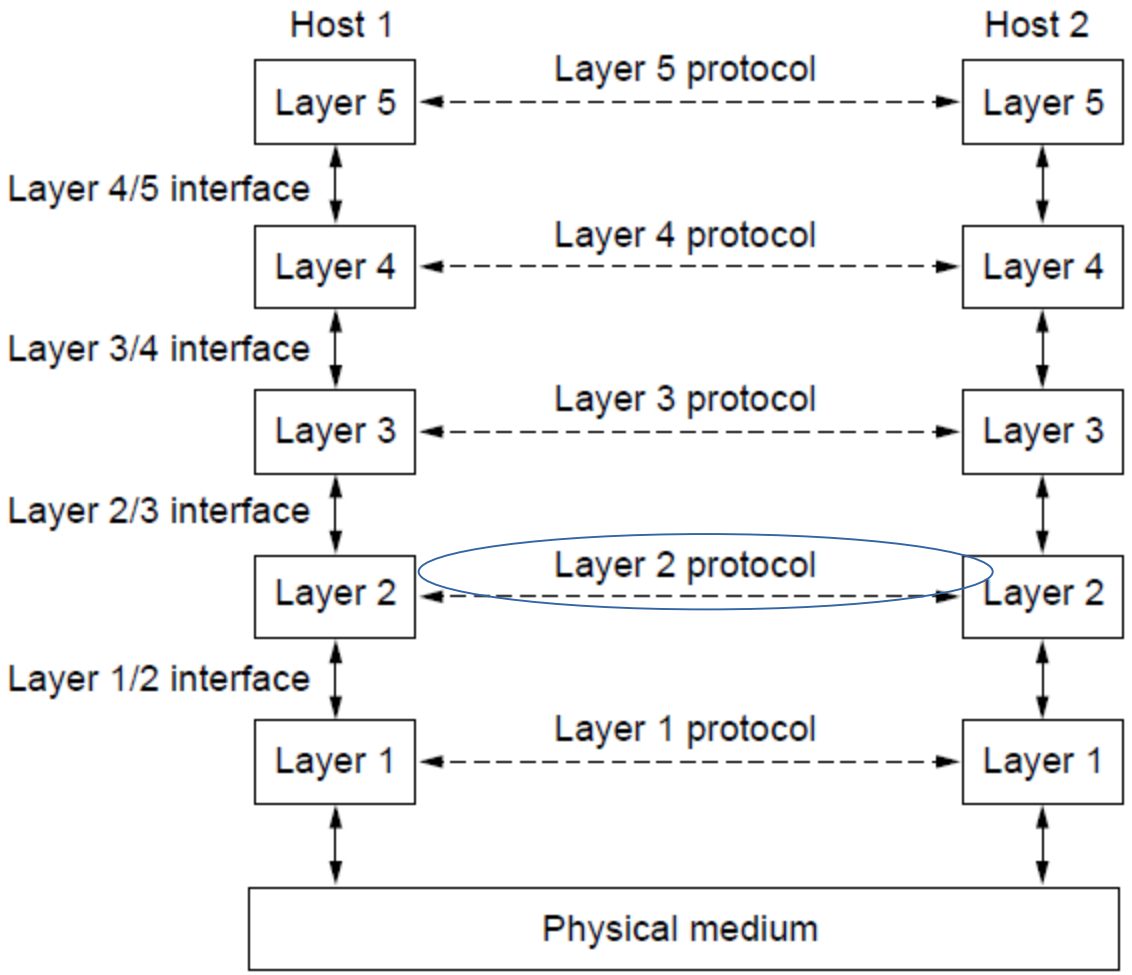
Layers, protocols, and interfaces.

Protocol Hierarchies



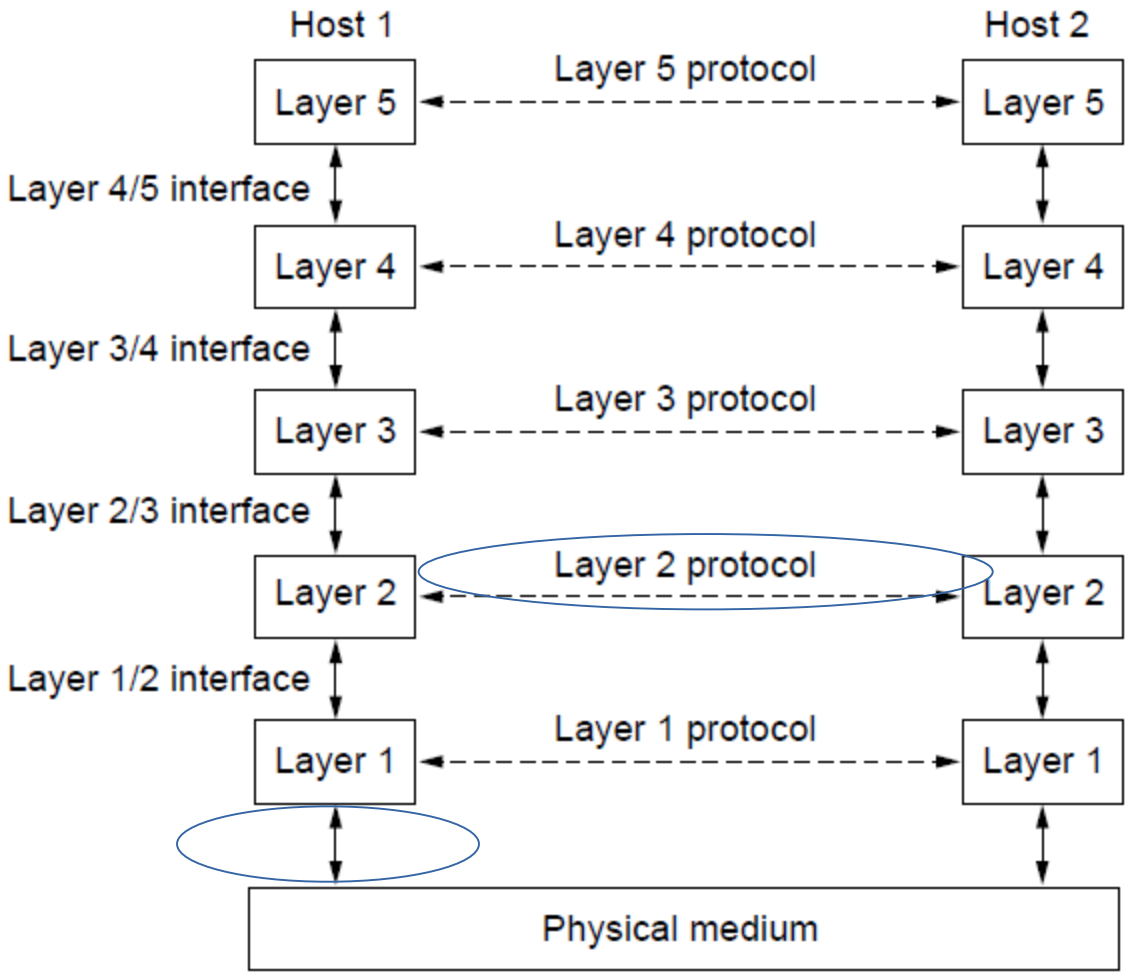
Layers, protocols, and interfaces.

Protocol Hierarchies



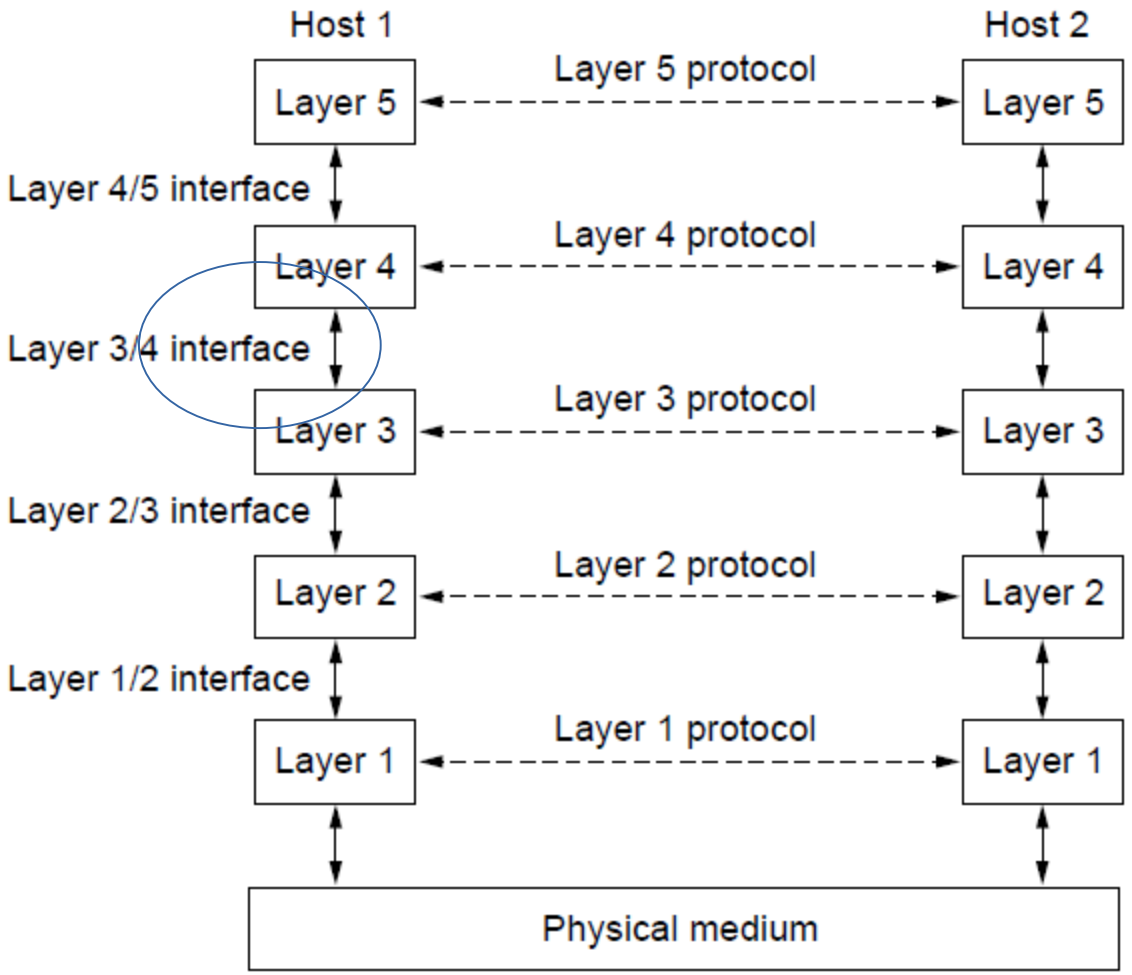
Layers, protocols, and interfaces.

Protocol Hierarchies



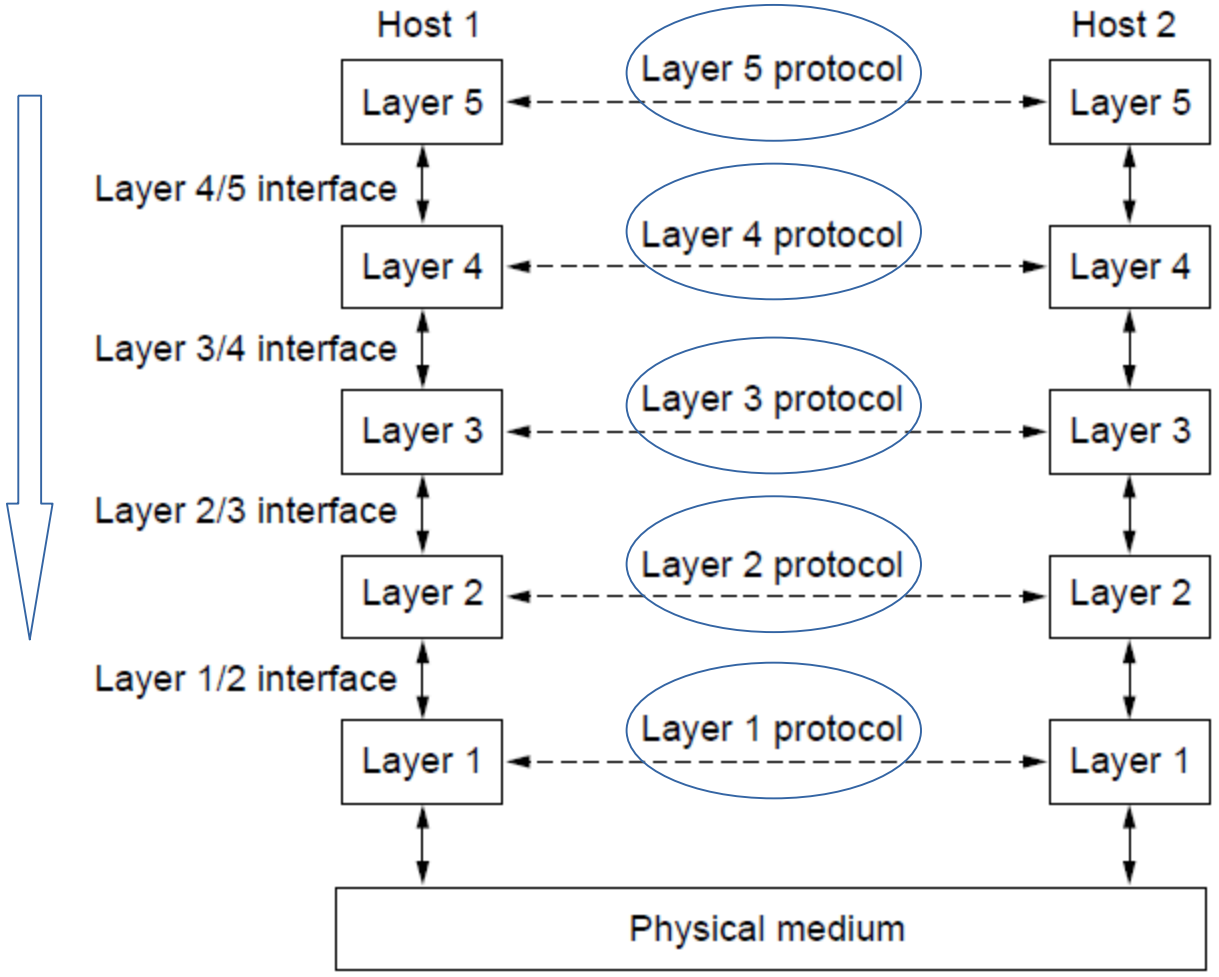
Layers, protocols, and interfaces.

Protocol Hierarchies



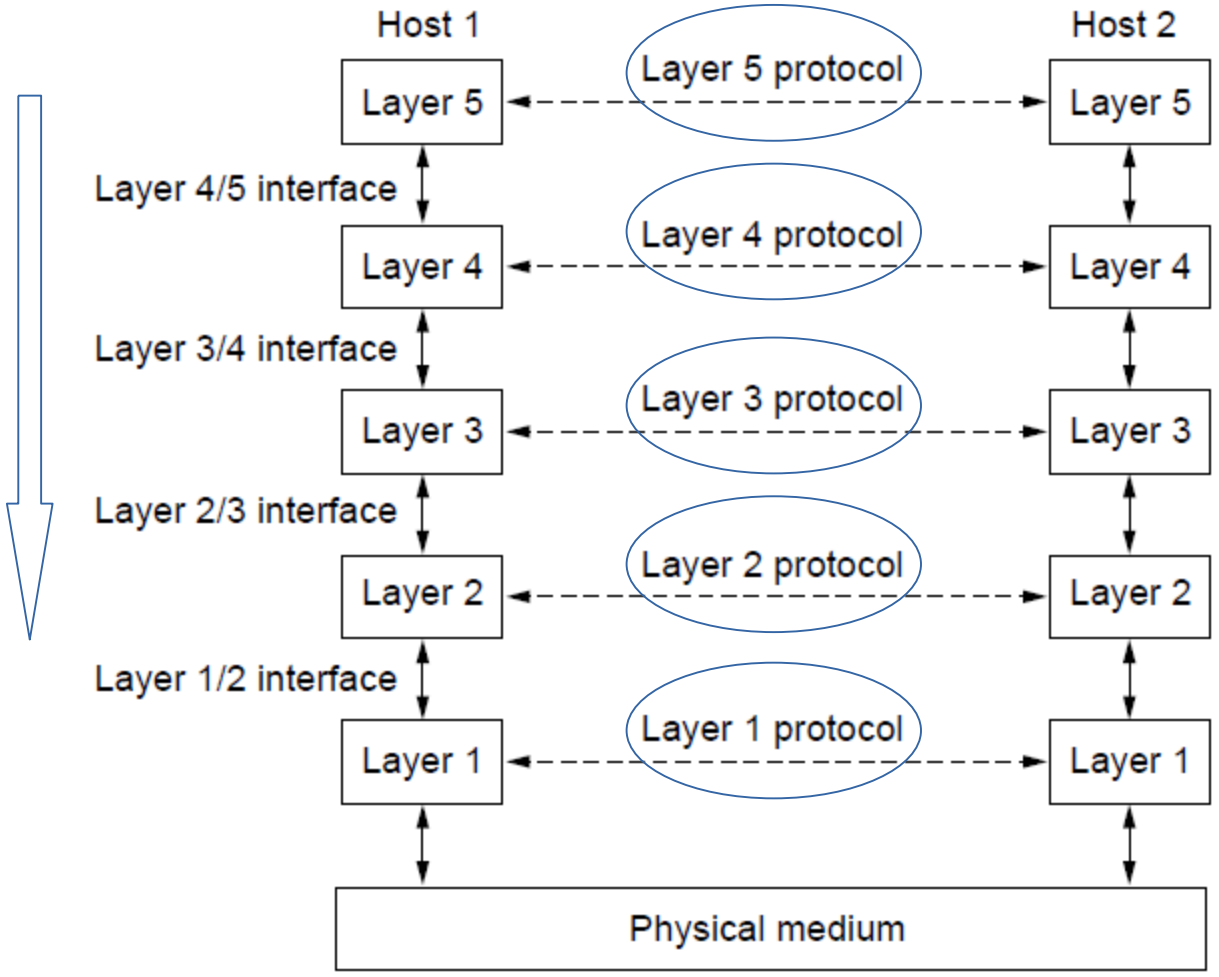
Layers, protocols, and interfaces.

Protocol Hierarchies



Layers, protocols, and interfaces.

