Computer Networks

Lecture by:

Jalauddin Mansur

Chapter 1: Introduction to Computer Network

Topics to cover:

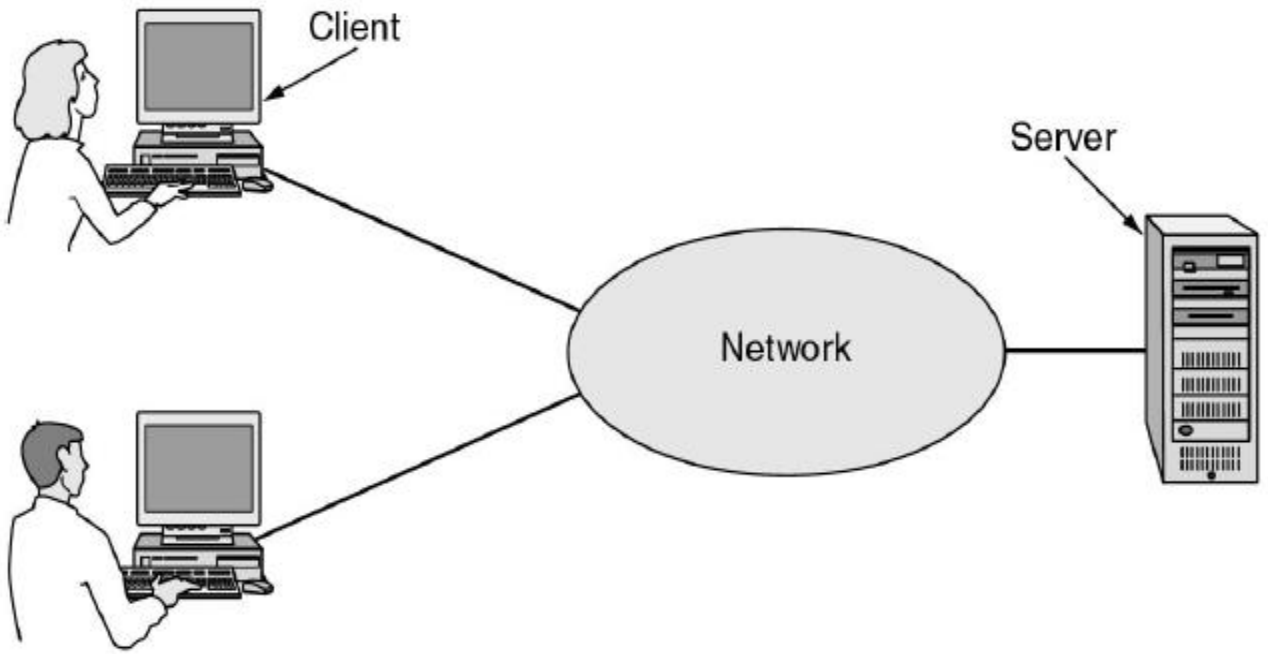
- Uses of Computer Network
- Networking model client/server, p2p, active network
- Protocols and Standards
- OSI model and TCP/IP model
- Comparison of OSI and TCP/IP model
- Example network: The Internet, X.25, Frame Relay, Ethernet, VOIP, NGN and MPLS, XDSL

Uses of Computer Networks (Application)

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

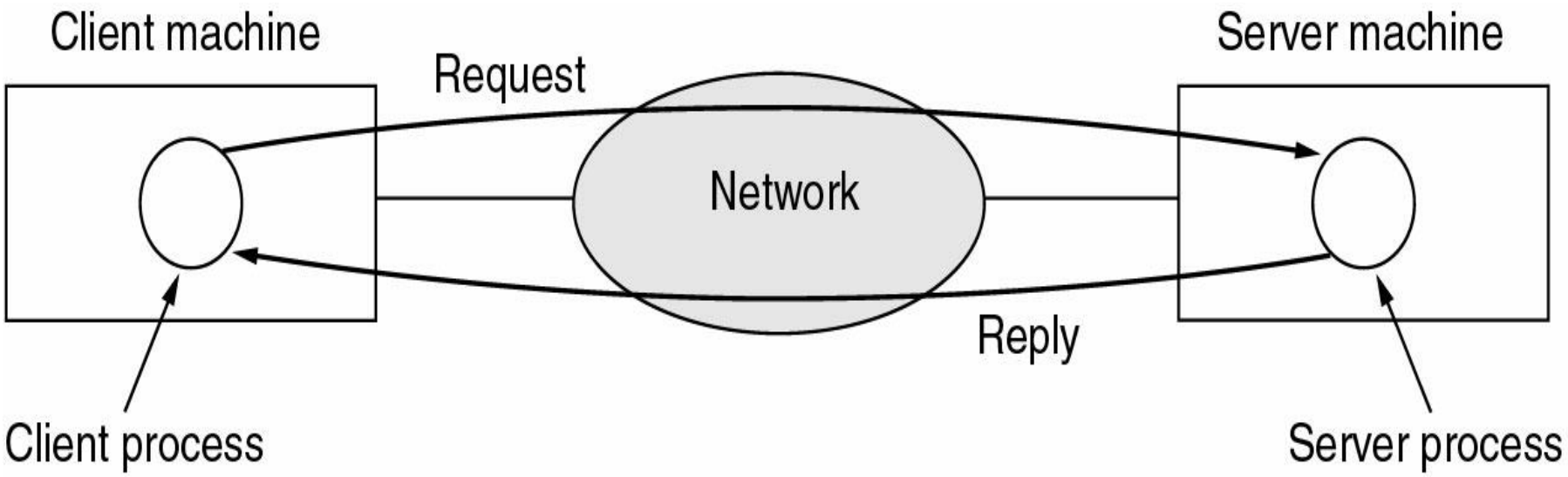
Business Application

Business Applications of Networks



A network with two client and one server

Business Applications of Networks

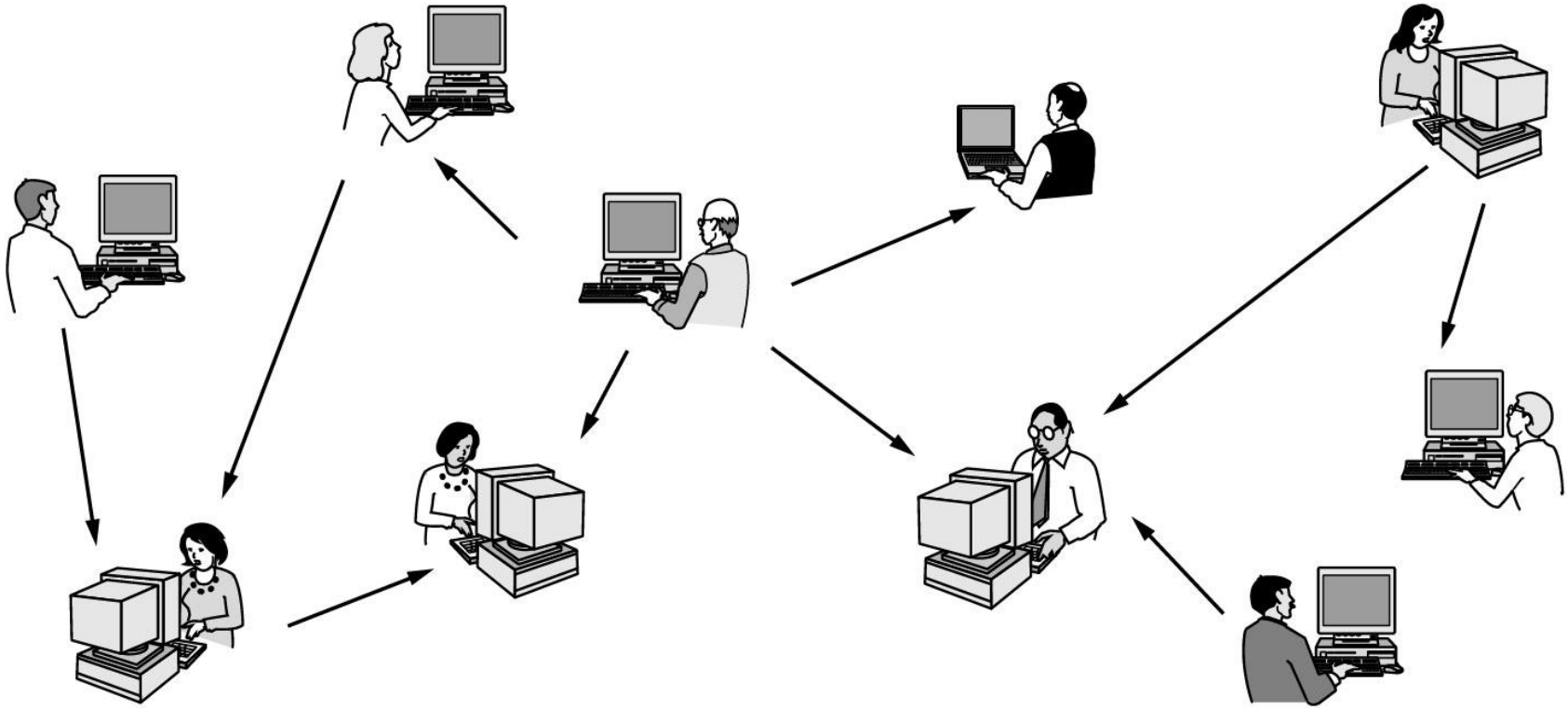


The client-server model involves requests and replies

Home Network Applications

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

Home Network Applications



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

Home Network Applications

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

Mobile Users

- Mobile computers, such as laptop and handheld computers, are one of the fastest-growing segments of the computer industry.
- Their sales have already overtaken those of desktop computers.
- Why would anyone want one?
  - People on the go often want to use their mobile devices to
    - read and send email
    - tweet, watch movies, download music, play games, or
    - simply to surf the Web for information.
- Naturally, they want to do them from anywhere on land, sea or in the air.

Social Issues

- Social networks
- message boards
- content sharing sites
- host of any applications allow people to share their views with like-minded individuals.
- As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise.
- The trouble comes with topics that people actually care about, like politics, religion, or sex.

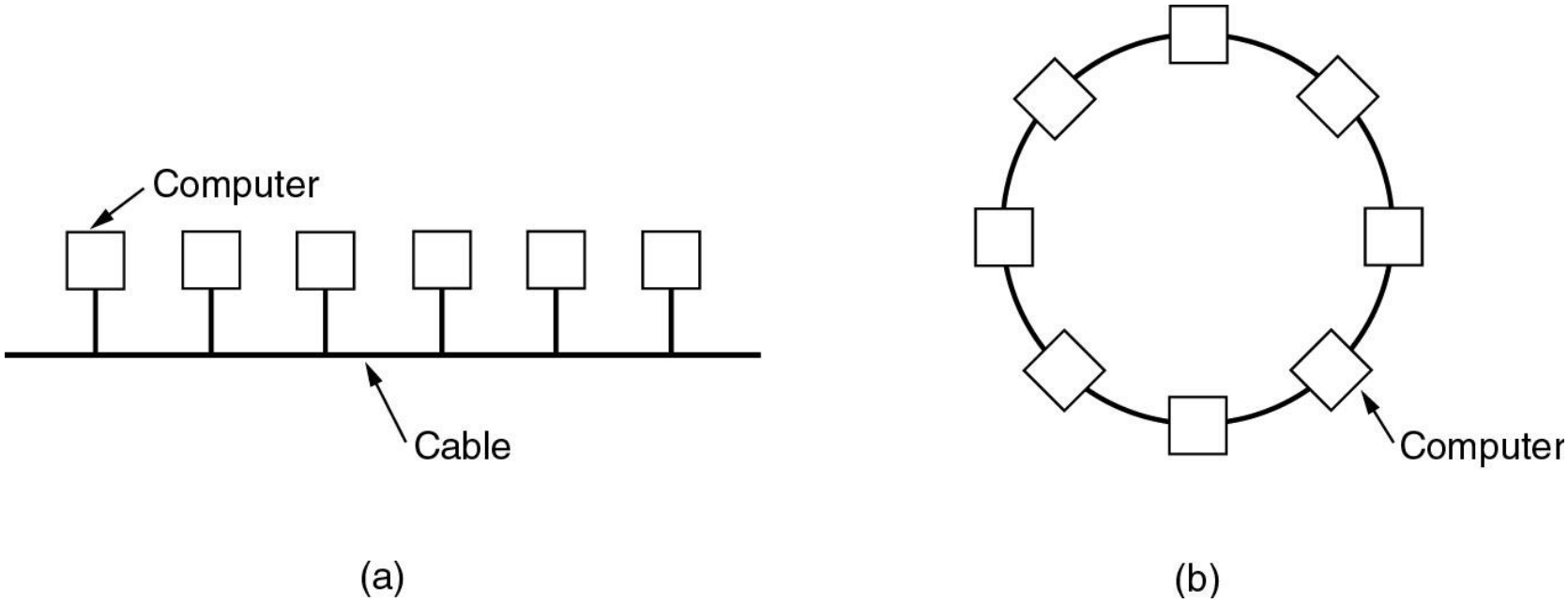
Network Hardware

- Local Area Networks
- Metropolitan Area Networks
- Wide Area Networks
- Wireless Networks
- Home Networks
- Internetworks

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

Classification of interconnected processors by scale

Local Area Networks (LAN)



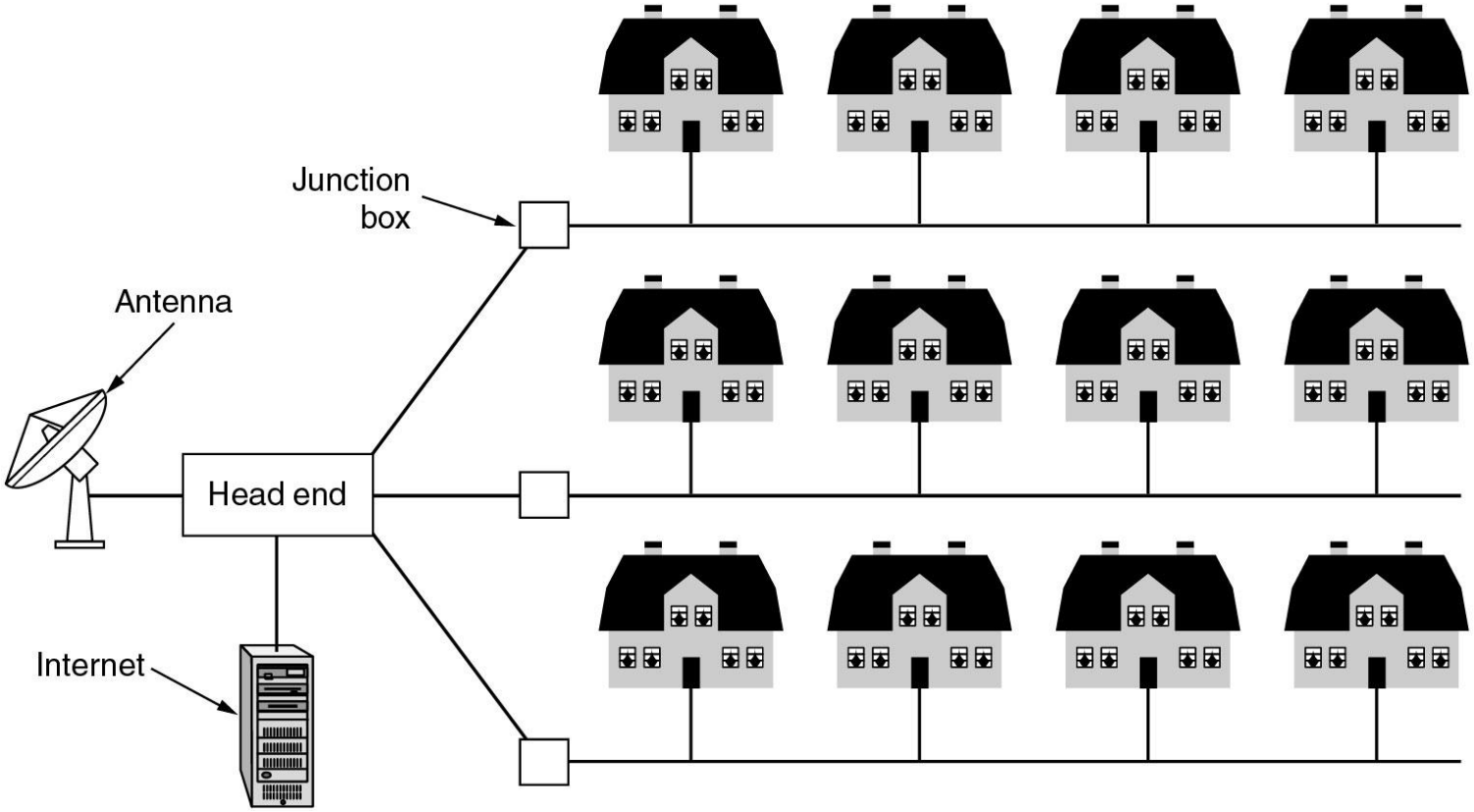
Two broadcast networks

- Bus
- Ring

LAN Contd..

