Networking

Lecture 11

Introduction

- ✓Physical and Logical Topologies
- ✓Topologies
  - ✓Bus
  - ✓Ring
  - ✓Star
  - ✓Extended Star
  - ✓Mesh
  - ✓Hybrid

Physical vs. Logical Topology

- The actual layout of a network and its media is its Physical Topology

- The way in which the data access the medium and transmits packets is the Logical Topology

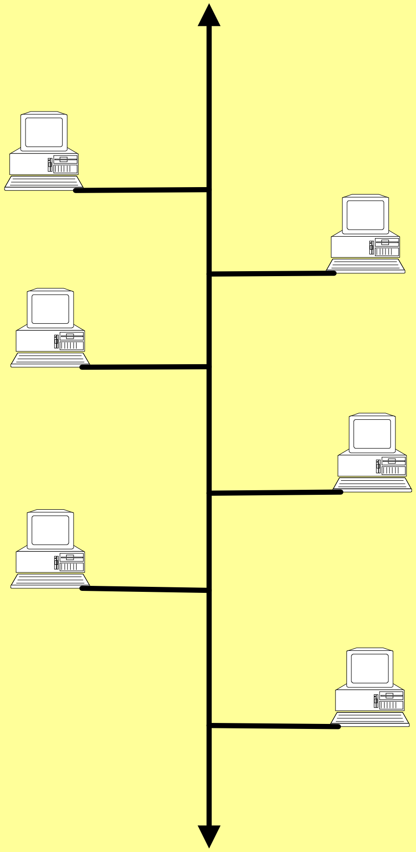
Physical vs. Logical Topology (2)

- Your choice of Logical Topology will affect the Physical Topology – and vice versa
- Design carefully – it may be difficult to change part way through the installation
- Your choice will determine cable installation, network devices, network connections, protocols

Factors

- Cost
- Scalability
- Bandwidth Capacity
- Ease of Installation
- Ease of fault finding and maintenance

Bus Topology



Bus Topology (2)

- Network maintained by a single cable
- Cable segment must end with a terminator
- Uses thin coaxial cable (backbones will be thick coaxial cable)
- Extra stations can be added

Bus Topology (3)

- Standard is IEEE 802.3
- Thin Ethernet (10Base2) has a maximum segment length of 200m
- Max no. of connections is 30 devices
- Four repeaters may be used to a total cable length of 1000m
- Max no. of nodes is 150

Bus Topology (4)

- Thick Ethernet (10Base5) used for backbones
- Limited to 500m
- Max of 100 nodes per segment
- Total of four repeaters , 2500m, with a total of 500 nodes

Bus Topology (5)

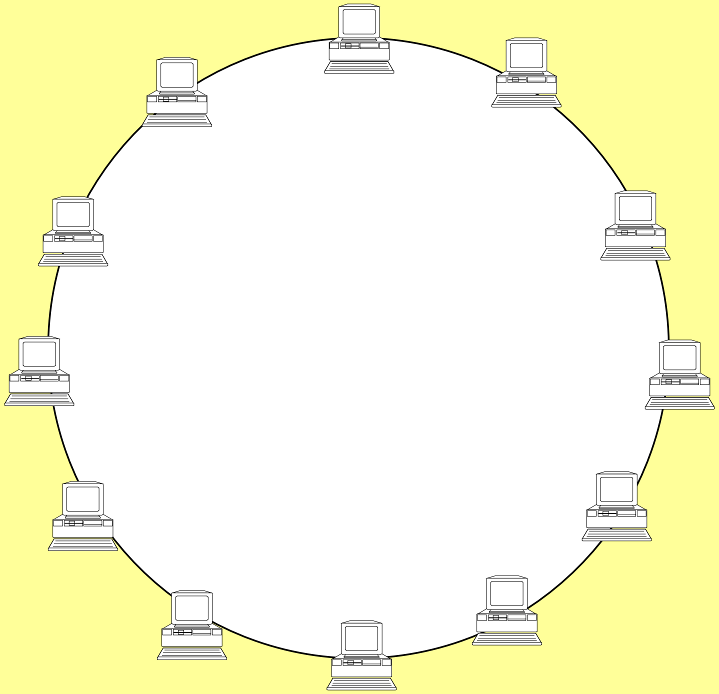
Advantages

- Inexpensive to install
- Easy to add stations
- Use less cable than other topologies
- Works well for small networks

Disadvantages

- No longer recommended
- Backbone breaks, whole network down
- Limited no of devices can be attached
- Difficult to isolate problems
- Sharing same cable slows response rates

Ring Topology



Ring Topology (2)

- No beginning or end
- All devices of equality of access to media
- Single ring – data travels in one direction only
- Each device has to wait its turn to transmit
- Most common type is Token Ring (IEEE 802.5)
- A token contains the data, reaches the destination, data extracted, acknowledgement of receipt sent back to transmitting device, removed, empty token passed on for another device to use

Ring Topology (3)

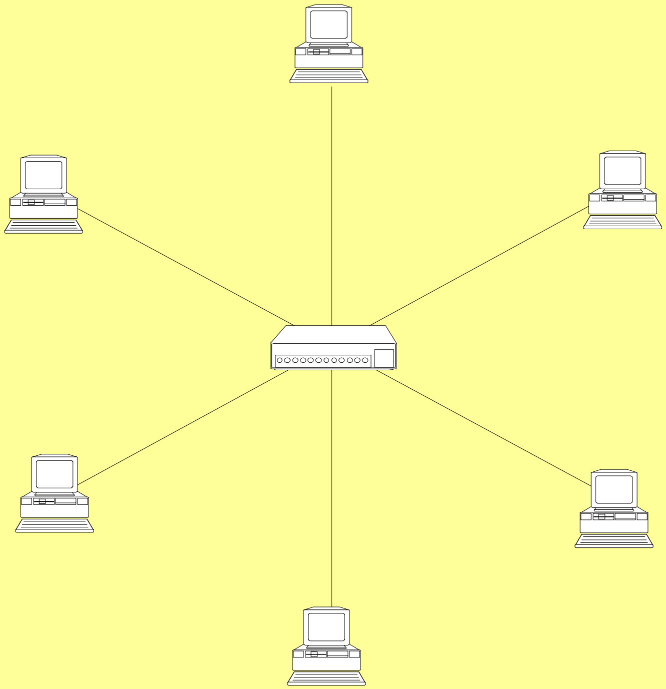
Advantages

- Data packets travel at great speed
- No collisions
- Easier to fault find
- No terminators required

Disadvantages

- Requires more cable than a bus
- A break in the ring will bring it down
- Not as common as the bus – less devices available

Star Topology



Star Topology (2)

- Like the spokes of a wheel
- Centre point is a Hub
- Segments meet at the Hub
- Each device needs its own cable to the Hub
- major type of topology
- Easy to maintain and expand

Star Topology (3)

Advantages

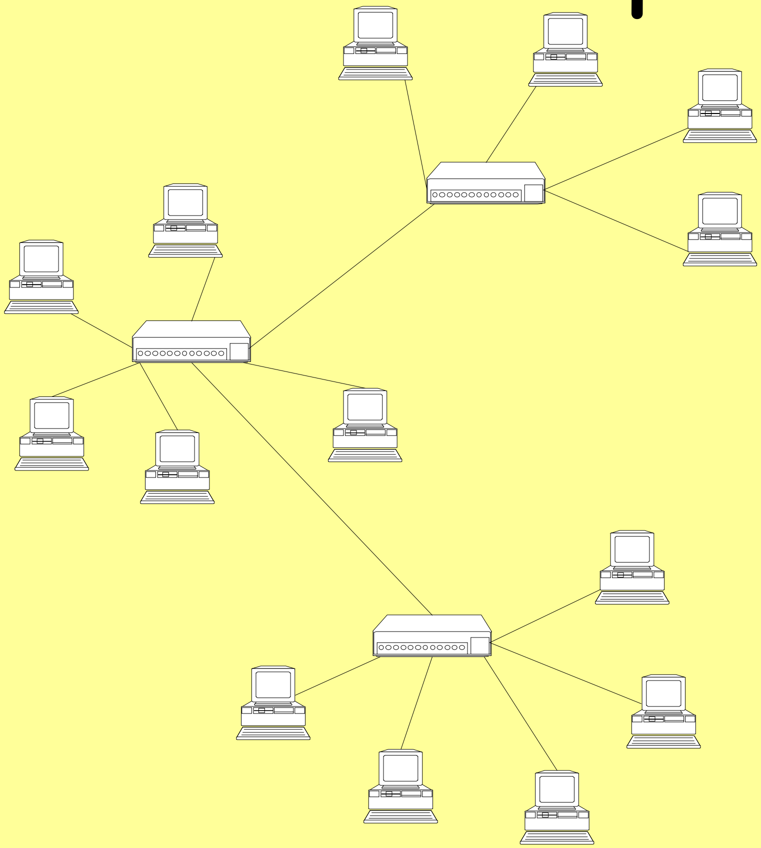
- Easy to add devices as the network expands
- One cable failure does not bring down the entire network.
- Hub provides centralised management
- Easy to find device and cable problems
- Can be upgraded to faster speeds
- Lots of support as it is the most used

Disadvantages

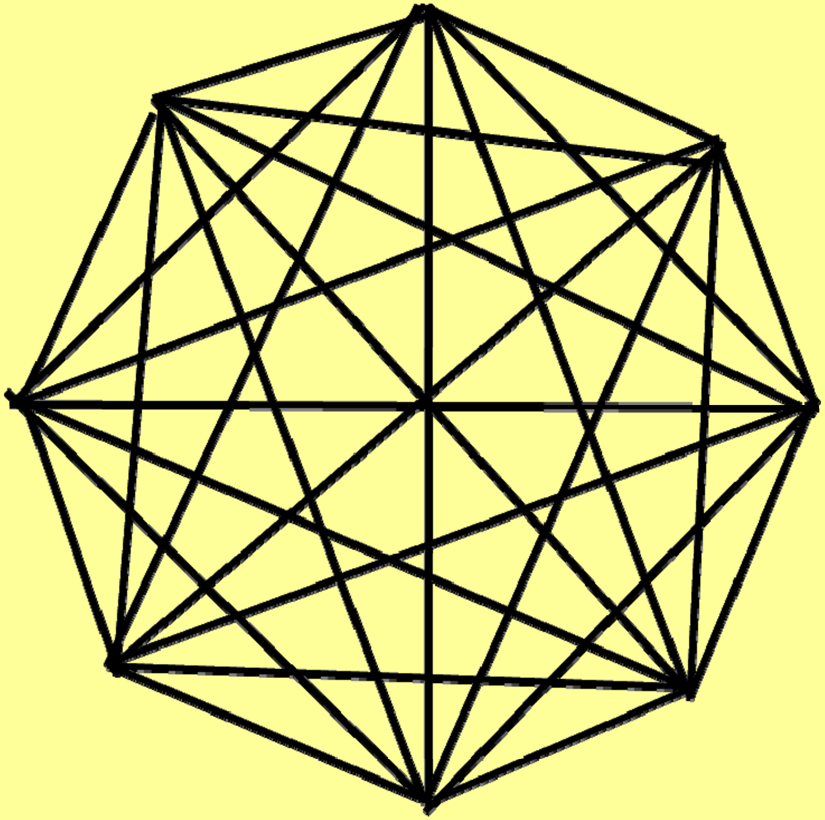
- A star network requires more cable than a ring or bus network
- Failure of the central hub can bring down the entire network
- Costs are higher (installation and equipment) than for most bus networks

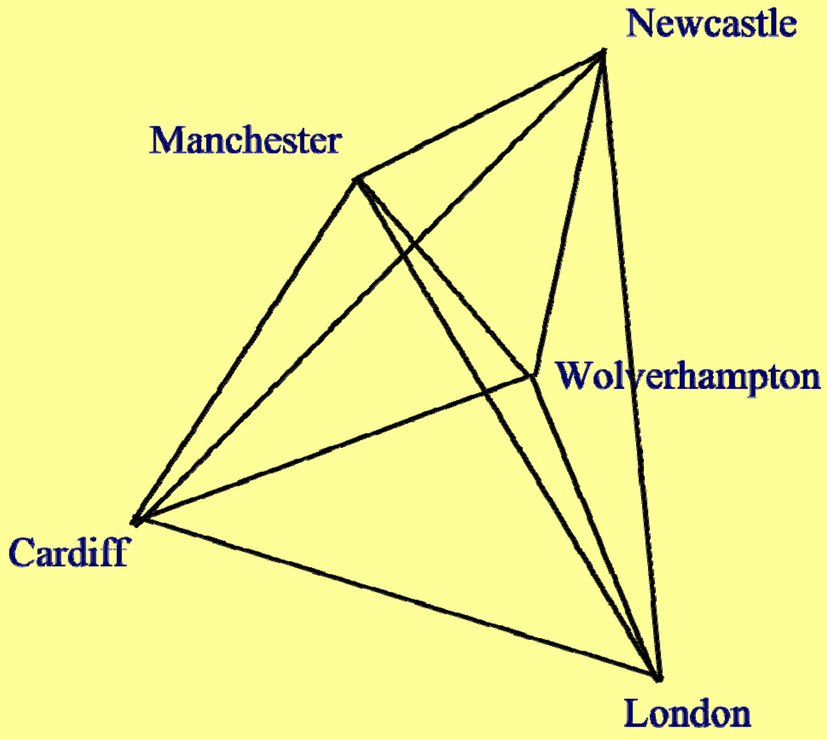
Extended Star Topology

A Star Network which has been expanded to include an additional hub or hubs.



Mesh Topology (Web)





Mesh Topology (2)

- Not common on LANs
- Most often used in WANs to interconnect LANS
- Each node is connected to every other node
- Allows communication to continue in the event of a break in any one connection
- It is “Fault Tolerant”

Mesh Topology (3)

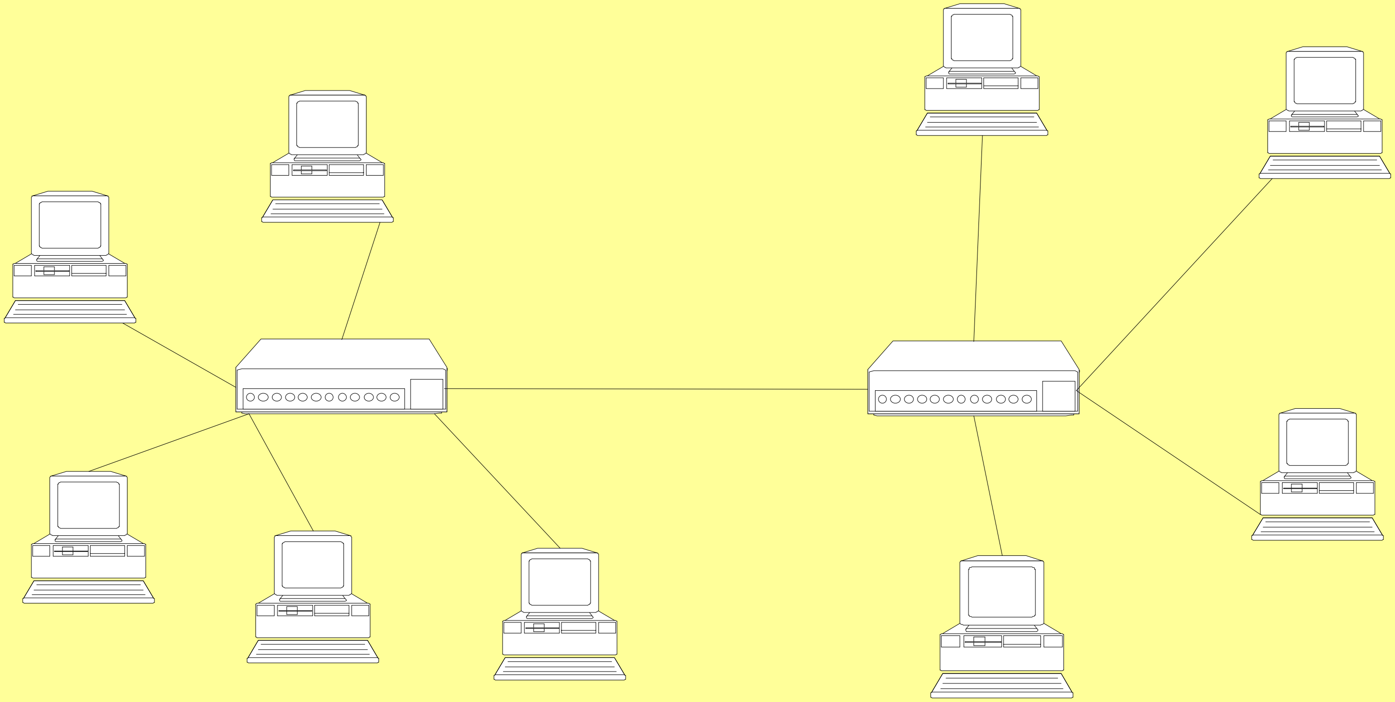
Advantages

- Improves Fault Tolerance

Disadvantages

- Expensive
- Difficult to install
- Difficult to manage
- Difficult to troubleshoot

Hybrid Topology



Hybrid Topology (2)

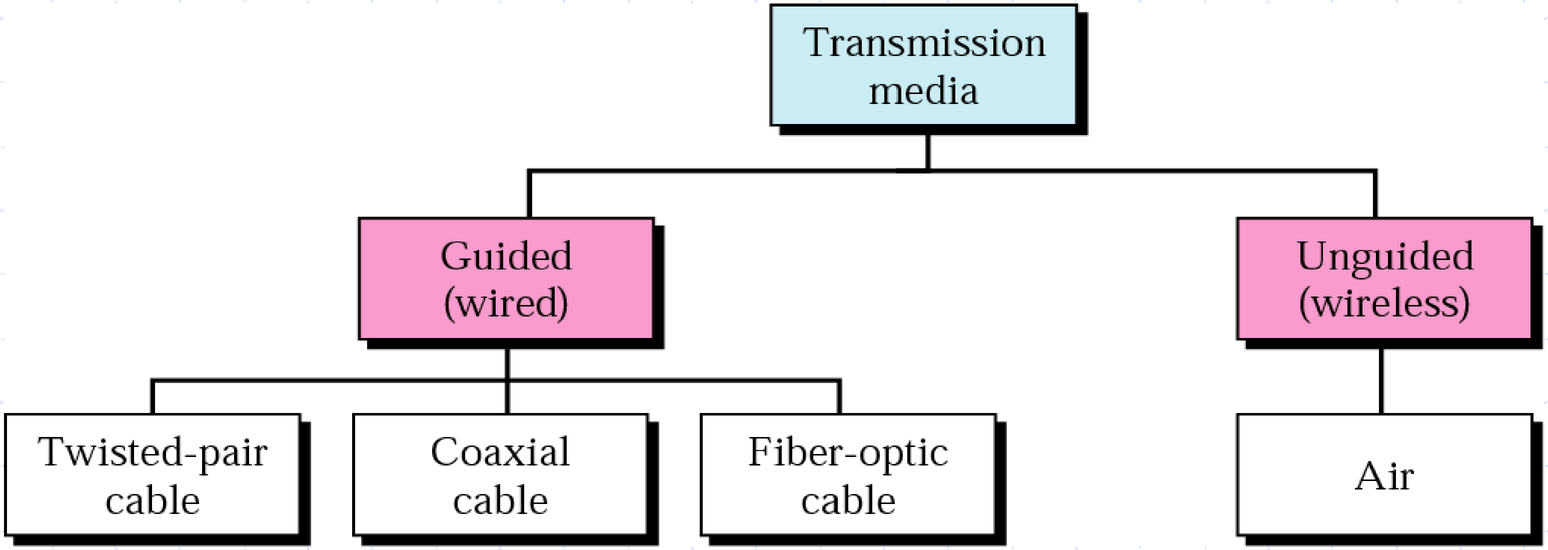
- Old networks are updated and replaced, leaving older segments
- Hybrid Topology – combines two or more different physical topologies
- Commonly Star-Bus or Star-Ring
- Star-Ring uses a MAU (Multistation Access Unit

Transmission Media

Transmission Media

- The transmission medium is the physical path by which a message travels from sender to receiver.
- Computers and telecommunication devices use signals to represent data.
- These signals are transmitted from a device to another in the form of electromagnetic energy.
- Examples of Electromagnetic energy include power, radio waves, infrared light, ultraviolet light, and X and gamma rays.