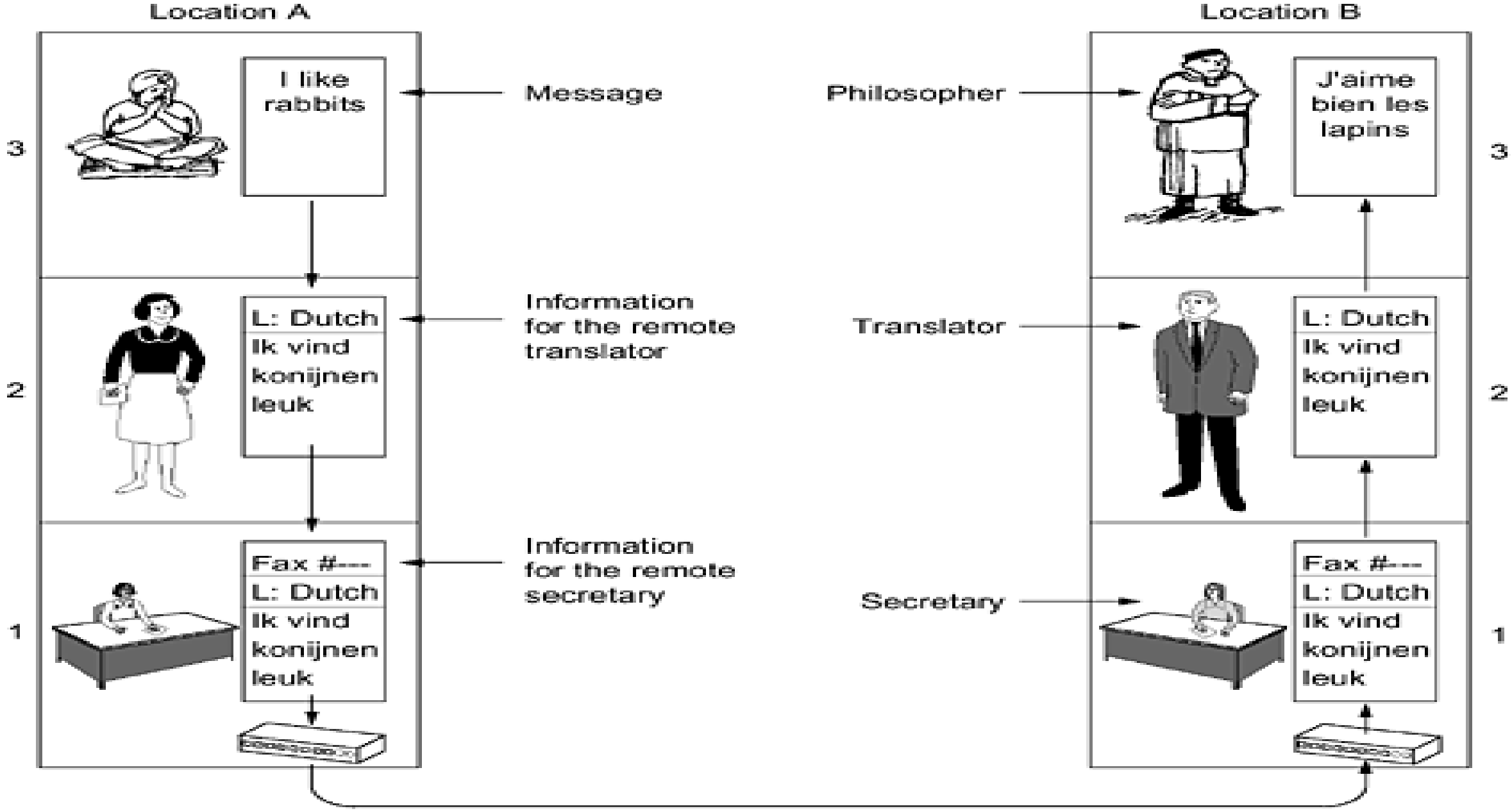
Protocol Hierarchies



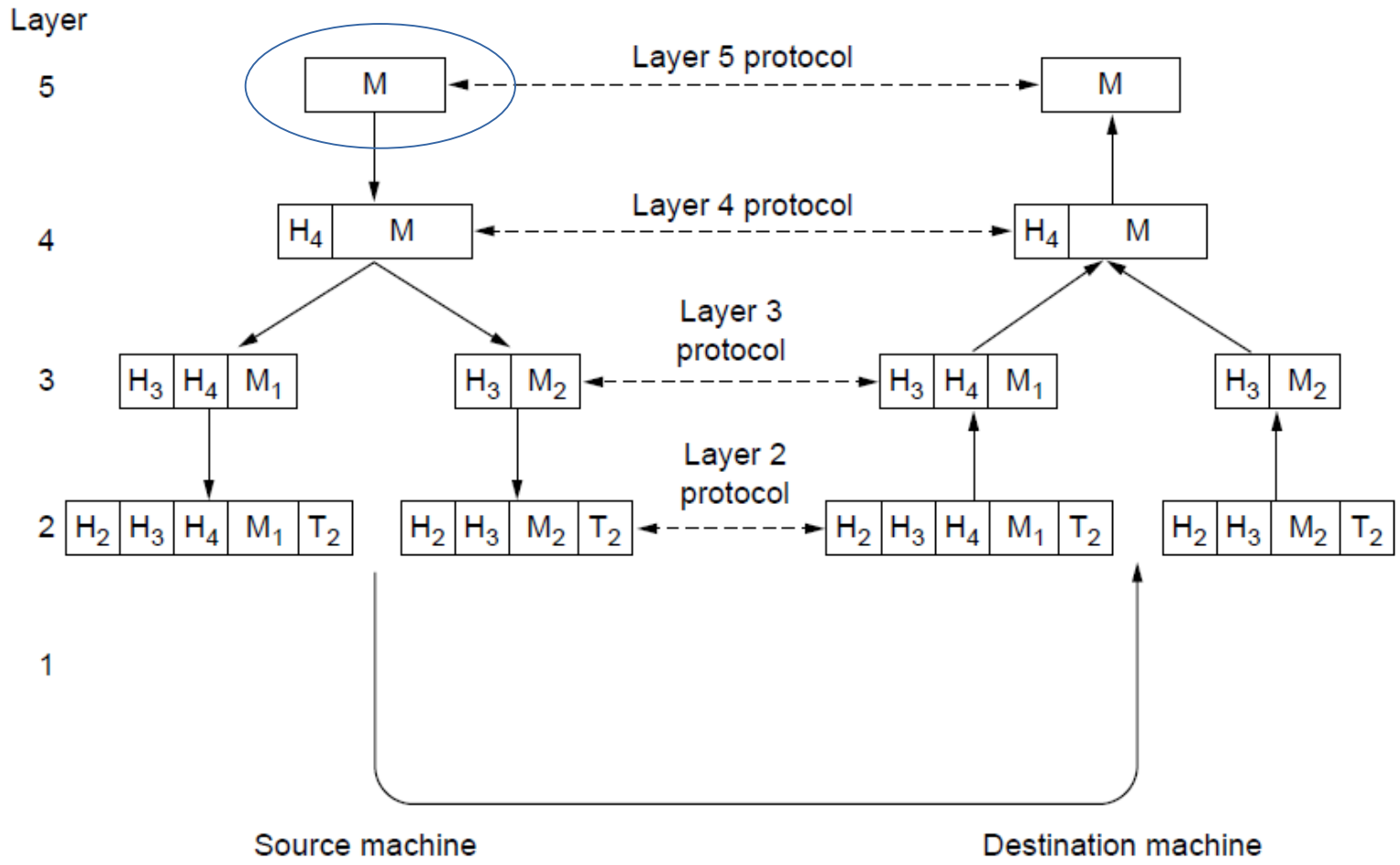
Network Architecture

Layers, protocols, and interfaces.

- **Idea of multilayer communication: The philosopher-translator-secretary architecture**

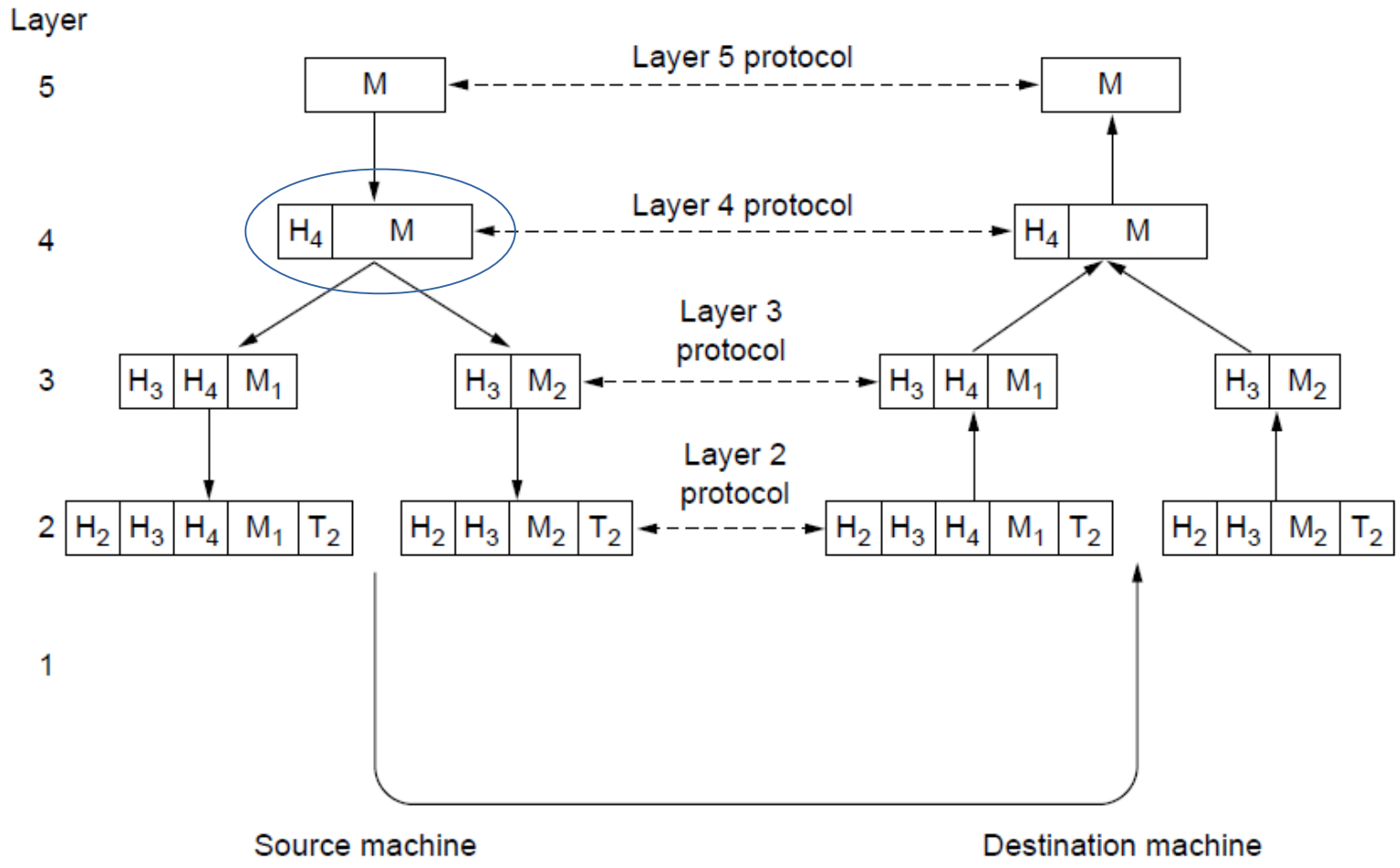


Protocol Hierarchies:



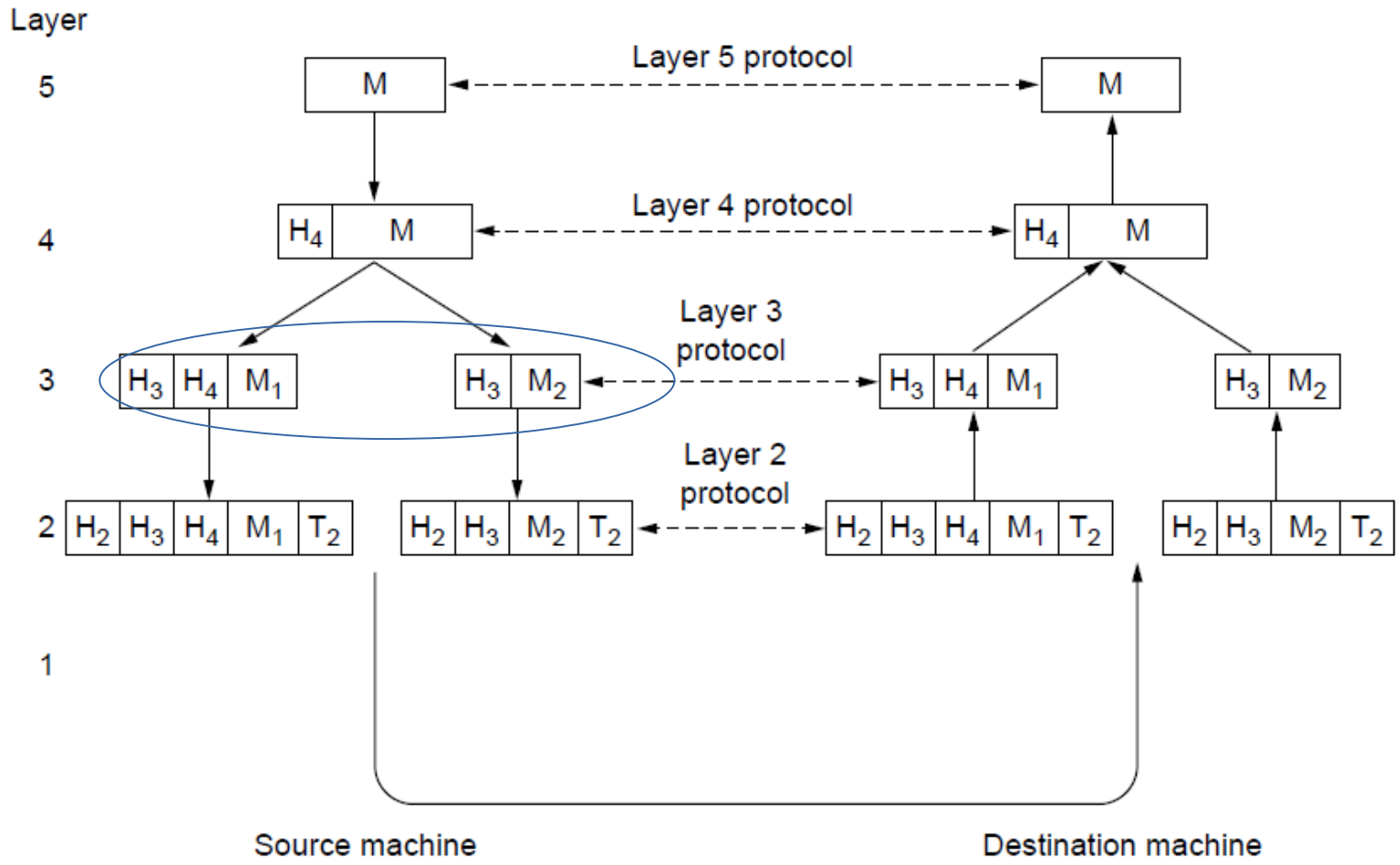
Example information flow supporting virtual communication in layer 5.

Protocol Hierarchies:



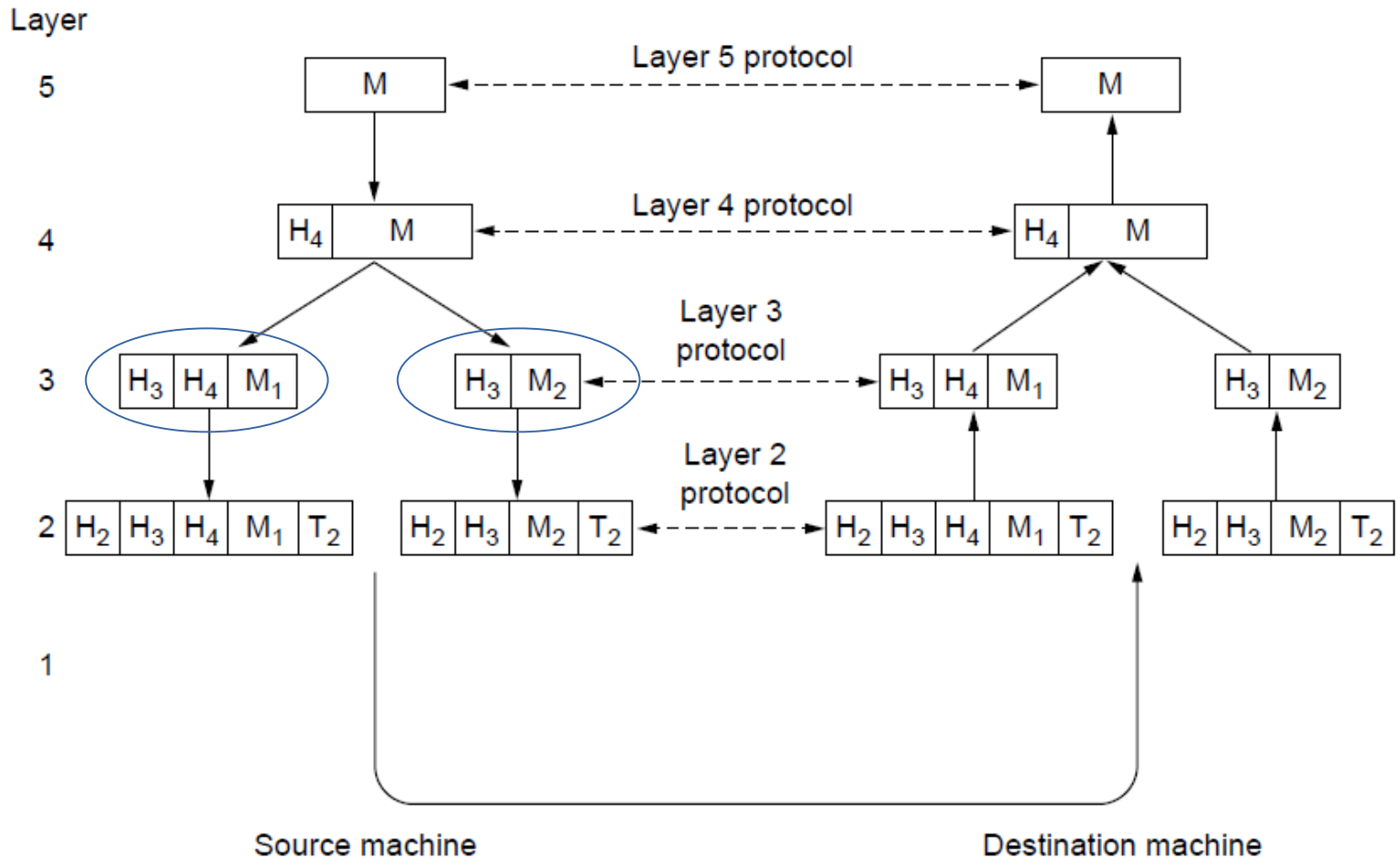
Example information flow supporting virtual communication in layer 5.