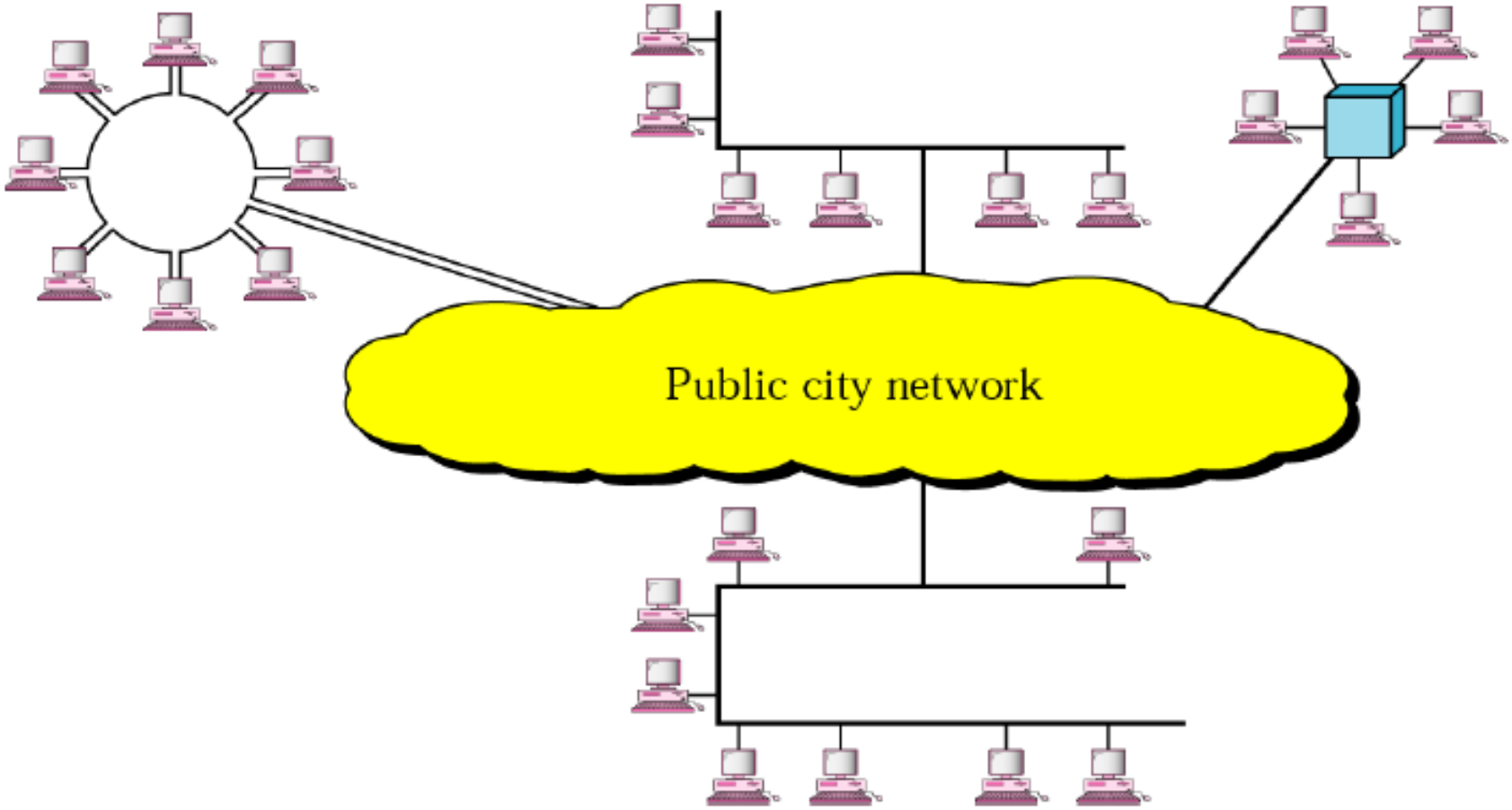
- A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory.
- When LANs are used by companies, they are called **enterprise networks.**
- WLAN is the wireless LAN in which the devices use the radio spectrum to communicate with the other devices.
- There is a standard for wireless LANs called IEEE 802.11, popularly known as **WiFi**

Metropolitan Area Networks (MAN)



A metropolitan area network based on cable TV

MAN Example



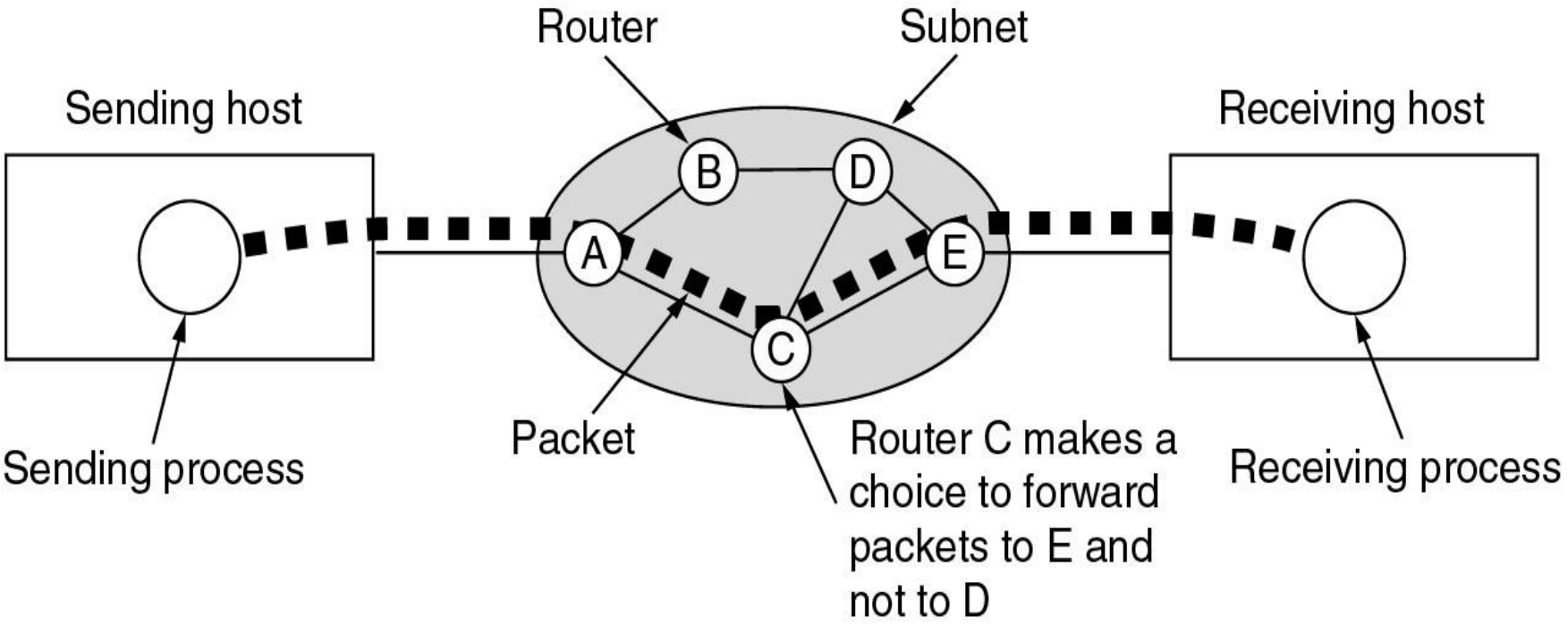
MAN Contd..

- Computer network larger than a LAN, covering an area of a few city(By Cable Networks) blocks to the area of an entire city
- Might be owned and operated by a single organization, but it usually will be used by many individuals and organizations.
- Backbone of MAN is high-capacity and high-speed fiber optics. MAN works in between Local Area Network and Wide Area Network.

Wide Area Networks (WAN)

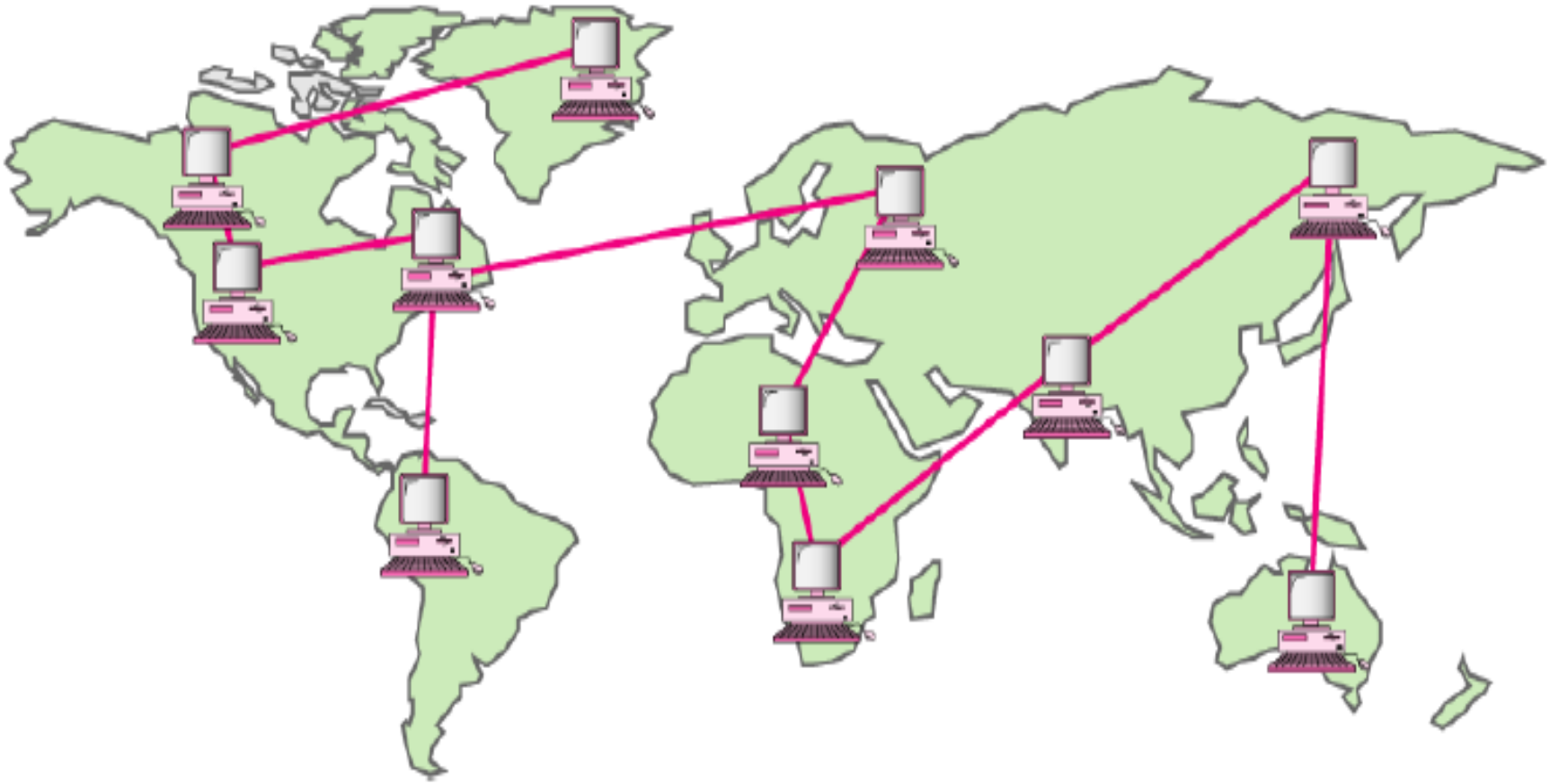
- Spans a large geographical area, often a country or continent.
- Telecommunication networks are Wide Area Network.
- These networks provides connectivity to MANs and LANs.
- Equipped with very high speed backbone, WAN uses very expensive network equipment.

WAN



A stream of packets from sender to receiver

WAN Contd..



Home Network Categories

- Computers (desktop PC, PDA, shared peripherals)
- Entertainment (TV, DVD, VCR, camera, stereo, MP3)
- Telecom (telephone, cell phone, fax)
- Appliances (microwave, fridge, clock, lights)
- Telemetry (burglar alarm, babycam).

Internetworks

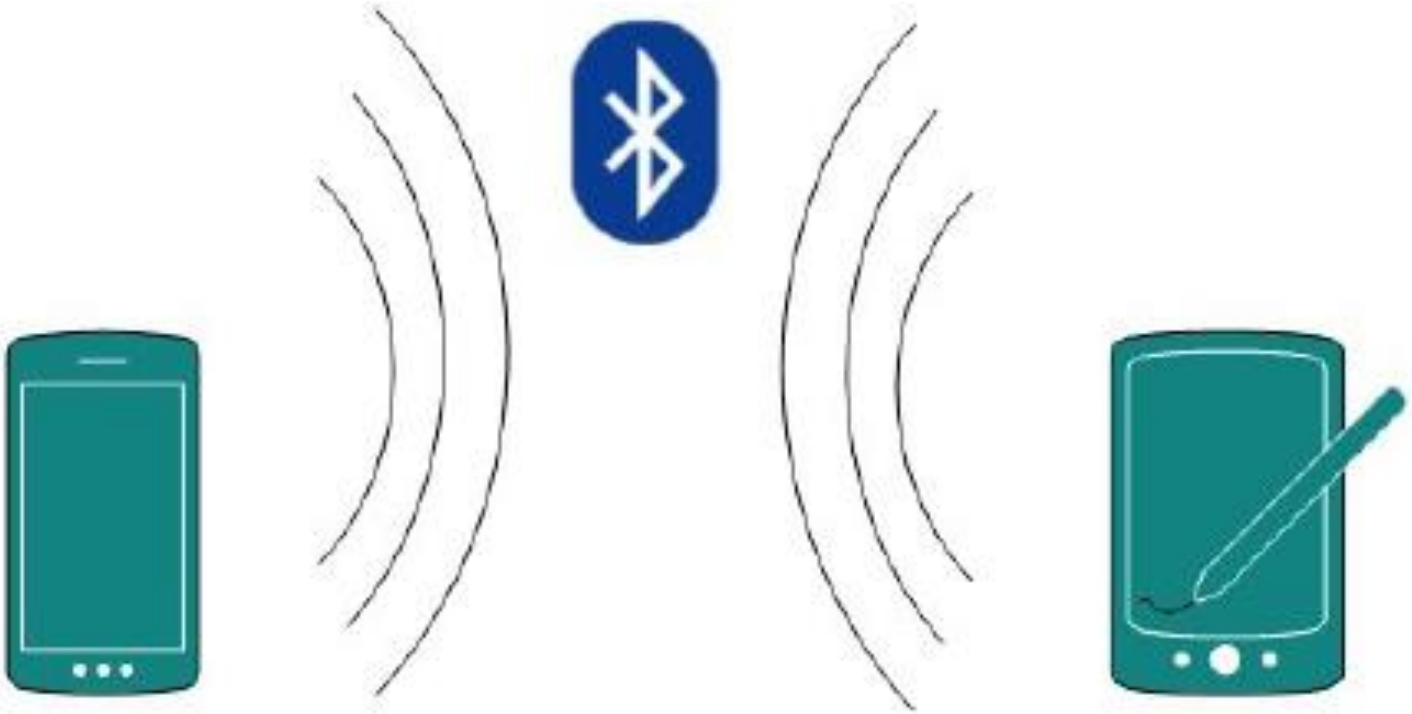
- Any interconnection among or between public, private, commercial, industrial, or governmental networks.
- Internet
  - The Internet consists of a worldwide interconnection of governmental, academic, public, and private networks.
- Intranet
  - An intranet is the internal network of an organization

- Under the control of a single administrative entity.

- Extranet
  - An extranet cannot consist of a single LAN; it must have at least one connection with an external network.

PAN (Personal Area Network)

- Computer network used for data transmission among devices such as computers, telephones and personal digital assistants
- Communication among the personal devices themselves (**intra personal communication)**



PAN example

Networking Model/Network Classification

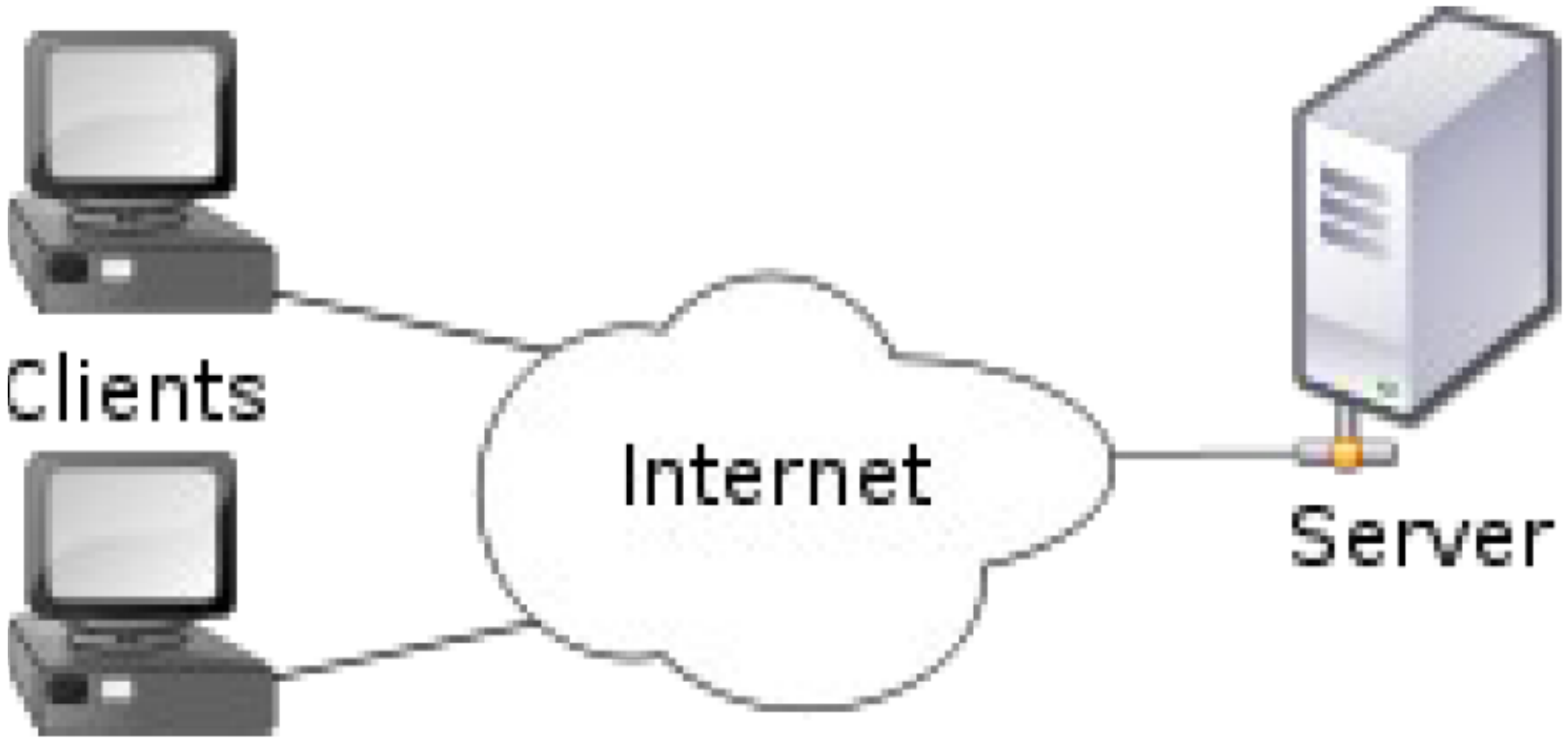
By Structure / Functional Relationship

- Client / Server
- Peer to Peer (P2P)
- Active Network Model

Client/Server network

- Suitable for larger networks.
- Nodes and servers share data roles
- Nodes are called clients
- Servers are used to control access
- Database software
  - Access to data controlled by server
- Server is the most important computer
- Examples:
  - Email, Network Printing, WWW