Classes of transmission media



Classes of Transmission Media

- Conducted or guided media
  - use a conductor such as a wire or a fiber optic cable to move the signal from sender to receiver
- Wireless or unguided media
  - use radio waves of different frequencies and do not need a wire or cable conductor to transmit signals

Design Factors for Transmission Media

- Bandwidth: All other factors remaining constant, the greater the band-width of a signal, the higher the data rate that can be achieved.
- Transmission impairments. Limit the distance a signal can travel.
- Interference: signals overlapping frequency bands can distort or wipe out a signal.
- Number of receivers: Each attachment introduces some, limiting distance and/or data rate.

Guided Transmission Media

- Transmission capacity depends on the distance and on whether the medium is point-to-point or multipoint
- Examples
  - twisted pair wires
  - coaxial cables
  - optical fiber

Twisted Pair Wires

- Consists of two insulated copper wires arranged in a regular spiral pattern to minimize the electromagnetic interference between adjacent pairs
- Often used at customer facilities and also over distances to carry voice as well as data communications
- Low frequency transmission medium

Figure 7.4 *Frequency range for twisted-pair cable*

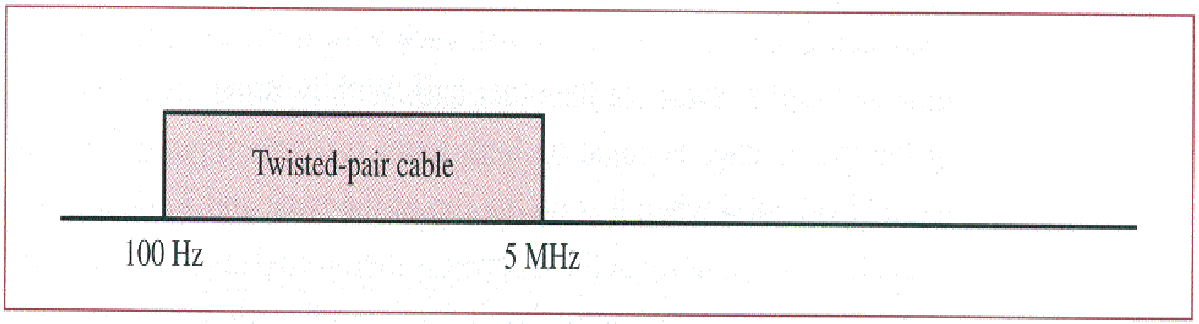
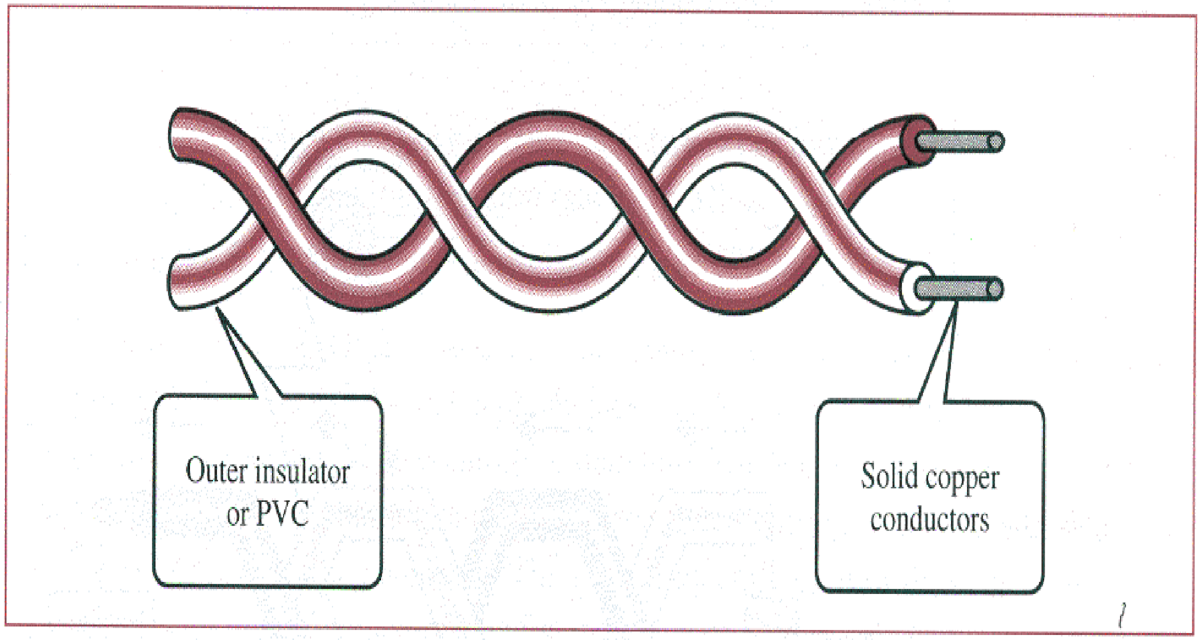


Figure 7.5 *Twisted-pair cable*



Twisted Pair - Applications

- Most common medium
- Telephone network
  - Between house and local exchange (subscriber loop)
- For local area networks (LAN)
  - 10Mbps or 100Mbps

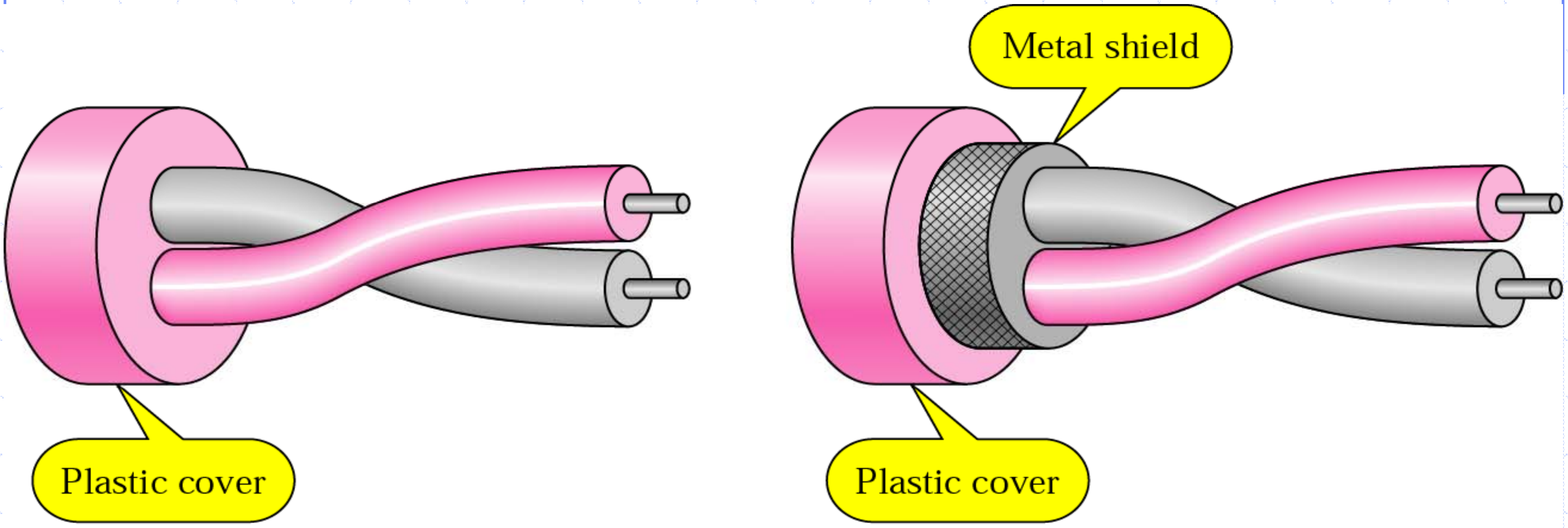
Twisted Pair - Transmission Characteristics

- Analog
  - Amplifiers every 5km to 6km
- Digital
  - repeater every 2km or 3km
- Limited distance
- Limited bandwidth (1MHz)
- Limited data rate (100MHz)

Types of Twisted Pair

- STP (shielded twisted pair)
  - the pair is wrapped with metallic foil or braid to insulate the pair from electromagnetic interference
- UTP (unshielded twisted pair)
  - each wire is insulated with plastic wrap, but the pair is encased in an outer covering

UTP and STP



a. UTP

b. STP

Unshielded and Shielded TP

- Unshielded Twisted Pair (UTP)
  - Ordinary telephone wire
  - Cheapest
  - Easiest to install
  - Suffers from external EM interference
- Shielded Twisted Pair (STP)
  - More expensive
  - Harder to handle (thick, heavy)

Ratings of Twisted Pair

- Category 3 UTP
  - data rates of up to 16mbps are achievable
- Category 5 UTP
  - data rates of up to 100mbps are achievable
  - more tightly twisted than Category 3 cables
  - more expensive, but better performance
- STP
  - More expensive, harder to work with

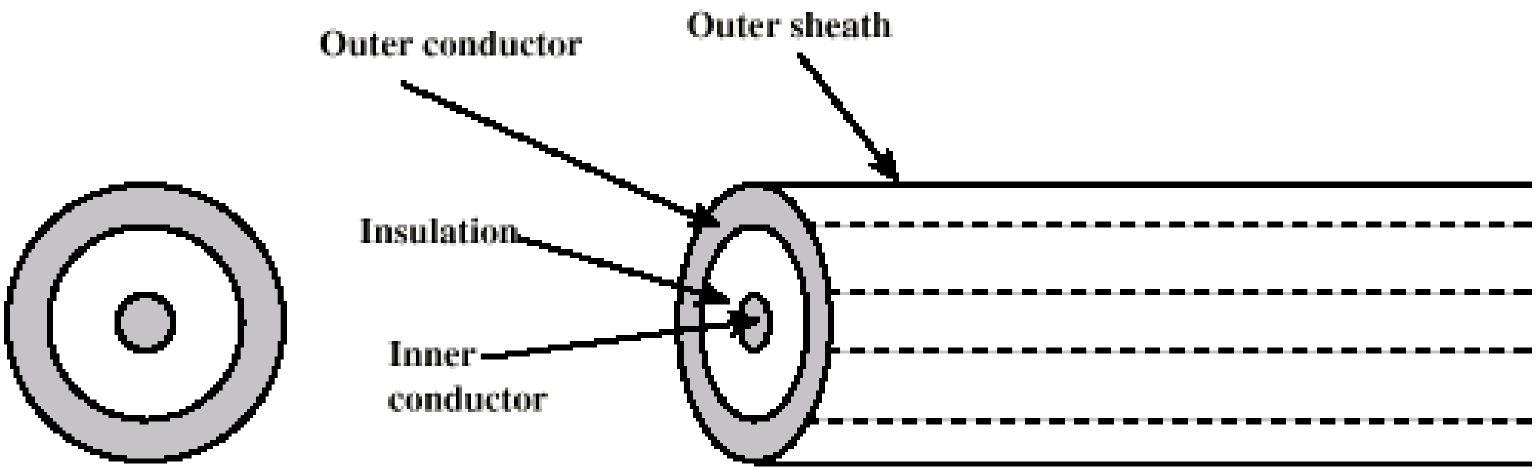
Twisted Pair Advantages

- Inexpensive
- Flexible and light weight
- Easy to work with and install

Twisted Pair Disadvantages

- defenselessness to interference and noise
- reduction problem
  - For analog, repeaters needed every 5-6km
  - For digital, repeaters needed every 2-3km
- Relatively low bandwidth

Coaxial Cable



—Outer conductor is braided shield
—Inner conductor is solid metal
—Separated by insulating material
—Covered by padding

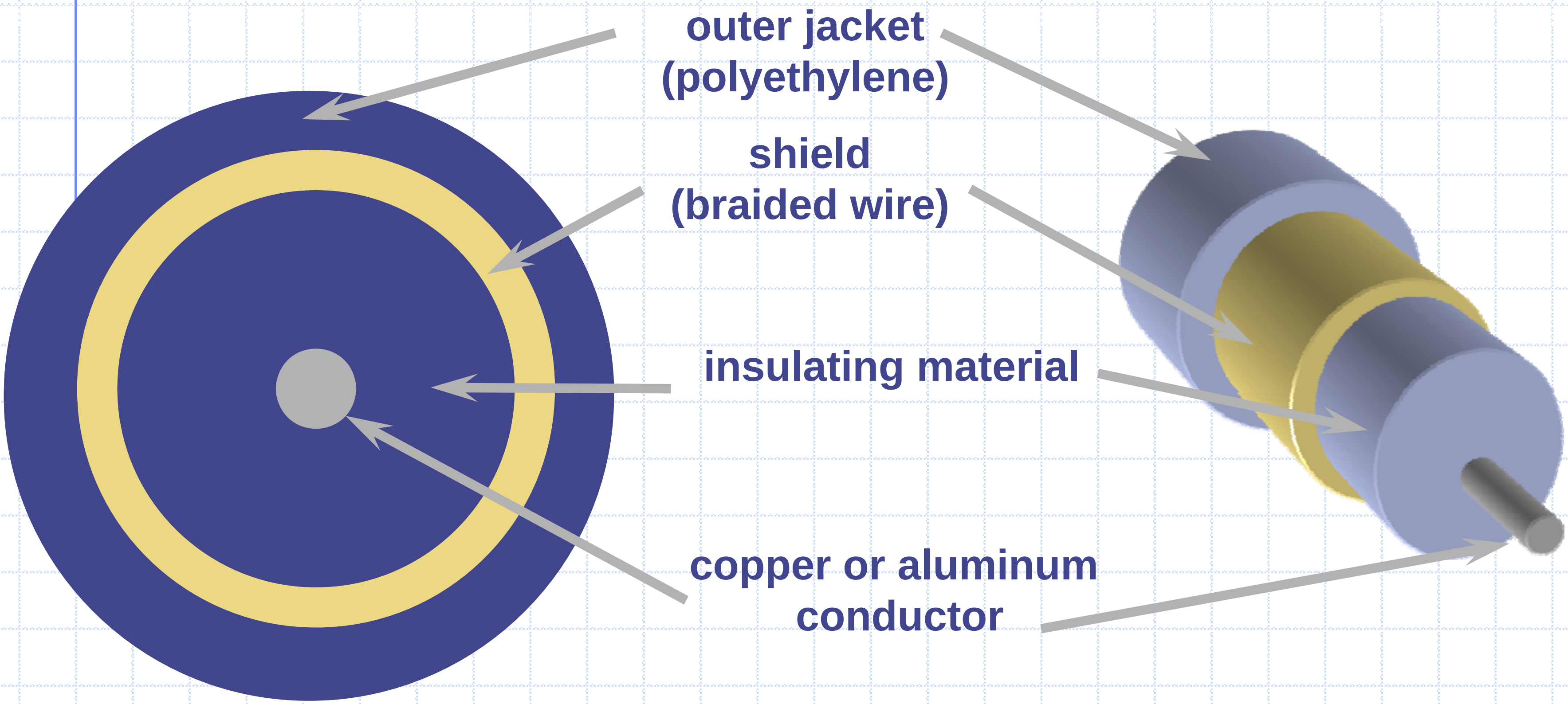
Coaxial Cable Applications

- Most versatile medium
- Television distribution
  - Ariel to TV
  - Cable TV
- Long distance telephone transmission
  - Can carry 10,000 voice calls simultaneously
  - Being replaced by fiber optic
- Short distance computer systems links
- Local area networks

Coaxial Cable - Transmission Characteristics

- Analog
  - Amplifiers every few km
  - Up to 500MHz
- Digital
  - Repeater every 1km
  - Closer for higher data rates