Protocol Hierarchies:



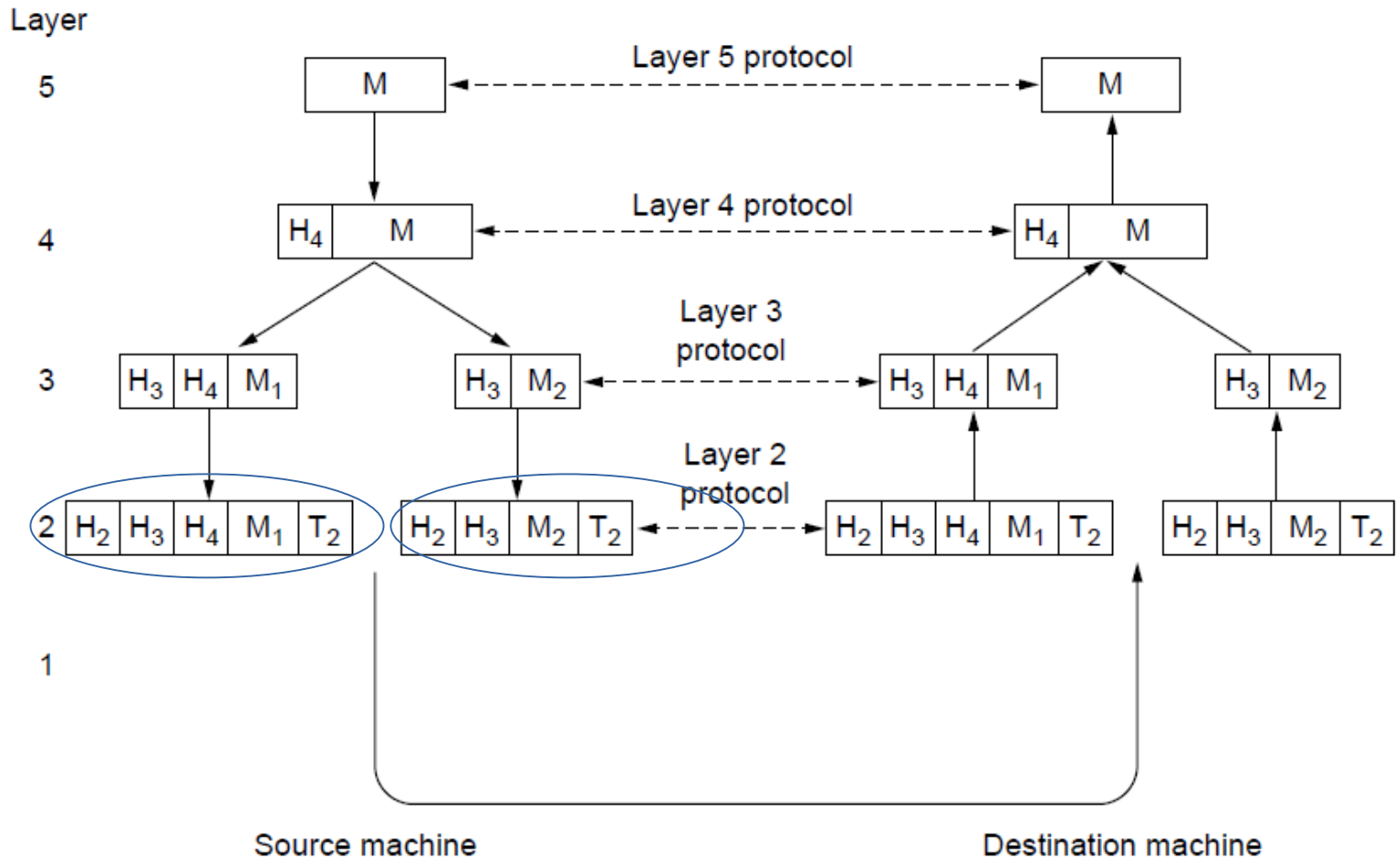
Example information flow supporting virtual communication in layer 5.

Protocol Hierarchies:



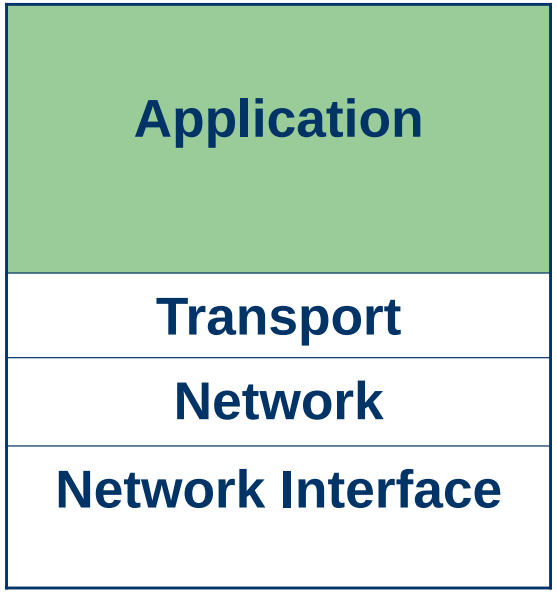
Example information flow supporting virtual communication in layer 5.

Protocol Hierarchies:

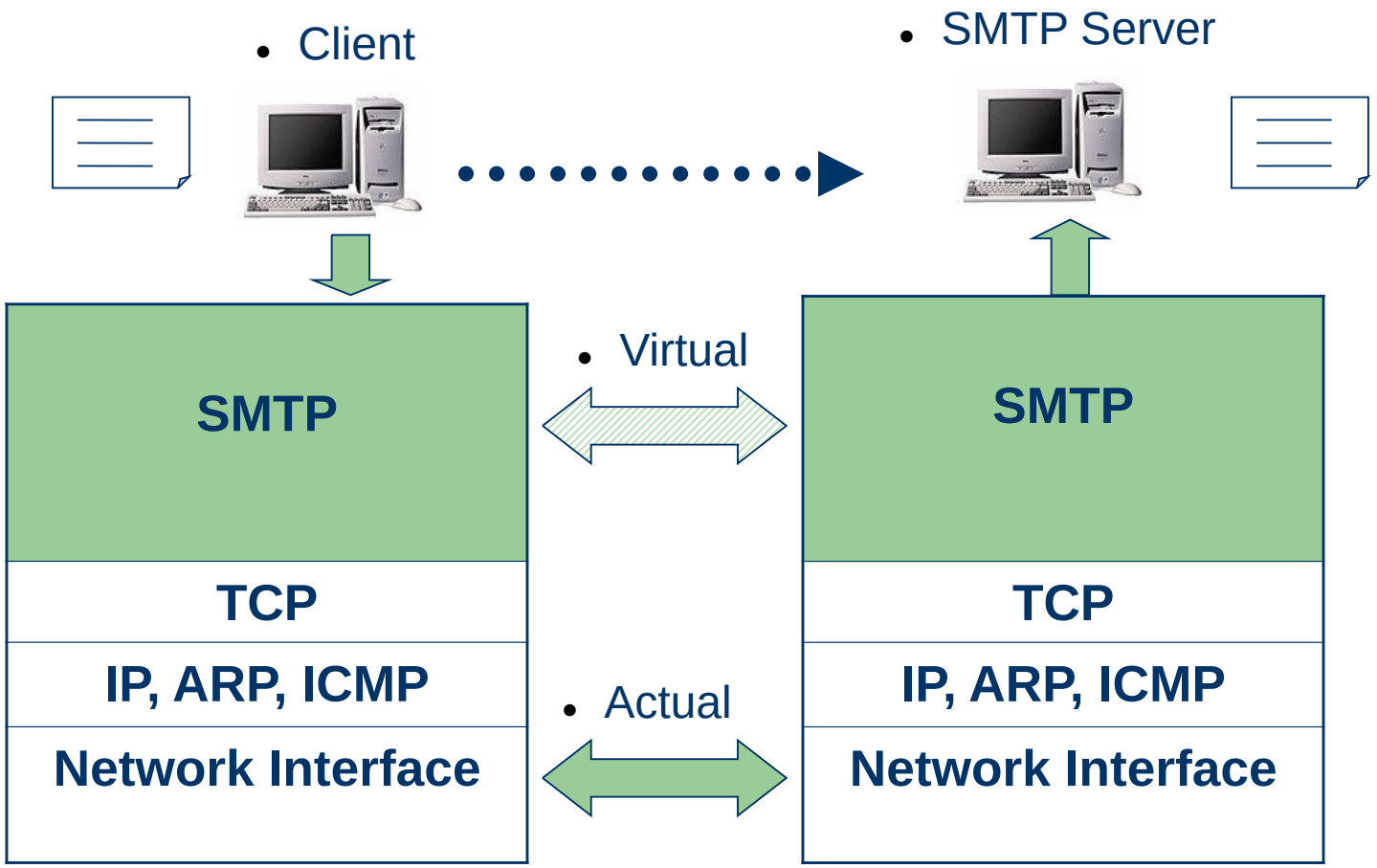


Example information flow supporting virtual communication in layer 5.

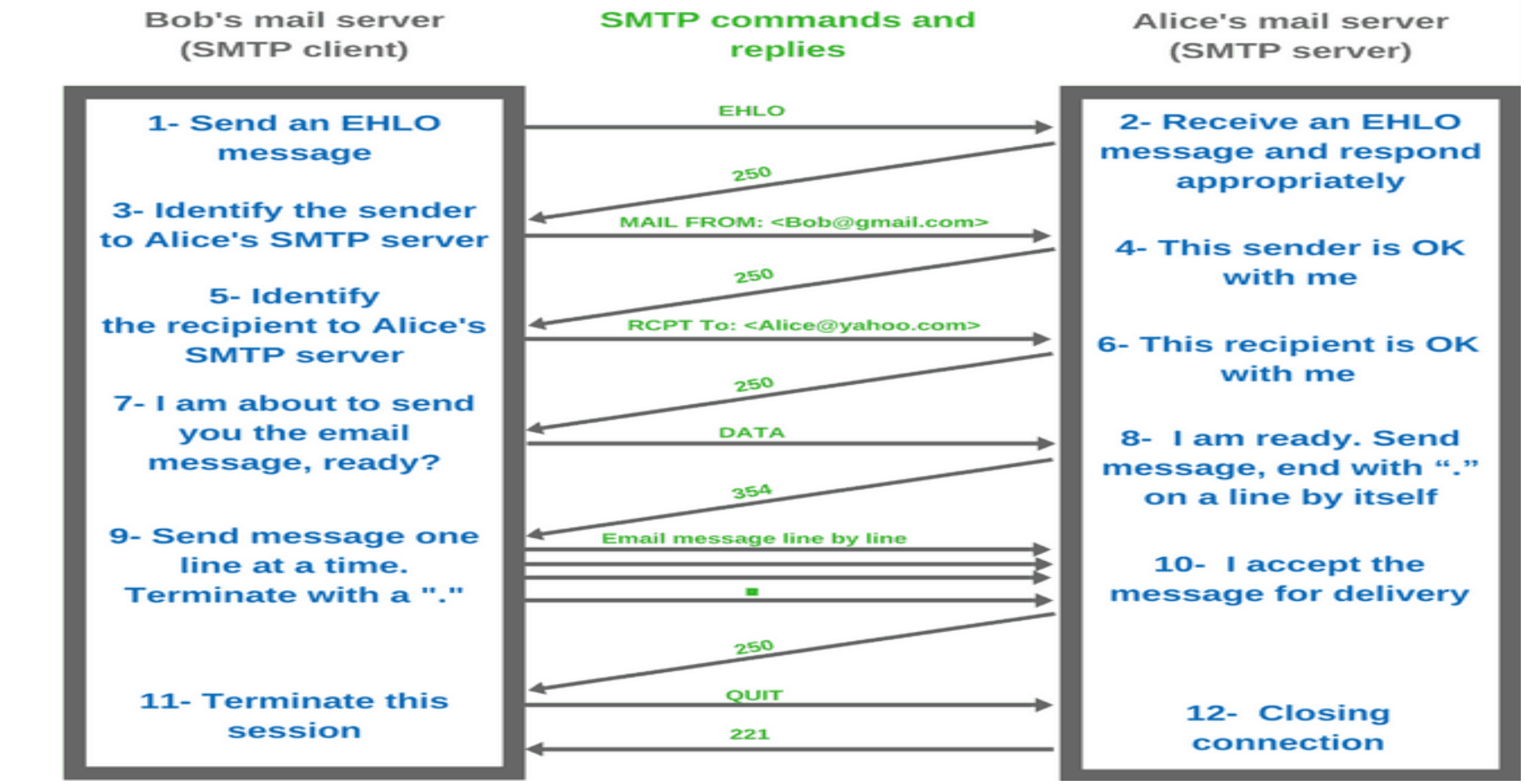
Application Layer



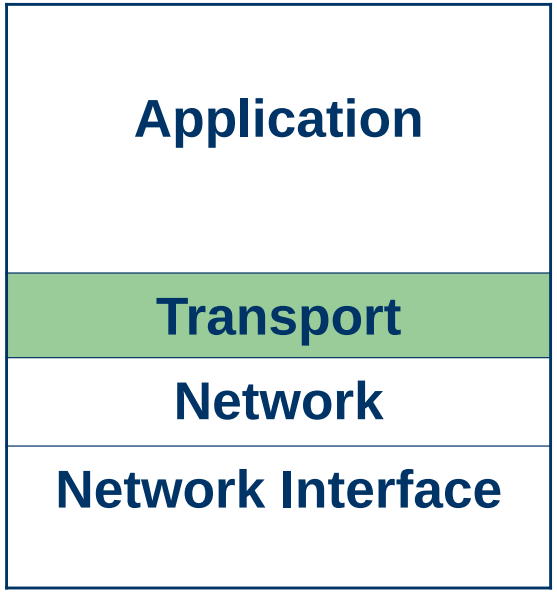
Example: SMTP

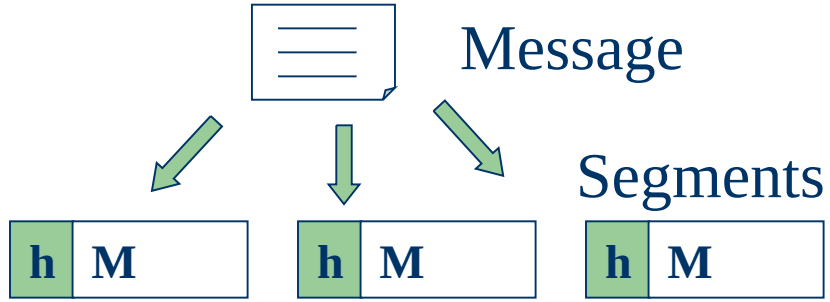


Example: SMTP



Transport Layer



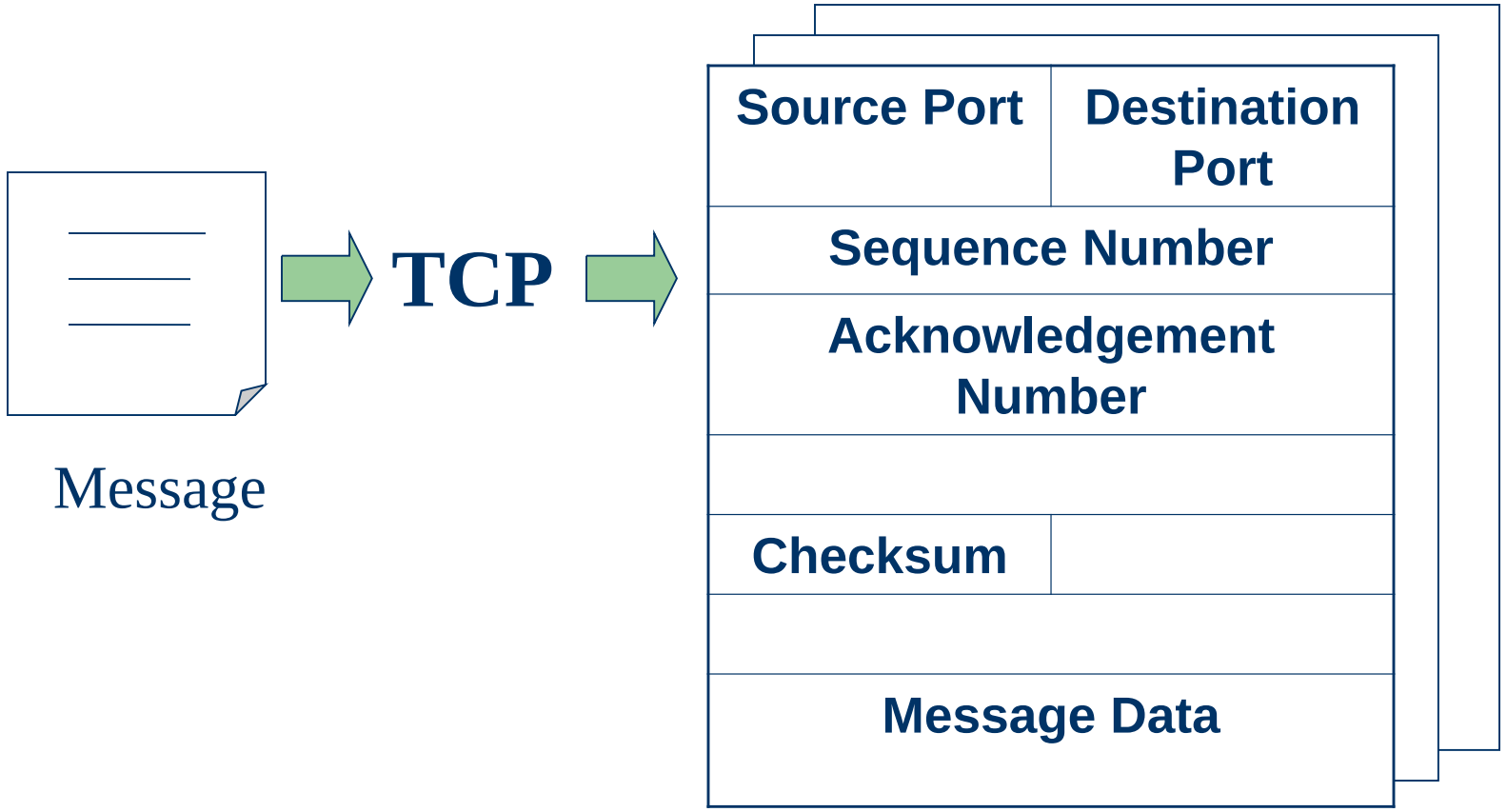


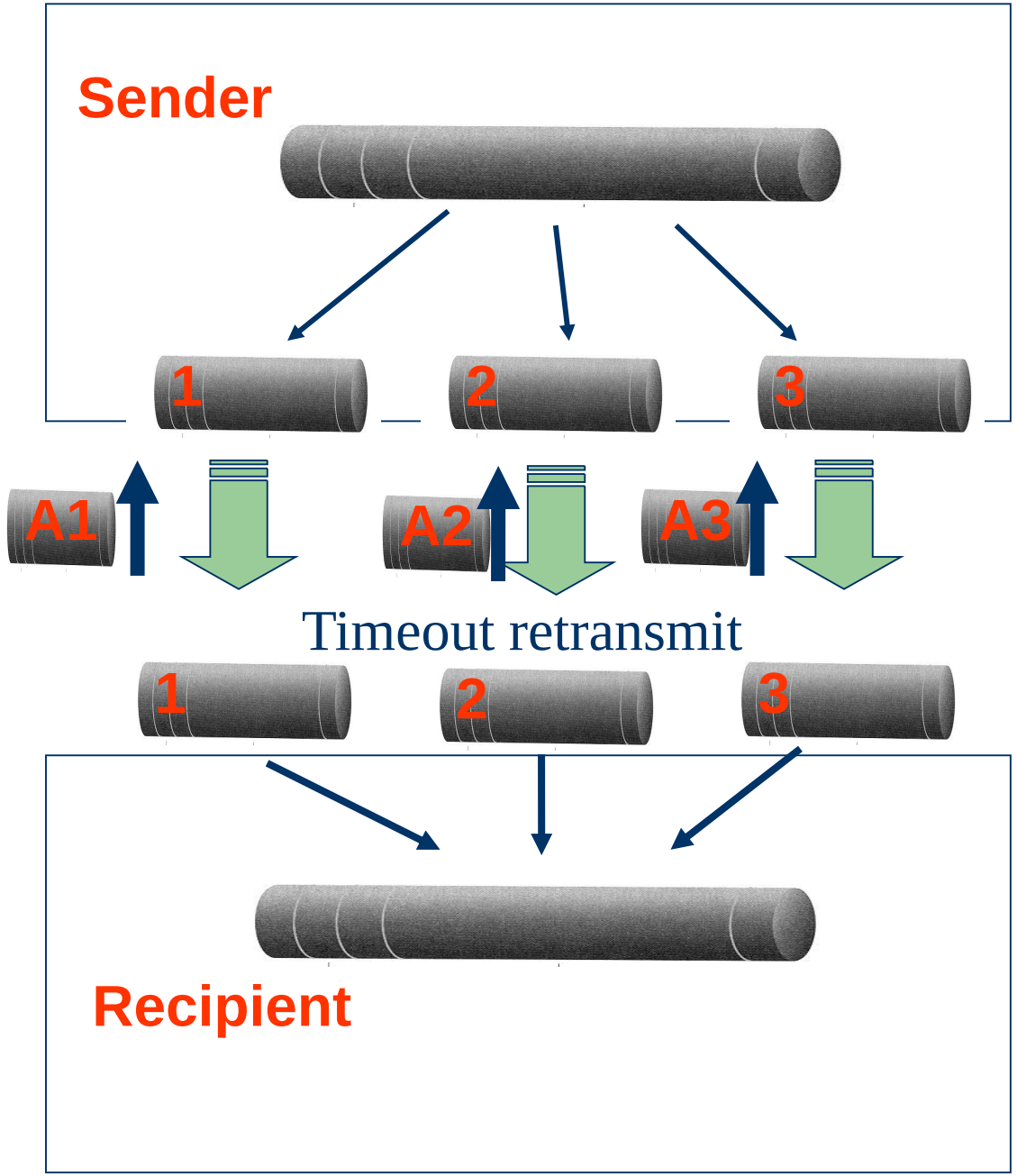
TCP and UDP

TCP – Transmission Control Protocol

- TCP is a connection-oriented protocol
  - Does not mean it has a physical connection between sender and receiver
  - TCP provides the function to allow a connection virtually exists – also called virtual circuit
- TCP provides the functions:
  - Dividing a chunk of data into segments
  - Reassembly segments into the original chunk
  - Provide further the functions such as reordering and data resend
- Offering a reliable byte-stream delivery service