- Types of Client
  - Thin Client
  - Thick Client
- Types of server
  - Database server
  - Web server
  - Messaging server
  - Application Server
  - DNS server, etc

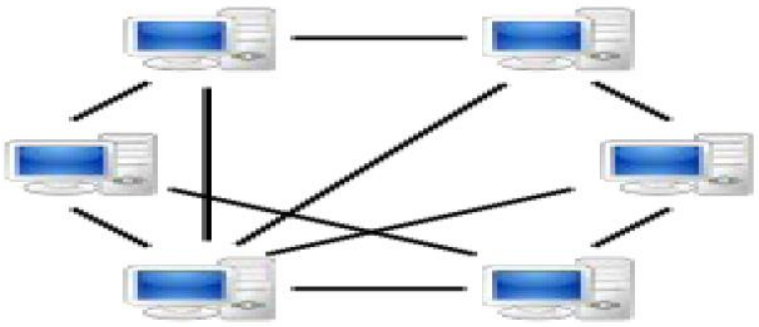


Client Server Model

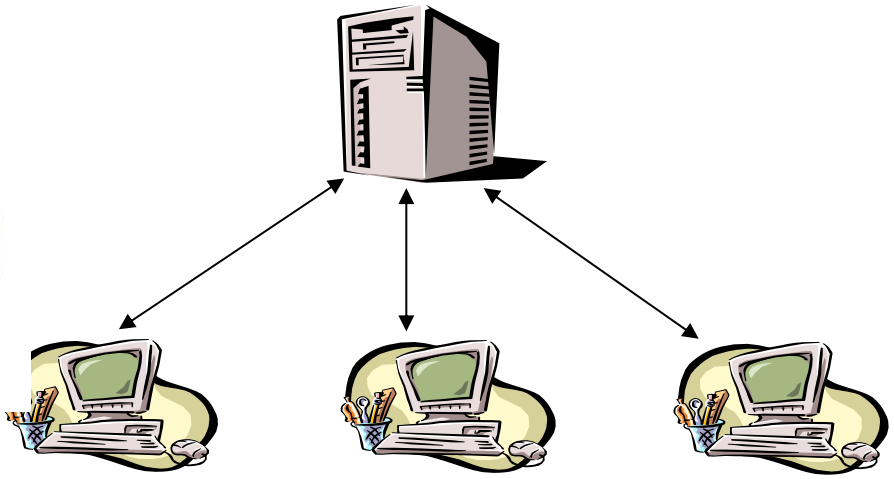
Peer to Peer Networks (P2P)

- Peer-to-Peer computing is inspired by the controversial music-sharing service Napster
- Instead of Internet information being held in a few central locations, Peer-to-Peer computing makes it theoretically possible to access the files and data residing on every personal computer connected to the Internet

P2P



Not P2P



What is P2P?

- Is a technology which “enables any network-aware device to provide services to another network-aware device”
- A peer in P2P network acts as both a client and a server in traditional client/server architecture
- Problem with Server-Client Model
  - Scalability
    - As the number of users increases, there is a higher demand for computing power, storage space, and bandwidth associated with the server-side
  - Reliability
    - The whole network will depend on the highly loaded server to function properly

Advantage of P2P model

- The system is based on the direct communication between peers
- There is zero reliance on centralized service or resources for operations
- The system can survive extreme changes in network composition
- They thrive in a network with heterogeneous environment
- This model is highly scalable

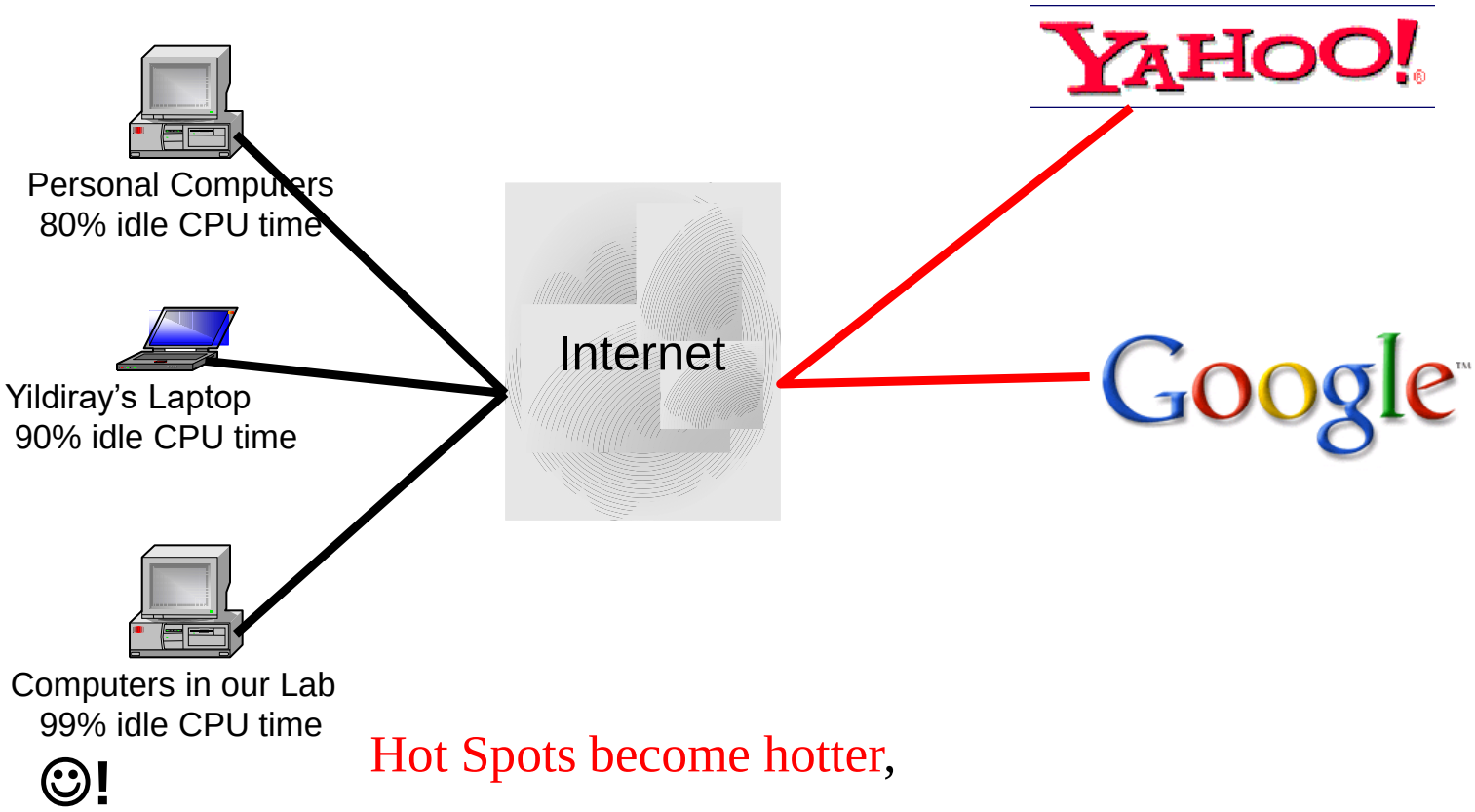
Why P2P?

- The Internet has three valuable fundamental assets
  - Information
  - Computing resources
  - Bandwidth
- All of which are vastly under utilized, partly due to the traditional client-server model
- First, no single search engine or portal can locate and catalog the ever-increasing amount of information on the Web in a timely way
- Moreover, a huge amount of information is transient and not subject to capture by techniques such as Web crawling
  - Google claims that it searches about 1.3×10^8 web pages
  - Finding useful information in real time is increasingly difficult!
- Many information can not be captured by web crawling.
  - The world produces 2 exabyte(10^{18}) of information every year, only publishes 300 terabyte(10^{12})

Why P2P Contd..

- Second, although miles of new fiber have been installed, the new bandwidth gets little use if everyone goes to Yahoo for content and to eBay
- Instead, hot spots just get hotter while cold pipes remain cold
- This is partly why most people still feel the congestion over the Internet while a single fiber's bandwidth has increased by a factor of 10^6 since 1975, doubling every 16 months.
- Finally, new processors and storage devices continue to break records in speed and capacity, supporting more powerful end devices throughout the network
- However, computation continues to accumulate around data centers, which have to increase their workloads at a crippling pace, thus putting immense pressure on space and power consumption

Why P2P Contd..



Hot Spots become hotter,

Yet Cold spots keep cold

Why P2P?

- Eliminating the single-source bottleneck
- P2P can be used to distribute data and control and load-balance requests across the Network.
- Eliminating the risk of a single point of failure
- P2P infrastructure allows direct access and shared space, and this can enable remote maintenance capability

Basic P2P elements

- Peer
  - Simple peer
  - Rendezvous Peer
  - Router Peer
  - Peer Group
- Network Transport
  - **Endpoints**—The initial source or final destination of any piece of data being transmitted over the network
  - **Pipes**—Unidirectional, asynchronous, virtual communications channels connecting two or more endpoints
  - **Messages**—Containers for data being transmitted over a pipe from one endpoint to another

Basic P2P elements Contd..

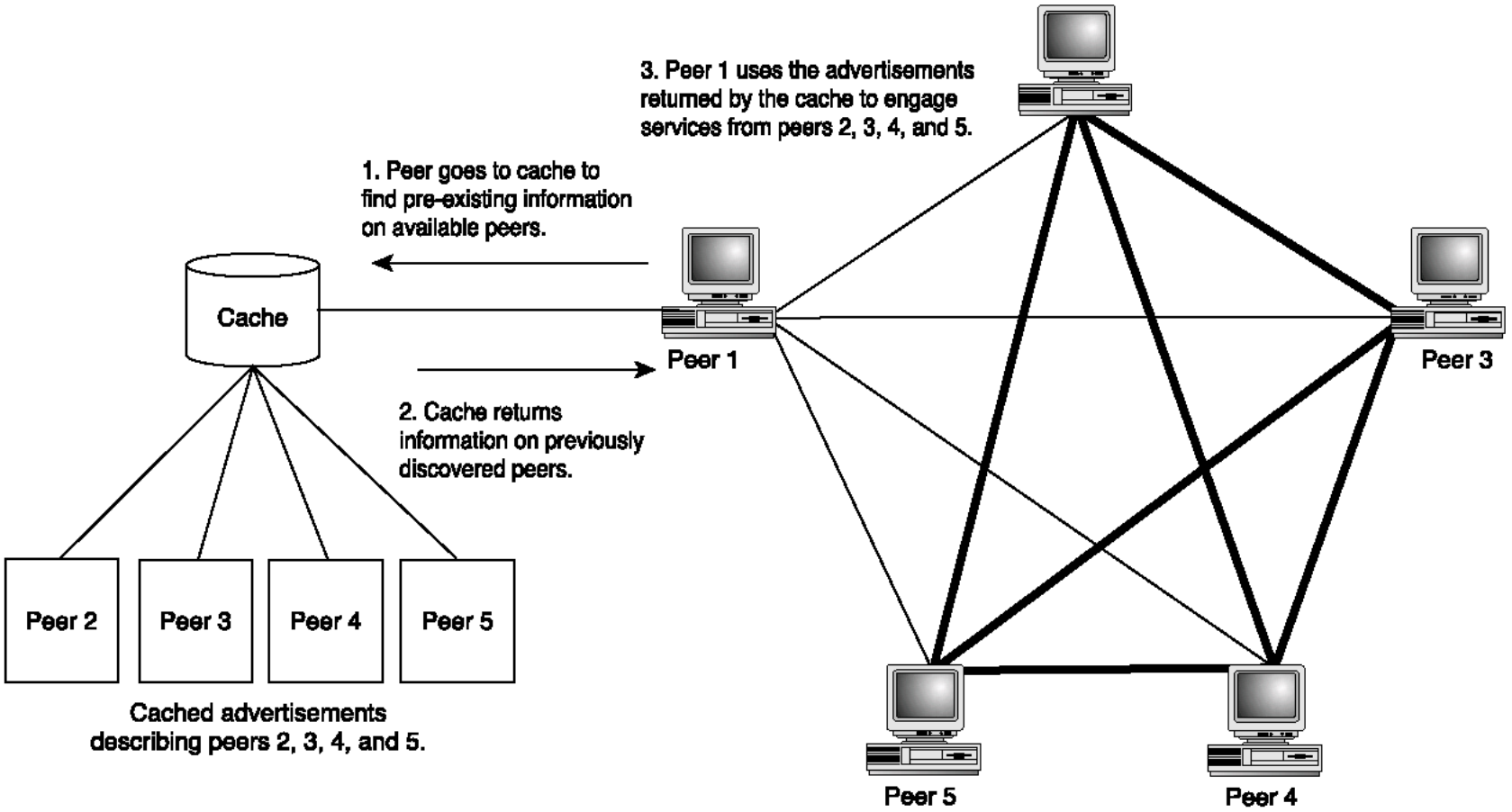
- Services
  - provide functionality that peers can engage to perform useful work on a remote peer
    - ❖transferring a file
    - ❖providing status information
    - ❖performing a calculation
- Peer group services
  - Functionality offered by a peer group to members of the peer group
  - This functionality could be provided by several members of the peer group, thereby providing redundant access to the service
- Advertisement
  - A structured representation of an entity, service, or resource made available by a peer or peer group as a part of a P2P network
  - Every entity can be described by advertisements, including peers, peer groups, pipes, endpoints, services, and content

How does P2P work?

- How does a device find peers and services on a P2P network?
- How does a device in a private network participate in P2P?
- Solution is:
  - Finding Advertisement
    - No discovery
    - Direct discovery
    - Indirect discovery

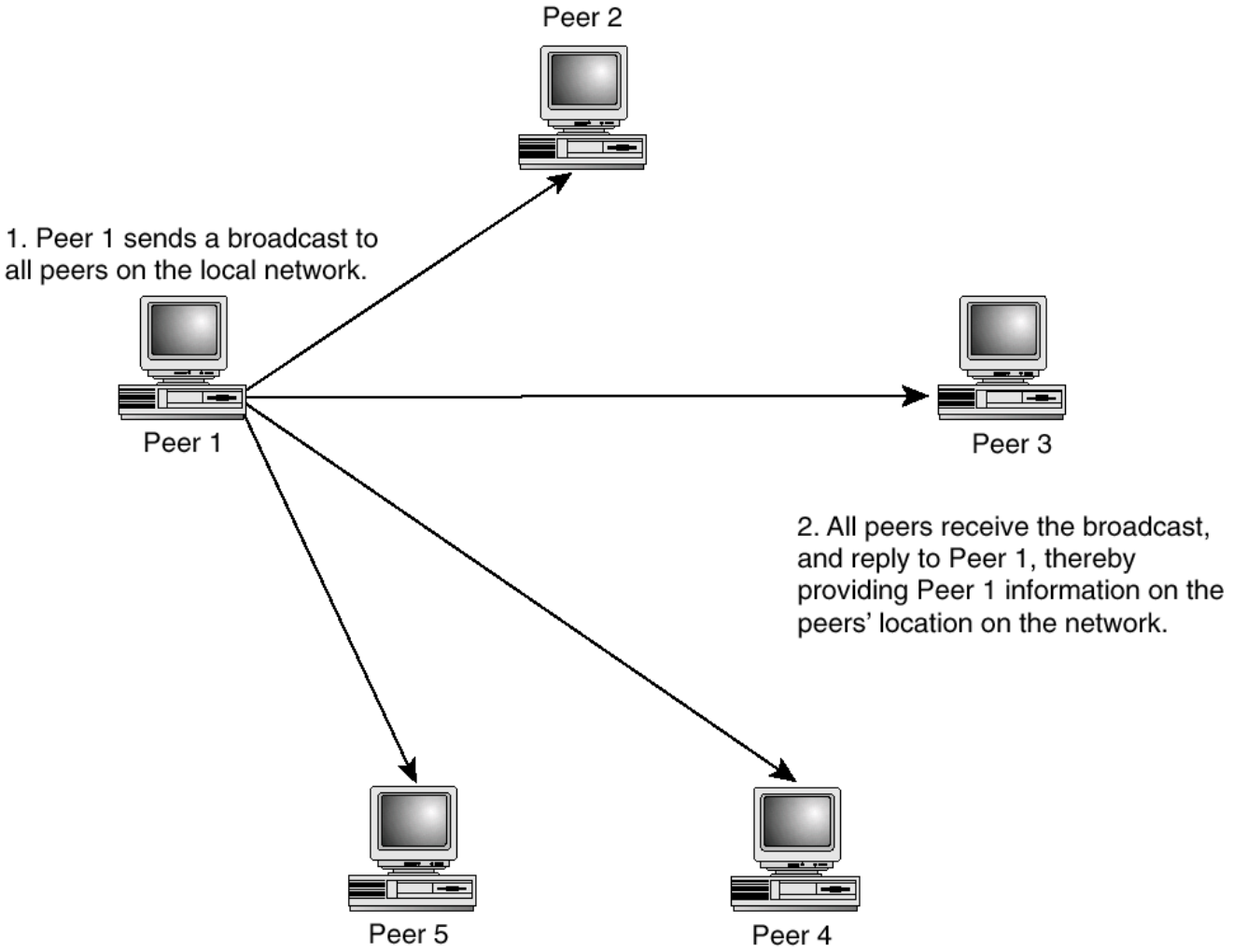
How does it work? Contd..