Coax Layers



outer jacket
(polyethylene)

shield
(braided wire)

insulating material

copper or aluminum
conductor

Coax Advantages

- Higher bandwidth
  - 400 to 600Mhz
- Can be tapped easily (pros and cons)
- Much less at risk to interference than twisted pair

Fiber Optic Cable

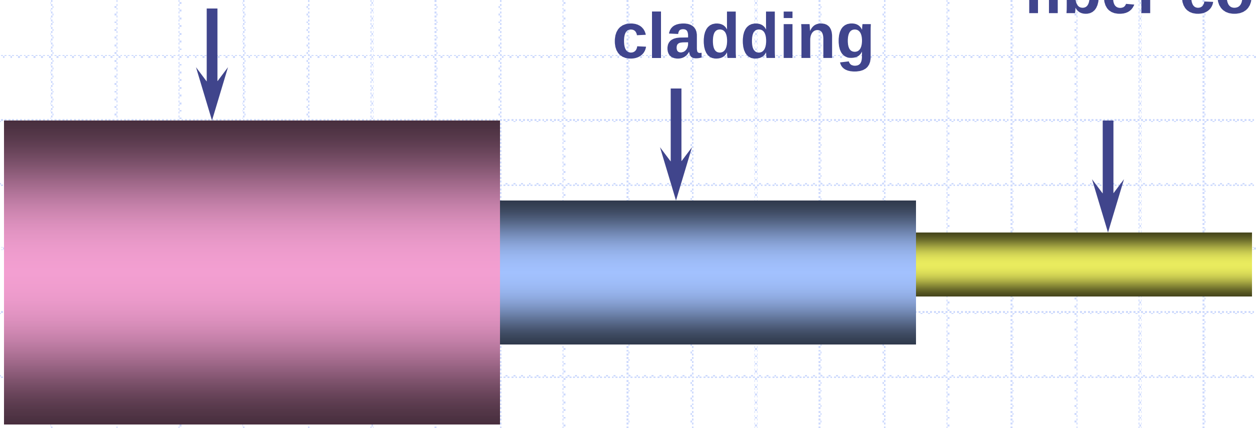
- Relatively new transmission medium used by telephone companies in place of long-distance trunk lines
- Also used by private companies in implementing local data communications networks
- Require a light source with injection laser diode (ILD) or light-emitting diodes (LED)

Optical Fiber - Benefits

- Greater capacity
  - Data rates of hundreds of Gbps
- Smaller size & weight
- Lower attenuationElectromagnetic isolation
- Greater repeater spacing
  - 10s of km at least

Fiber Optic Layers

- consists of three concentric sections



plastic jacket

glass or plastic cladding

fiber core

Fiber Optic Advantages

- greater capacity (bandwidth of up to 2 Gbps)
- smaller size and lighter weight
- lower attenuation
- immunity to environmental interference
- highly secure due to tap difficulty and lack of signal radiation

Fiber Optic Disadvantages

- expensive over short distance
- requires highly skilled installers
- adding additional nodes is difficult

Wireless (Unguided Media) Transmission

- transmission and response are achieved by means of an antenna
- directional
  - transmitting antenna puts out focused beam
  - transmitter and receiver must be aligned
- omnidirectional
  - signal spreads out in all directions
  - can be received by many antennas

Wireless Examples

- terrestrial microwave
- satellite microwave
- broadcast radio
- infrared

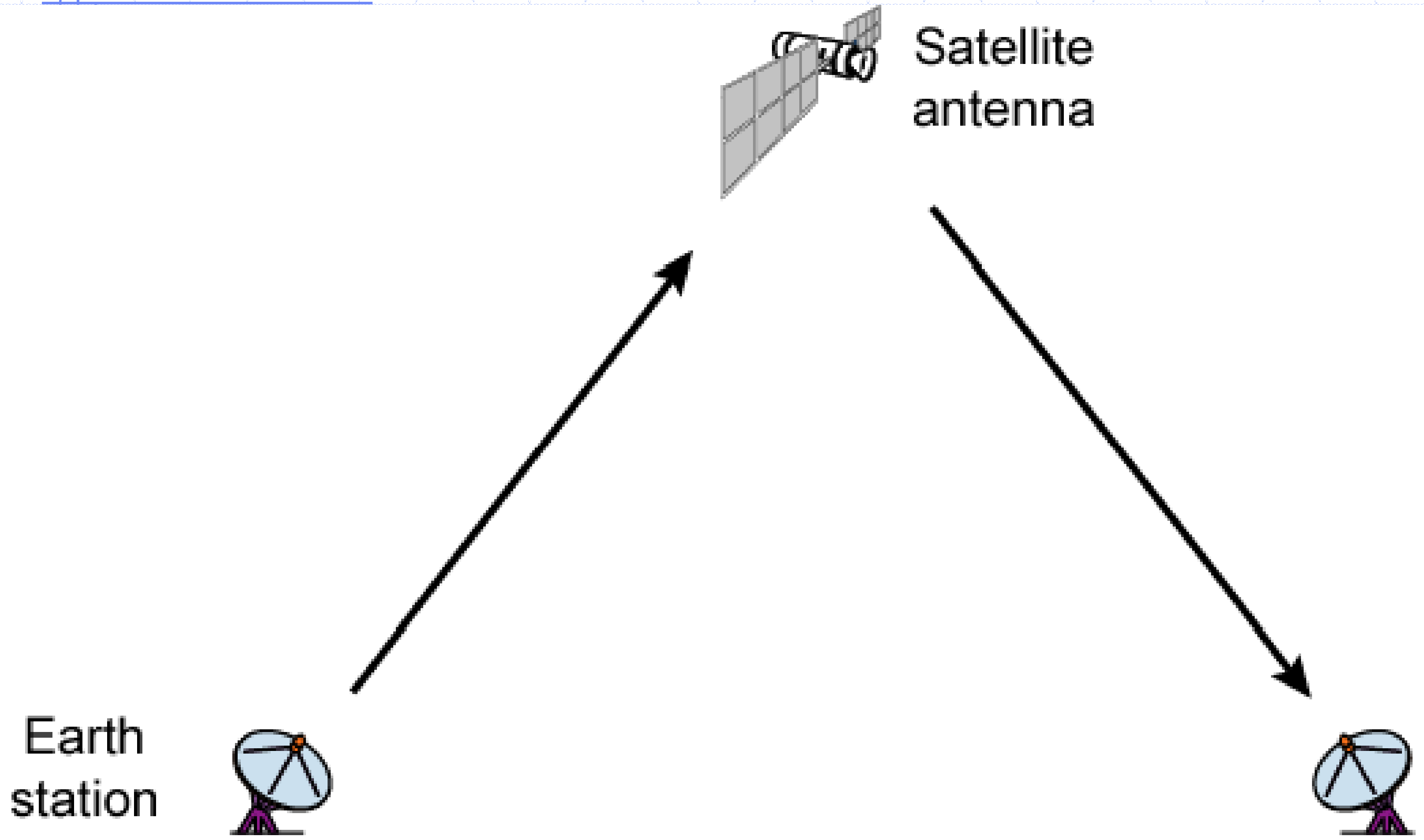
Terrestrial Microwave

- used for long-distance telephone service
- uses radio frequency spectrum, from 2 to 40 Ghz
- parabolic dish transmitter, mounted high
- used by common carriers as well as private networks
- requires unobstructed line of sight between source and receiver

Satellite Microwave

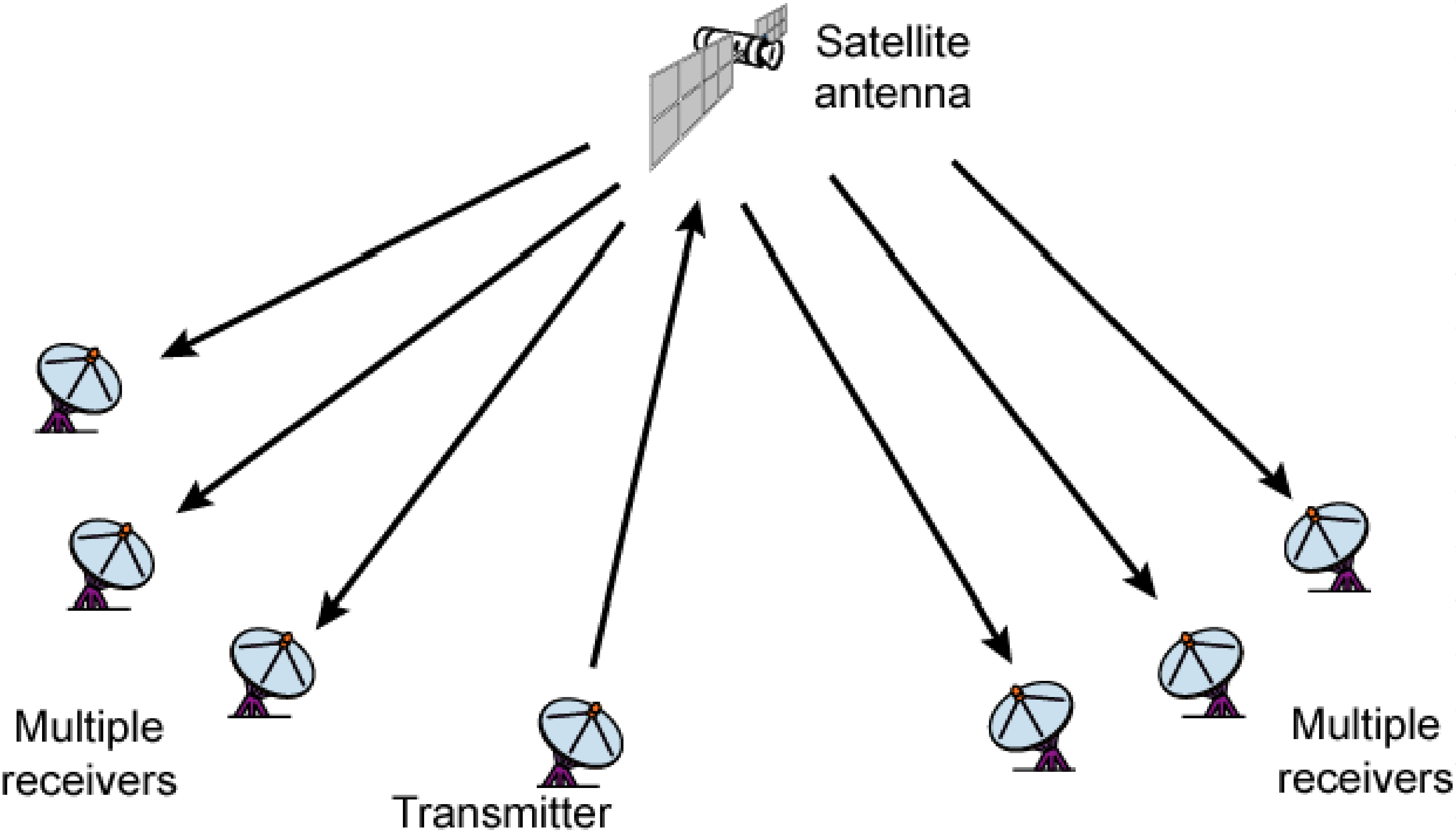
- Satellite is relay station
- Satellite receives on one frequency, amplifies or repeats signal and transmits on another frequency
- Requires geo-stationary orbit
  - Height of 35,784km
- Television
- Long distance telephone
- Private business networks

Satellite Point to Point Link



(a) Point-to-point link

Satellite Broadcast Link



(b) Broadcast link

Satellite Microwave Applications

- Television distribution
- Long-distance telephone transmission
- Private business networks

Microwave Transmission Disadvantages

- line of sight requirement
- expensive towers and repeaters
- subject to interference such as passing airplanes and rain

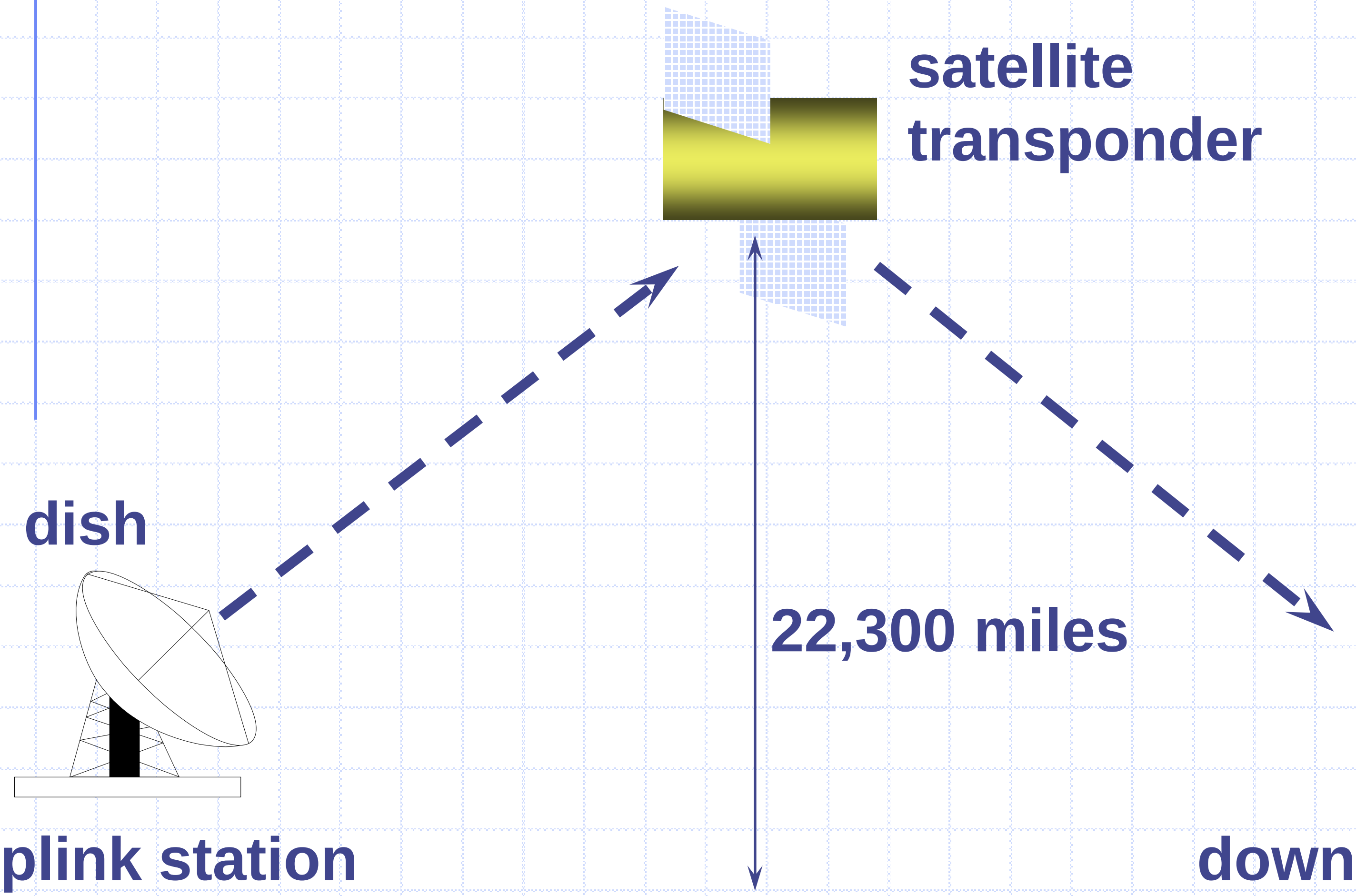
Satellite Microwave Transmission

- a microwave relay station in space
- can relay signals over long distances
- geostationary satellites
  - remain above the equator at a height of 22,300 miles (geosynchronous orbit)

Satellite Transmission Links

- earth stations communicate by sending signals to the satellite on an uplink
- the satellite then repeats those signals on a downlink
- the broadcast nature of the downlink makes it attractive for services such as the distribution of television programming

Satellite Transmission Process



Radio

- radio is omnidirectional and microwave is directional
- Radio is a general term often used to encompass frequencies in the range 3 kHz to 300 GHz.
- Mobile telephony occupies several frequency bands just under 1 GHz.

Infrared

- Uses transmitters/receivers (transceivers) that modulate noncoherent infrared light.
- Transceivers must be within line of sight of each other (directly or via reflection).
- Unlike microwaves, infrared does not penetrate walls.