Dividing and Reassembly




Sender
1
2
3
A1
A2
A3
Timeout retransmit
1
2
3
Recipient

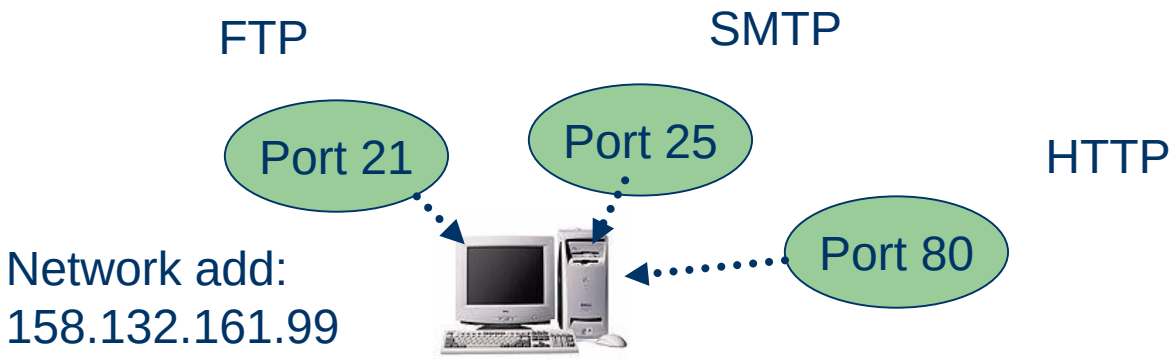
- A Typical Procedure
  - Sender
    - TCP divides a message into segments
    - Add sequence no.
    - Send the segments in sequence and wait for acknowledgement
    - If an acknowledgement for a segment is not received for a certain period of time, resend it until an acknowledgement is received
  - Recipient
    - When receiving segments, send the acknowledgement with correct number
    - Reassembly the segments back to the message

Port Multiplexing

- **A computer may perform a number of network applications at the same time**
  - **FTP + SMTP + HTTP etc.**

- **Each computer has only one network address, how can it serve so many applications at the same time?**

⇒ by port multiplexing



Well-known Port Numbers

- Some port numbers are reserved for some purposes
  - Port 21: FTP – file transfer
  - Port 25: SMTP – mail transfer
  - Port 23: TELNET – remote login
  - Port 80: HTTP – Web access

- These port numbers are well known to all computers in the network

- E.g. whenever a client access port 25 of the server, it means the client needs SMTP service

- Client

SMTP port = 1357

- Located by: network address + TCP port no.

- SMTP Server

SMTP port = 25

Source Port = 1357	Destination Port = 25
Sequence Number	
Acknowledgement Number	
Checksum	
Message Data	

- Client A

SMTP port
= 1357

- Network address:
- 158.132.161.99

- SMTP + FTP Server

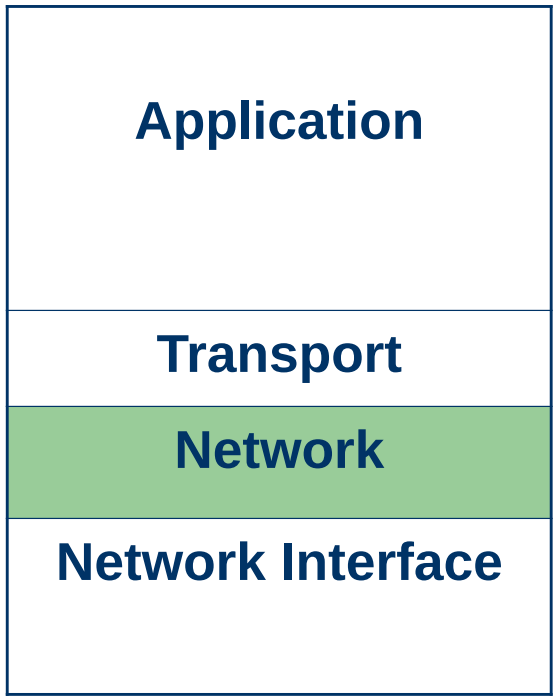
SMTP port
= 25

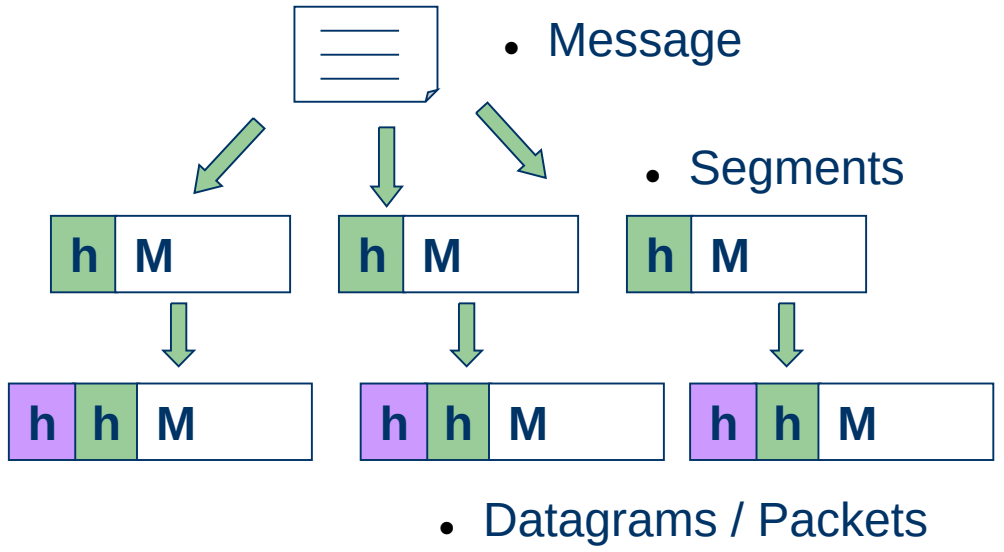
FTP port
= 21

- Client B

FTP port
= 1361

Network Layer

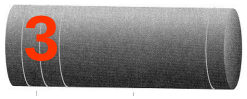




- Message
- Segments
- Datagrams / Packets

Network Addresses and Subnets

- **A header is added to each segment in the Network layer**



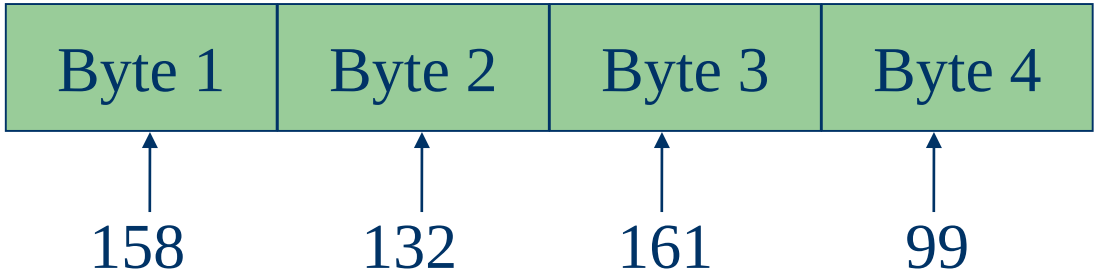
Segment

IP

		Total Length
Time to Live	**Protocol**	**Header CheckSum**
Source Address		
Destination Address		
Segment		

- **Total Length – Total length of a packet (up to 65535 bytes)**
- **Time to Live – How many times this packet can be routed on the network (up to 255)**
- **Protocol – The transport layer protocol that the packet belongs to**
  - **TCP: 6**
  - **UDP: 17**
  - **ICMP: 1**
- **Source address – the network address of the computer that sends the data**
- **Destination address – the network address of the computer that the data is sending to `**

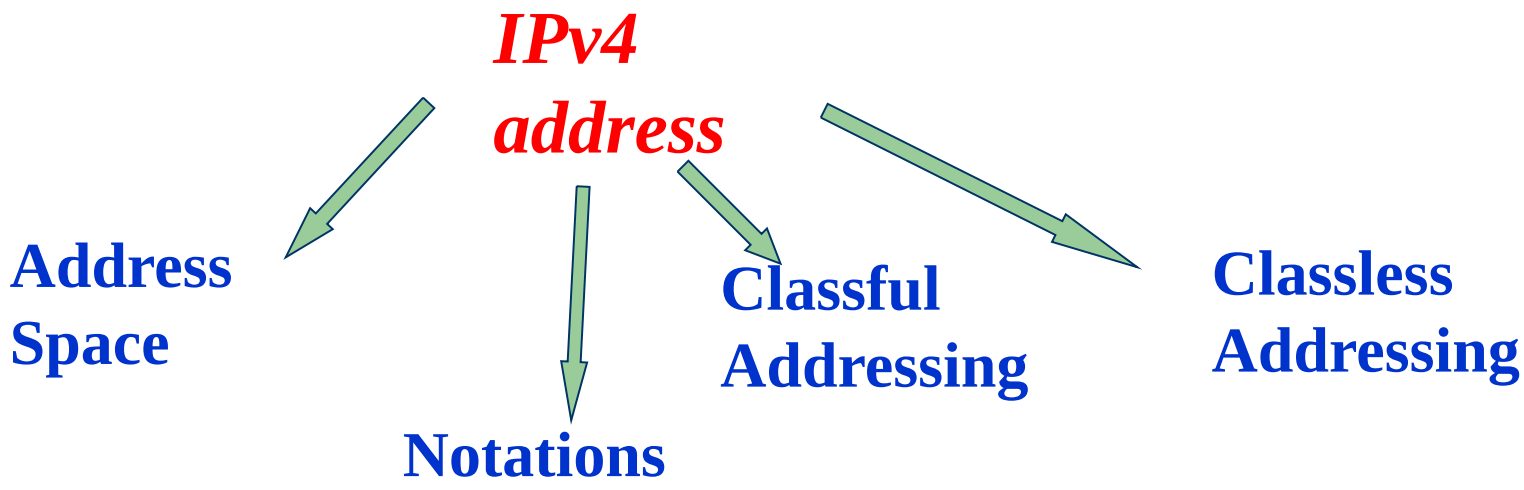
- (Already mentioned)
- Each computer (host) must have a unique network address (or IP address for TCP/IP suite)
- Each IP address is 32-bit long (four bytes)(IPV4 adrressing)
- The four-byte address is written out as a.b.c.d
  - e.g.



  - IP addresses are hierarchical
    - network I.D. and host I.D.
  - Each Network I.D. on the Internet needs to be registered to the Internet Assigned Number Authority

IPv4 ADDRESSES

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.

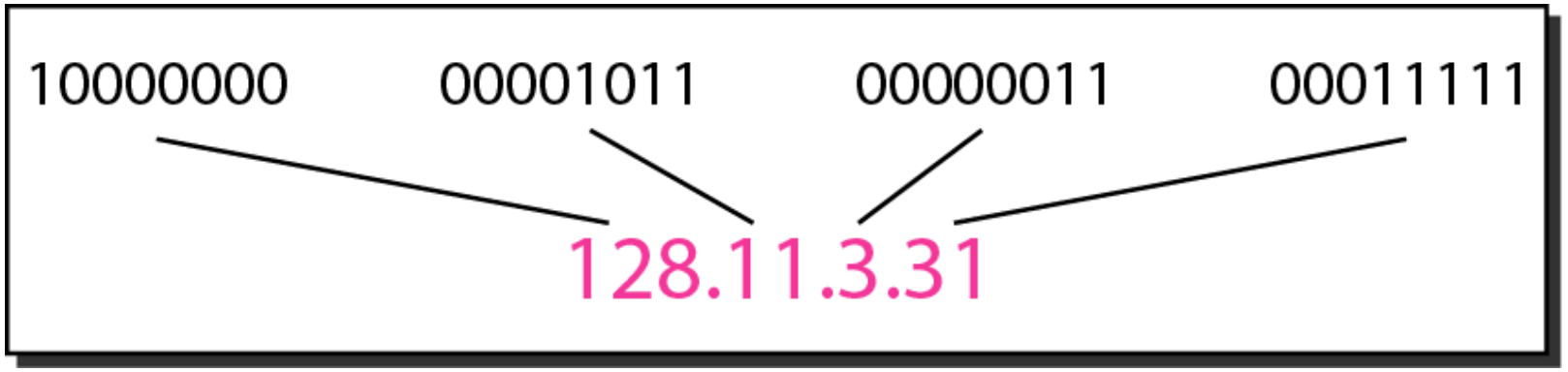


ADDRESS Space

The IPv4 addresses are unique and universal (all nodes connecting Internet must have IP addresses).

The address space of IPv4 is 2^{32} or 4,294,967,296.

Dotted-decimal notation and binary notation for an IPv4 address



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

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

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

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number (see Appendix B) and add dots for separation.

a. 129.11.11.239

b. 193.131.27.255

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

a. 111.56.45.78

b. 221.34.7.82

Solution

We replace each decimal number with its binary equivalent (see Appendix B).

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

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

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

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

a. 111.56.045.78
b. 221.34.7.8.20
c. 75.45.301.14
d. 11100010.23.14.67

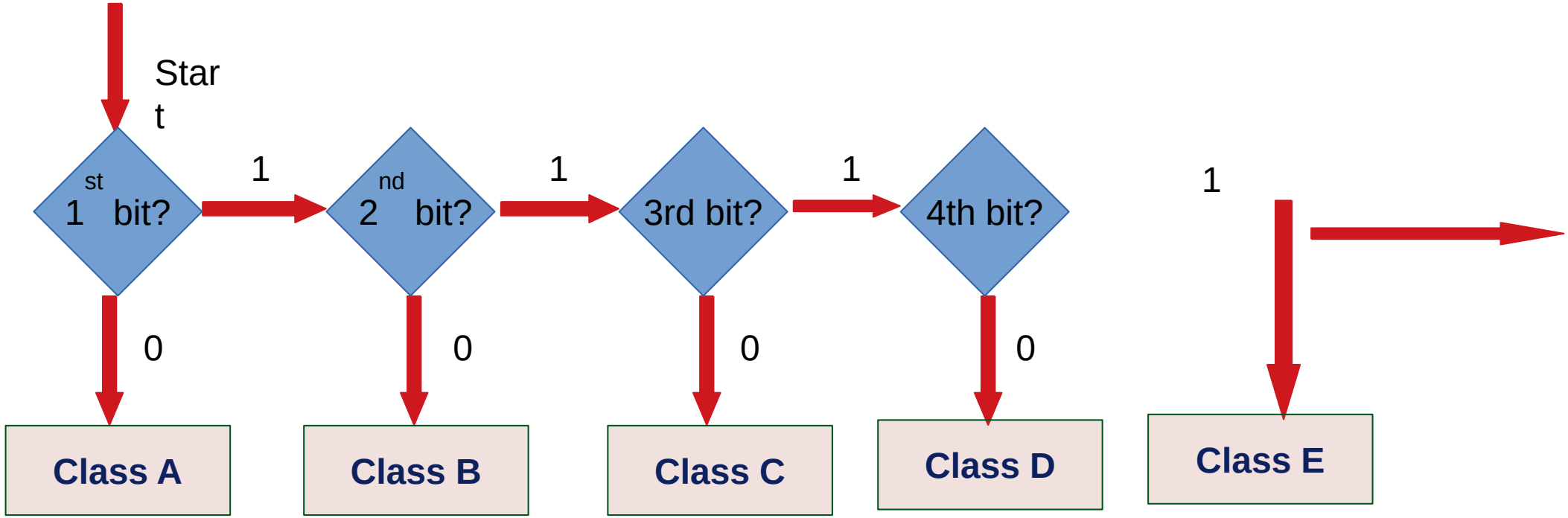
Solution

a. There must be no leading zero (045).
b. There can be no more than four numbers.
c. Each number needs to be less than or equal to 255.
d. A mixture of binary notation and dotted-decimal notation is not allowed.

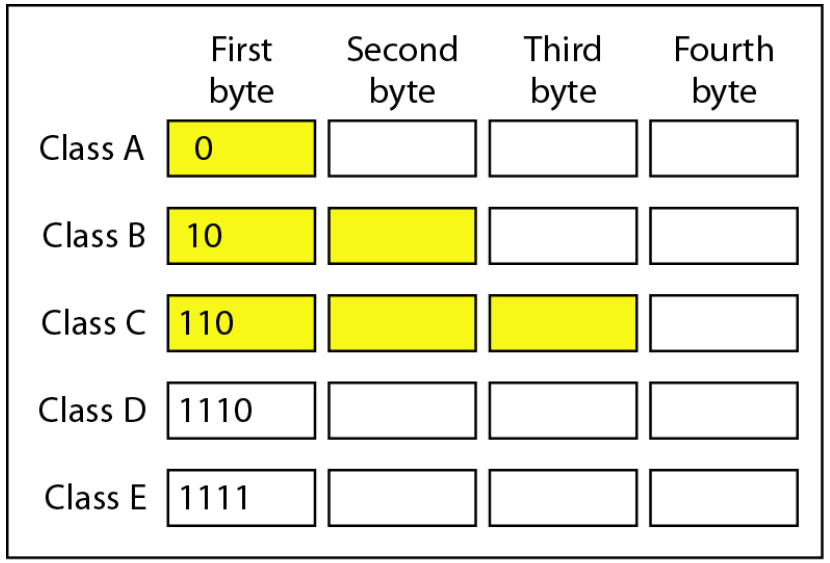
Note

In classful addressing, the address space is divided into five classes: A, B, C, D, and E.