- No discovery



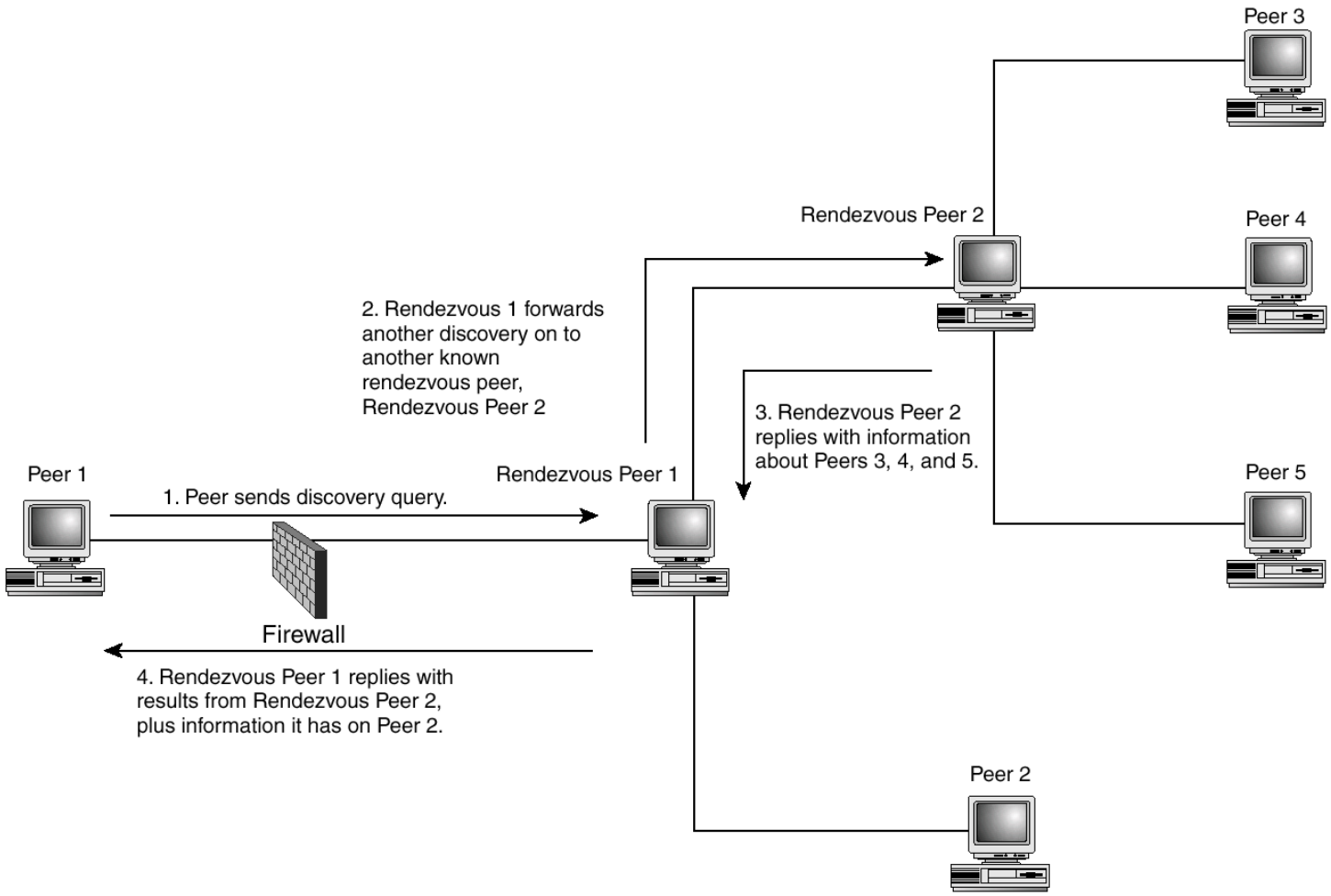
How does it work? Contd..

- Direct Discovery

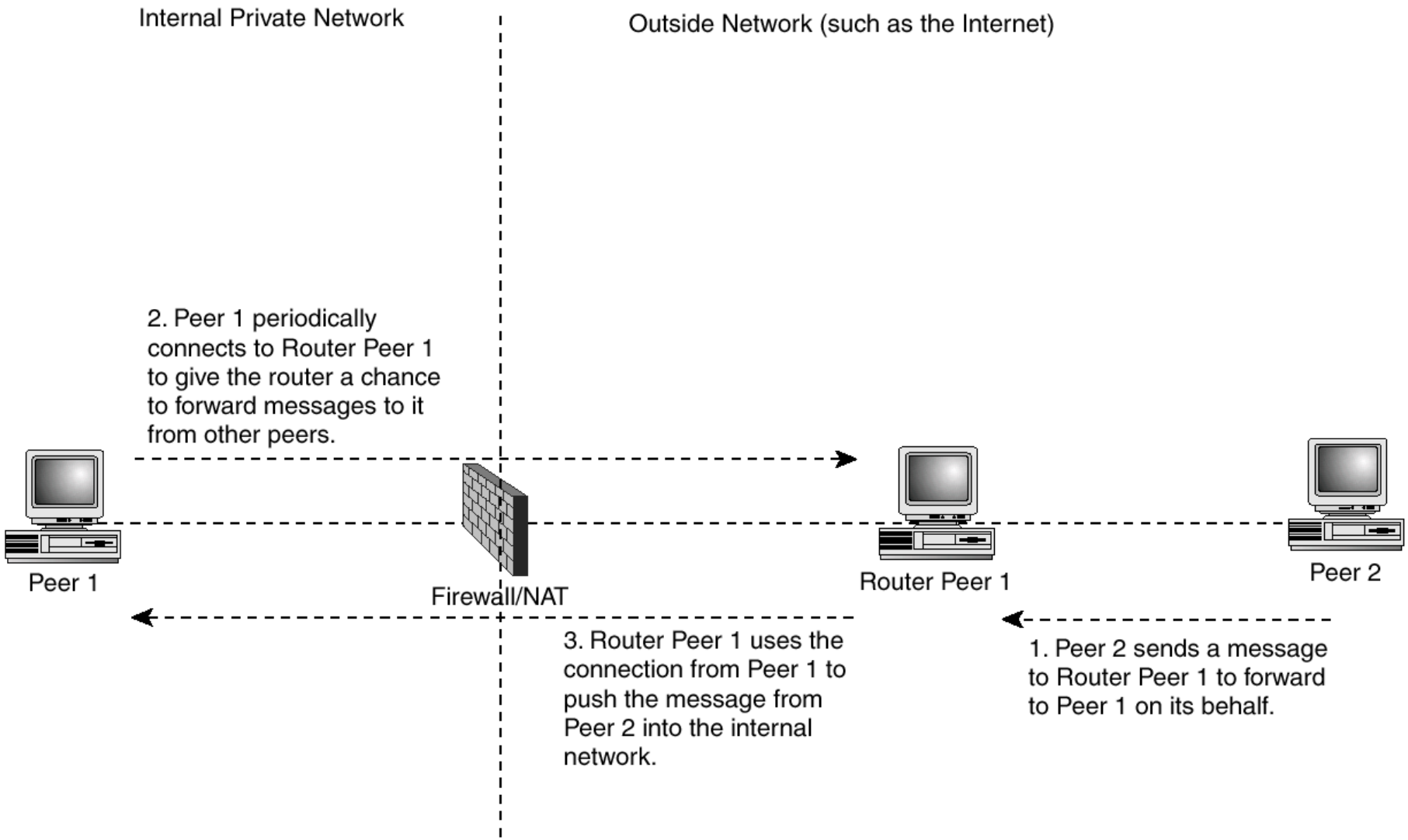


How does it work? Contd..

- Indirect Discovery



How does it work? Contd..



New problems in P2P

- How do peers distribute messages to each other without flooding the network?
  - Search is done via flooding — a distributed form of broadcast
  - Messages are sent to the neighbors who pass them on to their neighbors and so on
  - The number of hosts which are contacted in this way increases exponentially with each jump
  - 80% of the reply messages are wrong or redundancy (From paper “Experimenting with Gnutella Communities” by Jean Vaucher and …)

New problems Contd..

- How can the network encourage resource sharing?
  - In some P2P systems,
    - Peers can use the resources (bandwidth and storage space) of others on the network
    - Restrict their resources availability to the network
  - As more users choose not to share their resources
    - Those peers that do share resources come under increased load
    - Network begins to revert to the classic client/server architecture
  - Logical conclusion: The network eventually collapses, benefiting no one.

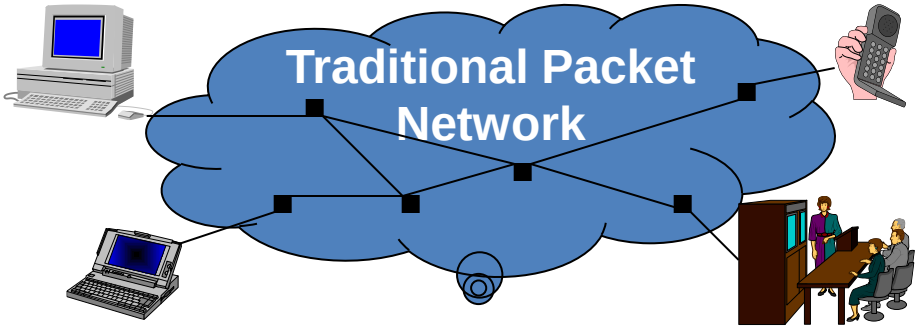
P2P Applications

- In Peer-to-Peer (P2P) computing, applications are segregated into three main categories:
  - distributed computing,
  - file sharing, and
  - collaborative applications
- Distributed computing applications typically require the decomposition of larger problem into smaller parallel problems (e.g., SETI@home)
- File sharing applications require efficient search across wide area networks *(*e.g., Napster, Gnutella, Freenet)
- Collaborative applications require update mechanisms to provide consistency in multi-user environment (e.g., Magi, Groove, Jabber)

Active Network Model

- Type of Network Architecture
- Allow packets traveling through the network to dynamically modify the operation of network
- Active network architecture is composed of execution environments (similar to a UNIX shell that can execute active packets)
- Network where switches perform custom computation on packets
- Example
  - Trace program running on each router
  - Middle-boxes: firewall, proxies, etc

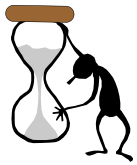
Active Networking: A Natural Evolution



Adaptive Monitoring, And Predictive Control

Devices Become Network-aware and Smart

Custom Code Injected By Applications/devices Makes Network Intelligent



Reduces Protocol Deployment Time From Years to Months

Origin of Active Networks

- DARPA research community (1994-1995)
- Identified problems with today's network
  - Difficulty of integrating new technology
  - Poor performance due to redundant operations in different protocol layer
  - Difficulty accommodating new services

Motivation of Active Networks

- Accelerating innovation
  - Internet innovation relies on consensus
  - Takes 10 years from prototype to deployment (standardization, procurement, deployment)
- Active nodes allow routers to download new services into the infrastructure
  - User driven innovation
- Active routers coexist with legacy routers

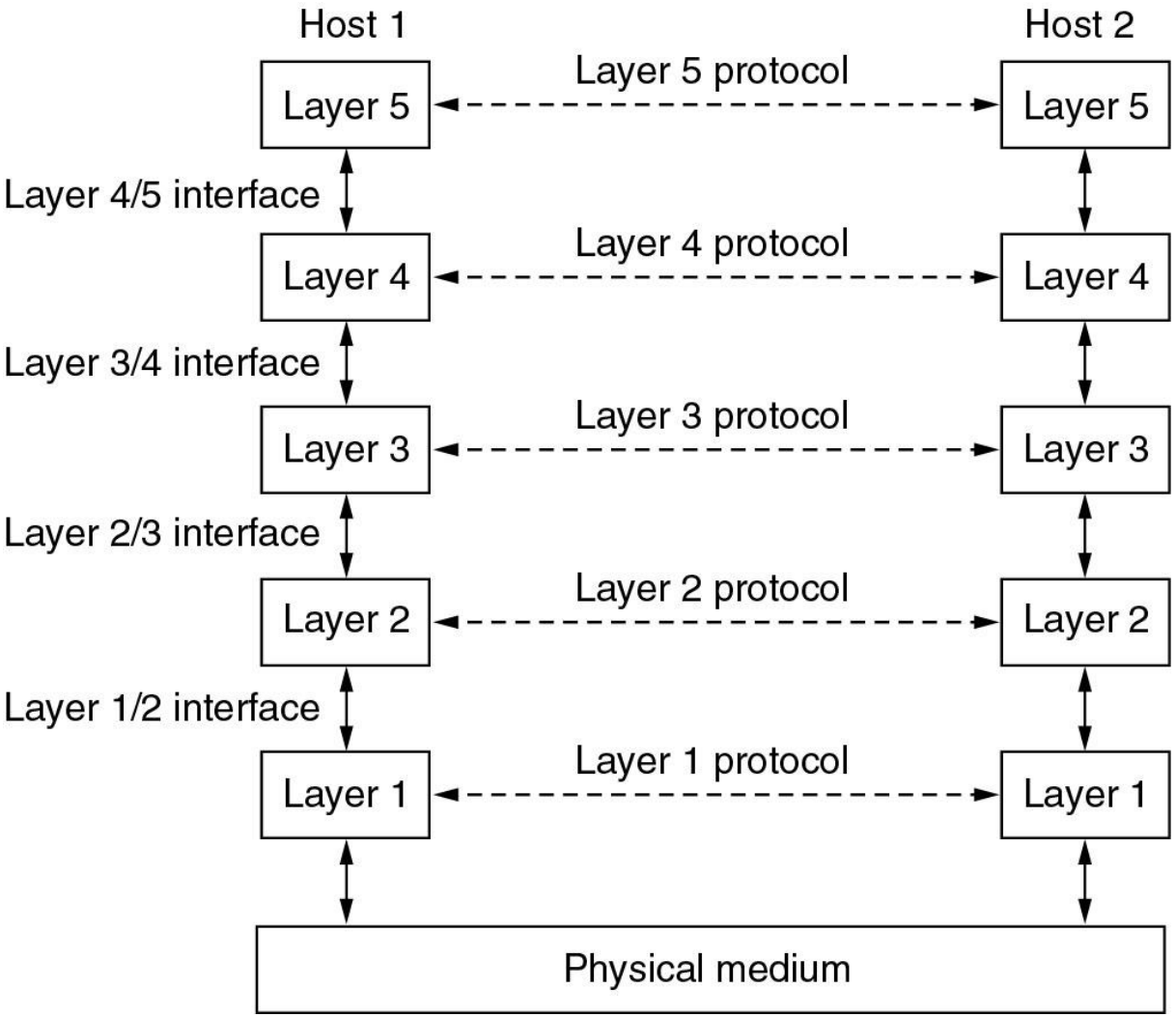
What happened to Active networks

- Timing was off
  - No clear application
  - Hardware support wasn't cheap
- Security, special language for safe code
- End user as programmer
- Interoperability