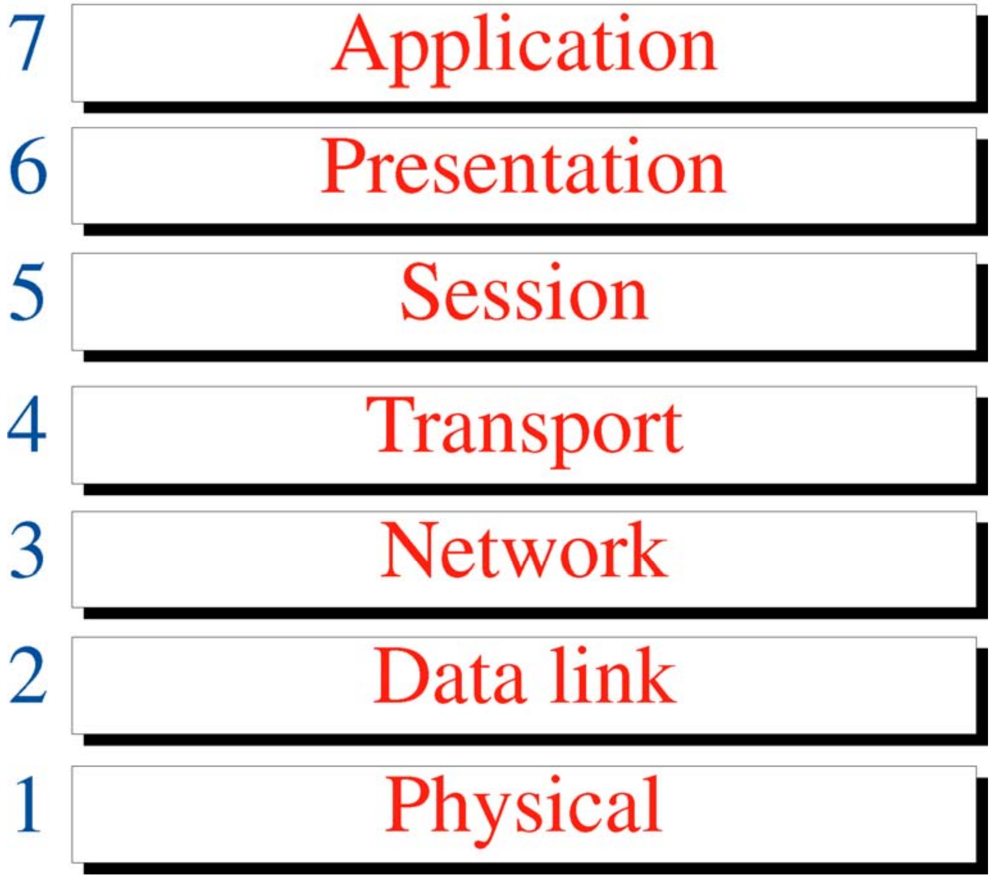
OSI Reference Model

Open Systems Interconnection (OSI) Model

- International standard organization (ISO) established a committee in 1977 to develop an architecture for computer communication.
- Open Systems Interconnection (OSI) reference model is the result of this effort.
- In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.
- Term "open" denotes the ability to connect any two systems which conform to the reference model and associated standards.

Figure 3-1

OSI Model
Layered Architecture



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data link

1 Physical

Benefits of layered Architecture

- Layer architecture simplifies the network design.

- It is easy to debug network applications in a layered architecture network.

- The network management is easier due to the layered architecture.

- Network layers follow a set of rules, called protocol.

- The protocol defines the format of the data being exchanged, and the control and timing for the handshake between layers.

Organization of the Layers

The Seven layer can be belong from three Subgroups.

Layer 1 (Physical Layer)
Layer 2 (Data Link Layer)
Layer 3 (Network Layer)

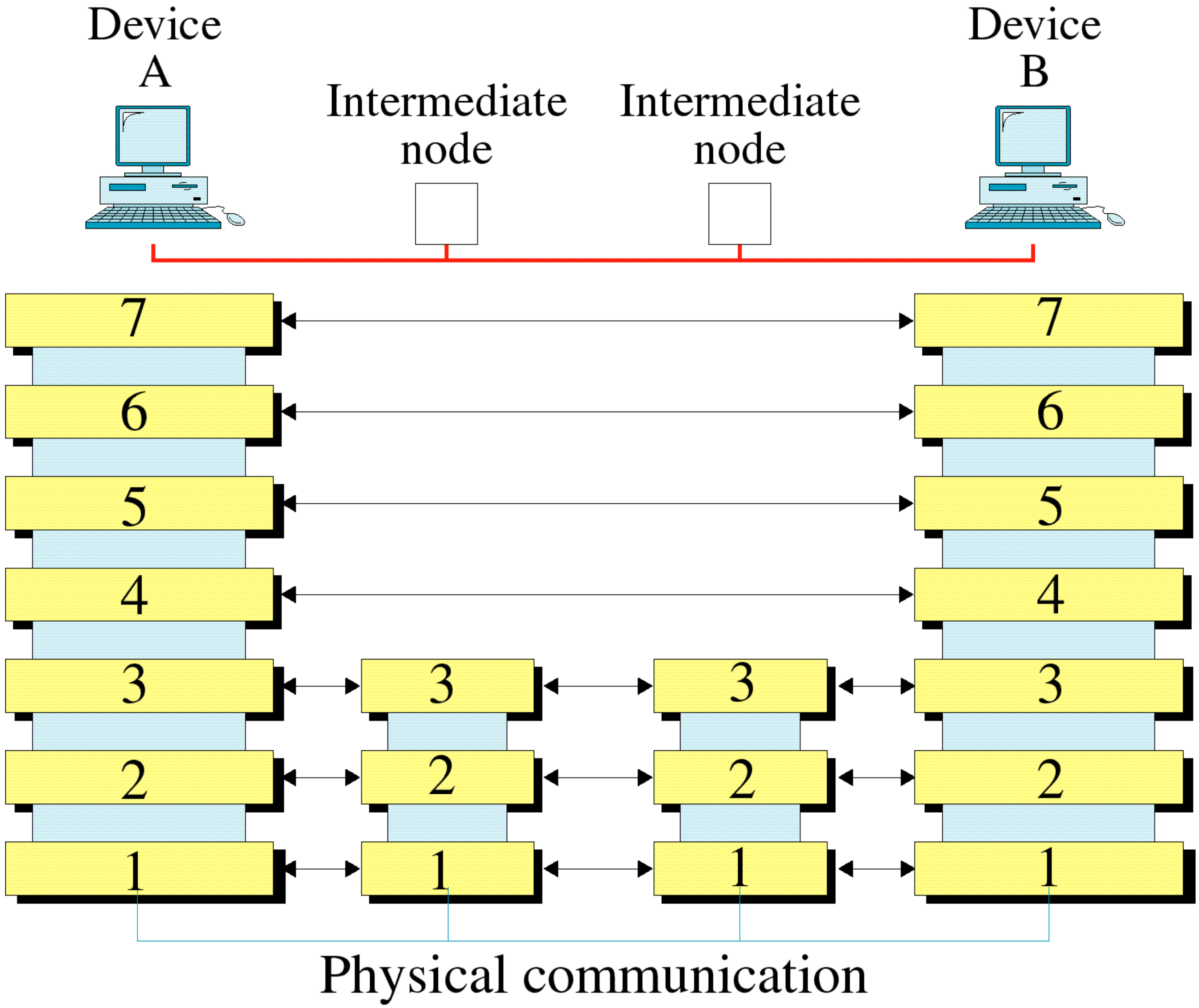
Network support layers

Layer 4 (Transport Layer)

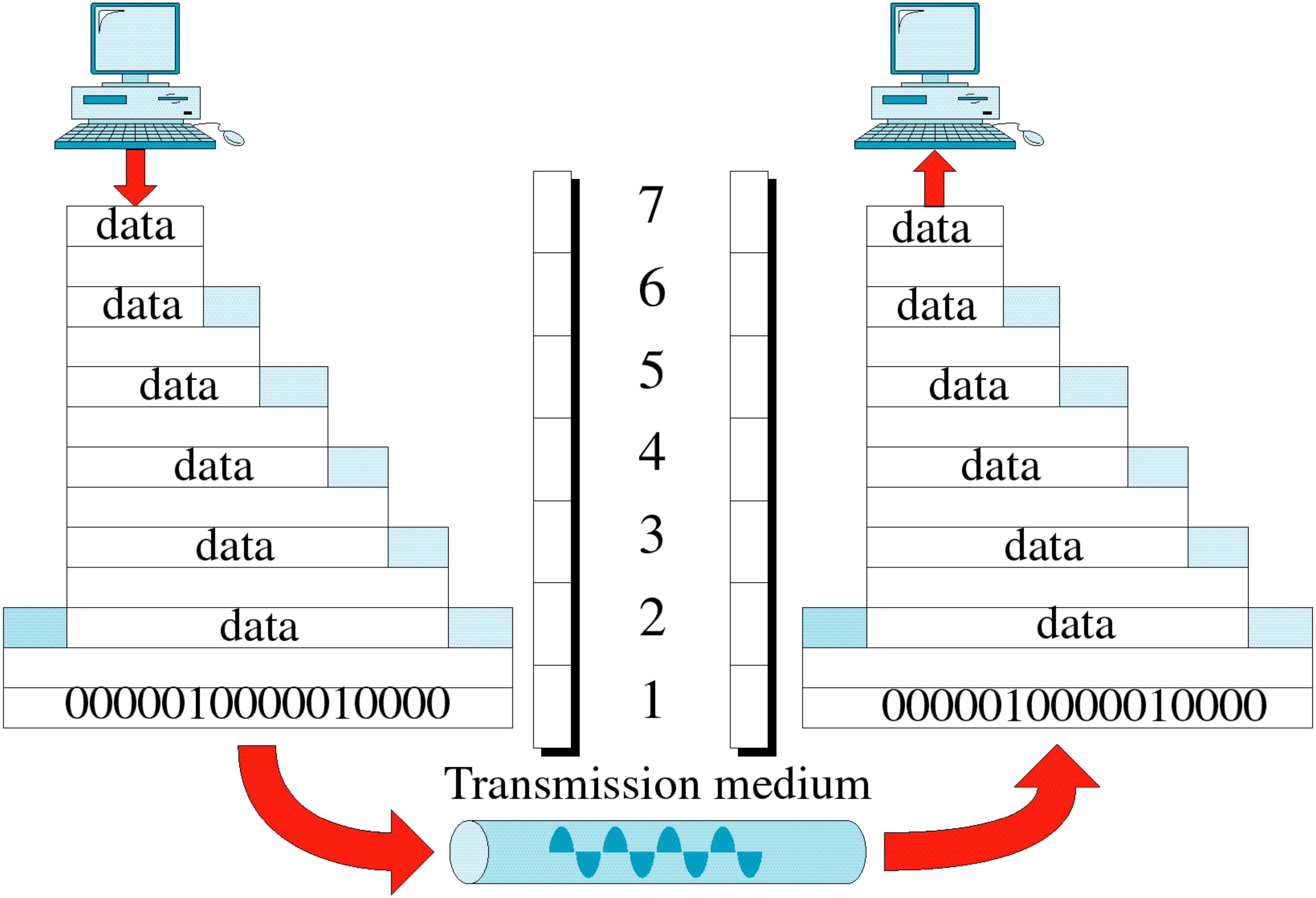
Layer 5 (Session Layer)
Layer 6 (Presentation Layer)
Layer 7 (Application Layer)

User support layers

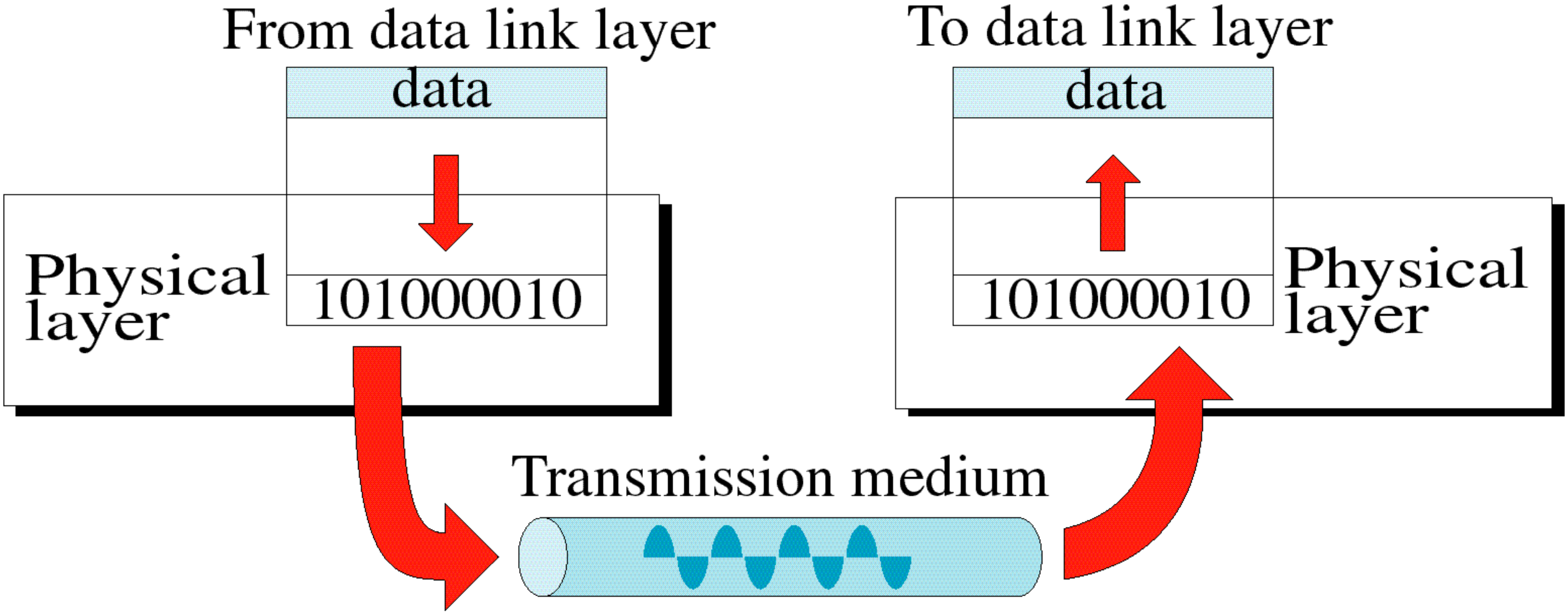
The interaction b/w layers in the OSI mode



An Exchange Using the OSI Model



Physical Layer

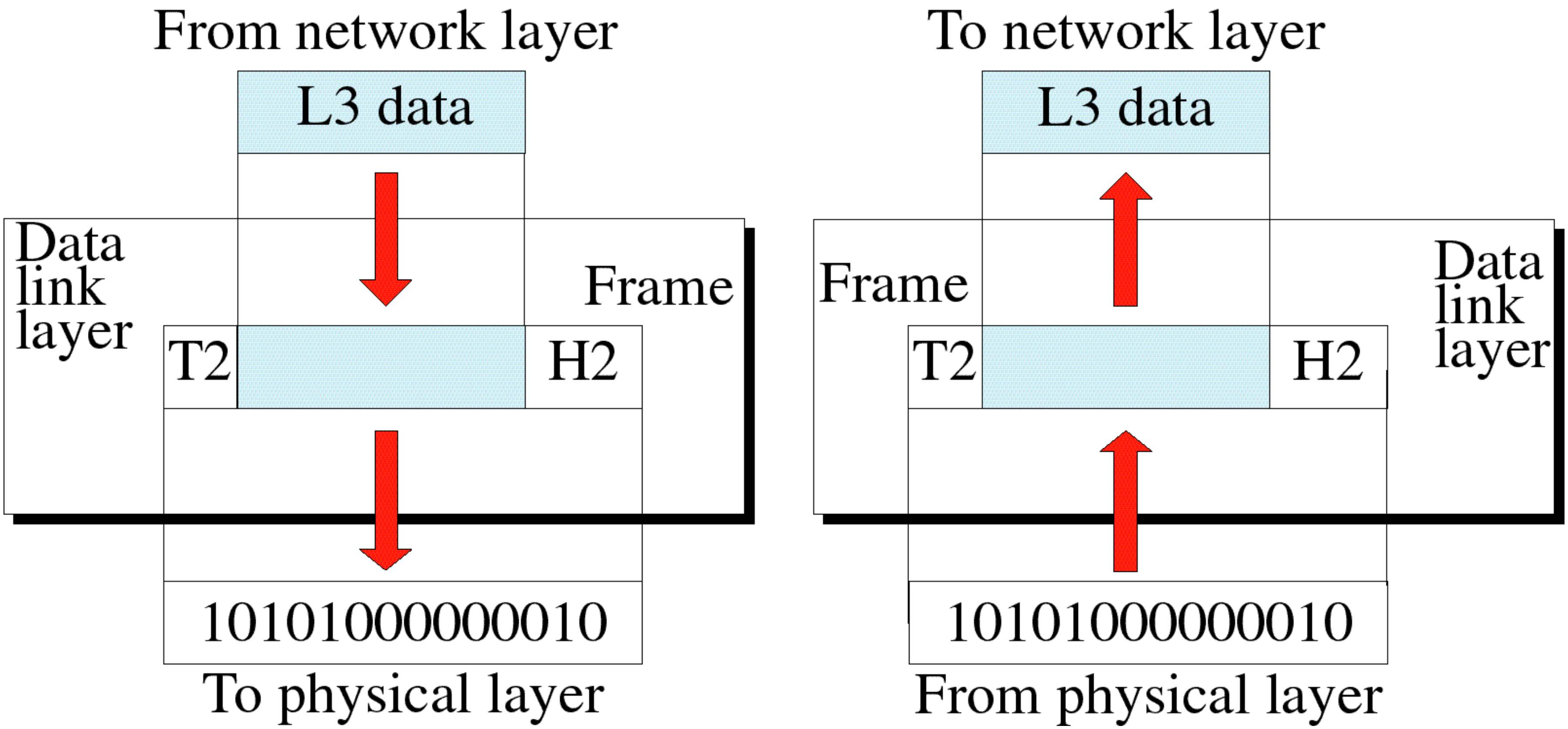


Physical Layer

The physical layer is concerned with the following

1. Physical characteristics of interface and medium
2. Representation of bit
3. Data Rate
4. Synchronization of bits
5. Line configuration (Type of connection)
6. Physical topology
7. Transmission mode