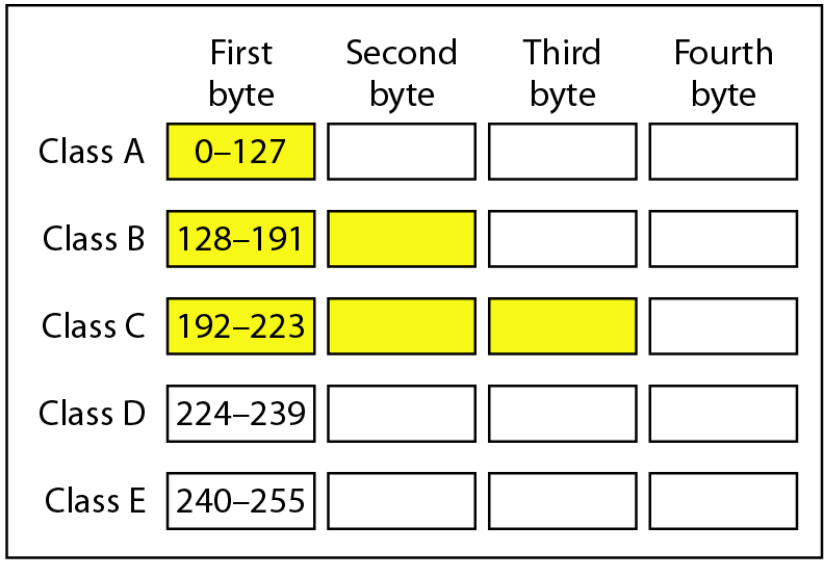
How do we identify the class Network Type



Finding the classes in binary and dotted-decimal notation



a. Binary notation



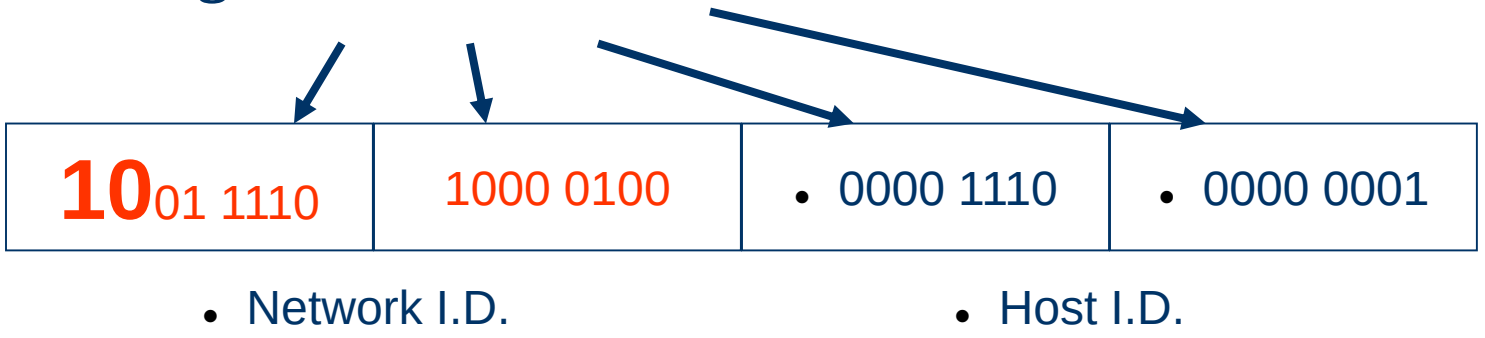
b. Dotted-decimal notation

Class A – for very large network

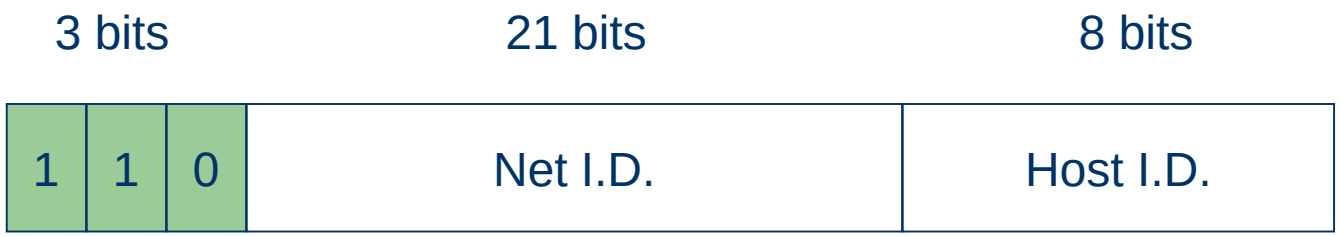
- **Only 2^7 (128) networks can belong to this class**
- **Each network, there are 2^{24} hosts or computers**
- **Very few class A networks in the world**
  - **e.g. Arpanet – the earliest packet switched WAN (started 40 years ago)**

Class B – for medium size network

- **2^{14} (16384) networks can belong to this class**
- **Each network, there are 2^{16} (65536) hosts or computers**
- **Polyu's address belongs to this group**
  - **e.g. 158.132.14.1**



Class C – for small network



- **2^{21} networks can belong to this class**
- **Each network, there are only 2^{8} (256) hosts or computers**

Class D – for multicast network

- **Packets are addressed to a multicast group**
- **Not often supported on Internet**

Find the class of each address.

a. **0**00000001 00001011 00001011 11101111

b. **110**00001 10000011 00011011 11111111

c. **14**.23.120.8

d. **252**.5.15.111

Find the class of each address.

a. **0**00000001 00001011 00001011 11101111

b. **110**00001 10000011 00011011 11111111

c. **14**.23.120.8

d. **252**.5.15.111

Solution

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

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

c. The first byte is 14; the class is A.

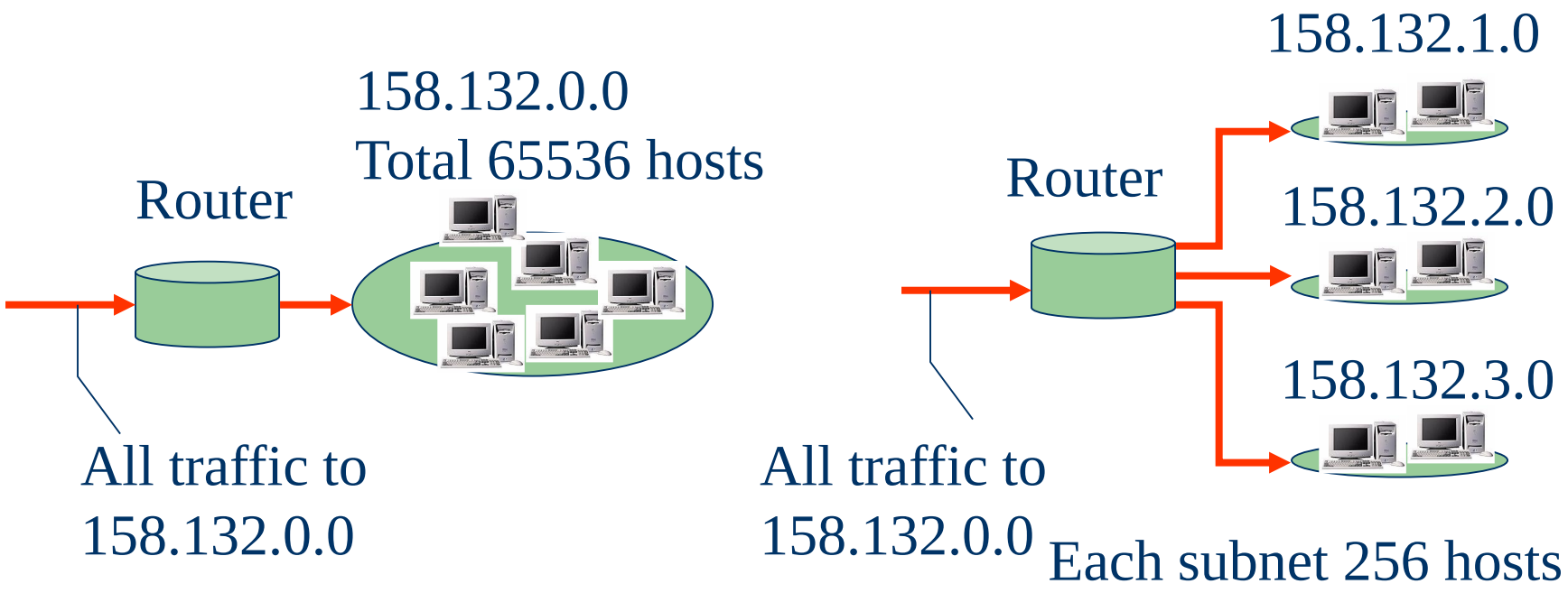
d. The first byte is 252; the class is E.

Table 19.1 *Number of blocks and block size in classful IPv4 addressing*

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Subnets

- **A class B address can have 65536 hosts**
- **Difficult to manage**
- **Usually subdivide into a few small subnets**
- **Subnetting can also help to reduce broadcasting traffic**

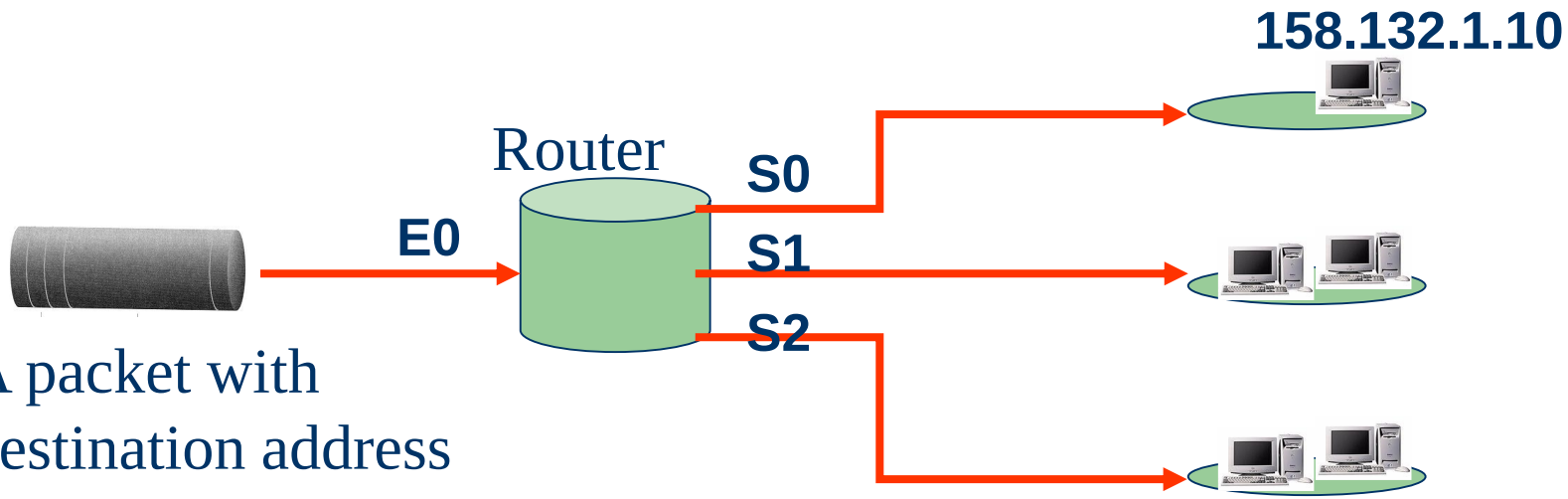


Subnet Mask

- **How does the router know which subnet a packet should go?**
- **For each interface of the router, a subnet mask is provided to redefine which part of the address is Net ID and which part is Host ID**
- **Become classless addressing**

A subnet mask: 255.255.255.0

‘1’s Net ID ‘0’s Host ID



Routing Table

	S0	S1	S2
Subnet	158.132.1.0	158.132.2.0	158.132.3.0
Mask	255.255.255.0	255.255.255.0	255.255.255.0

	158.132. 1. 10	1001 1110.1000 0100.0000 0001.0000 1010
AND	255.255.255. 0	AND 1111 1111. 1111 1111. 1111 1111. 0000 0000
	158.132. 1. 0	1001 1110.1000 0100.0000 0001.0000 0000

Advantage: easy to compute

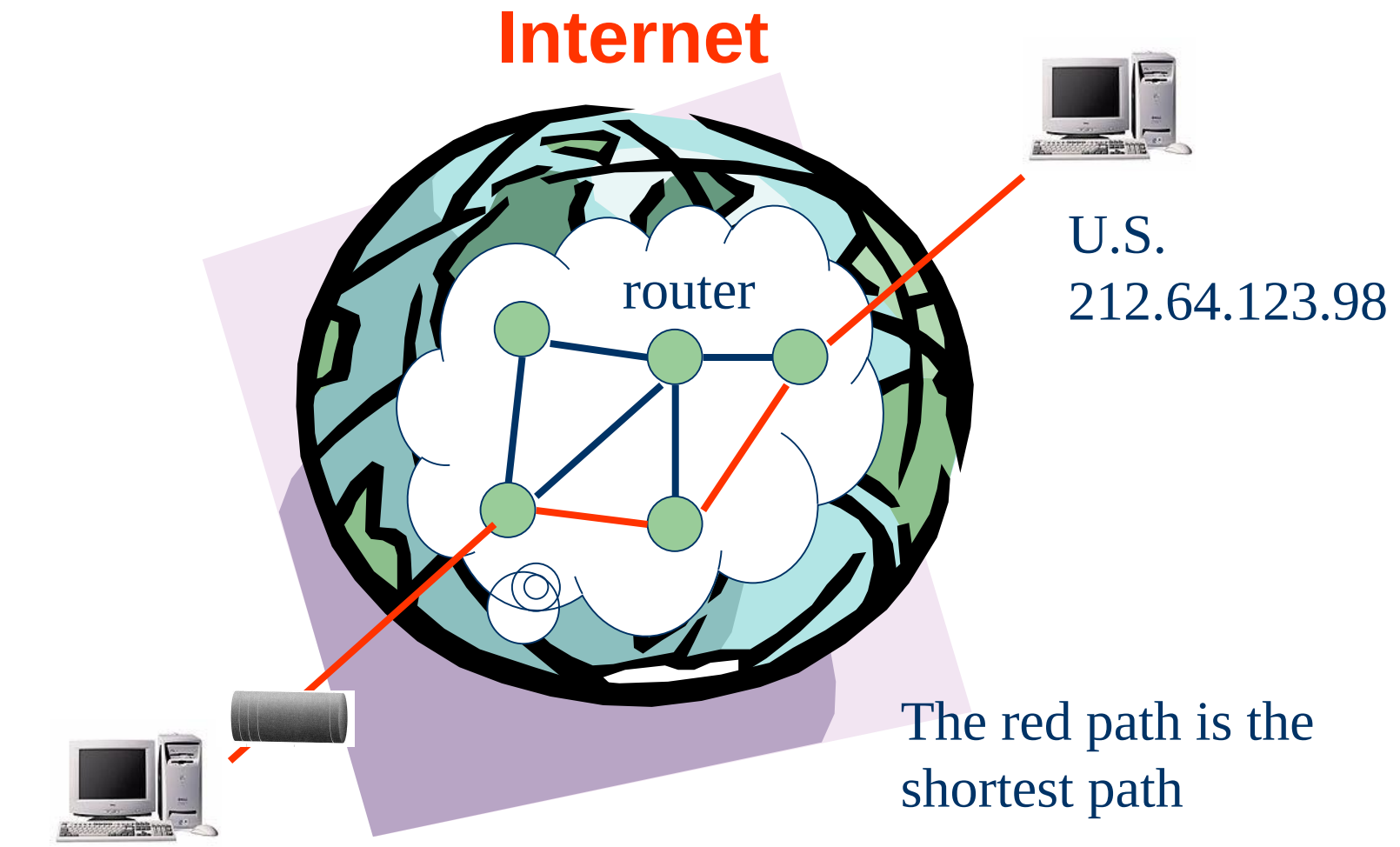
Routing

- How a packet finds its way to a computer in a network?
  - By using Routers

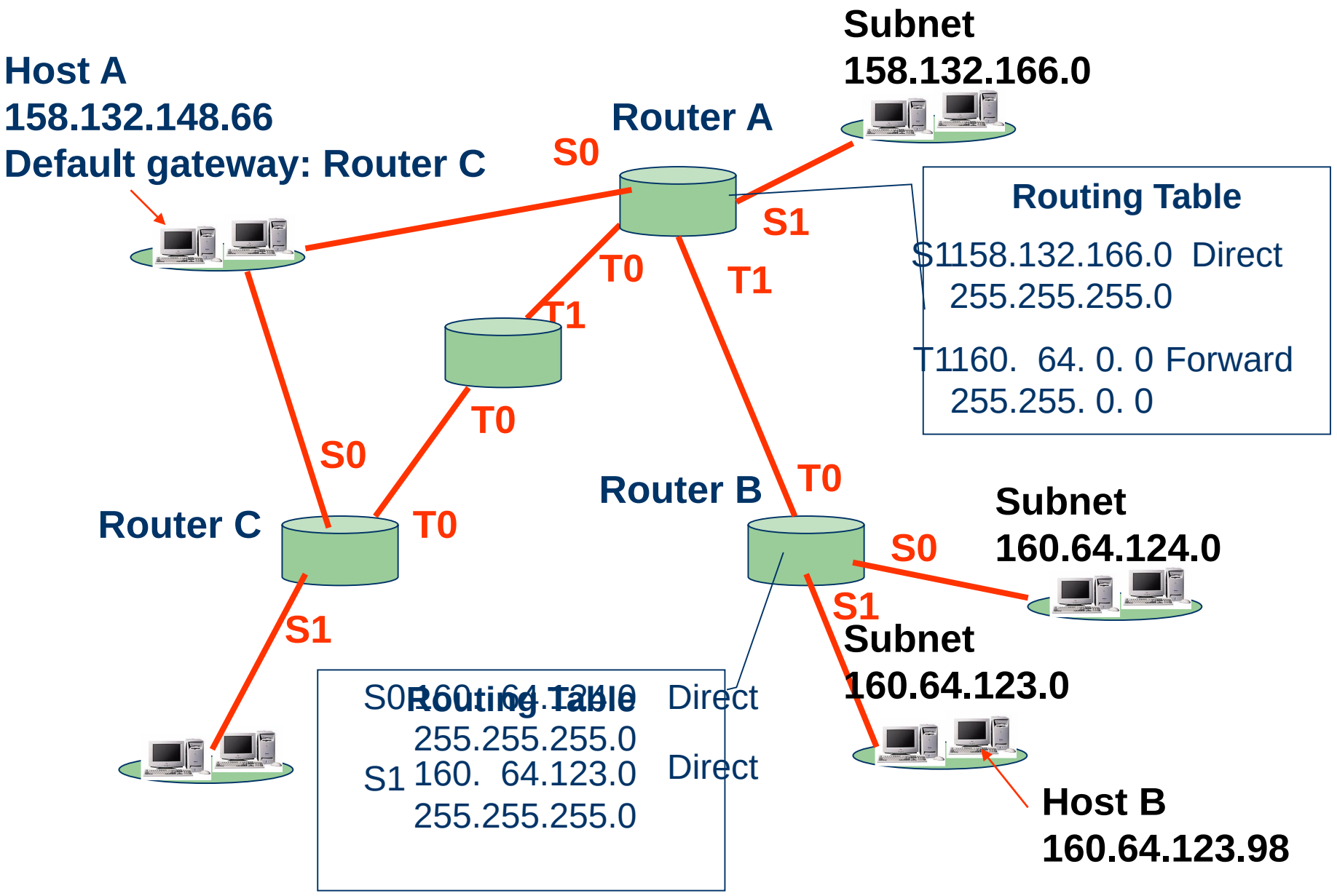
- Routing is the selection of a path to guide a packet from the source to the destination