Network Software

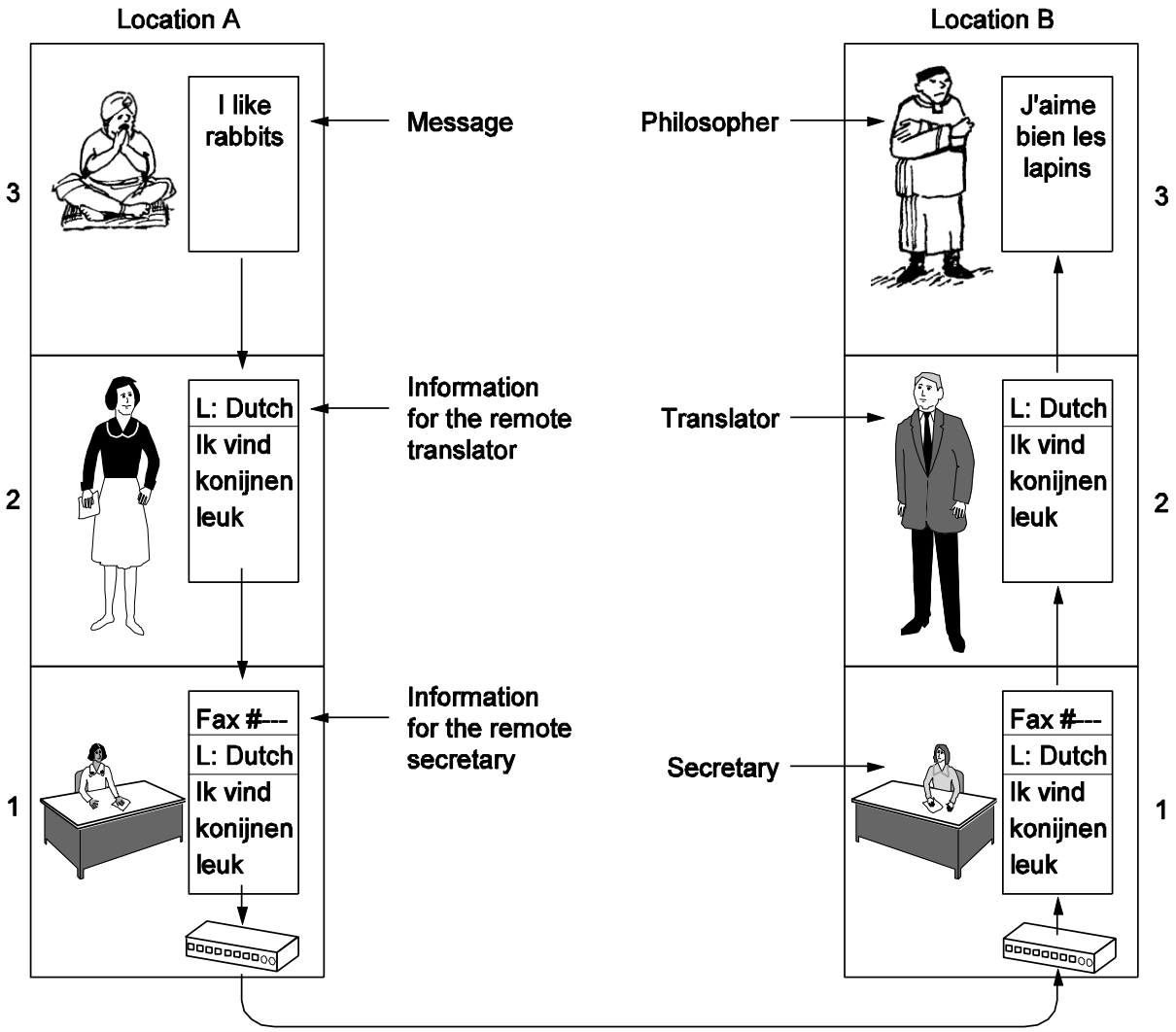
- Protocol Hierarchies
- Design Issues for the Layers
- Connection-Oriented and Connectionless Services
- Service Primitives
- The Relationship of Services to Protocols

Protocol Hierarchies



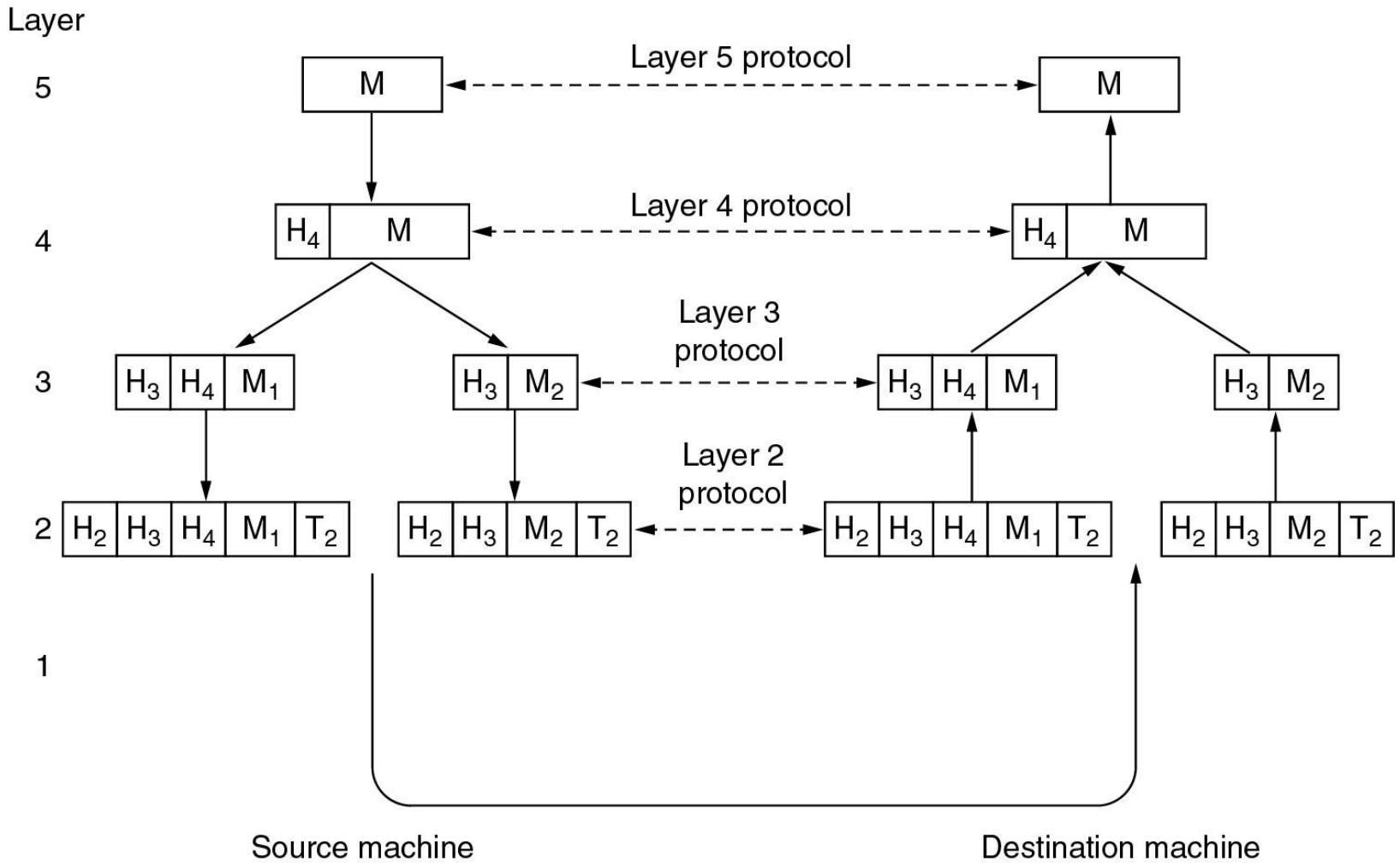
Layers, protocols, and interfaces

Protocol Hierarchies



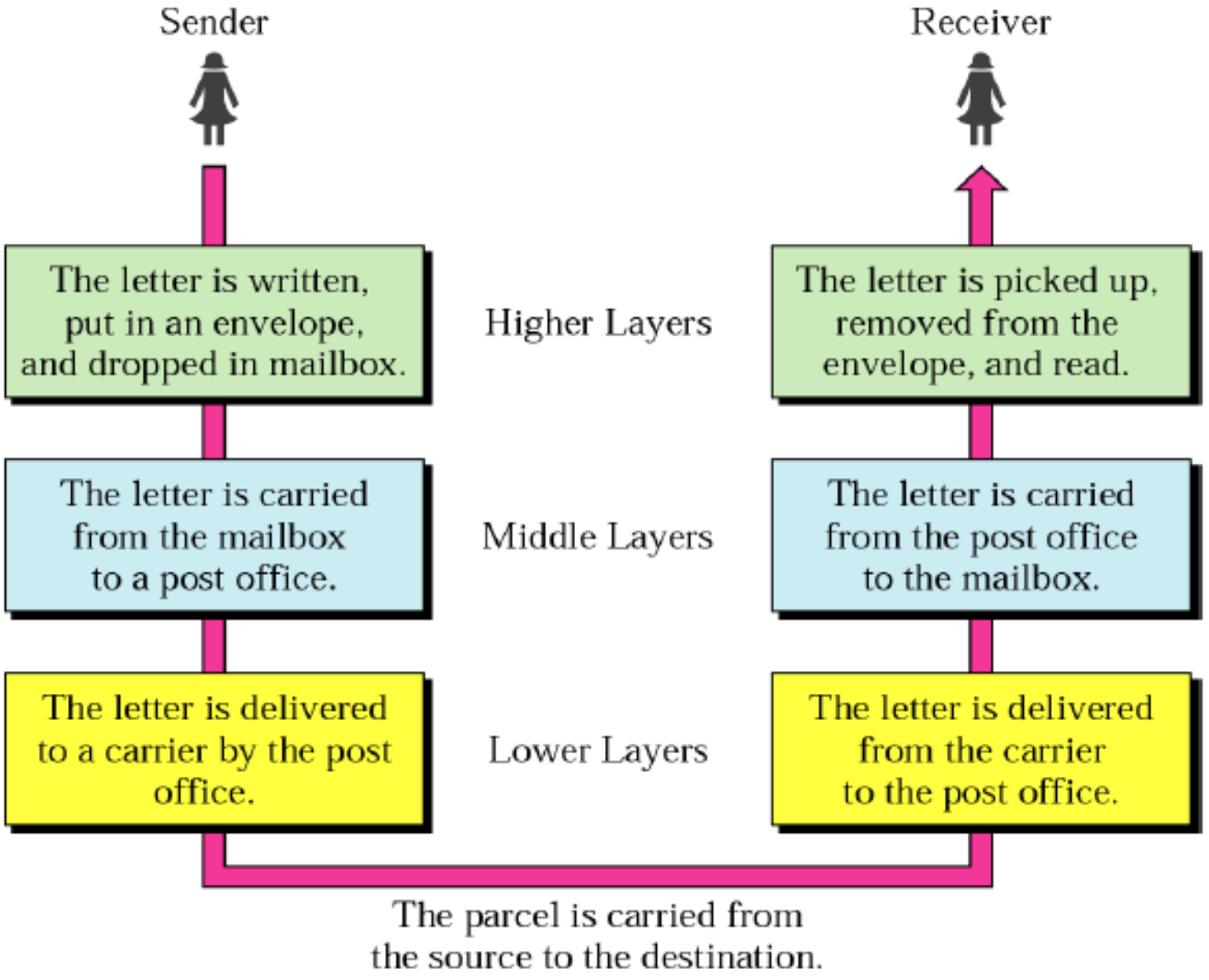
The philosopher-translator-secretary architecture.

Protocol Hierarchies



Example information flow supporting virtual communication in layer 5.

Protocol Analogy: Sending a Letter



Design Issues for the Layers

- Addressing
- Error Control
- Flow Control
- Multiplexing
- Routing

Connection-Oriented and Connectionless Services

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

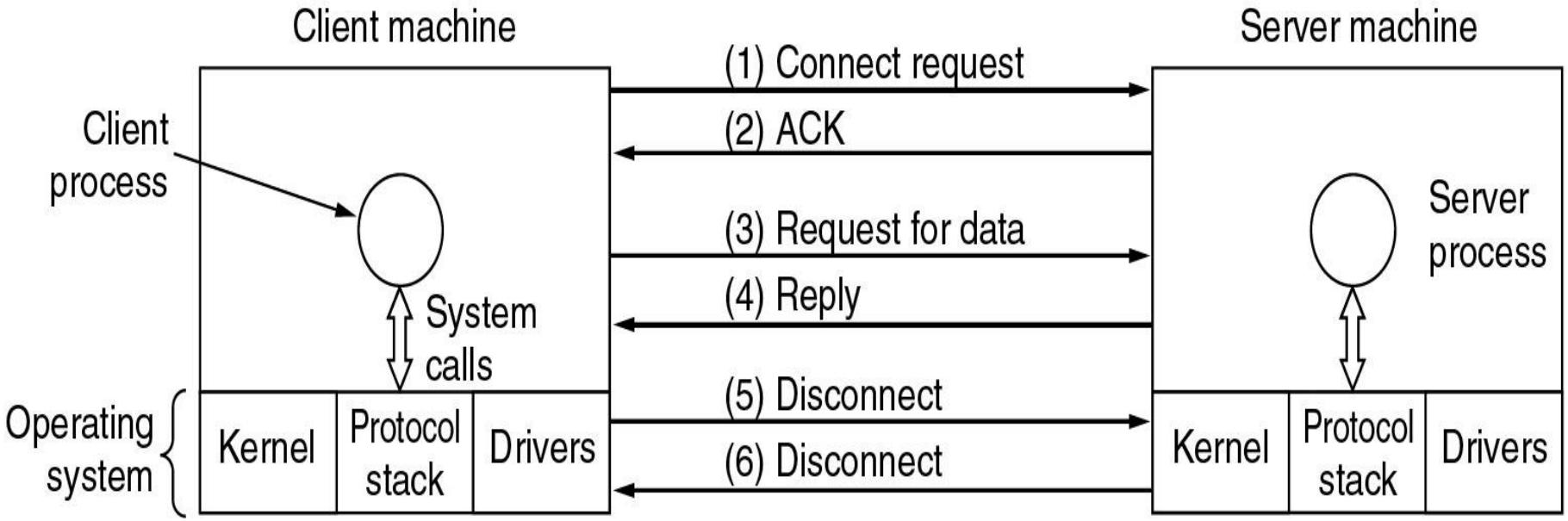
Six different types of service

Service Primitives

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

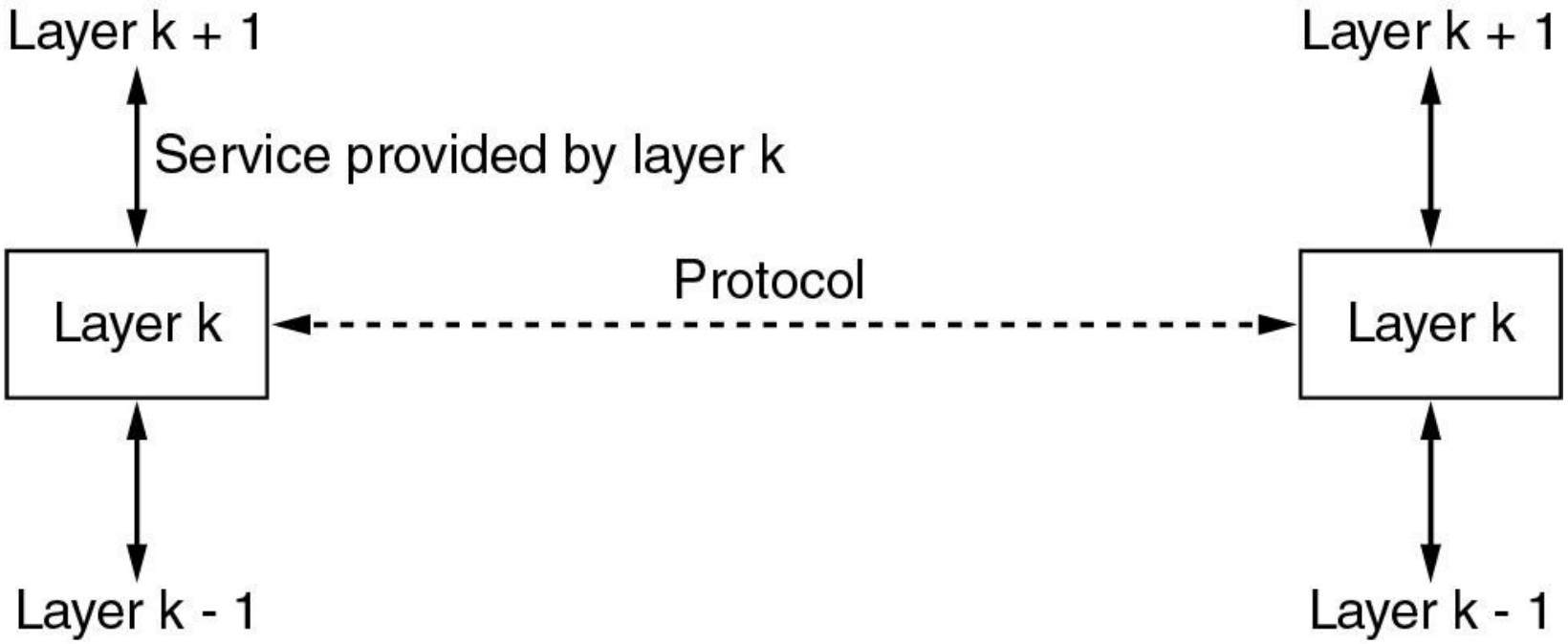
Five service primitives for implementing a simple connection-oriented service

Service Primitives



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

Services to Protocols Relationship



The relationship between a service and a protocol

Why Layering ??