Data Link Layer

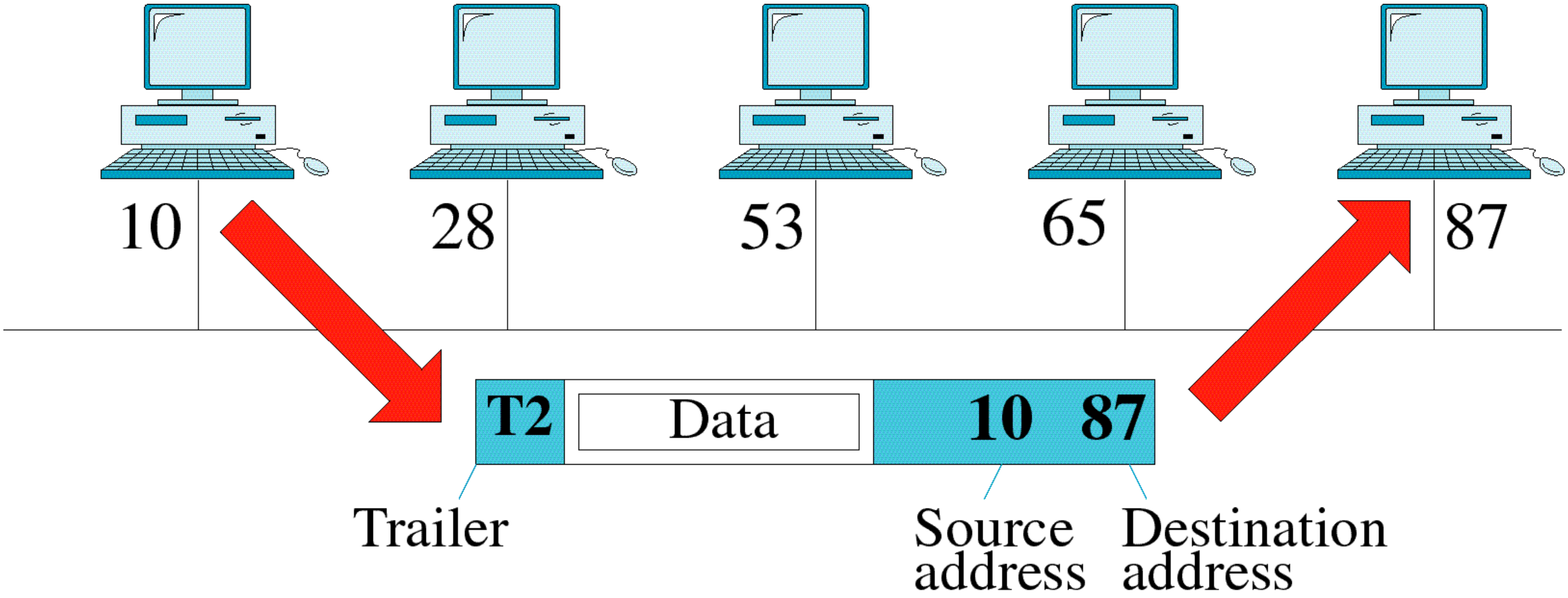


Data Link Layer

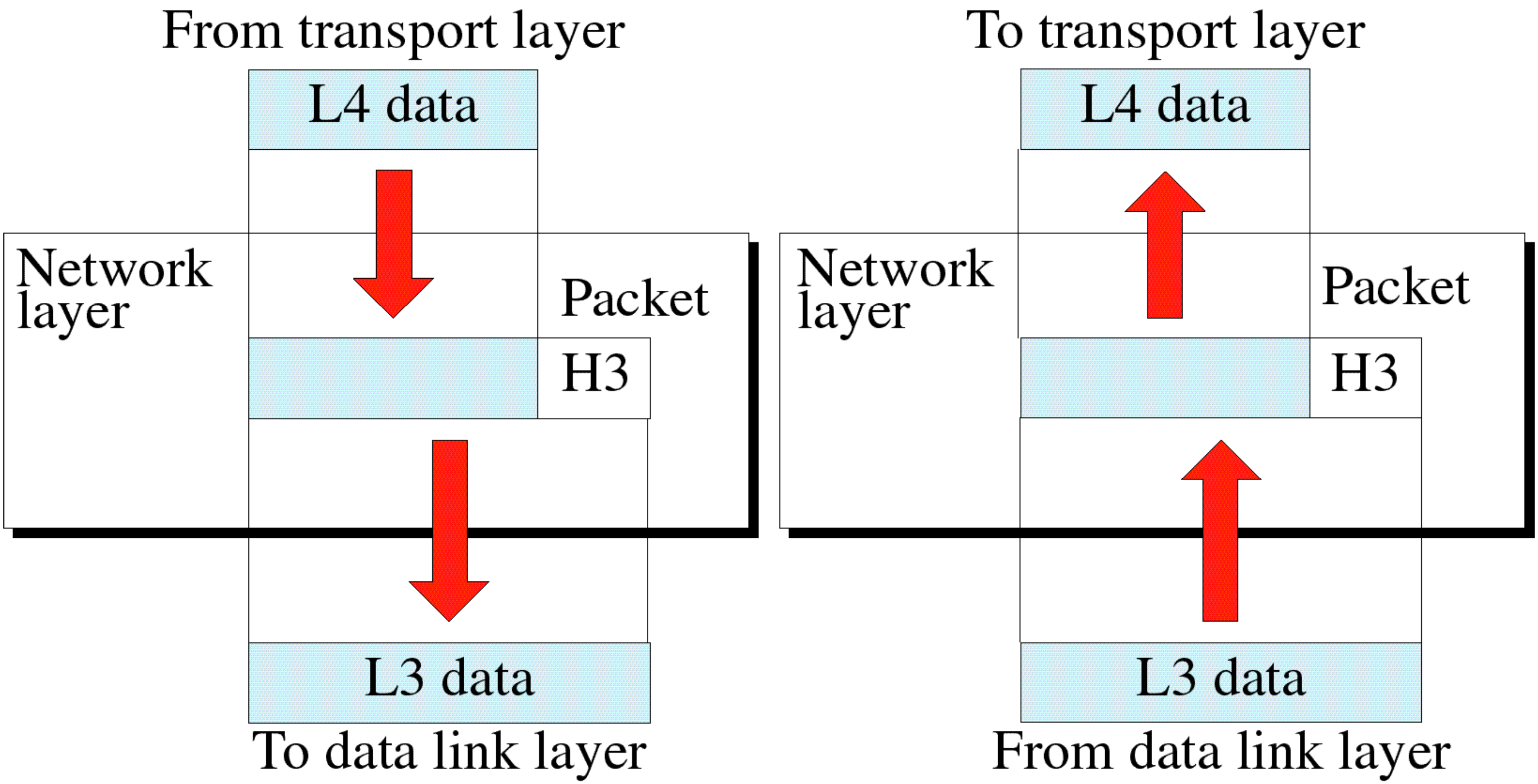
Responsibilities of data link layer

1. Framing
2. Physical address
3. Flow Control
4. Error Control
5. Access control

Data Link Layer Example



Network Layer

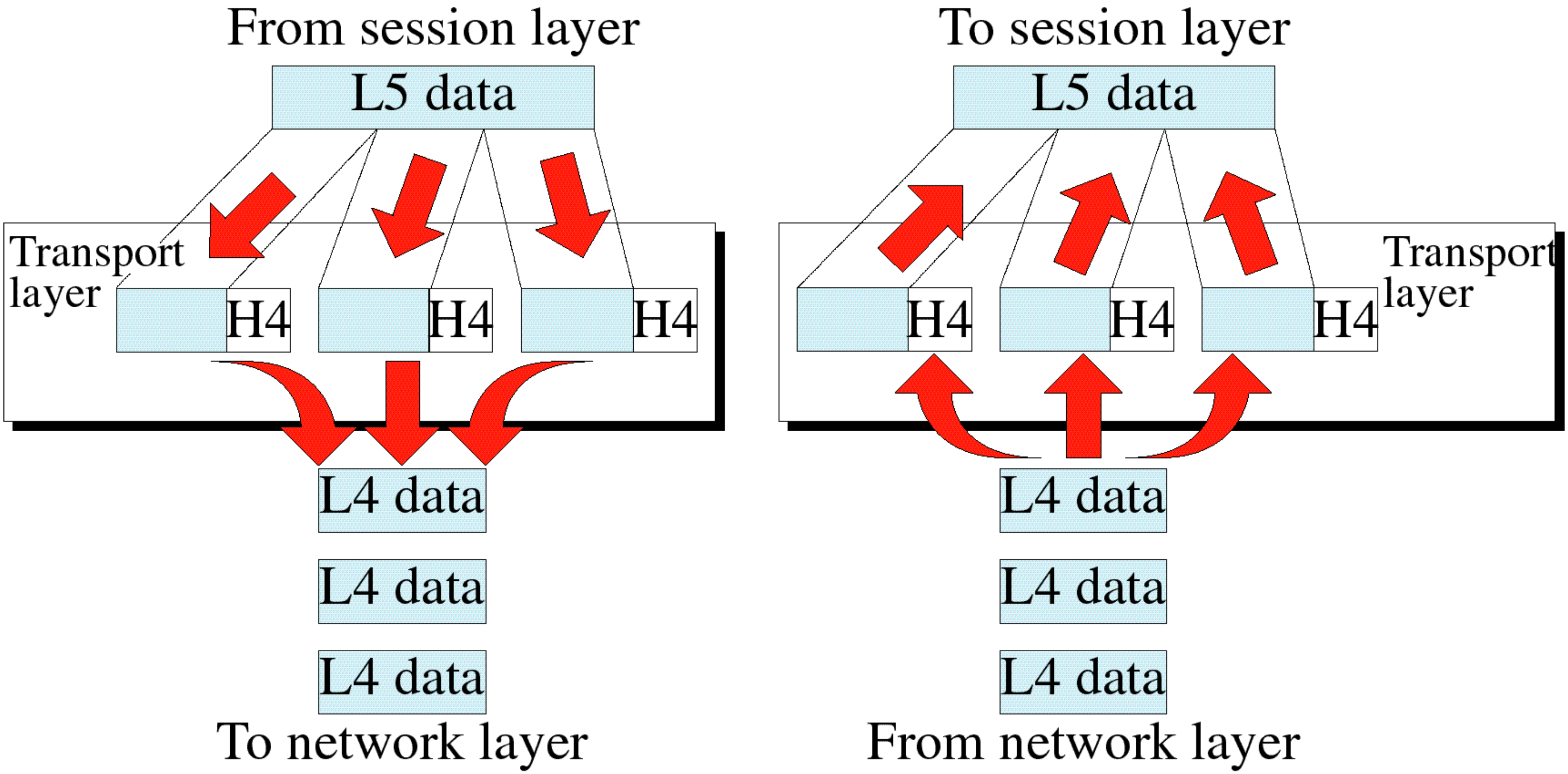


Network Layer

Responsibility of the network layer

- Implements routing of frames (packets) through the network.
- Defines the most optimum path the packet should take from the source to the destination
- Defines logical addressing so that any endpoint can be identified.
- Handles congestion in the network.
- The network layer also defines how to fragment a packet into smaller packets to accommodate different media.

Transport Layer

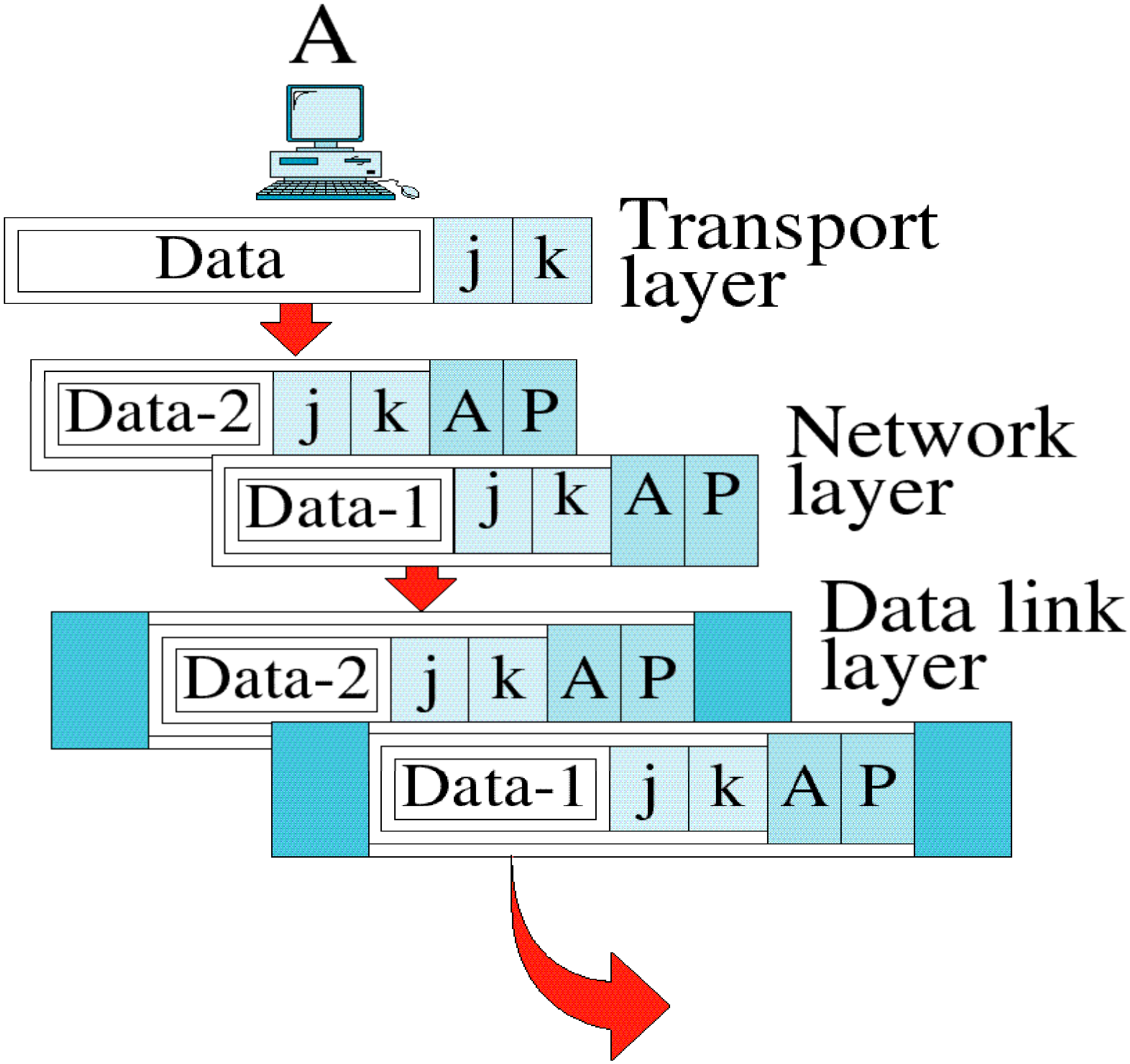


Transport Layer

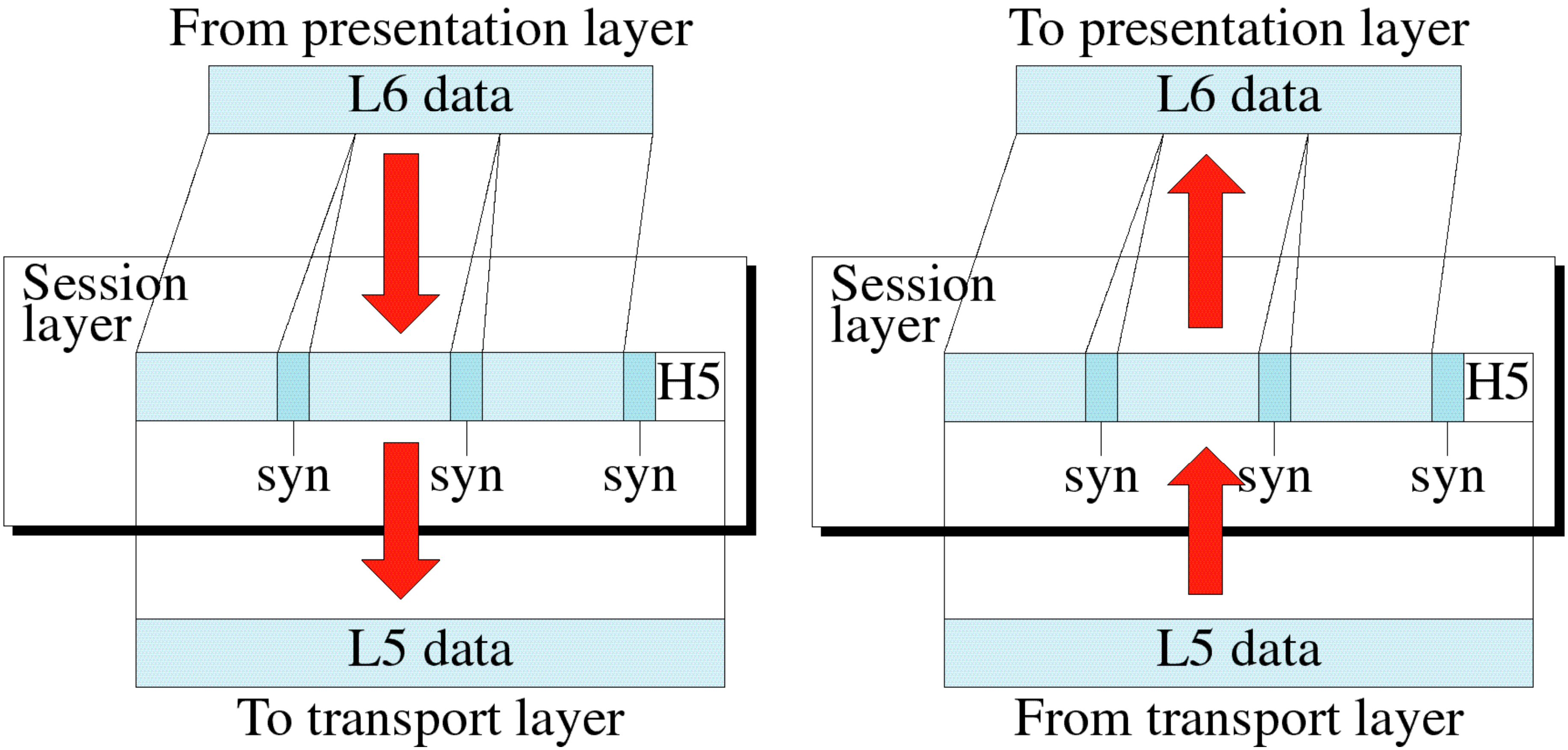
Responsibility of transport layer

- Purpose of this layer is to provide a reliable mechanism for the exchange of data between two processes in different computers.
- Segmentation and Reassembly
- Ensures that the data units are delivered error free.
- Ensures that data units are delivered in sequence.
- Ensures that there is no loss or duplication of data units.
- Provides connectionless or connection oriented service.