- Criteria in selecting a path may be:

  - Shortest path
  - Quickest path
  - Cheapest path

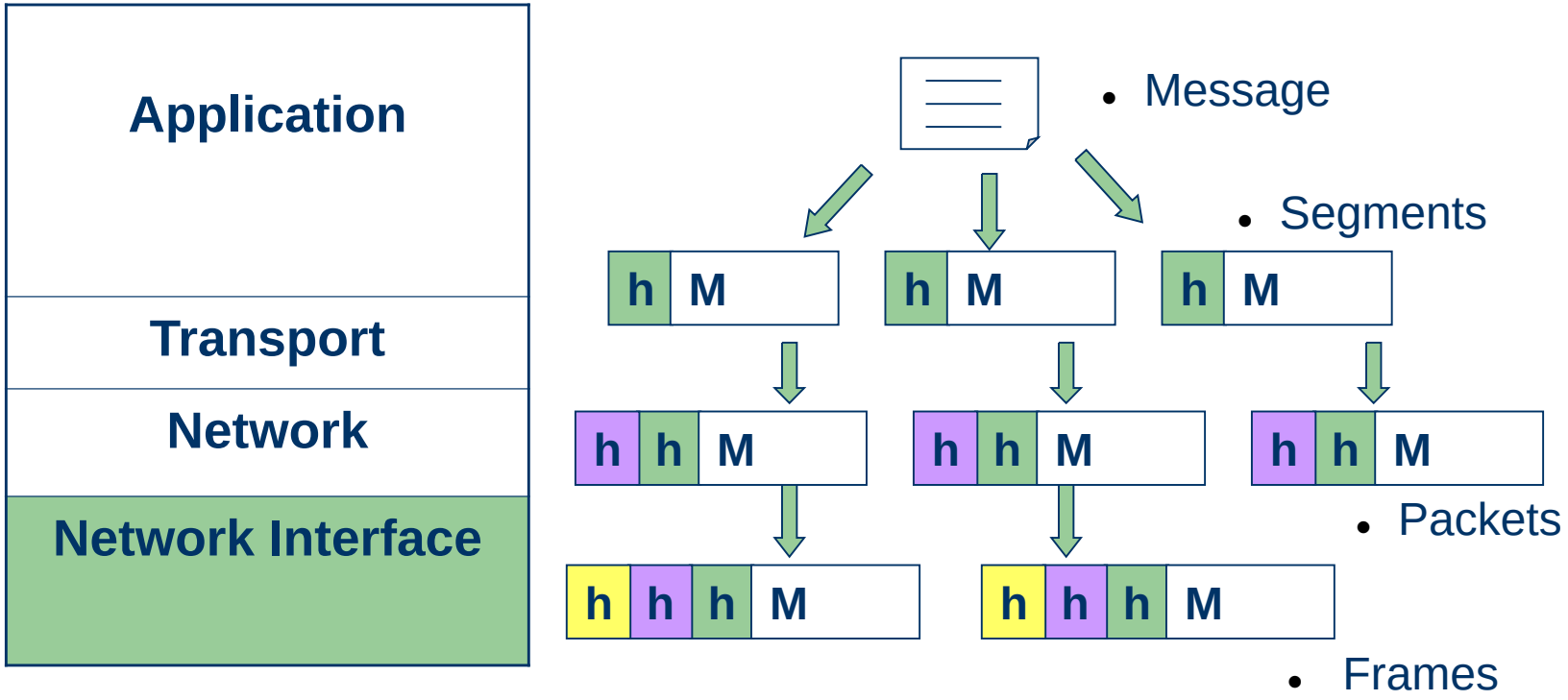

Internet
router
U.S.
212.64.123.98
The red path is the shortest path
Hong Kong
158.132.161.99

- Each router has a table that records the estimated distance to all other routers
- If a router knows the entire network topology, the shortest path can be calculated
- To achieve this, routers broadcast Link State Advertisement to all other routers periodically
  - By means of routing protocol
- Each router knows the exact topology, and then calculates the shortest path
- In practice, it is not possible for a router to all paths. Only the nearer ones are kept
- Hence can give wrong estimation


Host A
158.132.148.66
Default gateway: Router C
Subnet
158.132.166.0
Router A
S0
S1
T0
T1
T1
T0
Routing Table
S1158.132.166.0 Direct
255.255.255.0
T1160. 64. 0. 0 Forward
255.255. 0. 0
S0
T0
Router C
T0
Router B
S0
Subnet
160.64.124.0
S1
S1
Subnet
160.64.123.0
Routing Table
S0 160.64.124.0 Direct
255.255.255.0
S1 160. 64.123.0 Direct
255.255.255.0
Host B
160.64.123.98

1. **Host A wants to send a packet to Host B with address 160.64.123.98**
2. **Host A checks that 160.64.123.98 is not in the same network**
3. **Send packet to default gateway (Router C)**
4. **Default gateway finds that it cannot provide the best route for the packet, inform Host A to send the packet to Router A next time**
5. **Router C sends the packet to Router A**
6. **Router A checks from the table the packet should forward to Router B**
7. **Router B receives the packet and checks in its table the packet should directly deliver to subnet 160.64.123.0**
8. **Host B (160.64.123.98) receives the packet**

Data Link and Physical Layers



Design Issues:

- **Addressing and Naming:**

  Every layer needs a mechanism for identifying the senders and receivers that are involved in a particular message.

- **Error Detection:**

  It typically uses codes to locate the erroneously transmitted bit(s) and request re-transmission.

- **Error Correction**

  Correct messages is recovered from the possibly incorrect bit(s) that were originally received.

- **Routing:**

  Finding a working path through a network.

Multiplexing:

- Expensive to set up a separate connection for pair of communicating processes
- Underlying layer may decide to use the same connection for multiple, unrelated conversations.

Flow Control:

- Feedback from the receiver to the sender is often used to alleviate the problem of the sender swamping the slow receiver with data.

Congestion:

- The problem may occur when the network is oversubscribed because to 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:

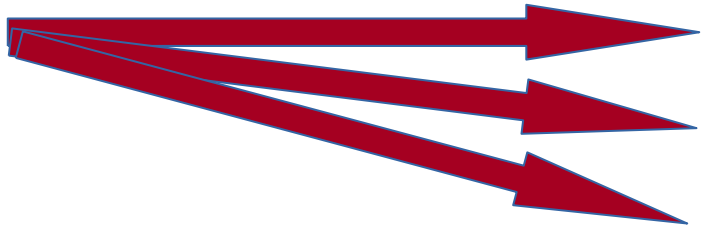
- Additional Resources (other then Bandwidth),
- Real-time delivery (for applications that require high throughput),
- Live Video

Network Security:

- How good is the network against different kinds of threats
  - Confidentiality,
  - Authentication,
  - Integrity, etc.

Example Networks:

Internet

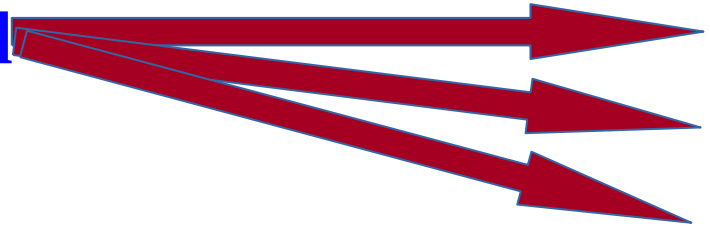


ARPANET

NSFNET

WWW

Connection-oriented Network



X.25

Frame Relay

ATM

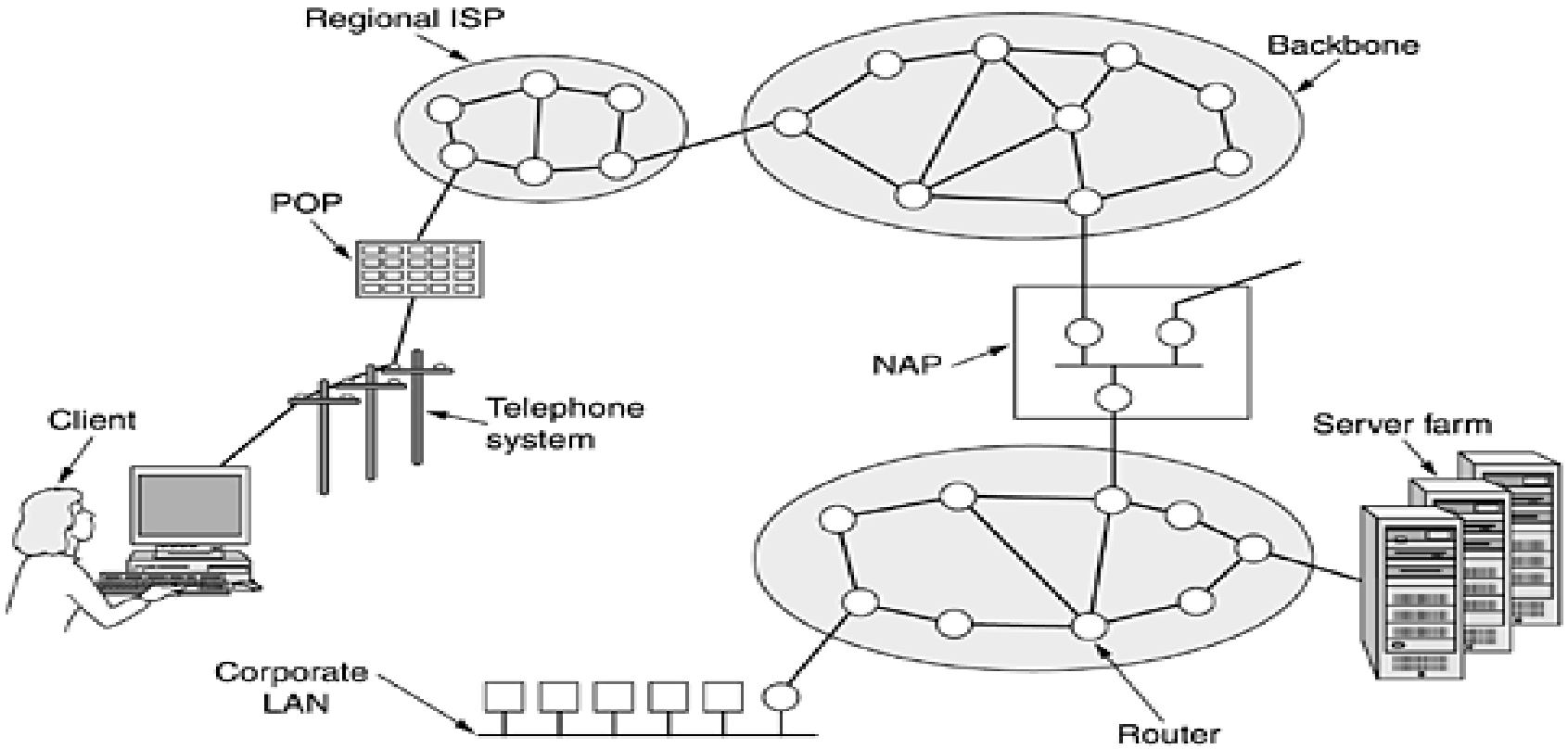
Ethernet

Wireless LANs: 802.11

The Internet:

- The ***Internet is not a network at all, but a vast collection of different networks*** that use certain common protocols and provide certain common services.

- It is an unusual system in that it was **not planned by anyone and is not controlled by anyone.**



How it works?

E.g a telephony call.

Let us assume a client calls his or her **ISP (Internet service provider)** over a dial-up telephone line.

Step-1

The modem is a card within the PC that converts the digital signals the computer produces to analog signals that can pass unhindered over the telephone system.

Step-2

These signals are transferred to the ISP's ***POP (Point of Presence),*** where they are removed from the telephone system and injected into the ISP's regional network.

Step-3

The ISP's regional network consists of interconnected routers in the various cities the ISP serves. If the packet is destined for a host served directly by the ISP, the packet is delivered to the host. Otherwise, it is handed over to the **ISP's backbone operator**.

Step-4

If a packet given to the **backbone** is destined for an ISP or company served by the backbone, it is sent to the closest router and handed off there.

Step-5

To allow packets to hop between backbones, all the major backbones connect at the **NAPs (Network Access Point).**

Step-6

A ***Network Access Point*** was a public network exchange facility where Internet service providers connected with one another in peering arrangements.

The ARPANET :

- It is abbreviated as ***"Advanced Research Project Agencies Network".***

- In mid 60's, DoD (Department of Defense) started ARPANET to build network that could resist any attacks from USSR

- **Paul Baran** proposed a complete form.

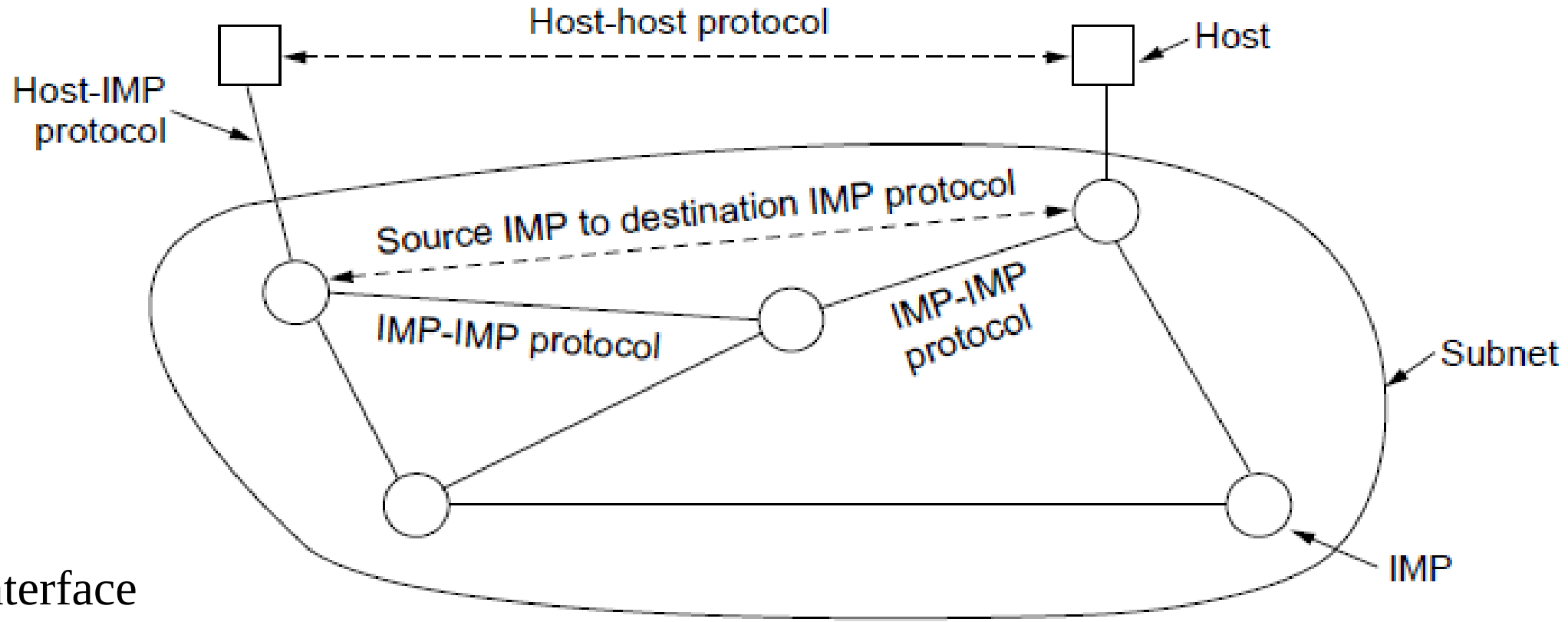
The ARPANET :

- It was in response to USSR’s Sputinik lunch in 1957.