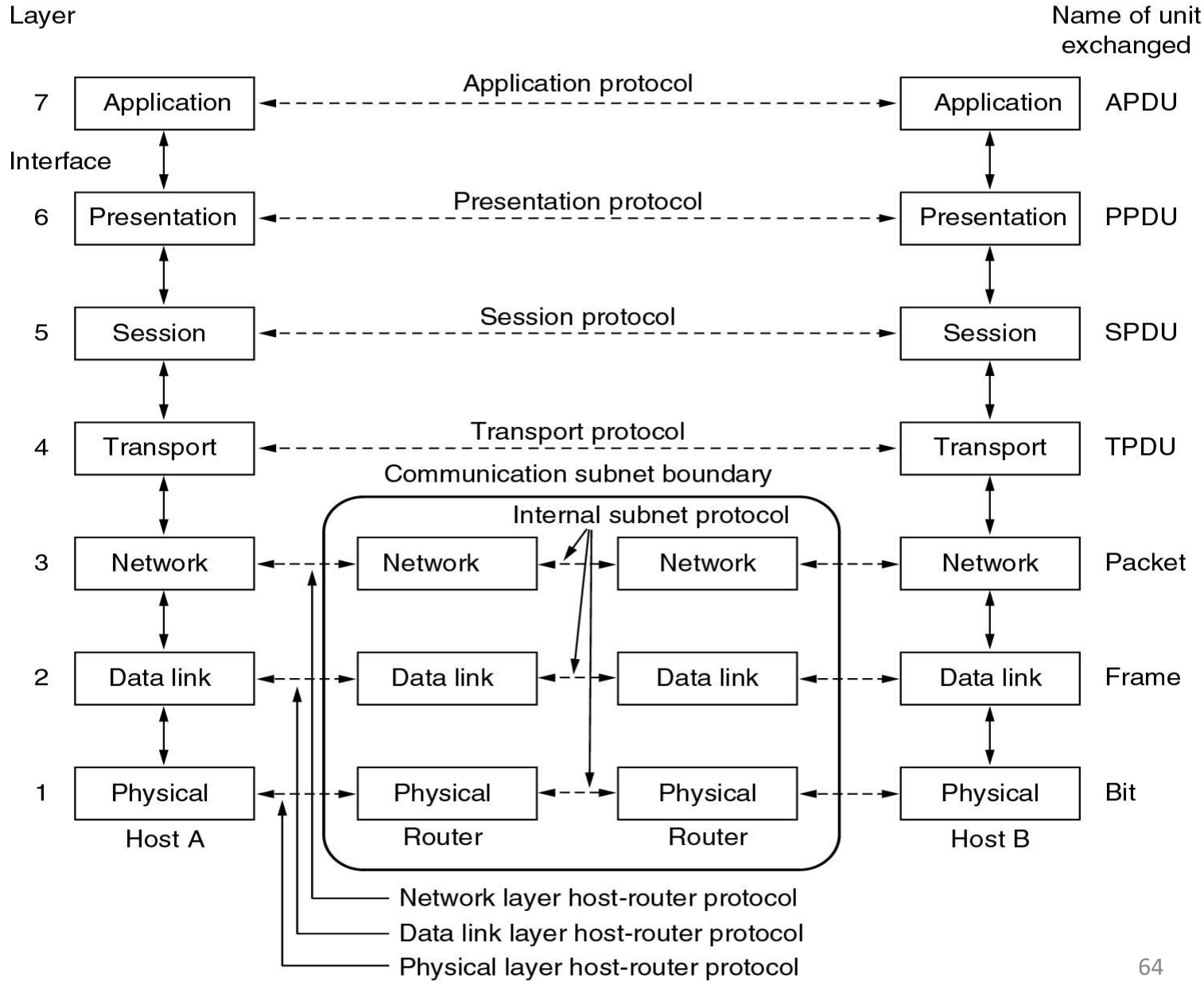
- To Separate Specific Functions in Each Layer.
- Each Layer Should Define a Unique Function.
- To make their Implementation Transparent to Other Components.
- Allows Independent Design and Testing of Each Components.
- Modularization Eases Maintenance and Updating of System.

Reference Models

- The OSI Reference Model
- The TCP/IP Reference Model
- A Comparison of OSI and TCP/IP
- A Critique of the OSI Model and Protocols
- A Critique of the TCP/IP Reference Model

OSI Reference Models

The OSI Reference Model.



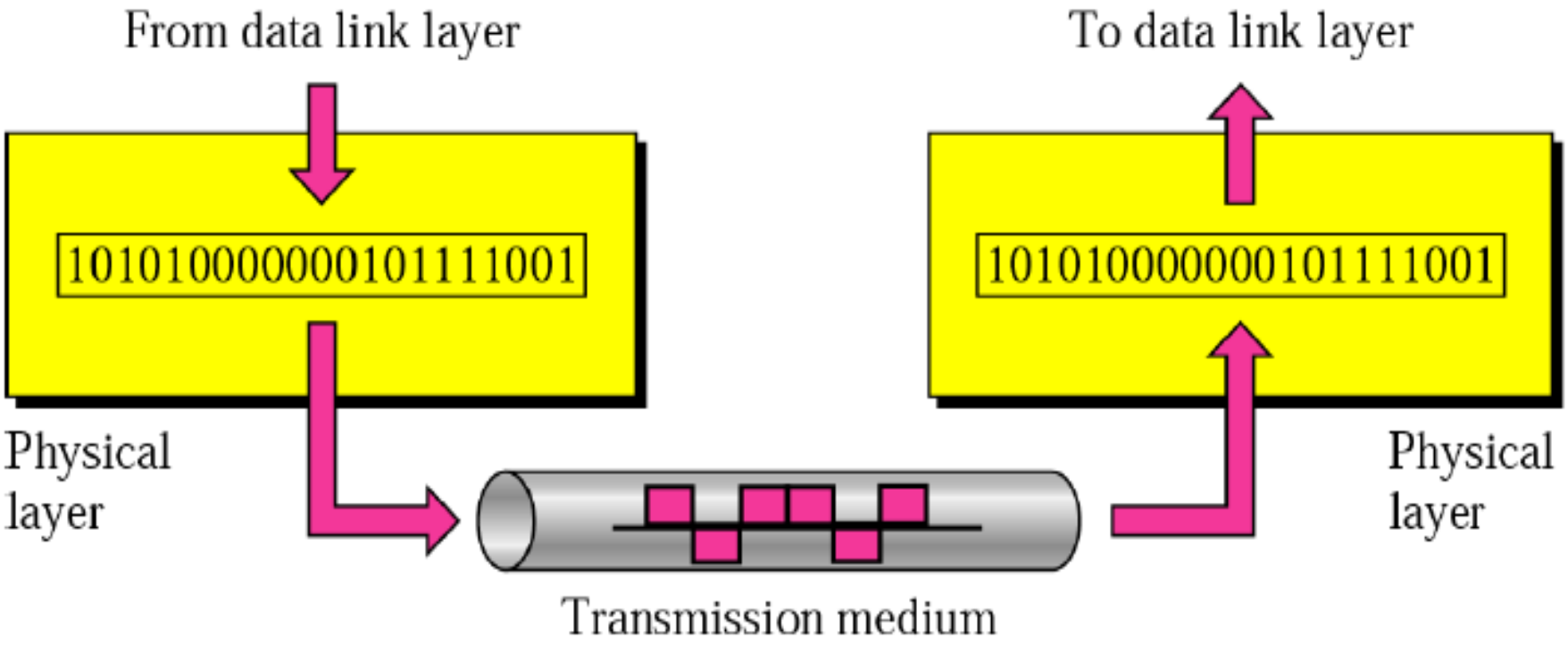
Ideas behind the model

- Layers should be created where different abstraction is needed.
- Each layer should perform a well-defined function.
- The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
- The layer boundaries should be chosen to minimize the information flow across the interfaces.
- There should not be too many or too few layers.

The Physical Layer

- Concerned with transmitting raw bits over communication channel.
- Deals with physical characteristics of interfaces and media (electrical, mechanical and timing)

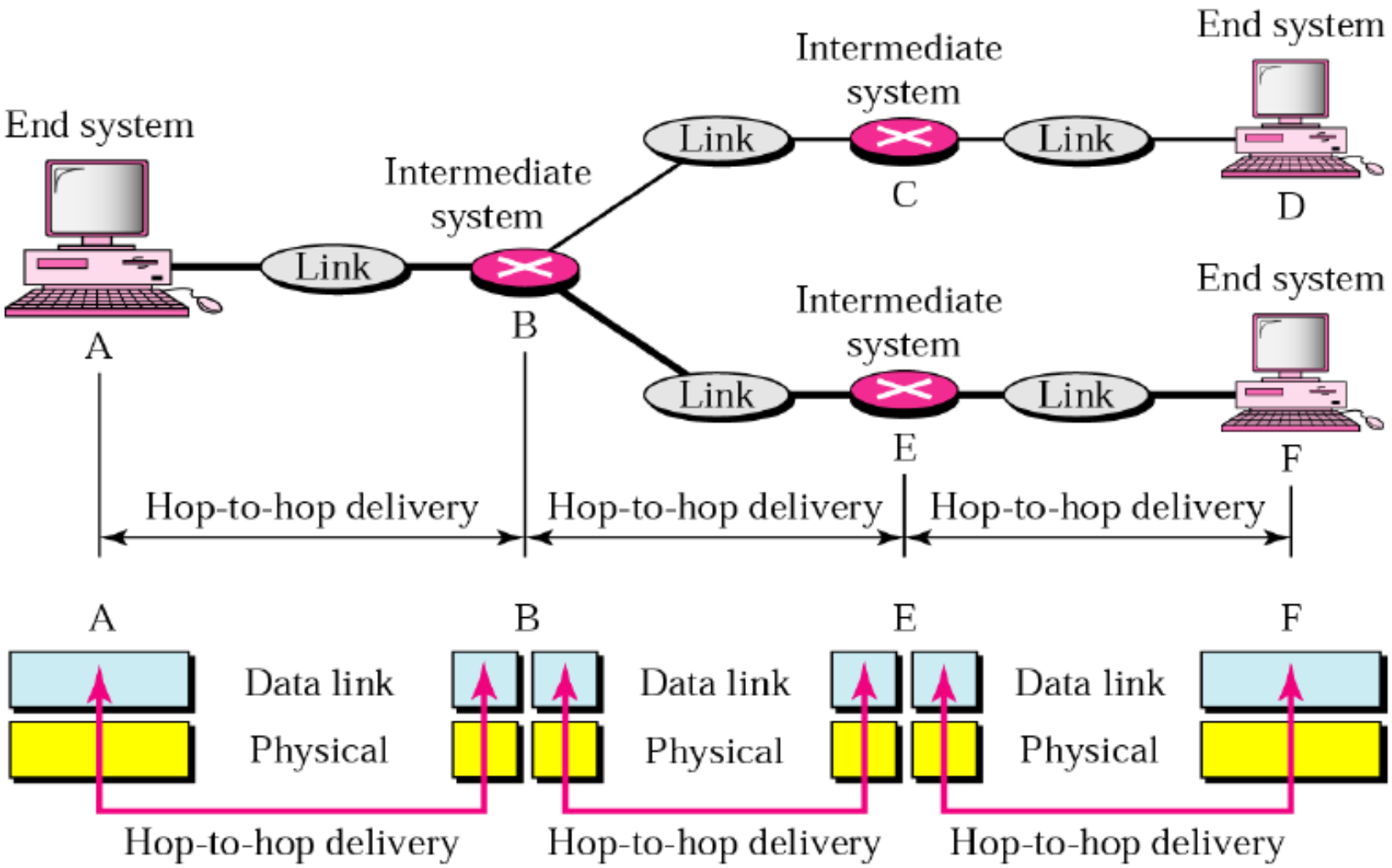
The Physical Layer



The Data Link Layer

- Enables Node to Node Communication.
- Framing
- Responsible for Transmitting Frames From One Node to Next.
- Error Control
- Flow Control

The Data Link Layer

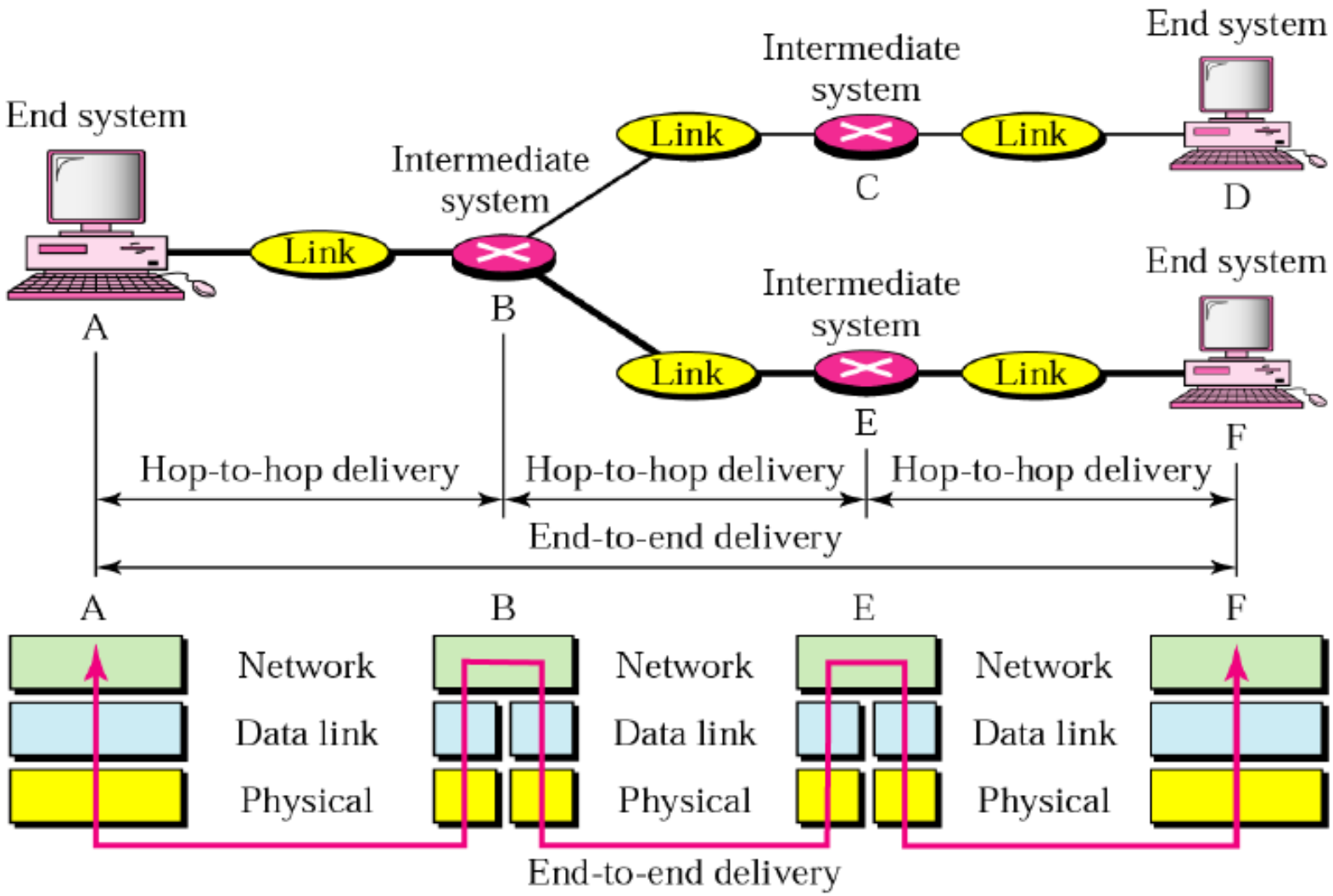


Node to Node Delivery

The Network Layer

- Enables Host to Host Communication
- Responsible for Delivery of Packets
- Routing
- Congestion Control

The Network Layer



End to End Delivery

The Transport Layer

- Segmentation and Reassembly.
- Connection Control
- Flow Control
- Error Control

The Session Layer

- Dialog Control
  - Whose Turn is To Transmit ??
- Token Management
  - Prevent same operation at same time
- Synchronization
  - Continue from point of crash