Transport Layer Example



Session Layer



From presentation layer

L6 data

Session layer

H5

syn syn syn

L5 data

To transport layer

To presentation layer

L6 data

Session layer

H5

syn syn syn

L5 data

From transport layer

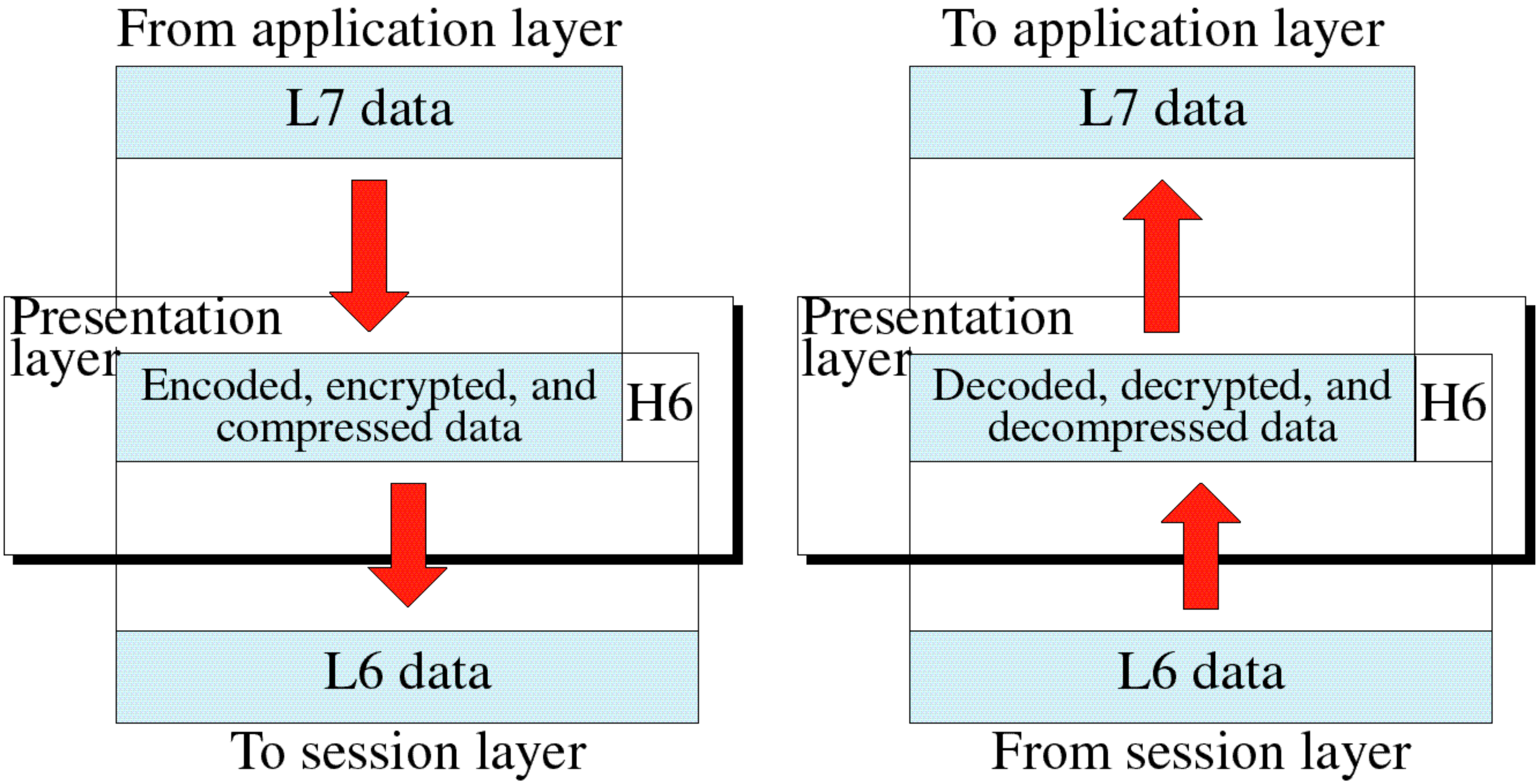
Session Layer

Responsibility of Session layer

- Session layer provides mechanism for controlling the dialogue between the two end systems. It defines how to start, control and end conversations (called sessions) between applications.

- This layer requests for a logical connection to be established on an end-user's request.
- Any necessary log-on or password validation is also handled by this layer.
- Session layer is also responsible for terminating the connection.
- This layer provides services like dialogue discipline which can be full duplex or half duplex.
- Session layer can also provide check-pointing mechanism such that if a failure of some sort occurs between checkpoints, all data can be retransmitted from the last checkpoint.

Presentation Layer

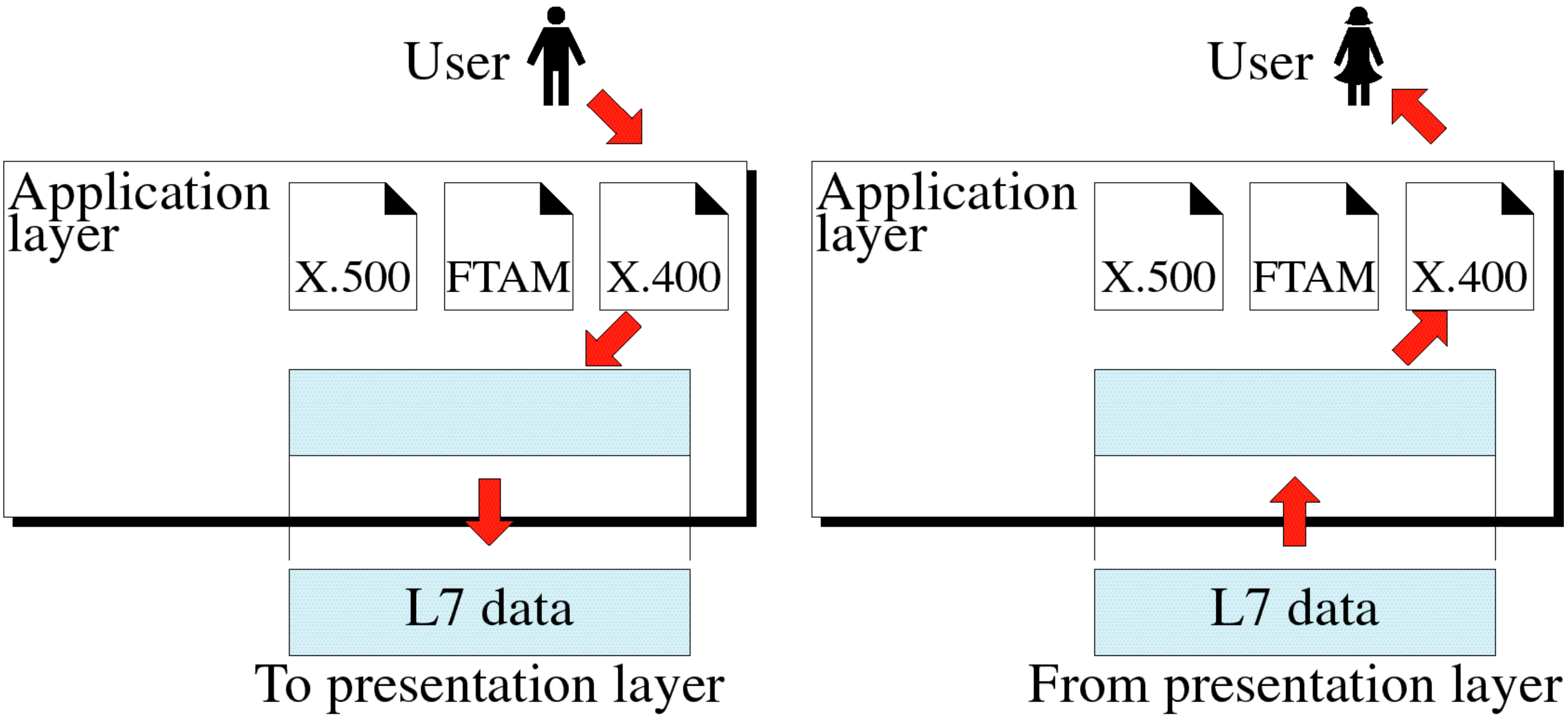


Presentation Layer

Responsibility of Presentation layer

- Presentation layer defines the format in which the data is to be exchanged between the two communicating entities.
- Also handles data compression and data encryption (cryptography).

Application Layer

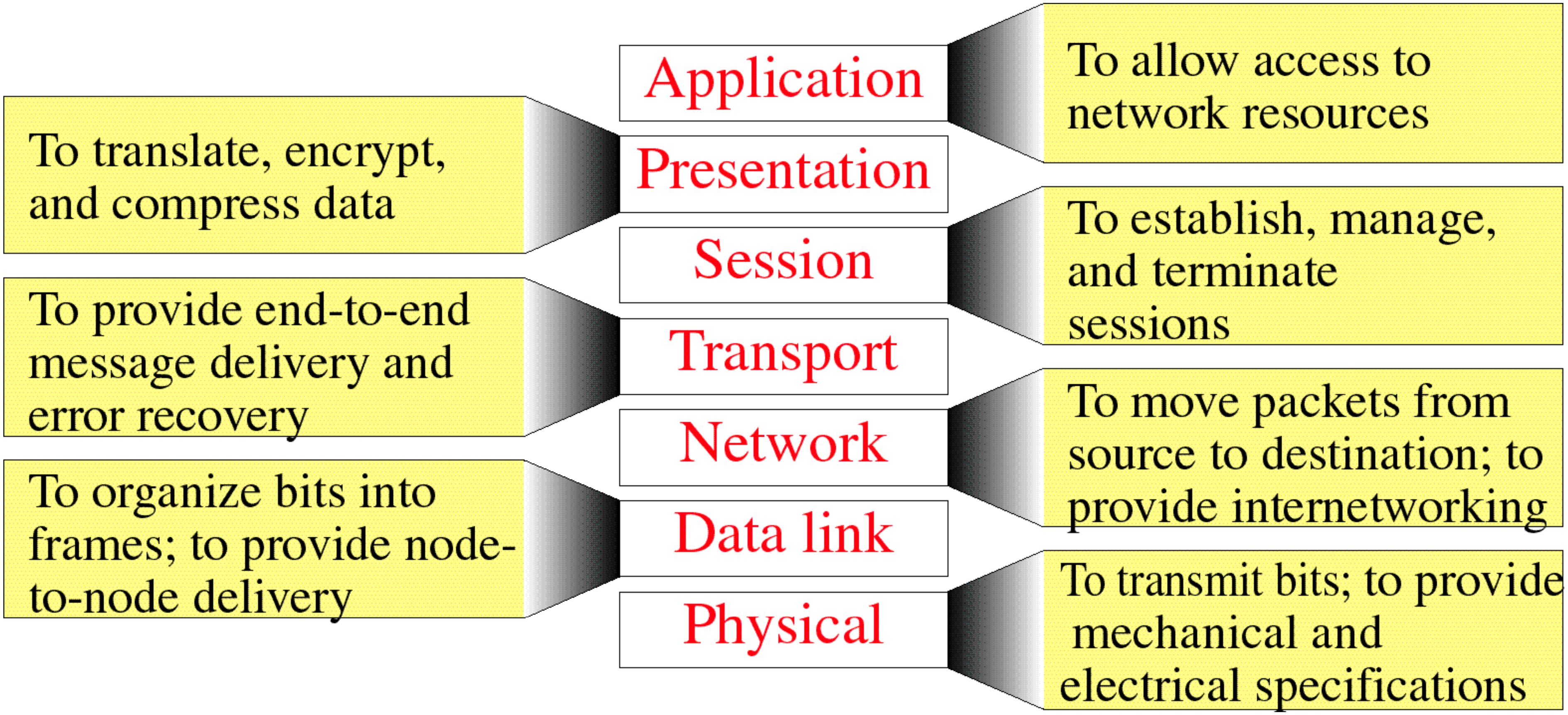


Application Layer

Responsibility of Application layer

- Application layer interacts with application programs and is the highest level of OSI model.
- Application layer contains management functions to support distributed applications.
- Examples of application layer are applications such as file transfer, electronic mail, remote login etc.

Summary of Layer Functions



Application

To allow access to network resources

Presentation

To translate, encrypt, and compress data

Session

To establish, manage, and terminate sessions

Transport

To provide end-to-end message delivery and error recovery

Network

To move packets from source to destination; to provide internetworking

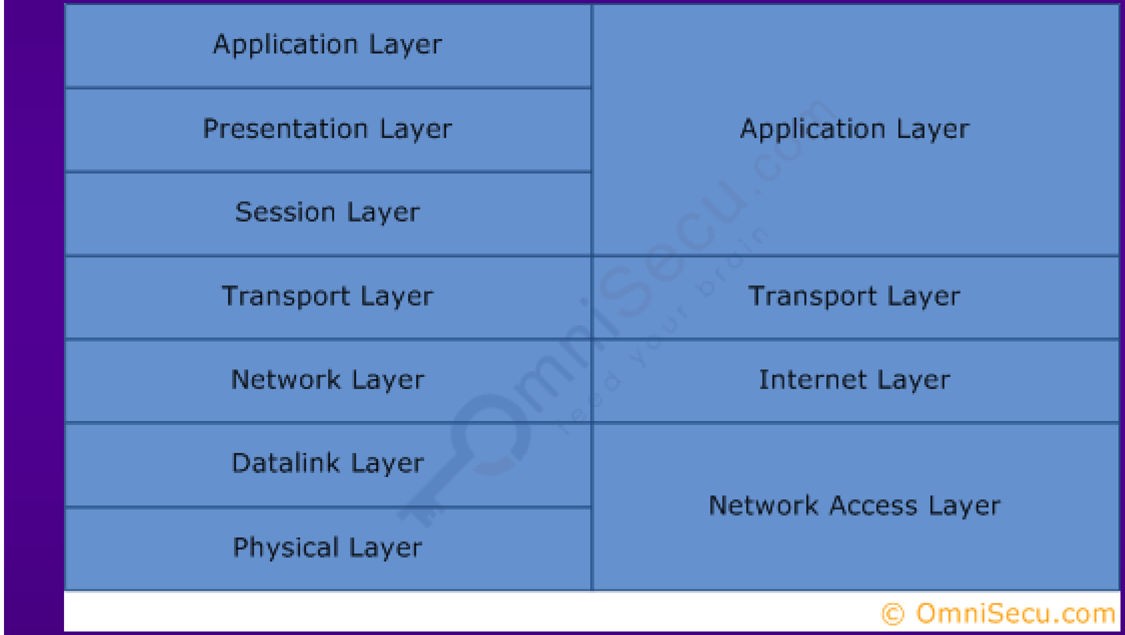
Data link

To organize bits into frames; to provide node-to-node delivery

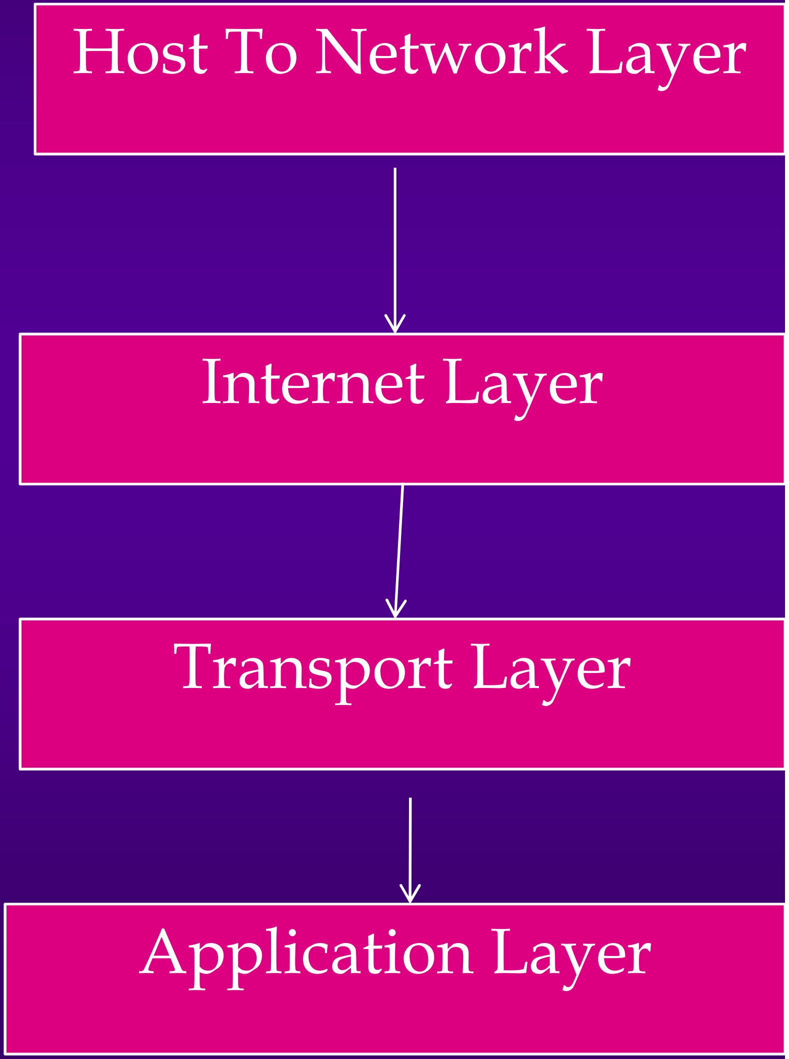
Physical

To transmit bits; to provide mechanical and electrical specifications

TCP/IP Reference Model



Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Datalink Layer	Network Access Layer
Physical Layer	



Host To Network Layer

Internet Layer

Transport Layer

Application Layer

1.Host to Network layer

Host connect to network using some protocols so that it can send IP packets over it

2. Internet layer

Its job is to permit hosts to inject packets into any network & have them travel independently to the destination. If they arrive out of order, it is the job of higher layers to rearrange them, if in-order delivery is desired