- Intially it is used to connect 4 major Uiversities

  - UCLA
  - UCSB
  - University of Utah
  - Stanford Research Institute

The ARPANET:



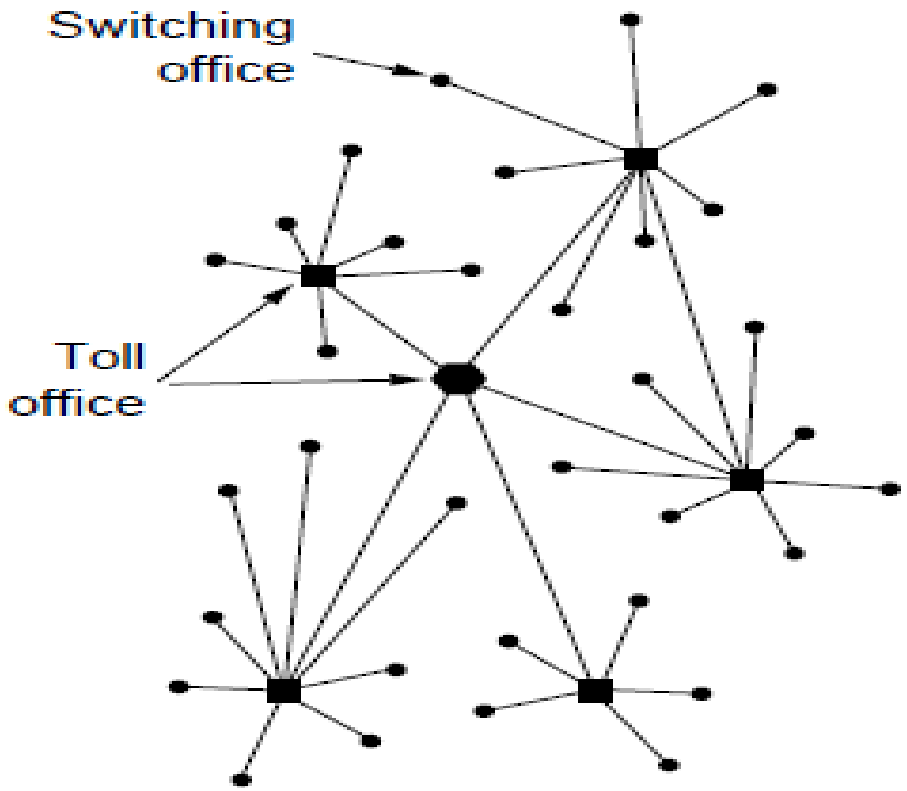
IMP: Interface Message Processor

The original ARPANET design

The ARPANET :

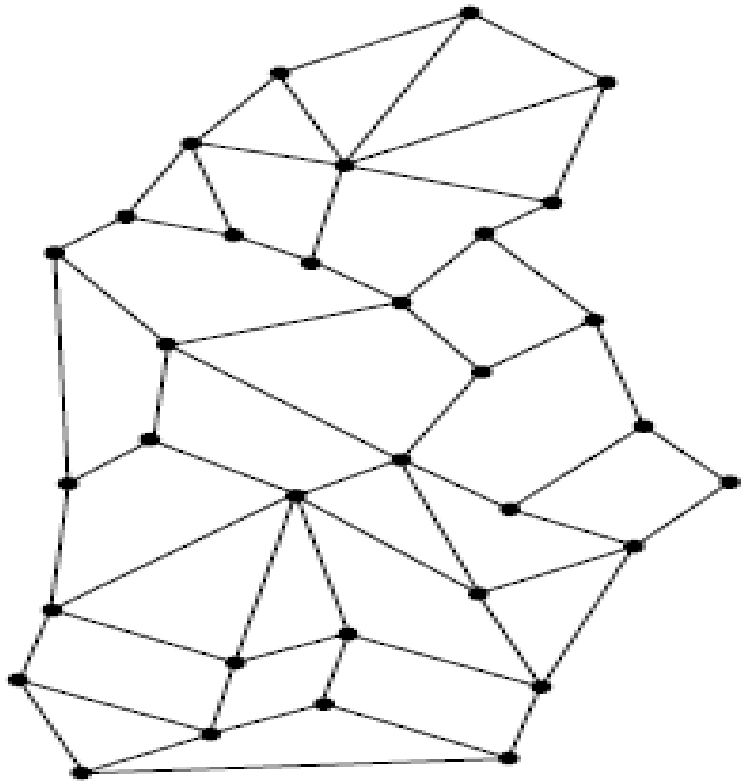
- ARPANET used the packet-switching technology to interconnect four nodes.
- DOD divided the network into host computers and subnets.
- Subnet consists of IMPs connected by transmission lines.
- Each IMP would be connected two at least 2 IMPs to provide high reliability.

The ARPANET :



(a)

a) Structure of the telephone system.



(b)

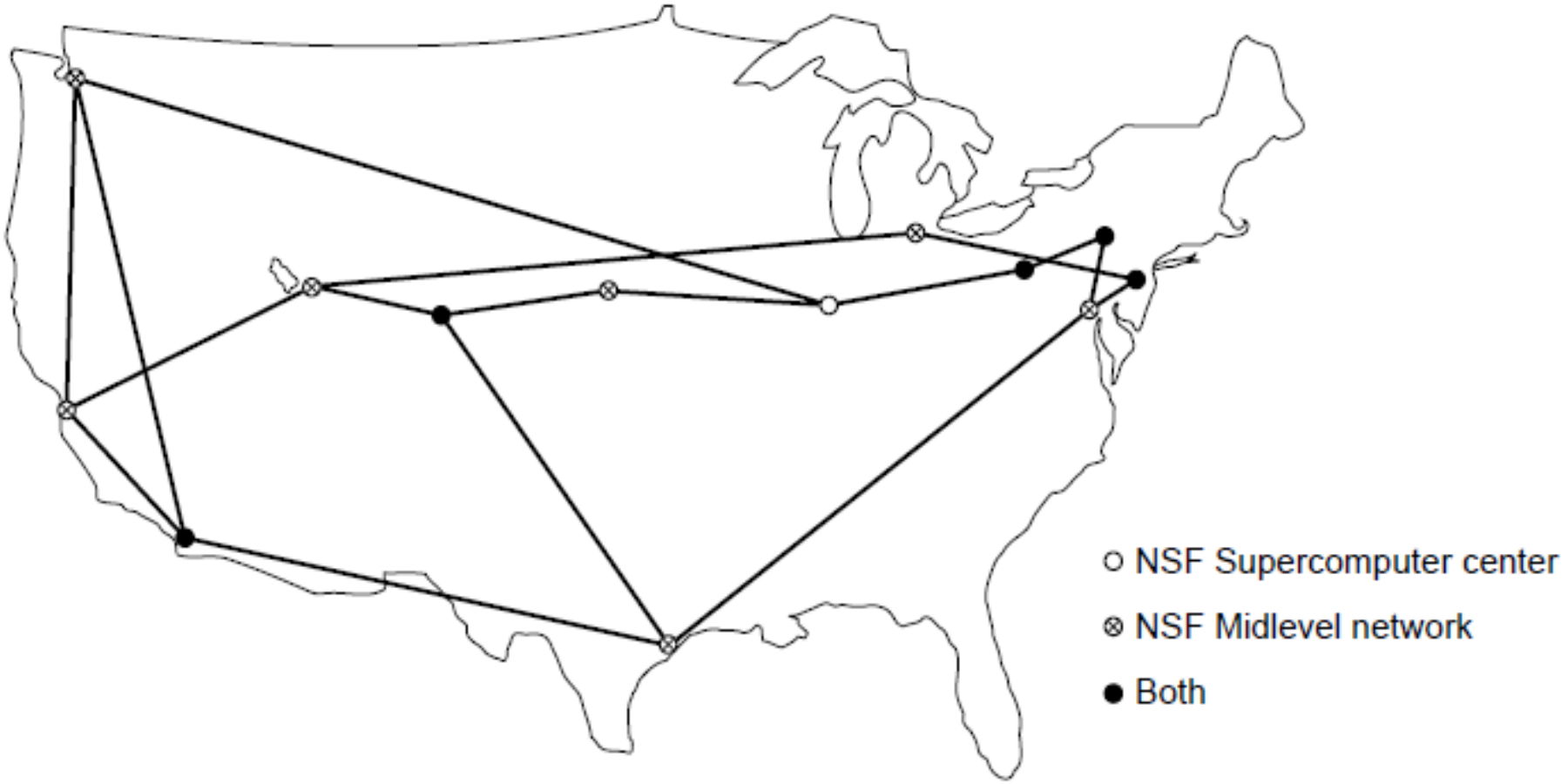
b) Baran's proposed distributed switching system.

NSFNET:

- The ***National Science Foundation Network*** **(NSFNET)** was a program of coordinated, evolving projects sponsored by the **National Science Foundation (NSF)** from 1985 to 1995 to promote advanced research and education networking in the United States.

- NSF decided to build a backbone network 48 to connect its six supercomputer centers, in San Diego, Boulder, Champaign, Pittsburgh, Ithaca, and Princeton. Each supercomputer was given a little brother, consisting of an LSI-11 microcomputer called a fuzzball.

NSFNET: (*National Science Foundation Network)*



The NSFNET backbone in 1988.

NSFNET:

- ***The fuzzballs*** were connected with 56-kbps leased lines and formed the subnet, the same hardware technology as the ARPANET used. The software technology was different however: the fuzzballs spoke TCP/IP right from the start, making it ***the first TCP/IP WAN.***

- The complete network, including the backbone and the regional networks, was called NSFNET. It connected to the ARPANET through a link between an IMP and a fuzzball. The first NSFNET backbone is illustrated in above figure.

ALOHANET:

- The concept of interconnecting, *prior to ethernet*, was available where communication was taking place through radio devices.
- Implemented by ***Huwaii*** in 1970.

Technology :

- No of user terminals was connected to a central computer.
- Communication between the user terminals and central computer was taking place using upstream (to the central computer) and downstream (from the central computer)

Disadvantages :

Fails when upstream traffic is heavy.

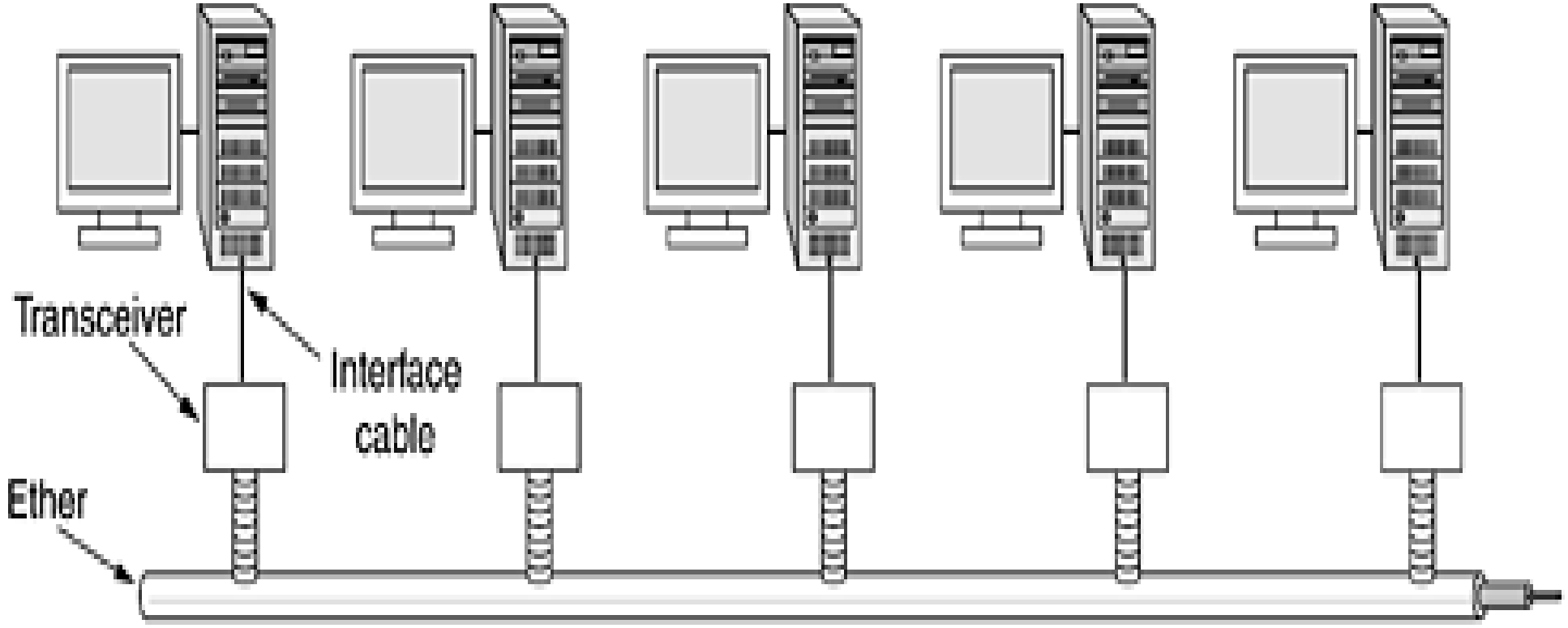
Ethernet:

- **Ethernet** was named after the *luminiferous ether*, through which electromagnetic radiation was once thought to propagate.
- It is the *most popular local area network* which was developed and implemented in Xerox PARC (Palo alto Research center) in 1976.

- Transmission medium was a coaxial cable.
- Length of coaxial cable is up to 2.5km with repeaters at every 500m distance. Up to 256 machines could be connected to the coaxial cable through transreceiver *ran at 2.94 Mbps.*

Architecture of original Ethernet

- The Xerox Ethernet was so successful that DEC (Digital equipment corporation), Intel, and Xerox drew up a standard in 1978 for a 10-Mbps Ethernet, called the **DIX standard**. With two minor changes, the DIX standard became the **IEEE 802.3** standard in 1983.



IEEE 802.3

Ethernet

Advantage Of Ethernet:

- Before transmitting, a computer listen to the cable to see if someone else was transmitting.
- A computer held back until the transmission finished.
- Doing so avoided interfering with existing transmissions, giving a much higher efficiency.

Disadvantage Of Ethernet:

- If two/more computers tries to send simultaneously once the transmission completes.

Solution:

Each computer listen during its own transmission and if it detects the interference, jam the ether to alert all senders and then back off and wait a random time before retrying it

- Ethernet continued to develop and is still developing. New versions at 100 Mbps, 1000 Mbps, and still higher have come out. Also the cabling has improved, and switching and other features have been added.

- Other LAN Standards: IEEE 802.4 (token bus)

  IEEE 802.5 (token ring)

Wireless LANs:IEEE802.11

The idea of **Wireless LAN** was developed when it was thought of to equip both the office and the notebook computers with *short-range radio transmitters and receivers* and to allow them to communicate.

But during its implementation some systems faces problem because technical incompatibility between devices.

Ex:

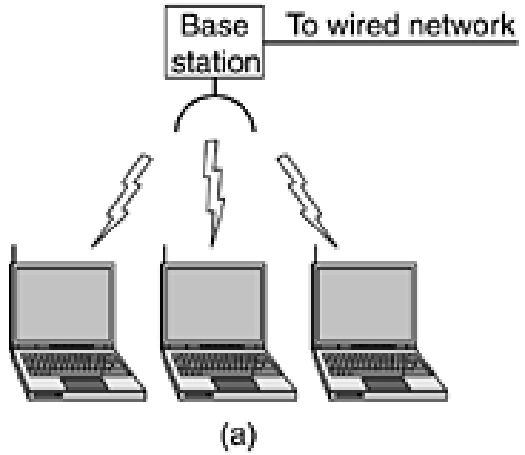
A computer equipped with ***a brand X radio could not work in a room equipped with a brand Y base station***. To short out this issue the IEEE committee that standardized the wired LANs was given the task of drawing up a *wireless LAN standard*.

The standard it came up with was named ***802.11. A common name for it is WiFi.***

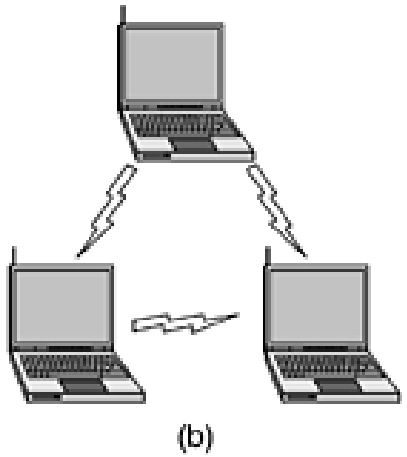
Wireless LANs

The proposed standard ***IEEE 802.11. (WiFi)*** had to work in two modes:

1. In the presence of a base station. (**Infrastructure Mode**)



2. In the absence of a base station. (**Ad Hoc Mode**)



Infrastructure Mode − Mobile devices or clients connect to an access point (AP) that in turn connects via a bridge to the LAN or Internet. The client transmits frames to other clients via the AP.

Ad Hoc Mode − Clients transmit frames directly to each other in a peer-to-peer fashion.

Wireless Network

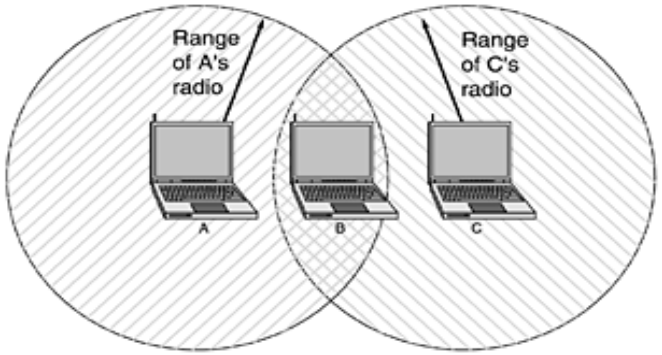
- In 1997, the Wireless LAN came to its operation with a **speed of 1 and 2 Mbps.**
- Further split in the standard as **802.11a and 802.11b** in 1999.
- The **802.11a standard uses a wider frequency band and runs at speeds up to 54 Mbps**.
- The **802.11b standard uses the same frequency band as 802.11, but uses a different modulation technique to achieve 11 Mbps.**
- In the current scenario, the **802.11 is being widely used in organizations like airports, railway stations, hotels, shopping malls, and universities** so far as the computational ability and internet access is concerned.

Advantages of Wireless Network

- They provide clutter-free homes, offices and other networked places.
- **The LANs are scalable in nature**, i.e. devices may be added or removed from the network at greater ease than wired LANs.
- The system is portable within the network coverage. Access to the network is not bounded by the length of the cables.
- **Installation and setup are much easier** than wired counterparts.
- The equipment and setup costs are reduced.

Disadv. Of Wireless Network

- **Using of short radio ranges.**



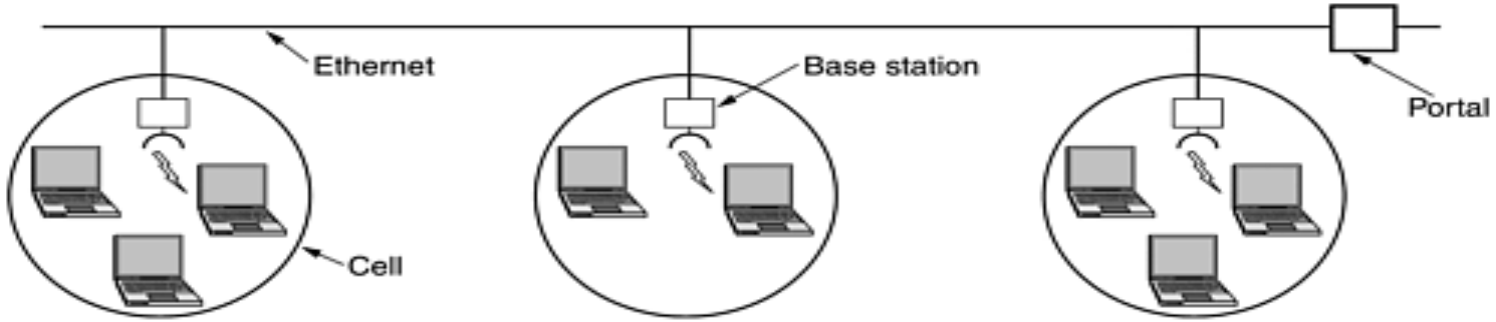
- **Multipath fading.**

A radio signal can be reflected off solid objects, so it may be received multiple times (along multiple paths). This interference results in what is called multipath fading.

- **Software is not aware of mobility**.

Ex: When the computer on which the word processor runs is taken into a new environment, the built-in list of printers becomes invalid.

- **If the note book is away from its base station it is using**



Connection Oriented Networks:

X.25:

- First public Network designed to support direct connection of terminals and computers over long distances.
- A computer established the connection to the remote computer
- X.25 packets uses a connection number.
- X.25 packets consist of 3-byte header and up to 128 bytes of dada.