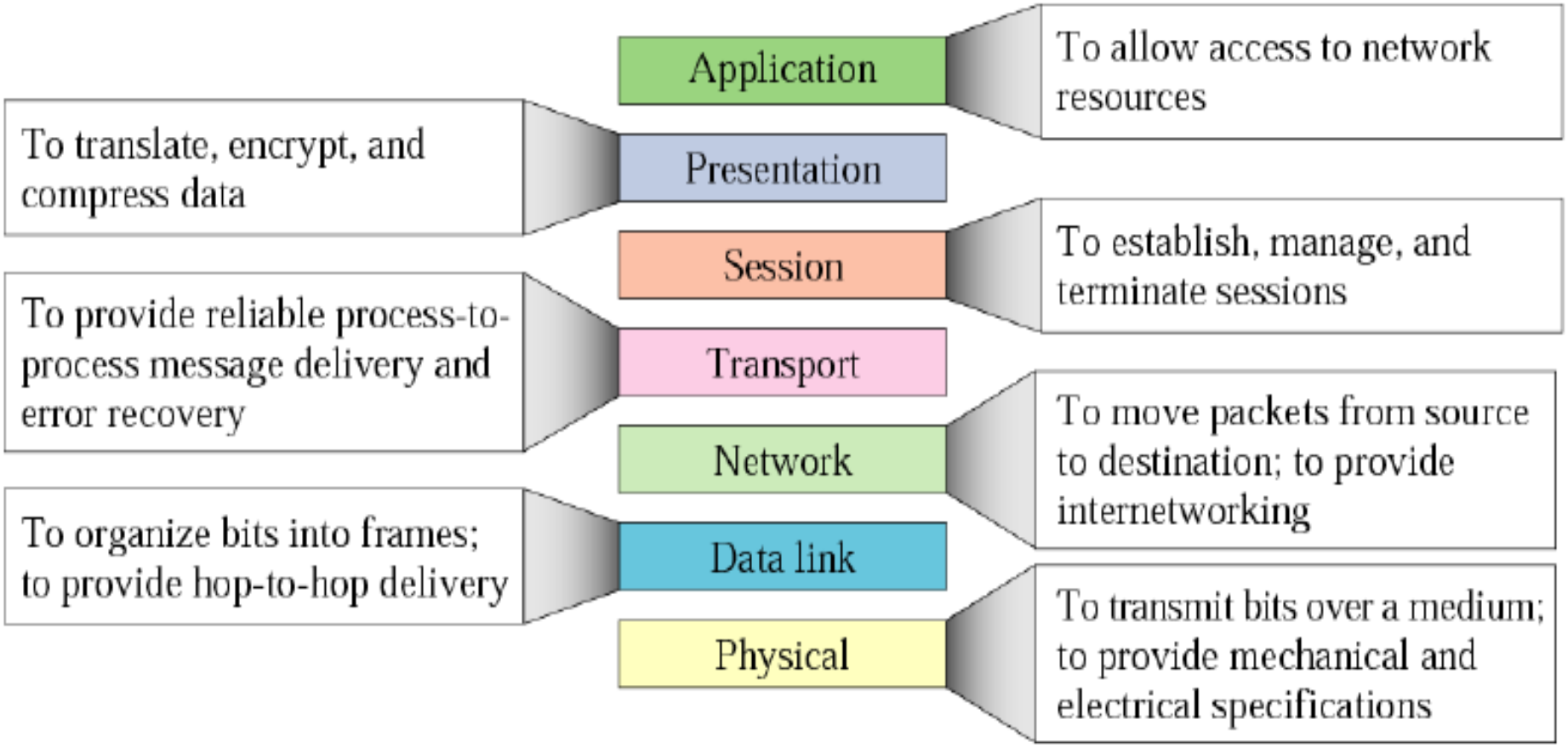
The Presentation Layer

- Data Formats and Coding.
- Data Compression
- Encryption

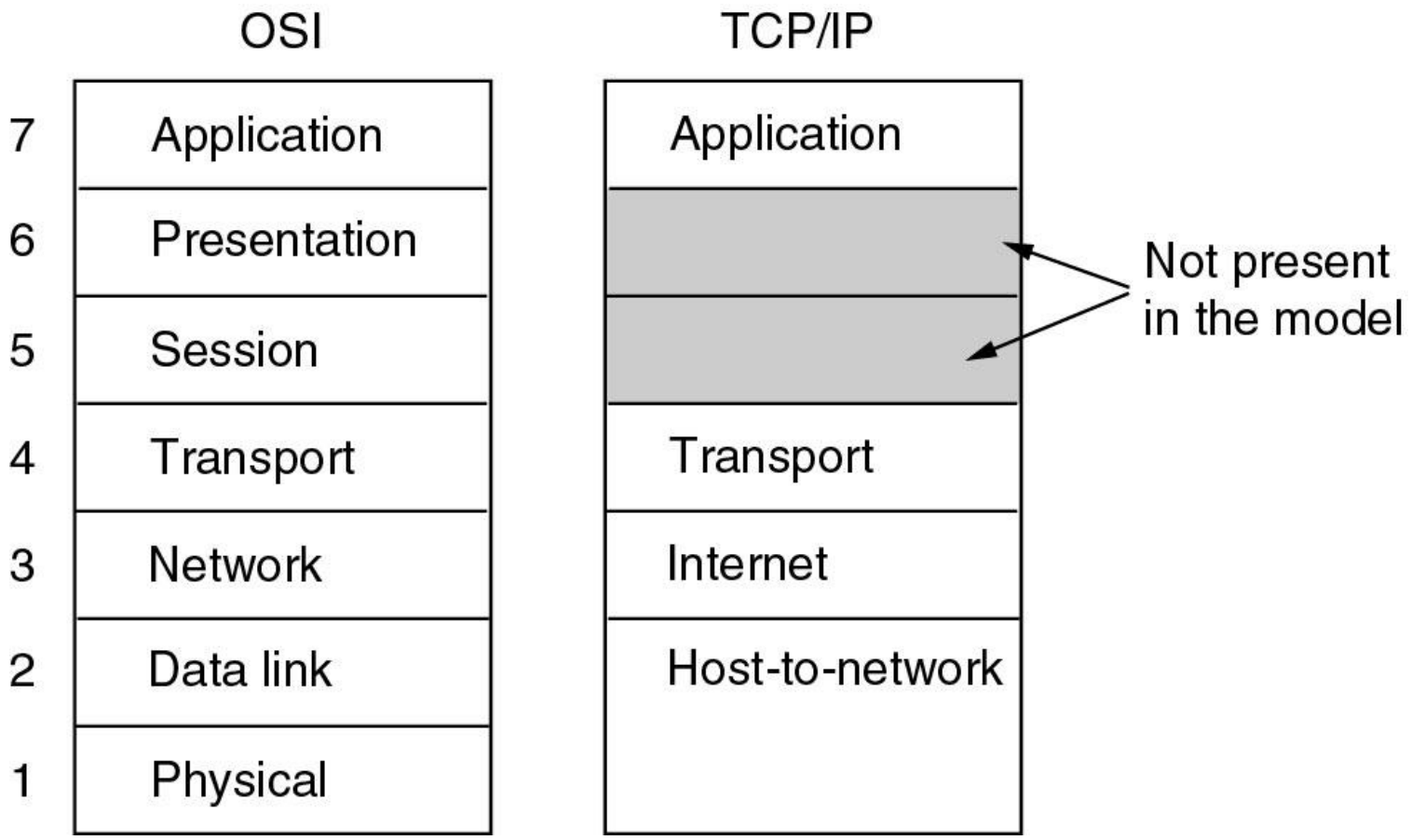
The Application Layer

- Responsible for Providing Service to End Users.
- Contains variety of protocols
  - HTTP (basis for WWW)
  - Simple Mail Transfer Protocol (SMTP)
  - File Transfer Protocol (FTP)

Summary of OSI layer function



TCP/IP Reference Models



The TCP/IP reference model

TCP/IP Model

4 layers of the TCP/IP model

- Layer 4: Application
- Layer 3: Transport
- Layer 2: Internet
- Layer 1: Network access (Host to Network)

The network access layer(Host to Network)

- Concerned with all of the issues that an IP packet requires to actually make the physical link.
- All the details in the OSI physical and data link layers.
  - Electrical, mechanical, procedural and functional specifications
  - Data rate, Distances, Physical connector.
  - Frames
  - Synchronization, flow control, error control.

The Internet Layer

- Concerned with Packet Addressing
  - Send source packets from any network and have them arrive at the destination independent of the path and networks they took to get there.
  - May arrive in different order to destination
  - Job of higher layer to arrange them
- Internet Protocol (IP)
  - Deliver packet to exact destination
- Packet Routing
  - Important to avoid congestion

The Transport Layer

- End-to-end flow control.
- Error detection and recovery.
- Allows end-to-end communication
- Connection establishment and termination

The Transport Layer

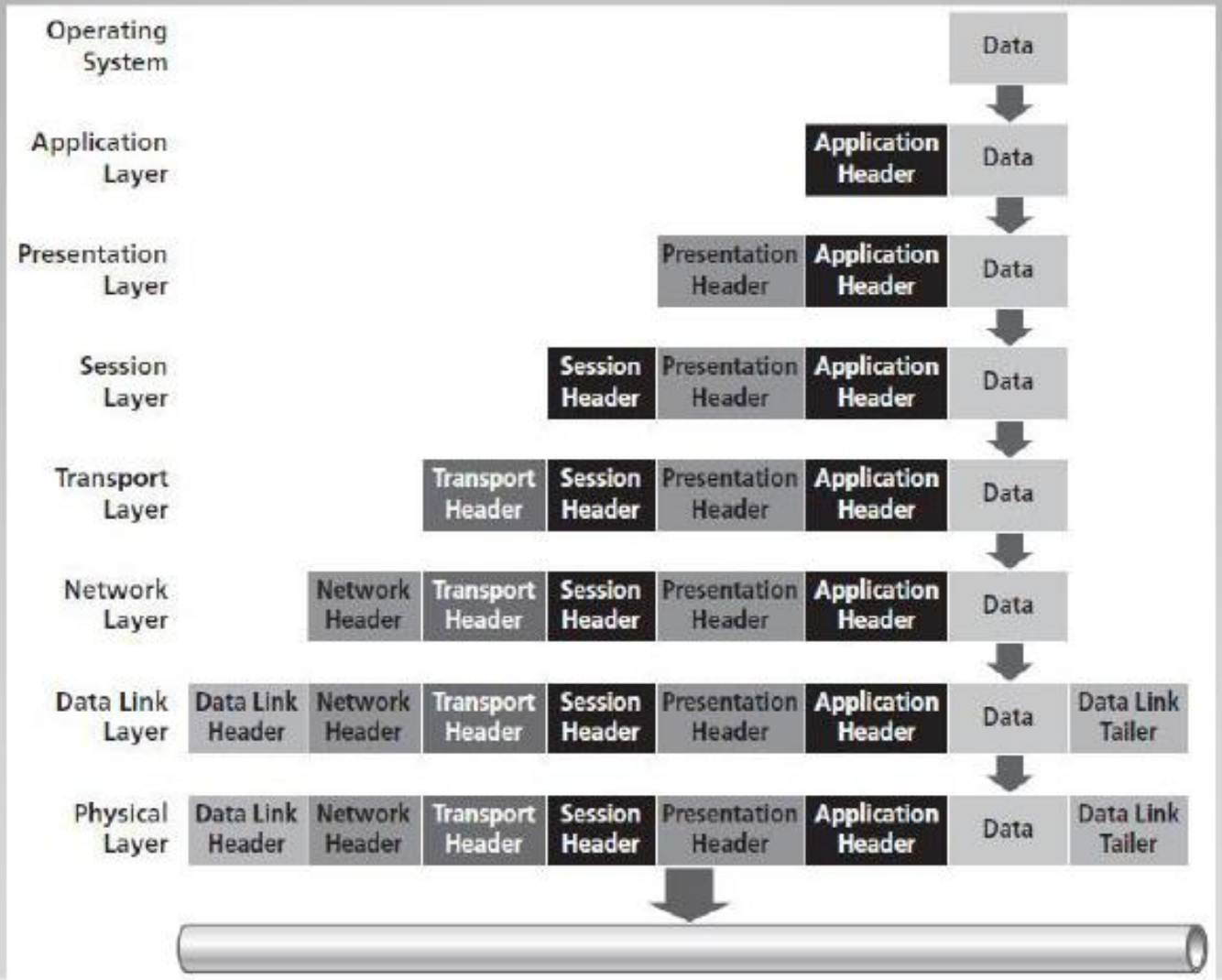
Two main protocol at transport layer are

- Transmission control protocol (TCP)
  - Connection oriented
  - Connection established before sending data
  - Reliable
- User datagram protocol (UDP)
  - Connectionless
  - Sending data without establishing connection
  - Fast but unreliable

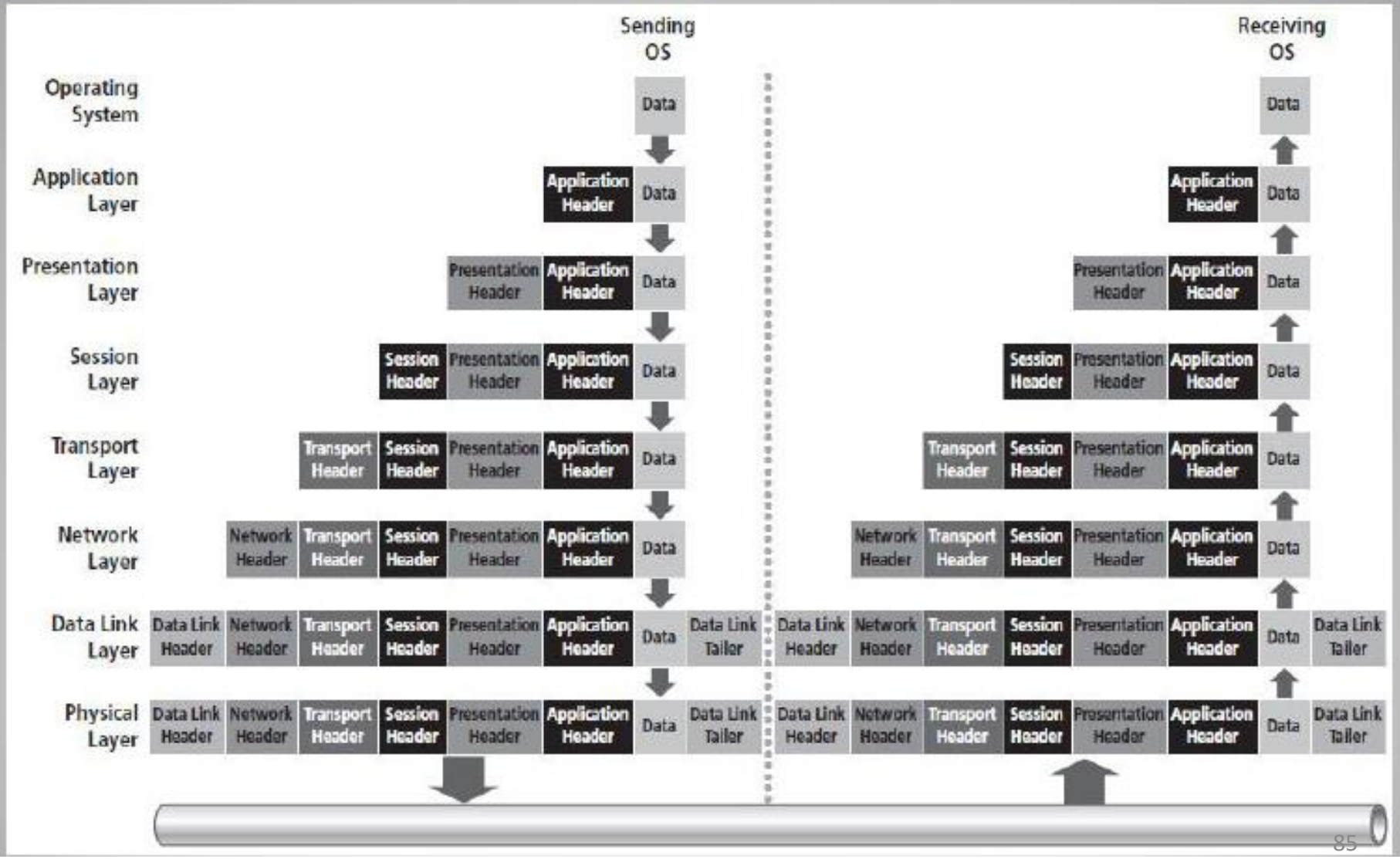
The Application Layer

- Handles high-level protocols
- Applications(Software) that works at Application Layer
  - FTP, HTTP, SMTP, DNS
  - Format of data, data structure, syntax and semantics.

How Data Moves Through the OSI Model

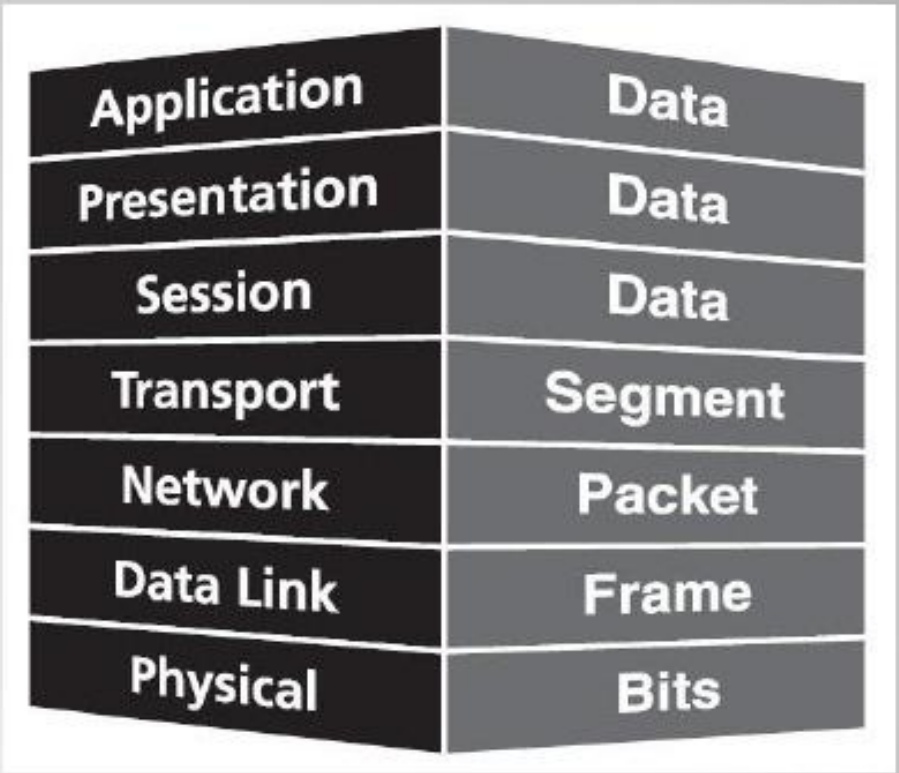


Data as It Moves Through OSI Layers, Sent by One Computer and Received by Another



Encapsulation/De-encapsulation

- The process of moving data between layers of the OSI Model
- **Encapsulation:**
  Data > segment > packet > frame > bits
- **De-encapsulation:**
  Bits > frame > packet > segment > data



- Data Encapsulation
  - The application, presentation and session layer creates data from user input
  - The transport layer converts data into segments
  - The network layer converts segments into packets
  - The data link layer converts packets into frames
  - The physical layer converts frames into bits
- Data De-encapsulation
  - Reverse Process occurs in the receiving end where bits are ultimately converted into data

Comparing OSI and TCP/IP Models

- Concepts central to the OSI model
  - Services
  - Interfaces
  - Protocols

Comparison contd..

- Services
  - Tells what the layer does, not how the layer works
- Interfaces
  - Tells the process above it how to access it
- Protocols
  - Can use any protocol as long as the job is done
- TCP/IP did not originally distinguish between services, interface and protocols.
- The protocols in the OSI model are better hidden than in TCP/IP model

Comparison Contd..

- The OSI reference model was devised before the corresponding protocols were invented
- With TCP/IP the protocols came first, and the model was description of existing protocols
- The OSI model has 7 layers and the TCP/IP has 4 layers.
- The OSI model supports both connection oriented and connectionless communication in the network layer but only connection oriented communication in transport layer.

Comparison Contd..

- The TCP/IP model has only connectionless mode in the network layer but supports both support both modes in the transport layer.

A Critique of the OSI Model and Protocols

Why OSI did not take over the world?