1.Transport layer

- allow peer entities on the source & destination hosts to carry on a conversation
- Two end to end protocols have been defined here:

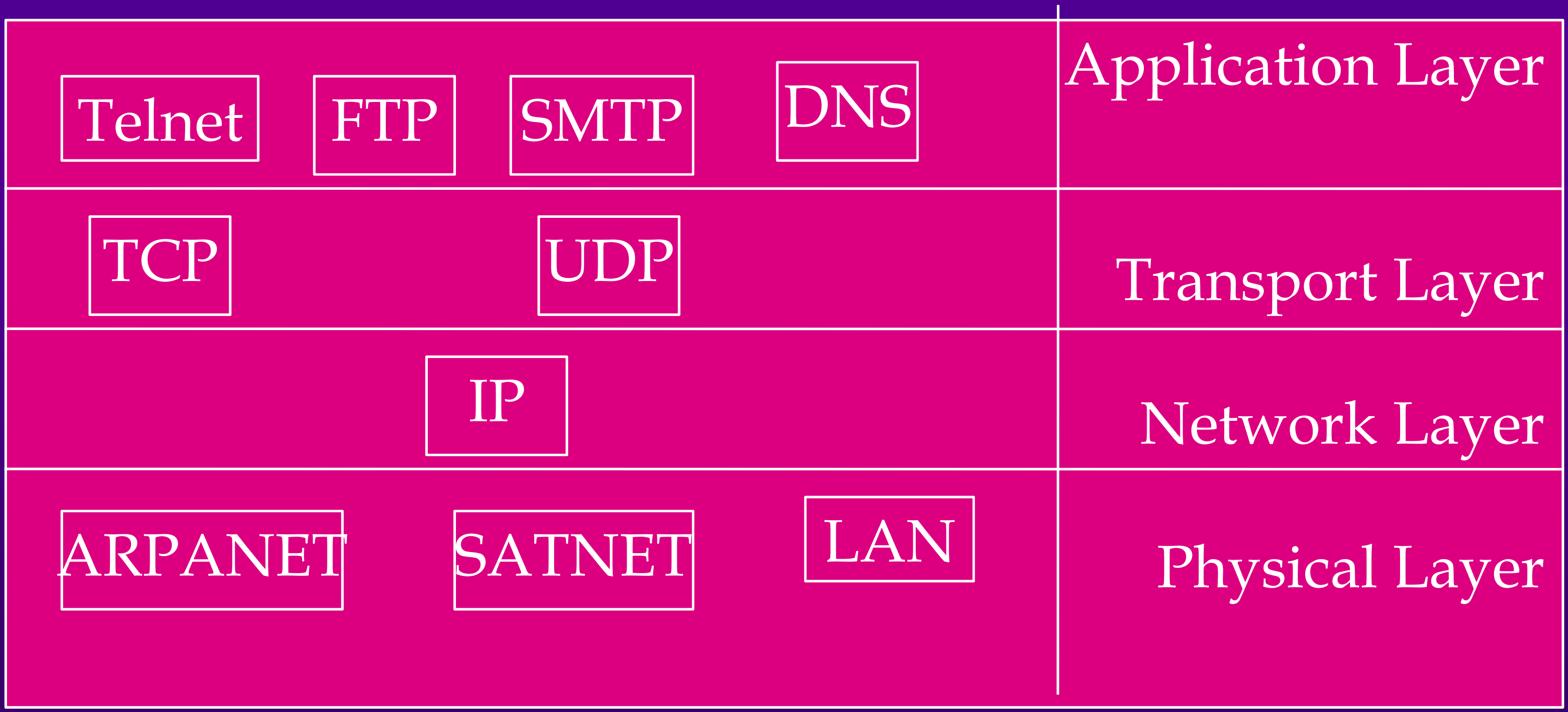
(1) TCP(Transmission Control Protocol) is a reliable connection oriented protocol that allow a byte origination on one machine to be delivered without errors on any other machine in the internet.

- Fragments the incoming byte stream into discrete message
- TCP also handles flow control.

1.Transport layer

(2) UDP(User Datagram Protocol) it is an unreliable, connectionless protocol for applications that do not want TCP’s sequencing or flow control.

Protocols and Networks in TCP/IP Model



Telnet FTP SMTP DNS	Application Layer
TCP UDP	Transport Layer
IP	Network Layer
ARPANET SATNET LAN	Physical Layer

Definition

- Backbone Network (BN) - a large high-speed central network that connects all the terminals, microcomputers, mainframes, local area networks, and other communications equipment on a single company or site. Sometimes called a Campus Area Network (CAN). Use Higher speed circuits for connectivity.

Definition

- Enterprise Network (EN) - a supernetwork that interconnects all of an organizations networks (LANs and WANs), regardless of whether it crosses state, national, or international boundaries.

Introduction

There are two approaches to providing high speed networking.

- “speed up” the technologies currently used in local area networks.
  - Fast Ethernet
  - Fast Token Ring
- develop new high speed technologies that provide dedicated point-to-point communication circuits
  - Switched Ethernet
  - Switched Token Ring

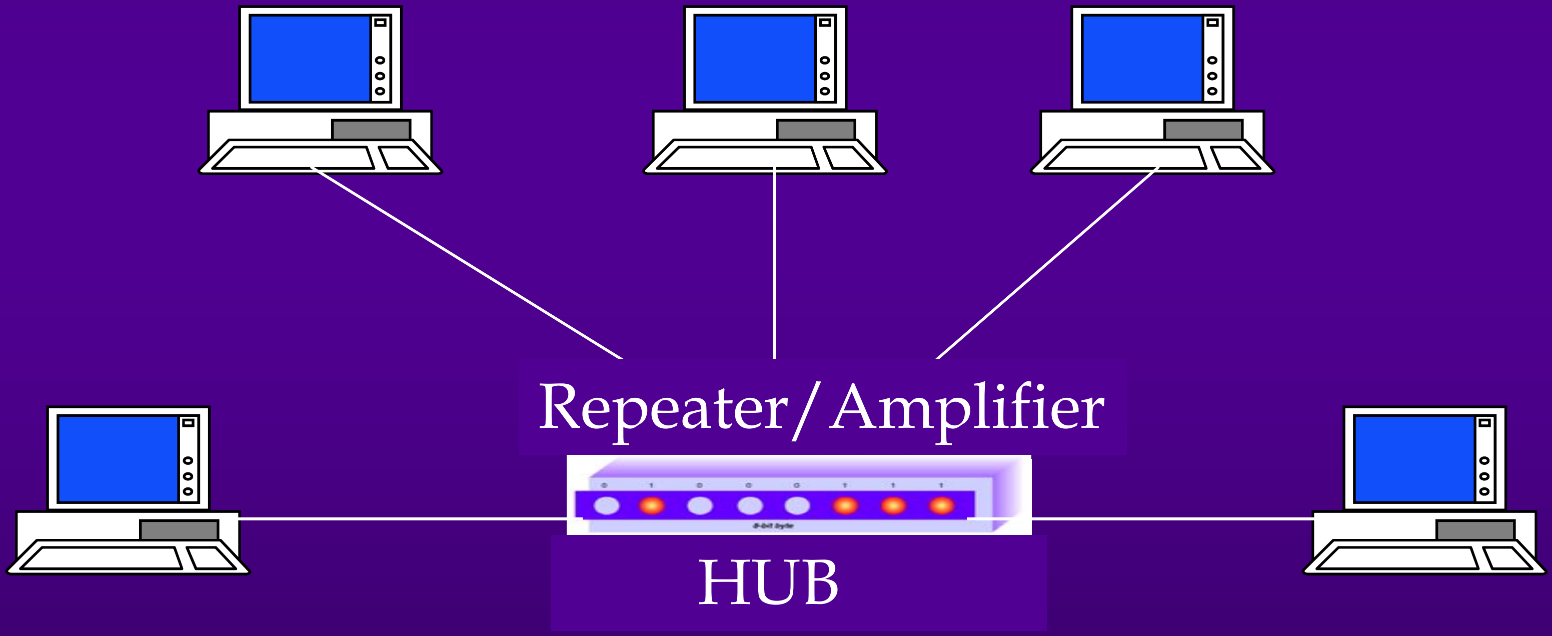
Backbone Network Components

- Two basic components to the BN
  - hardware devices that connect the networks to the backbone
    - hubs
    - bridges
    - switches
    - routers
    - brouters
    - gateways
  - network cable

Hubs

- very simple devices that pass all traffic in both directions between the LAN sections they link
- same or different cable types
- use physical layer protocols
- used to connect LANs of similar technology, or to extend the distance of one LAN
- can be called repeaters or amplifiers

HUB Devices



Repeater/Amplifier

HUB

Hubs

+

- inexpensive
- easy to Install
- can connect different media
- very little delay

−

- limited distance between devices
- limited on the number of repeaters
- no error detection
- does not filter

Bridges

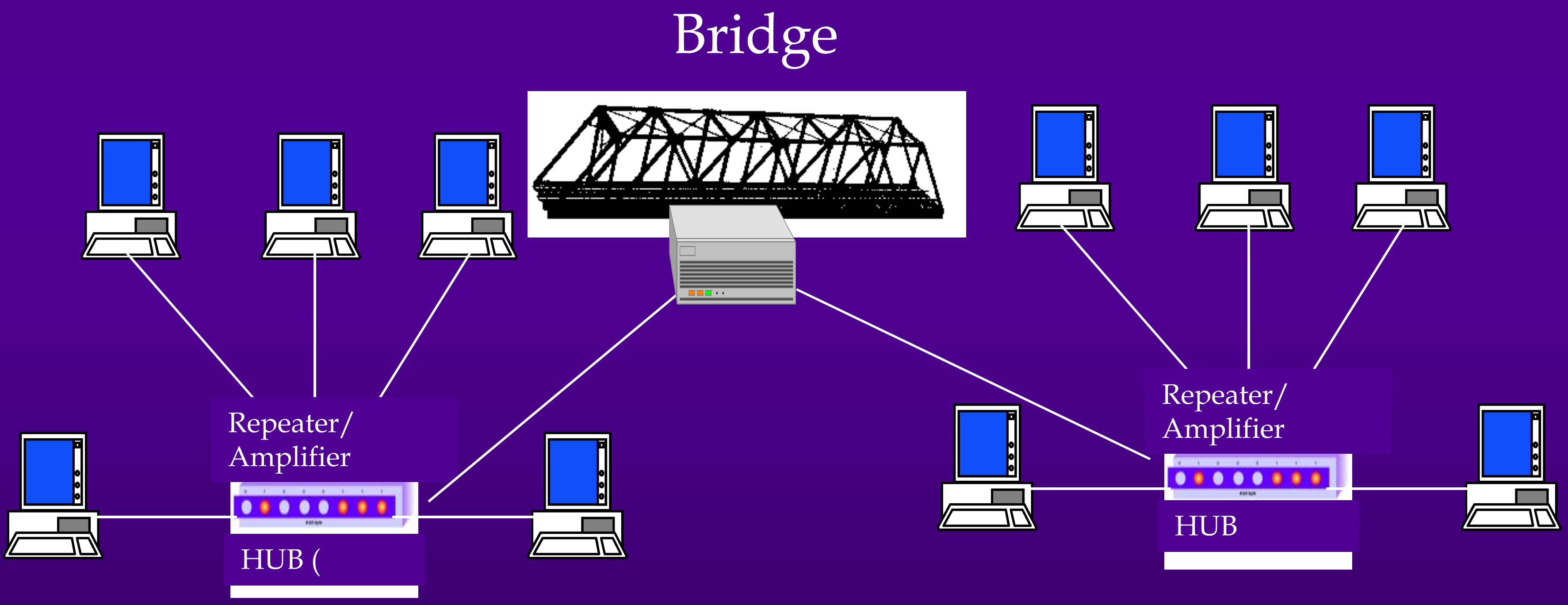
- connect two LAN segments that use the same data link and network protocol
- operated at the data link layer
- same or different cable types
- forward only those messages that need to go out (filtering)
- “learn” whether to forward packets
- internal routing table
- combination of “black box” hardware and software

Bridges

There are three types of bridges:

- Simple bridge
- Learning bridge
- Multiport bridge

Bridges Interconnecting



Bridges

+

- may be different data rates and different media easy to Install
- no modifications required to the communications software
- can learn the ports for data transmission

−

- understand only data link layer protocols and addresses
- no protocol conversion
- broadcasts when it does not know the address

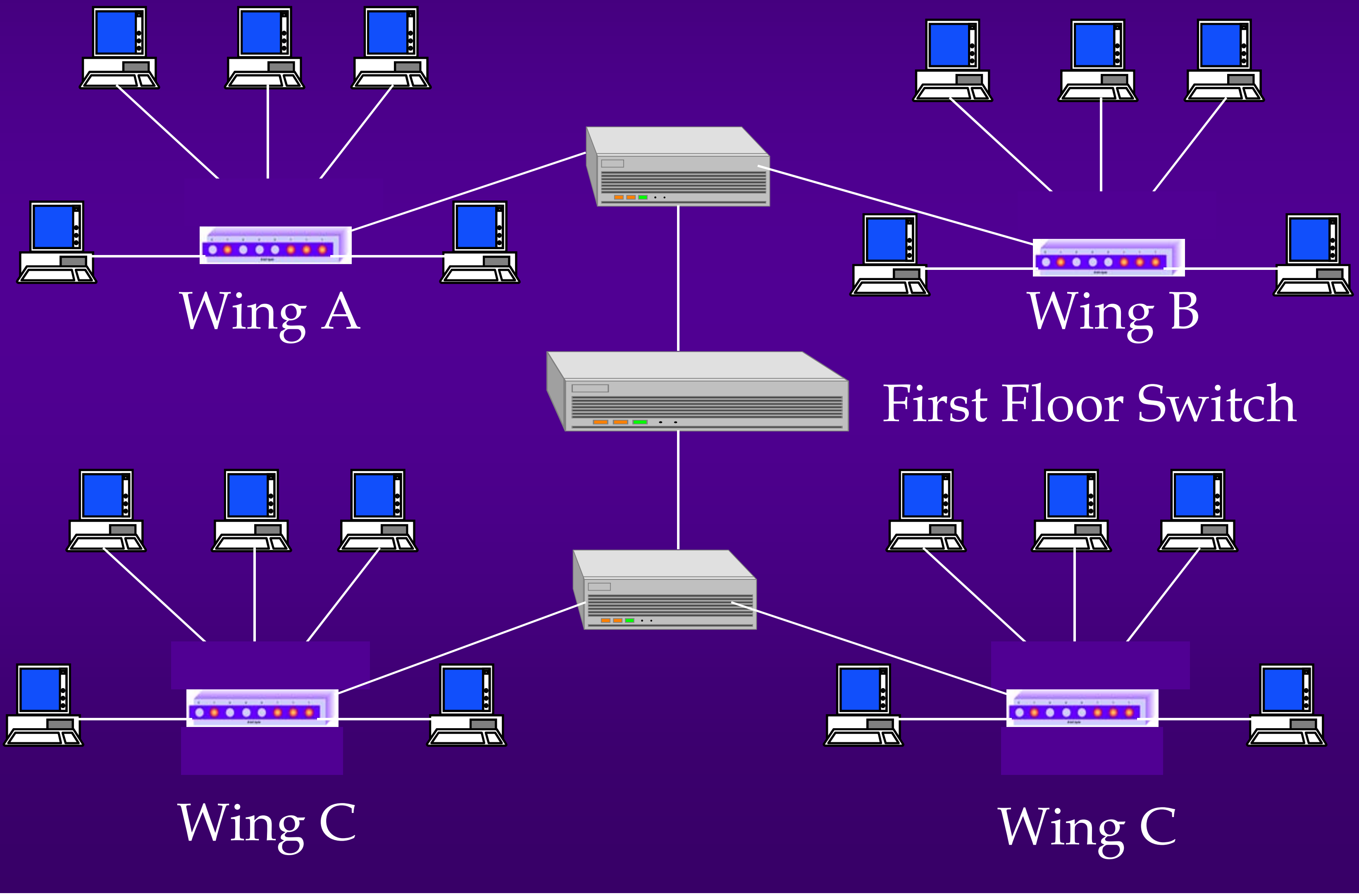
Switches

- connect more than two LAN segments that use the same data link and network protocol.
- operate at the data link layer
- same or different type cable
- ports are used simultaneously
- connect lower speed segments to high speed BN

Switches

- Cut-through switches
  - use circuit-switching to immediately connect the port with the incoming message to the correct outgoing port
  - very fast as decisions are done in hardware
  - outgoing packet is lost if port is in use
- Store-and-forward switches
  - copy the incoming packet to memory prior to processing the destination address -- transmit it when the outgoing port is ready

Switches Interconnecting



Switches

+

- much more sophisticated than previously
- enable all ports to work at the same time
- can convert protocols
- configurable
- high speed

−

- understand only data link layer protocols and addresses
- much more expensive then previous options
- higher maintenance

Routers

- connect two or more LANs that use the same or different data link protocols, but the same network protocol.
- same or different cable types
- operate at the network layer
- forward only messages that need to go out
- routers use the internetwork address
- internal routing tables
- only processes messages addressed to it