Frame Relay:

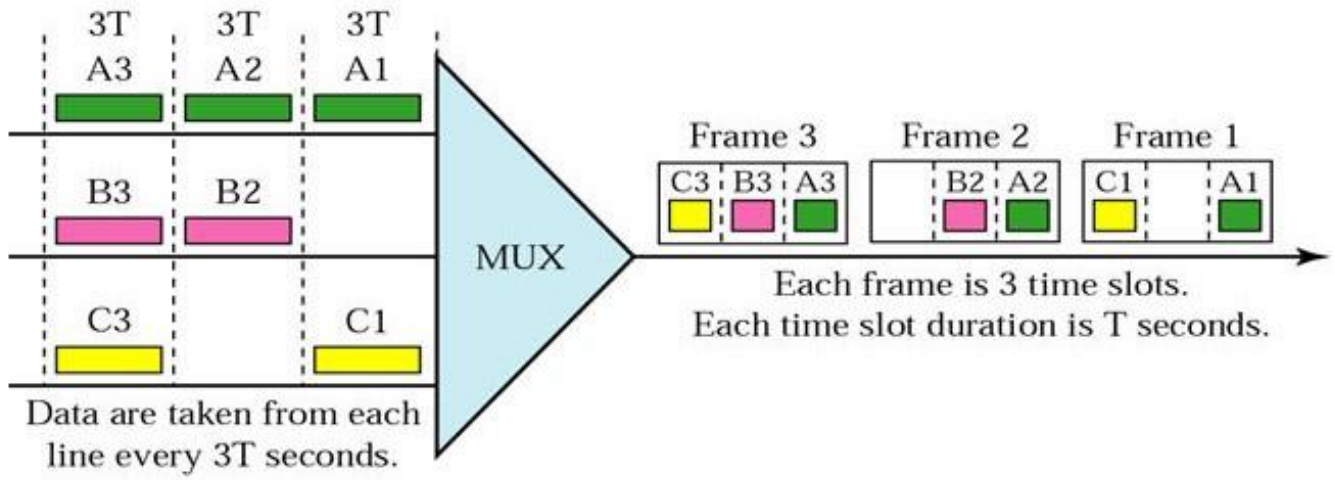
- Connection oriented network with no error control and no flow control.
- Packets are delivered in order.

Connection Oriented Networks: Asynchronous Transfer Mode (ATM)

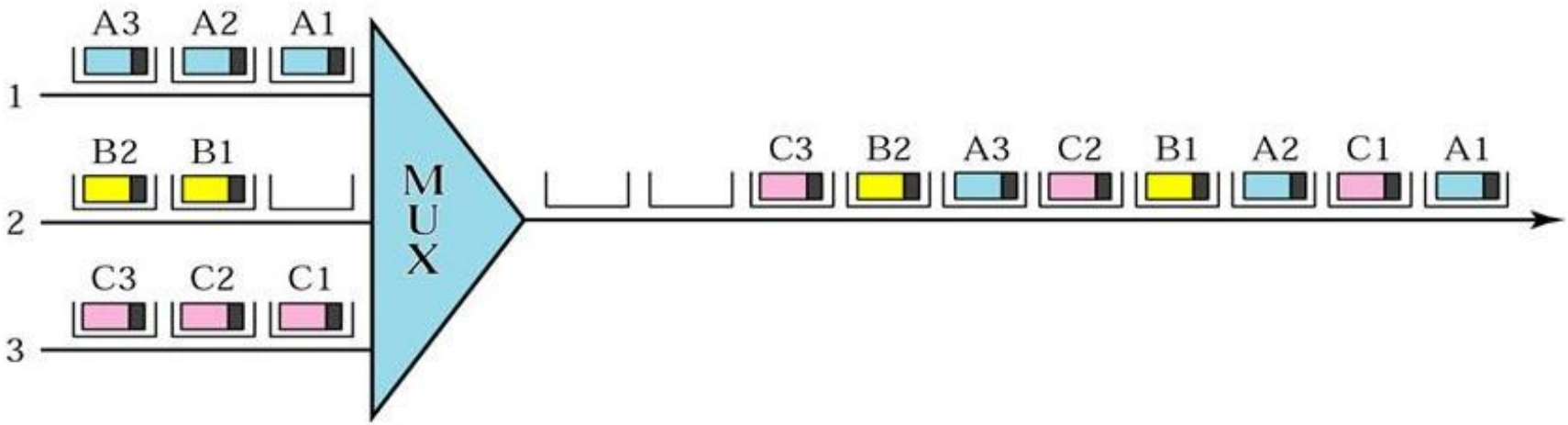
ATM

- By the mid 1980s, three types of communication networks had evolved.
- The ***telephone network*** carries ***voice calls***, ***television network*** carries ***video*** transmissions, and newly emerging ***computer network*** carries ***data***.
- The telecommunication industry decided to expand its business by developing networks to carry traffic other than voice.
- ATM is a connection-oriented, high-speed, low-delay switching and transmission technology that uses short and fixed-size packets, called ***cells***, to transport information.
- Using the ***cell switching technique***, ATM combines the benefits of both ***circuit switching*** (low and constant delay, guaranteed capacity) and ***packet switching*** (flexibility, efficiency for bursty traffic) to support the transmission of *multimedia traffic* such as voice, video, image, and data over the same network.

ATM



Normal mode of TDM

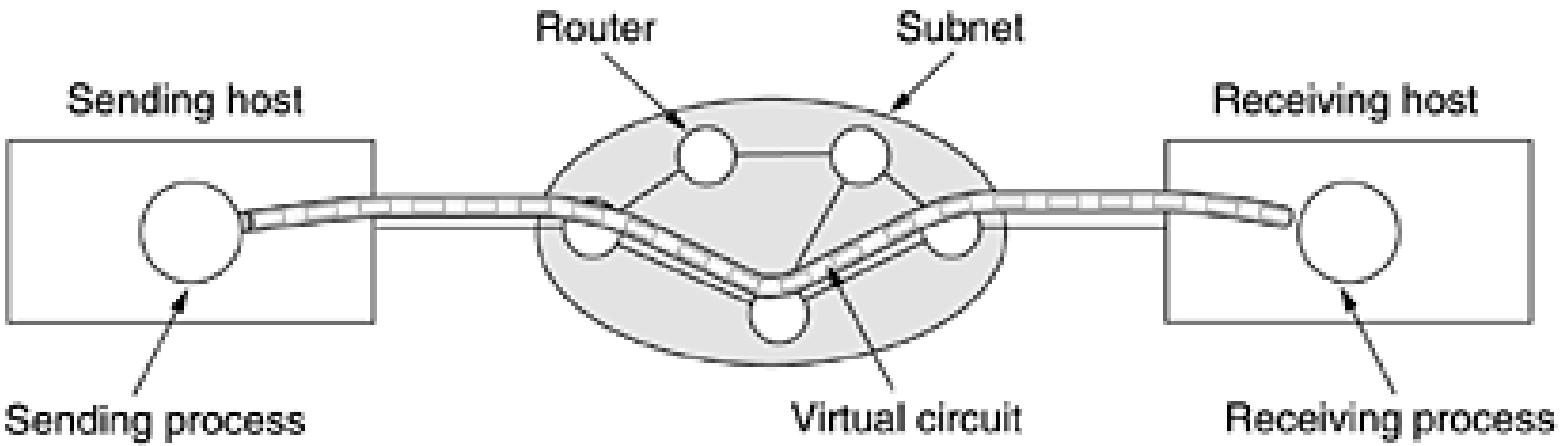


Asynchronous multiplexing of ATM

Why ATM?

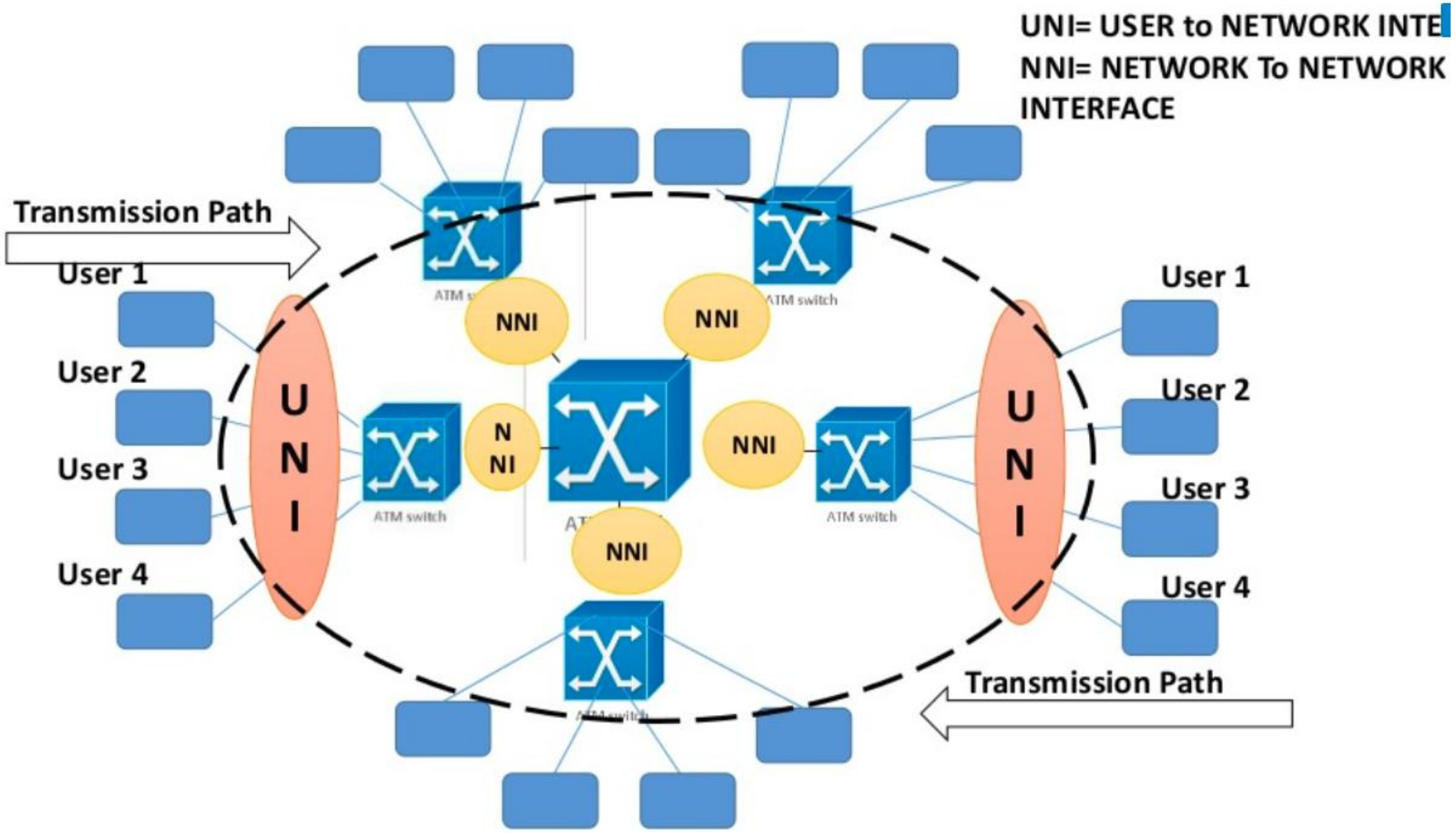
- International standard-based technology.
- Low network latency and Low variance of delay.
- Guaranteed quality of service.
- High capacity switching and Bandwidth flexibility.
- Scalability.
- Medium not shared for ATM LAN.
- Supports a wide range of user access speeds appropriate for LANs, MANs, and WANs
- Supports audio, video, imagery, and data traffic (for integrated services)

ATM Architecture



ATM Network Comprises ATM Switches and Endpoints

ATM Architecture



ATM Virtual Connections

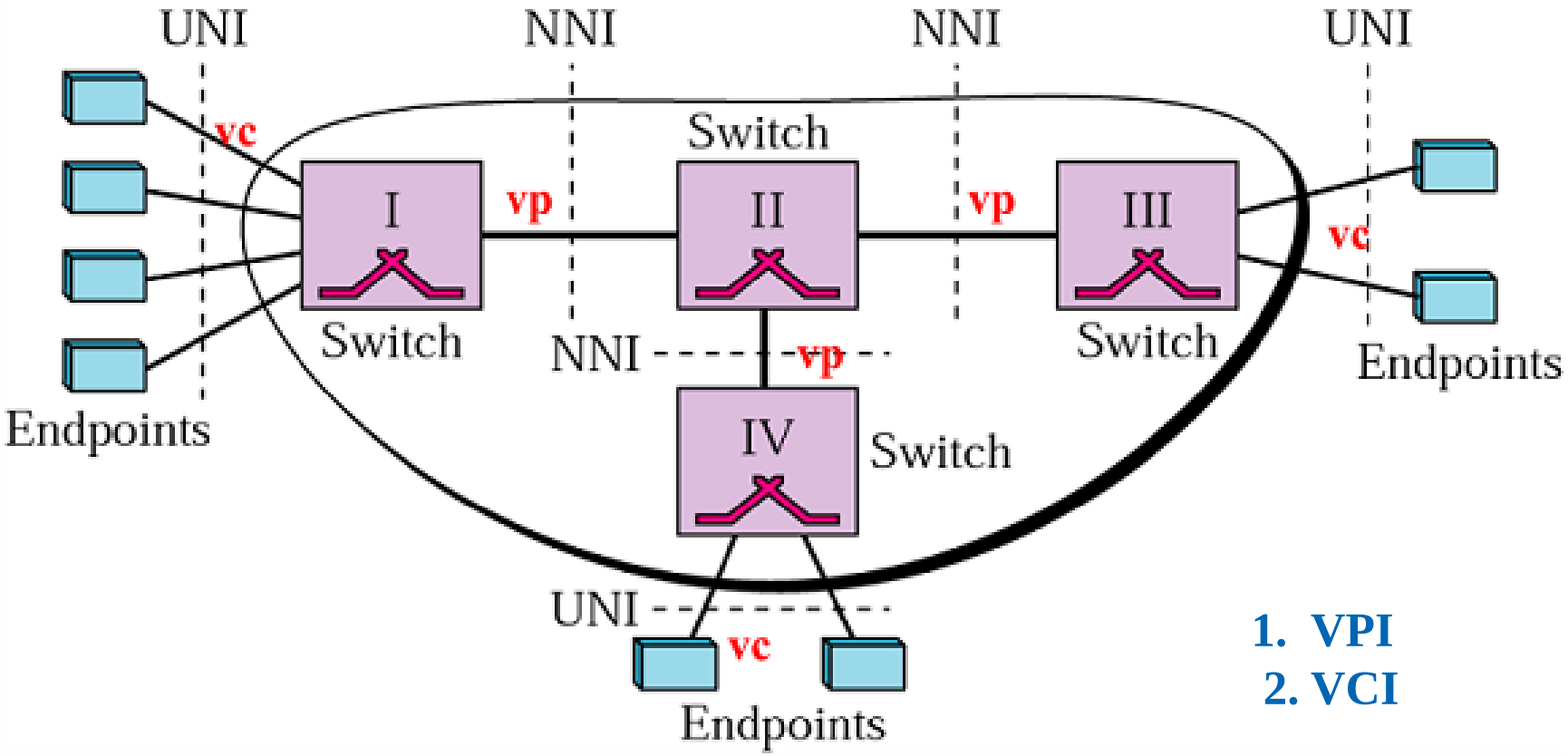
- **A Transmission path (TP) is the physical connection (wire, cable, satellite, and so on) between an end point and a switch or between two switches**

- **A Virtual Path (VP) transports ATM cells belonging to virtual channels which share a common identifier, called the Virtual Path Identifier VPI. Connects two switches.**

- **A Virtual Channel (VC) provides the transport of ATM cells which have the same unique identifier, called the Virtual Channel Identifier (VCI).**

ATM virtual connections

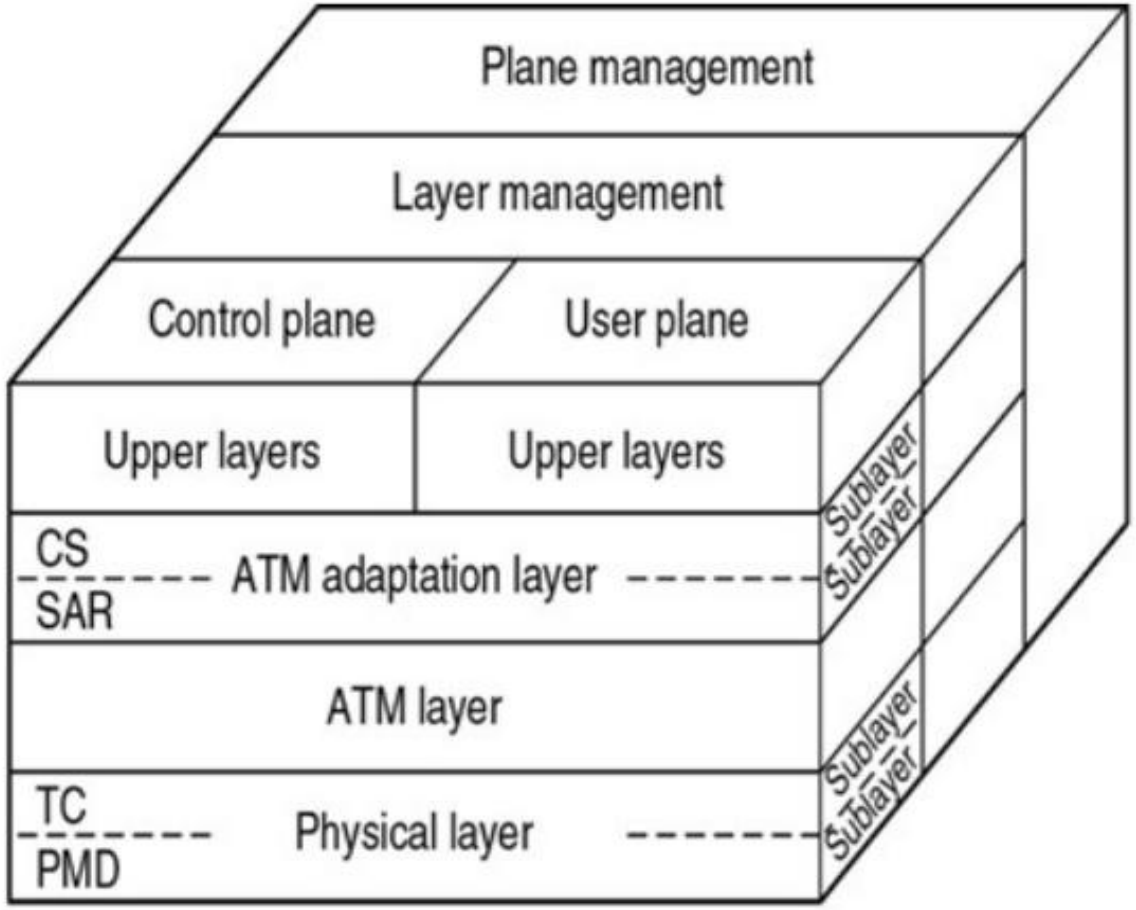
ATM Virtual Connections



1. **VPI**
2. **VCI**

ATM virtual connections

ATM Reference Model



CS: Convergence sublayer

SAR: Segmentation and reassembly sublayer

TC: Transmission convergence sublayer

PMD: Physical medium dependent sublayer

ATM Reference Model

- **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.

Physical Layer

- **Physical layer deals with the physical medium**: voltages, bit timing, and various other issues.
- No specific rules for the cells regarding the chose of transmission medium.
- ATM cells can be sent on a wire or fibre by themselves.

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.

ATM Adaptation Layer

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.).

SAR (Segmentation And Reassembly) sub layer:

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

END OF CHAPTER-1