- Bad timing
- Bad technology
- Bad implementations
- Bad politics

A Critique of the TCP/IP Reference Model

Problems:

- Service, interface, and protocol not distinguished
- Not a general model
- Host-to-network “layer” not really a layer
- No mention of physical and data link layers
- Minor protocols deeply entrenched, hard to replace

Example Network

- The Internet
- X.25
- Frame Relay
- Ethernet
- VOIP
- NGN
- MPLS
- xDSL

The Internet

- The Internet is a global system of interconnected computer networks.
- Applications of the Internet
  - Traditional core applications:
    - Email
    - News
    - Remote Login
    - File Transfer
  - The killer application:
    - World-Wide Web (WWW)
  - New applications:
    - Videoconferencing
    - Telephony
    - P2P applications
    - Internet Broadcast

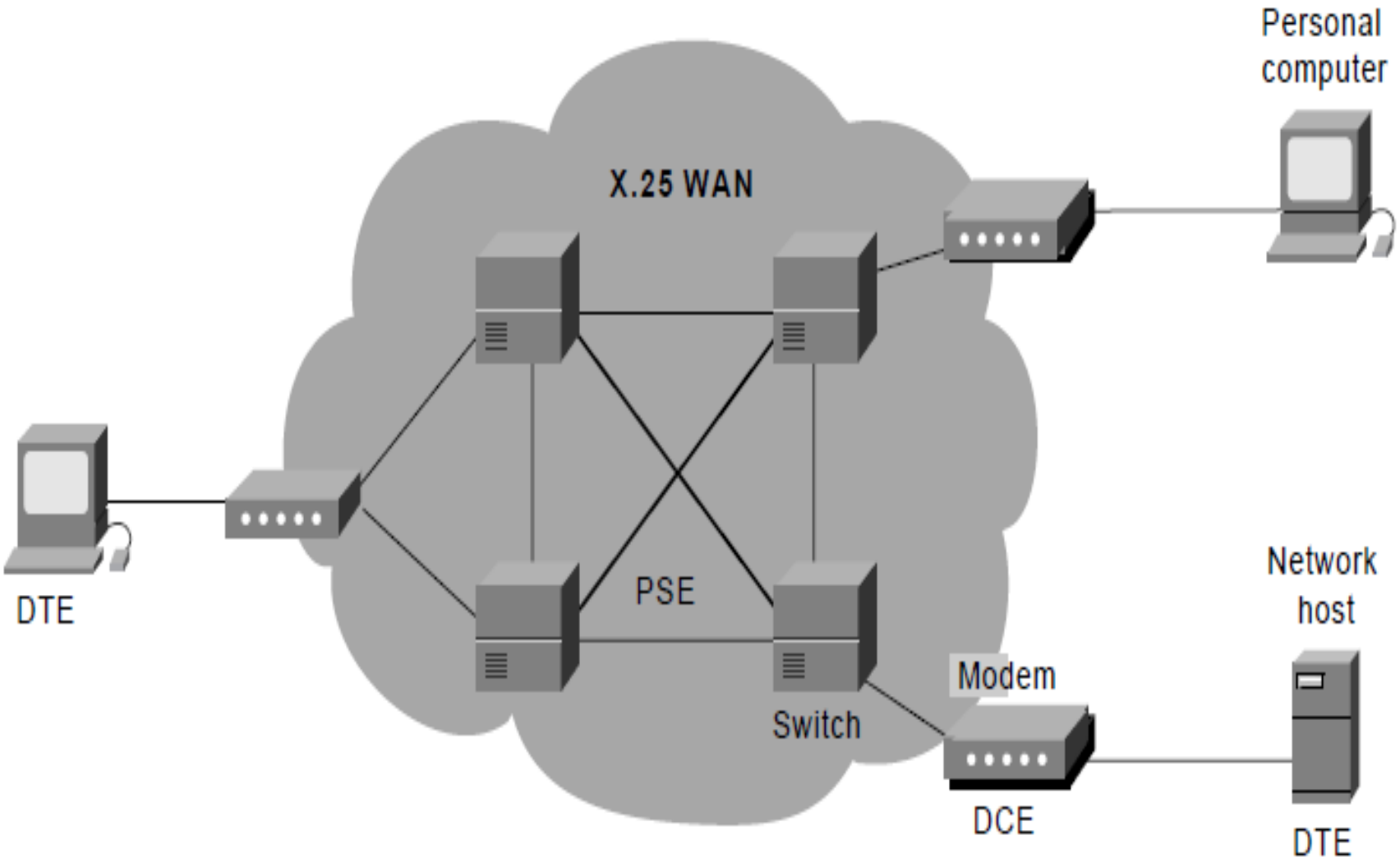
Design Principles for Internet

1. Make sure it works.
2. Keep it simple.
3. Make clear choices.
4. Exploit modularity.
5. Expect heterogeneity.
6. Avoid static options and parameters.
7. Look for a good design; it need not be perfect.
8. Be strict when sending and tolerant when receiving.
9. Think about scalability.
10. Consider performance and cost.

X.25

- *First popular packet switched network*
- *Deployed in 1970s*
- Allowed for the setup of data connections at speeds between 300bps to about 56kbps.
- *To use x.25*
  - *Computer first establishes a connection to remote computer*
  - *This connection is given a number to be used in the data transfer packets*
- *Data packets are simple consisting of 3 byte header and up to 128 bytes of data*

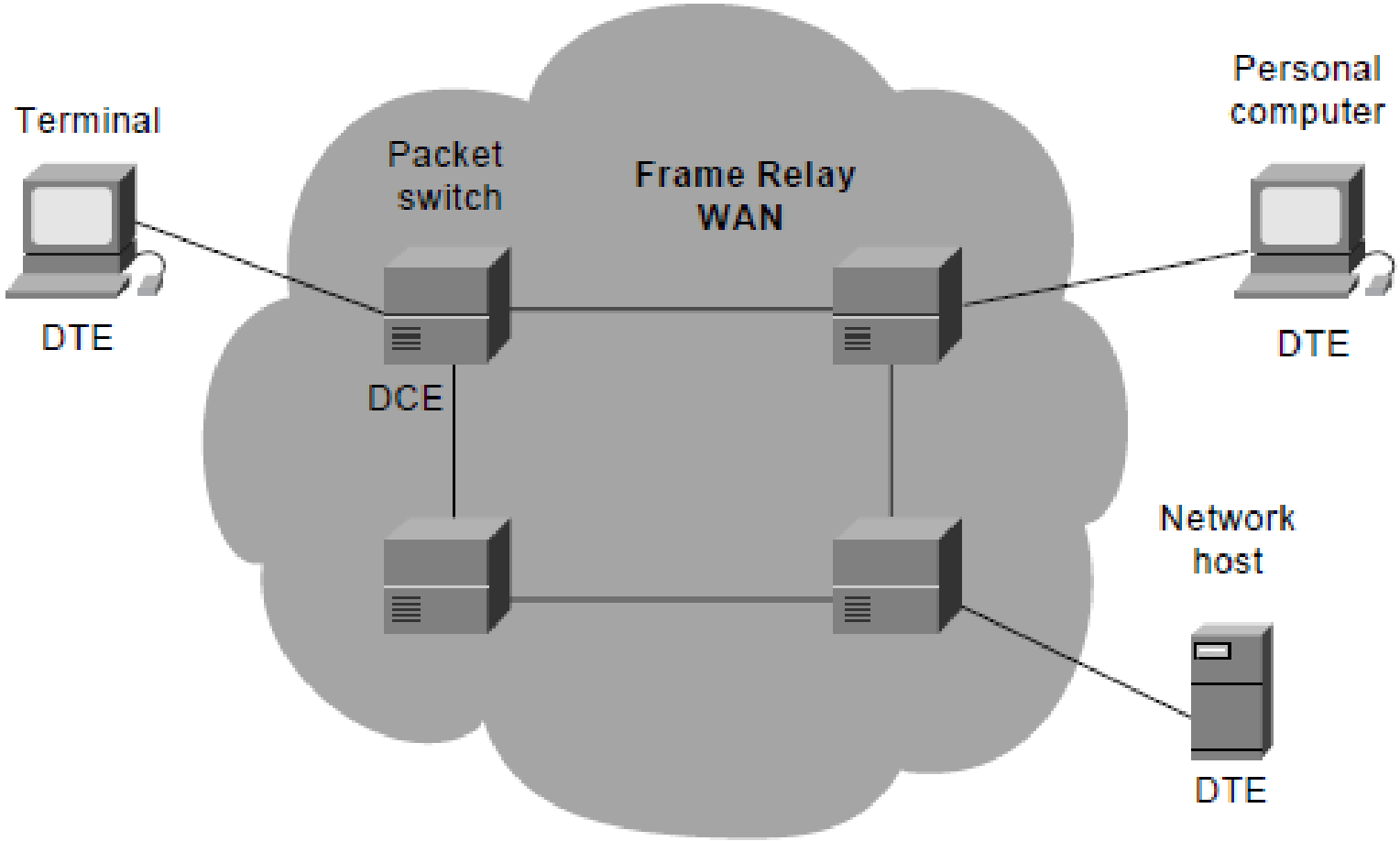
- Header consist of
  - 12 bit connection number
  - A packet sequence number
  - An acknowledgement number
  - And a few miscellaneous bits
- Subscribers are charged based on their use of the network.
- X.25 network devices fall into three general categories:
  - data terminal equipment (DTE)
  - data circuit-terminating equipment (DCE) and
  - packet-switching exchange (PSE)


Personal
computer
X.25 WAN
DTE
PSE
Network
host
Modem
Switch
DCE
DTE

Frame relay

- Frame Relay is the most popular WAN technology.
- Frame Relay is the same type of protocol as X.25.
- However, Frame Relay differs significantly from X.25 in its functionality and format.
- In particular, Frame Relay is a more streamlined protocol, facilitating higher performance and greater efficiency.

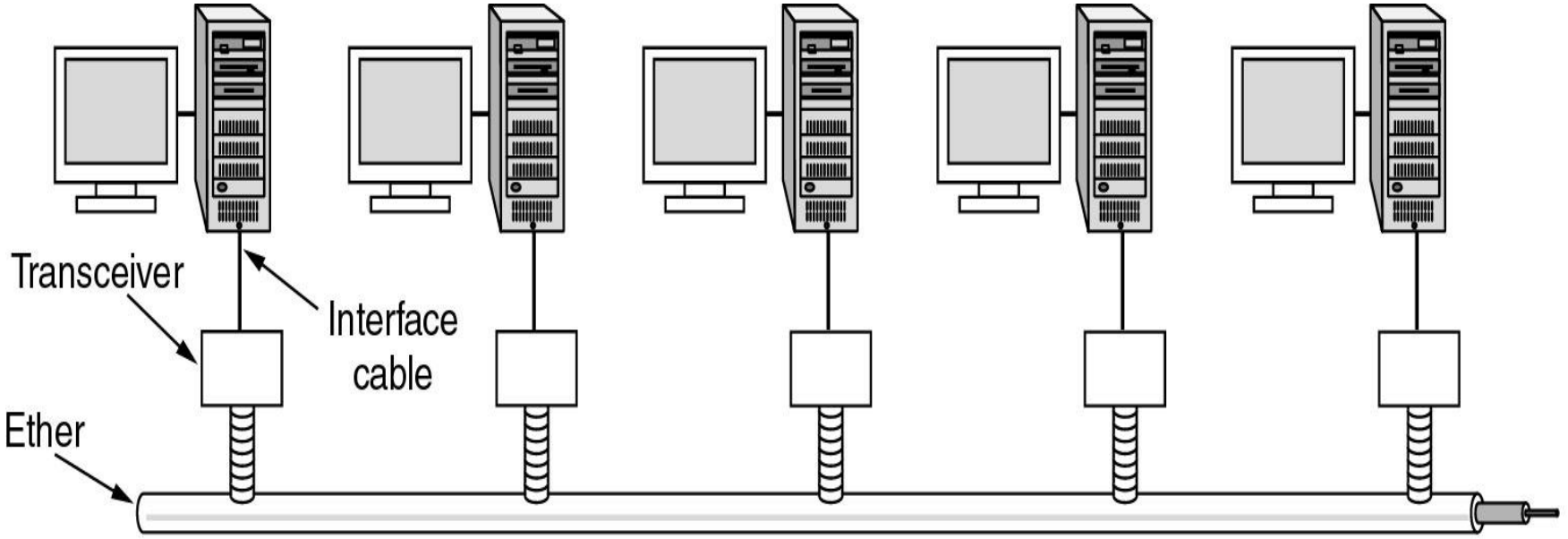
- Frame Relay most closely compares to the OSI data link layer (Layer 2).
- The frame relay frame is transmitted to its destination by virtual circuits (logical path from originating point in the network).
- Virtual circuits may be Permanent (PVCs) or Switched (SVCs)
- Virtual circuit consume bandwidth only when they transmit data so multiple virtual circuits can exist simultaneously


Terminal
DTE
Packet
switch
DCE
Frame Relay
WAN
Personal
computer
DTE
Network
host
DTE

Ethernet

- Ethernet has been a relatively inexpensive, reasonably fast, and very popular LAN technology for several decades.
- Bob Metcalfe and D.R. Boggs developed Ethernet beginning in 1972.
- Ethernet uses the CSMA/CD access method to handle simultaneous demands.
- The most commonly installed Ethernet systems are called 10BASE-T and provide transmission speeds up to 10 Mbps.

- Fast Ethernet or 100BASE-T provides transmission speeds up to 100 megabits per second.
- Ethernet only defines the physical and data link layer of OSI model.



Architecture of the original Ethernet.

VOIP

- communication that allows you to make phone calls over a broadband internet connection.
- Some VoIP services require a computer or a dedicated VoIP phone
- others allow you to use your landline phone to place VoIP calls through a special adapter.

VoIP configurations

- *Dedicated routers*
  - These devices allow you to use your traditional phone to place VoIP calls.
  - They are connected to cable/DSL modems (or any high-speed internet source) and allow you to attach an ordinary telephone.
  - Once configured, and with an appropriate VoIP provider and service plan, these devices require no special software or interaction with a computer.

- *Adapters (USB)*
  - These devices also allow you to use a traditional phone to place VoIP calls.
  - They usually come in the form of USB adapters
  - They feature a standard modular phone jack to which you can attach an ordinary phone line.
  - Once connected, your phone behaves as if it were connected to standard phone service.

- *Software-controlled VoIP applications:*
  - There are many software applications ("softphones") that allow you to place VoIP phone calls
  - Using an ordinary computer with a headset, microphone, and sound card.
  - Software-based VoIP applications are quite attractive to consumers
    - they often already have most of the components
    - Can start at little to no cost

- *Dedicated VoIP phones*
  - A VoIP phone looks like an ordinary corded or cordless telephone
  - it connects directly to a computer network rather than a traditional phone line.
  - may consist of a phone and base station that connects to the internet
  - it may also operate on a local wireless network.
  - Like the VoIP adapters mentioned above, dedicated VoIP phones also require a provider and service plan.

NGN

Introduction

- packet-based network
- QoS-enabled transport technologies
- independent of the underlying transport related technologies.
- It enables unfettered access for users to networks and to competing service providers and services of their choice.
- It supports generalized mobility

Characteristics

- packet-based transfer
- decoupling of service provision from transport
- support for a wide range of services
  - real time, streaming, non-real time and multimedia
- generalized mobility
- interworking with legacy networks via open interfaces
- unrestricted access by users to different service providers
- converged services between fixed/mobile

MPLS

- Multi-Protocol Label Switching
- Layer 2.5 networking protocol
- In the traditional OSI model:
  - Layer 2 covers protocols like Ethernet, which can carry IP packets, but only over simple LANs or point-to-point WANs.
  - Layer 3 covers Internet-wide addressing and routing using IP protocols.
  - MPLS sits between these traditional layers, providing additional features for the transport of data across the network.

- In a traditional IP network:
  - Each router performs an IP lookup ("routing"), determines a next-hop
  - based on its routing table, and forwards the packet to that next-hop.
  - Rinse and repeat for every router, until the final destination is reached.
- MPLS does "label switching" instead:
  - The first device does a routing lookup, just like before:
    - But instead of finding a next-hop, it finds the final destination router.
    - And it finds a pre-determined path from "here" to that final router.

- The router applies a “label” based on this information.
- Future routers use the label to route the traffic
  - Without any additional IP lookups.
- At the final destination router the label is removed.
  - the packet is delivered via normal IP routing

xDSL

- DSL stands for Digital Subscriber Line, and the ‘x’ in xDSL means there are many different varieties of DSL (HDSL, ADSL, etc.).
- Digital Subscriber Lines are nothing more than high-speed digital communications lines.
- DSL offers several key advantages over other high speed communications solutions.
  - The foremost of these is price.
  - The greatest savings come from the fact that DSL runs on existing copper lines.
  - Most DSL systems allow voice transmission simultaneously with data traffic.

DSL Technology

DSL Type	Download	Upload	Distance (feet)
ADSL (Asymmetrical)	1.5 - 8 Mbps	16 kbps to 640 kbps	9K to 18K
UDSL(a.k.a. G.lite, DSL Lite)	1.5 Mbps	384 kbps	12K to 18K
RADSL (Rate Adaptive)	Variable to 7 Mbps	Variable to 640 kbps	18K to 25K
VDSL (Very High Bit Rate)	26 Mbps to 52 Mbps	3 Mbps to 6 Mbps	1K to 3K
IDSL (ISDN over DSL)	144 kbps	144 kbps	18K (more w/ repeater)
SDSL (Symmetrical)	144 kbps to 2 Mbps	144 kbps to 2 Mbps	11.5K to 22K
HDSL (High Bit Rate)	1.544 Mbps	1.544 Mbps	12K on 2 pairs
HDSL (High Bit Rate)	2.048 Mbps	2.048 Mbps	12K on 3 pairs
HDSL2	1.544 Mbps	1.544 Mbps	12K on 1 pair
SHDSL (Single-pair HDSL)	192 kbps to 2.312 Mbps	3 Mbps to 6 Mbps	1K to 3K

Thank You!

If you have any Queries write to me

@

Jalauddin.mansur@gmail.com