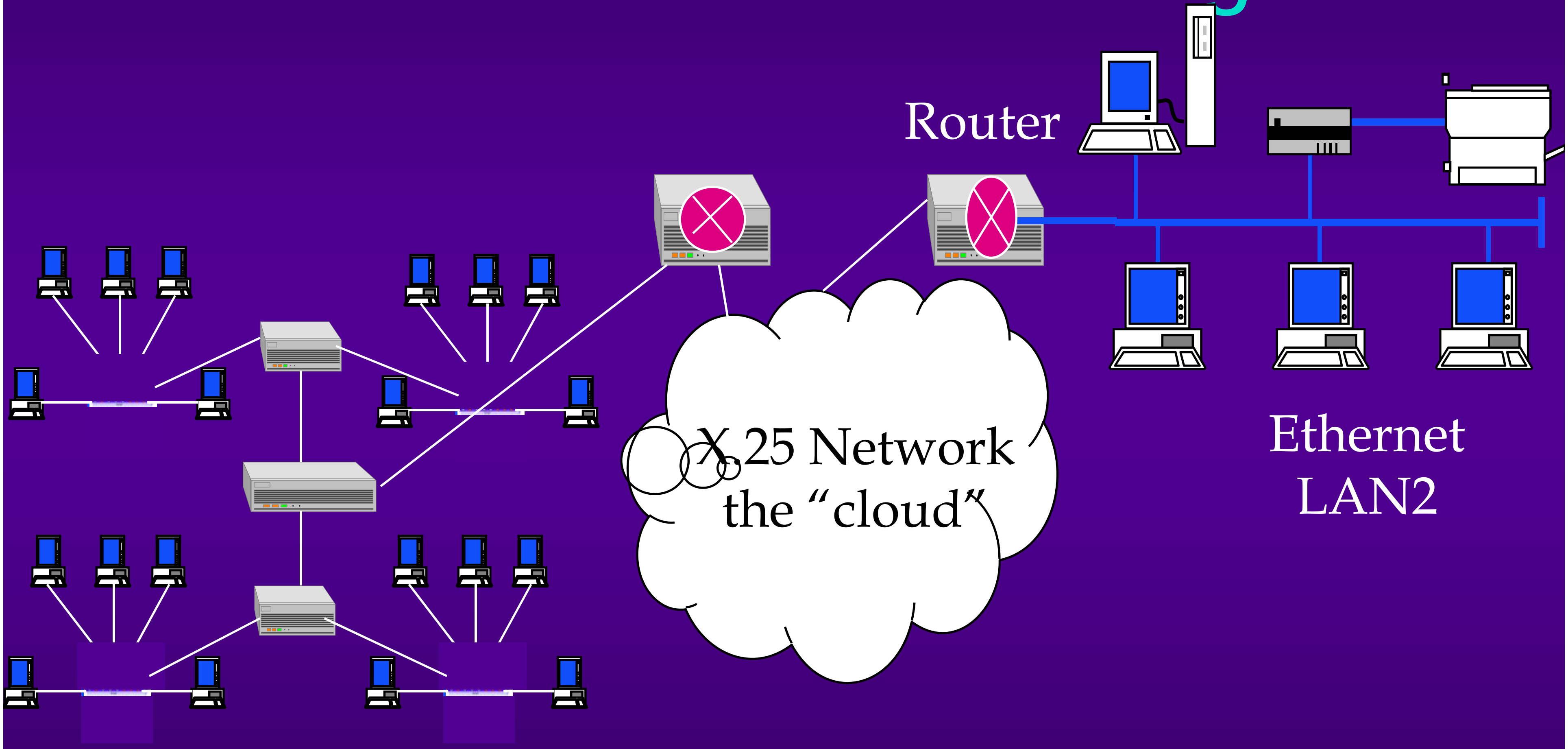
Routers

- choose the best route to send the packet (path)
  - IDs of other networks
  - paths to the networks
  - relative efficiency of the paths

Routers

- The router must deal with network differences:
  - addressing schemes
  - minimum packet size
  - interfaces
  - reliability

Routers Interconnecting



Token Ring
LAN1

Routers

+

- can mix-in-match protocols and convert them
- enable all ports to work at the same time
- can be used as an extra layer of security
- configurable
- high speed

−

- hard to configure and manage
- access lists must be kept current
- high maintenance/high training costs
- very expensive

Brouters

- devices that combine the functions of both bridges and routers
- operate at both the data link and network layers
- same or different data link protocol
- same network protocol
- as fast as bridges for same data link type networks

Gateways

- complex machines that are interfaces between two or more ***dissimilar*** networks
- connect two or more LANs that use the same or different data link layer, network layer, and cable types
- operates at the network layer (3) or higher layers (4-7)
- forwards only those messages that need to go out
- a combination of both hardware and software

Gateways

- translates one network protocol to another
- translates data formats
- translates open sessions between application programs
- translates to mainframes

Gateways

- Exists in four major types:
  - LAN-to-IBM mainframe
  - Network-to-network
  - System-to-network
  - System-to-system

Improving Backbone Performance

- use faster routing protocol
- upgrade computers that perform routing
- use switches from a single vendor
- eliminate need for switch-to-switch routing by use of collapsed backbone switch

Improving Circuit Capacity

How much bandwidth to expect

LAN Type	*Speed*
Ethernet	10 Mbps
Token Ring	16 Mbps
Fast Ethernet	100 Mbps
Faster Ethernet	1 Gbps
Fast Token Ring	100 Mbps
FDDI	100 Mbps
ATM	2.4 Gbps

Selecting a Backbone Network

5 important factors to consider:

- Throughput
- Network cost
- Type of application
- Ease of network management
- Compatibility with current and future technologies

Hypertext

- **Hypertext** is text displayed on a computer or other electronic device with references (hyperlinks) to other text that the reader can immediately access, usually by a mouse click or key press sequence.
- Apart from running text, hypertext may contain tables, images and other presentational devices.
- Hypertext is the underlying concept defining the structure of theWorld Wide Web.
- It is an easy-to-use and flexible format to share information over the Internet.

Types of hypertext

Hypertext documents can either be

1.Static

2.Dynamic

✓Static Hypertext documents(prepared and stored in advance)

Static hypertext can be used to cross-reference collections of data in documents, software applications, or books.

✓dynamic (continually changing in response to user input).

DNS

Hostnames

- IP Addresses are great for computers
  - IP address includes information used for routing.
- IP addresses are tough for humans to remember.
- IP addresses are impossible to guess.
  - ever guessed at the name of a WWW site?

The Domain Name

- A *domain name* is a string used to name Web sites and other servers on computer networks. On the Internet, these strings are managed by the Domain Name System (DNS). The DNS uses a system of multi-level strings separated by dots ('.') to organize domain names. For example, the Web site

compnetworking.about.com

The Domain Name

compnetworking.about.com

uses three levels of naming. The levels are listed in order of lowest to highest when reading from left to right.

- ➢ In this example, the first substring ('compnetworking') represents one specific Web site or *sub-domain*. Then,
- ➢ the second substring ('about') represents a *organizational domain* that points to a Web site but also contains numerous other sub-sites (sub-domains).
- ➢ Finally, the third substring ('.com') represents a *top level domain (TLD)* that encompasses numerous organizations worldwide.

TLDs (*top level domain)*

Common Domain Extensions

.com is the most commonly used top-level domain extension on the Internet. Many others exist, however. These other six TLDs were part of the original Internet specifications for domain extensions:

.edu **.mil**

.net **.gov** **.int**

- In recent years, many new TLDs have been deployed on the Internet. Some of these are intended for broad use worldwide, while others are designed to serve special interest groups.

.biz
.name
jobs

.mobi
.info.
.tel

.

TLDs (*top level domain)*

Country Domain Extensions

Besides the generic TLDs listed above, the Internet also maintains domain extensions for each country to help organize Web sites within each nation. These extensions are named according to worldwide standard two-letter *country codes* similar to those used by the postal system. Examples of country code TLDs include:

.br (Brazil)

.ca (Canada)

.cn (mainland China)

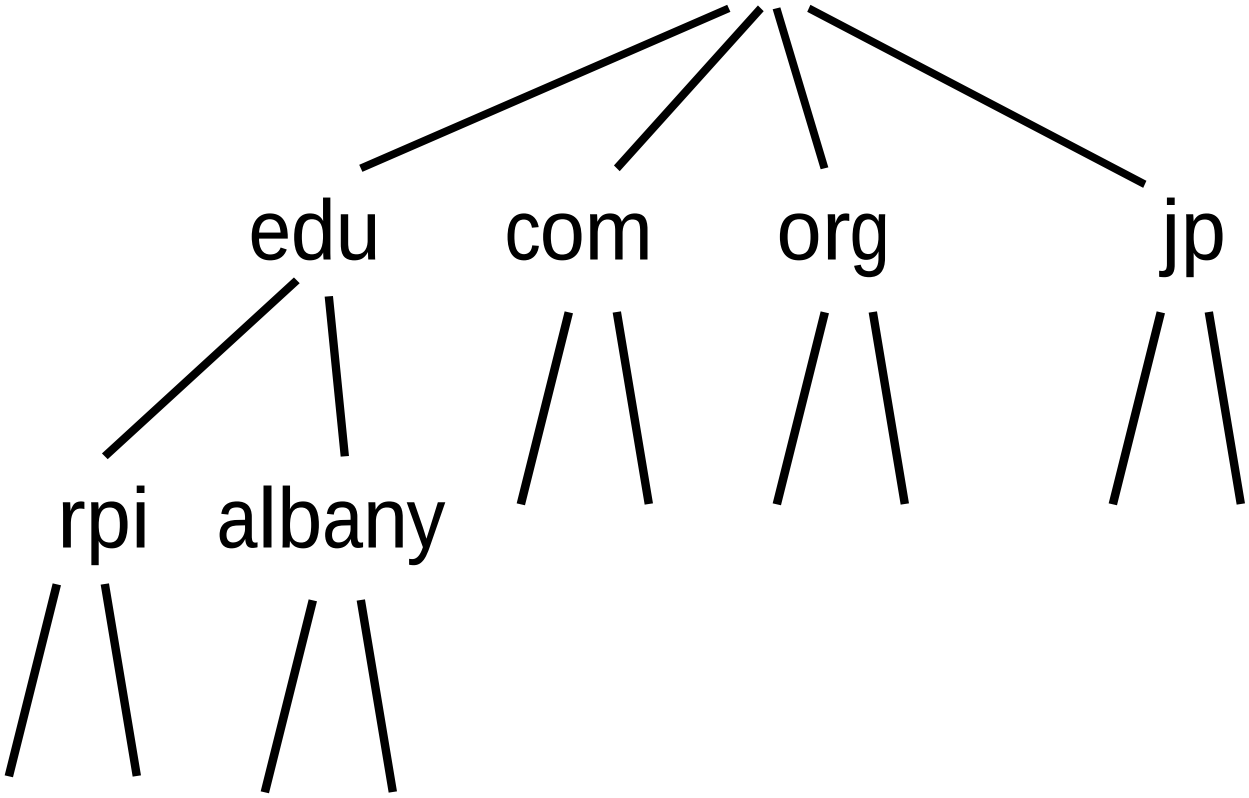
.fr (France)

.in (India)

.jp (Japan)

.ru (Russian Federation)

DNS Hierarchy



What Is a DNS Server?

The Domain Name System (DNS) is a standard technology for managing the names of Web sites and other Internet domains. DNS technology allows you to type names into your Web browser like *compnetworking.about.com* and your computer to automatically find that address on the Internet. A key element of the DNS is a worldwide collection of *DNS servers*.

A DNS server is any computer registered to join the Domain Name System. A DNS server runs special-purpose networking software, features a public IP address, and contains a database of network names and addresses for other Internet hosts.

DNS Root Servers

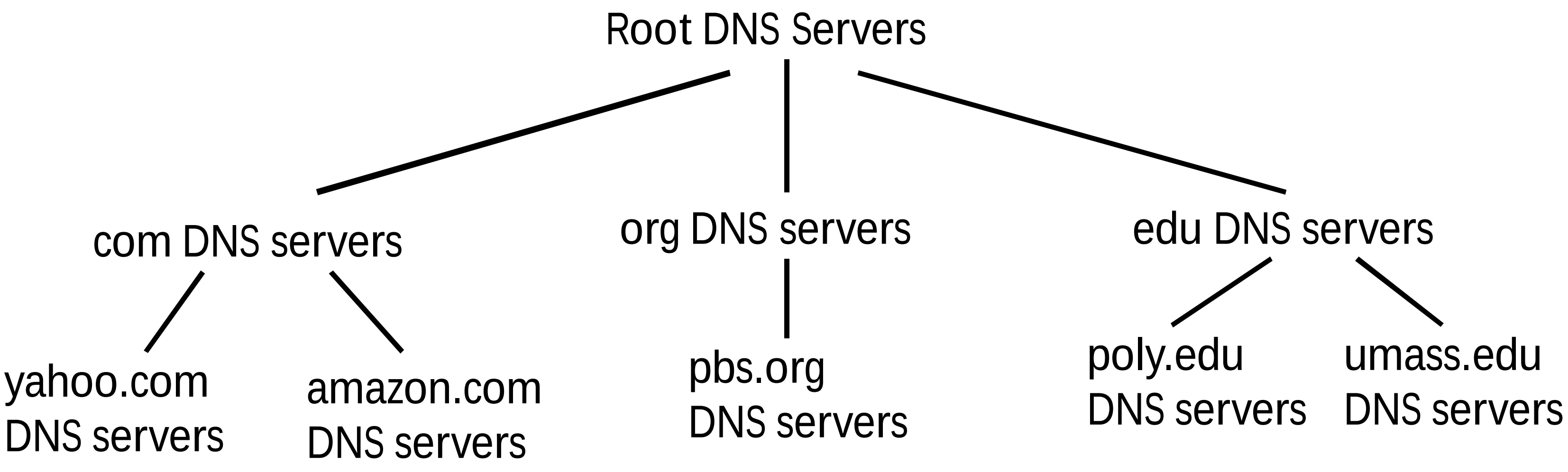
DNS servers communicate with each other using private network protocols. All DNS servers are organized in a hierarchy.

the top level of the hierarchy, so-called *root servers* store the complete database of Internet domain names and their corresponding IP addresses.

The Internet employs 13 root servers that have become somewhat famous for their special role. Maintained by various independent agencies, the servers are aptly named A, B, C and so on up to M.

Ten of these servers reside in the United States, one in Japan, one in London, UK and one in Stockholm, Sweden.

Distributed, Hierarchical Database

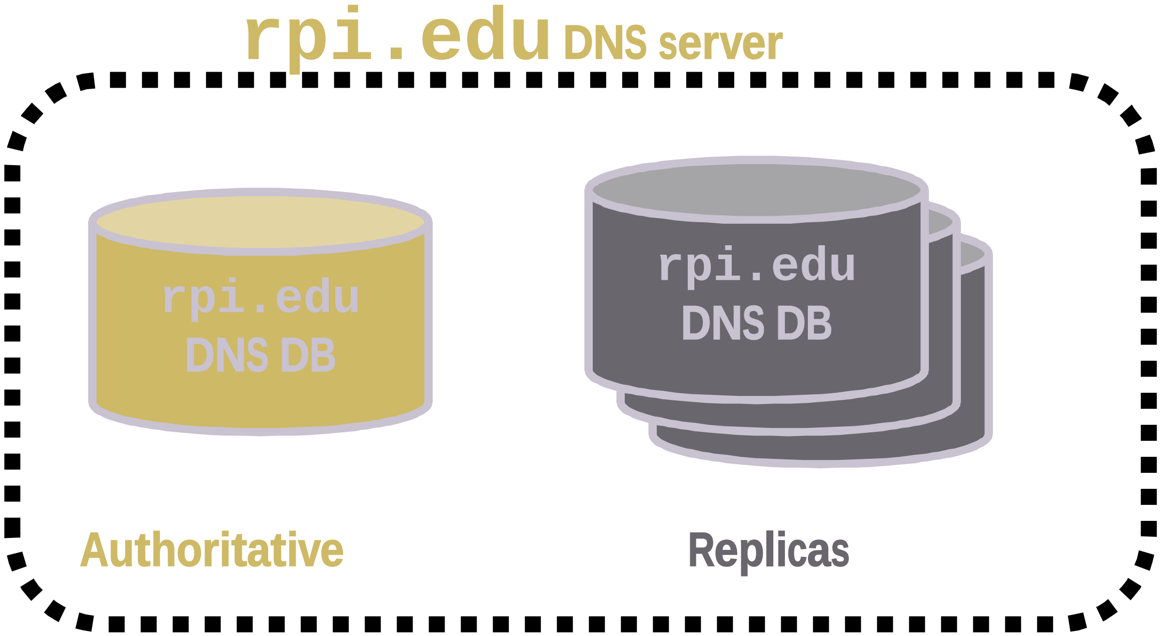


Client wants IP for www.amazon.com; 1st approx:

- client queries a root server to find com DNS server
- client queries com DNS server to get amazon.com DNS server
- client queries amazon.com DNS server to get IP address for www.amazon.com

DNS Distributed Database

- There is one primary server for a domain, and typically a number of secondary servers containing replicated databases.



WHAT IS NETWORK SECURITY?

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations.

An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

Threats to network security include:

Viruses : Computer programs written by programmers and designed to replicate themselves and infect computers when triggered by a specific event

Trojan horse programs : Delivery vehicles for destructive code, which appear to be harmless or useful software programs such as games

Attacks : Including investigation attacks (information-gathering activities to collect data that is later used to compromise networks); access attacks (which exploit network exposures in order to gain entry to e-mail, databases, or the corporate network); and denial-of-service attacks (which prevent access to part or all of a computer system)

Data interception : Involves eavesdropping on communications or altering data packets being transmitted

Social engineering : Obtaining confidential network security information through nontechnical means, such as posing as a technical support person and asking for people's passwords

Network security tools include:

Antivirus software packages : These packages counter most virus threats if regularly updated and correctly maintained.

Secure network infrastructure : Switches and routers have hardware and software features that support secure connectivity, perimeter security, identity services, and security management. Dedicated network security hardware and software-Tools such as firewalls and intrusion detection systems provide protection for all areas of the network and enable secure connections.

Virtual private networks : These networks provide access control and data encryption between two different computers on a network. This allows remote workers to connect to the network without the risk of a hacker or thief intercepting data.

Network security tools include:

Identity services : These services help to identify users and control their activities and transactions on the network. Services include passwords, digital certificates, and digital authentication keys.

Encryption : Encryption ensures that messages cannot be intercepted or read by anyone other than the authorized recipient.

Security management : This is the glue that holds together the other building blocks of a strong security solution.