STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

CS 146: Intro to Web Programming and Project Development

Instructor: Iraklis Tsekourakis

Email: itsekour@stevens.edu

Web fundamentals: Networking

Objectives

- Define a network and reasons for having one
- Identify various network topologies and classify networks by size
- Explain the layers in the OSI reference model

What is a network?

Network Definition

- *A network can be defined as two or more computers connected together in such a way that they can share resources.*

Connection is twofold:

- Physical, through wires, cables, and wireless media
- Logical, through the transport of data across the physical media

Resources

- The purpose of a network is to share resources
- A resource may be:
    - A file
    - A folder
    - A printer
    - A disk drive
    - Or just about anything else that exists on a computer

To be more specific…

- Several basic rules must be followed if the computers are to exchange data with each other:
  - There must be a sender and receiver
  - There must be a message
  - The machines in the network must use the same communications protocols
  - The data must be delivered without corruption
  - A method must be in place to acknowledge uncorrupted data and inform the sender when errors occur
  - Computers on a network must be capable of determining the origin and destination of a piece of information
    - Standardized addresses for all computers on the network
    - Means of identifying and verifying devices on the network

Why build a network?

- Enables faster communication between parties
- By sharing electronic data among perhaps thousands of people, a computer network encourages (*requires*) the use of standard policies and procedures
- Networks provide backup and recovery support for our data
- Easy to store copies of our data
- Shared resources lead to less expensive communications

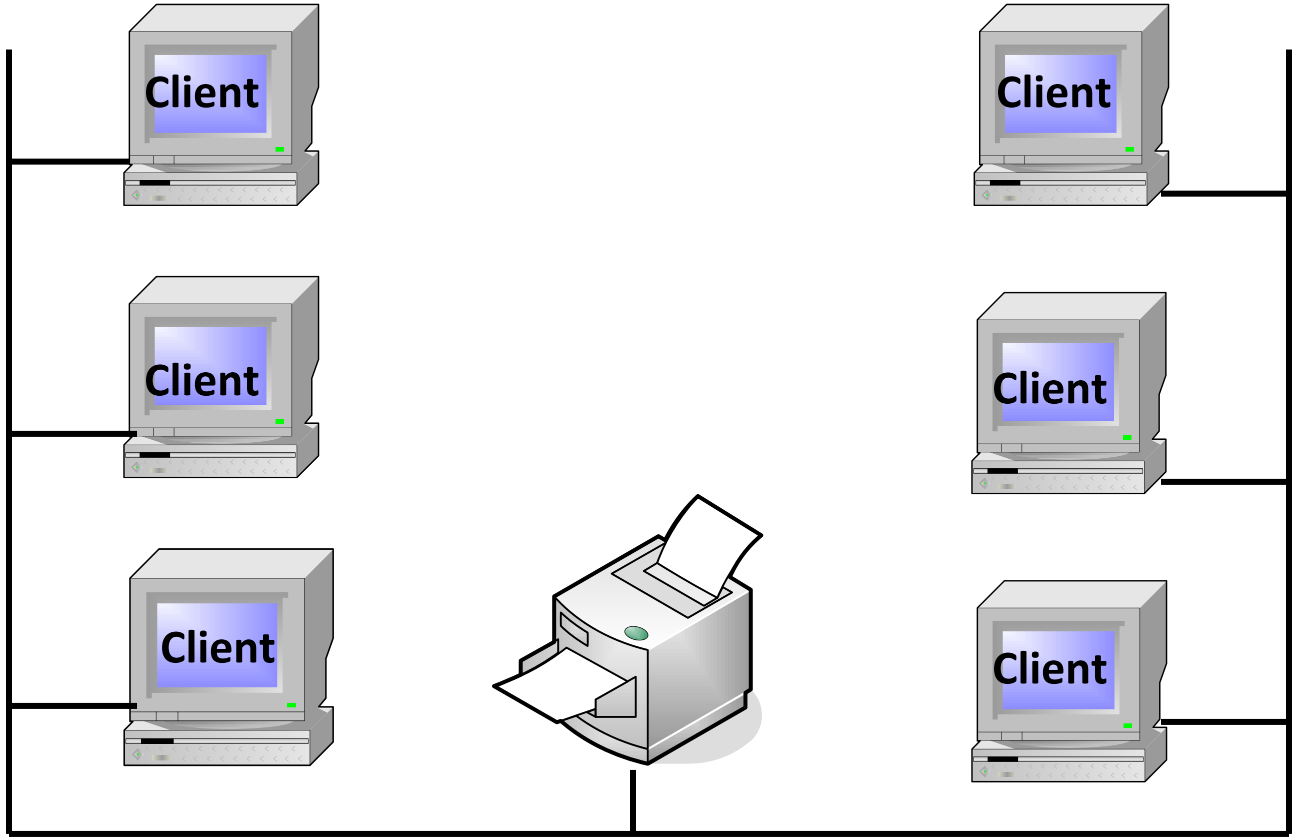
Disadvantages of networks

- Network Hardware, Software and Setup Costs
- Hardware and Software Management and Administration Costs
- Undesirable Sharing
- Illegal or Undesirable Behavior
- Data Security Concerns

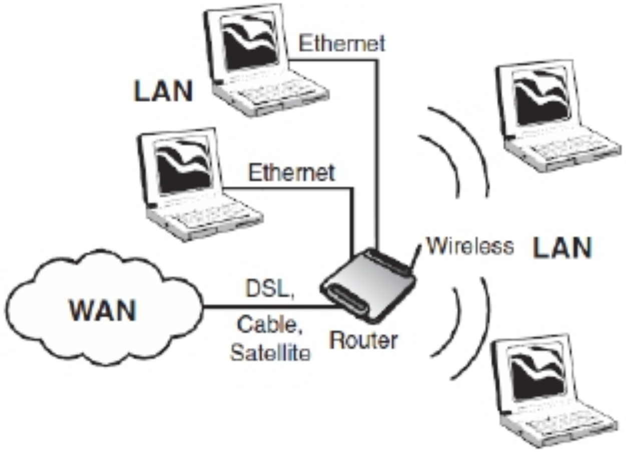
Types of networks

- **Local Area Network (LAN)** is a computer network covering a small geographic area, like a home, office, or group of buildings
- **Wide Area Network** (**WAN**) is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries)
  - The largest and most well-known example of a WAN is the Internet
  - WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations
- **Metropolitan Area Network (MAN)** is a network that interconnects users in a geographic area or region larger than LAN but smaller than WAN.
  - The term is applied to the interconnection of networks in a city into a single larger network

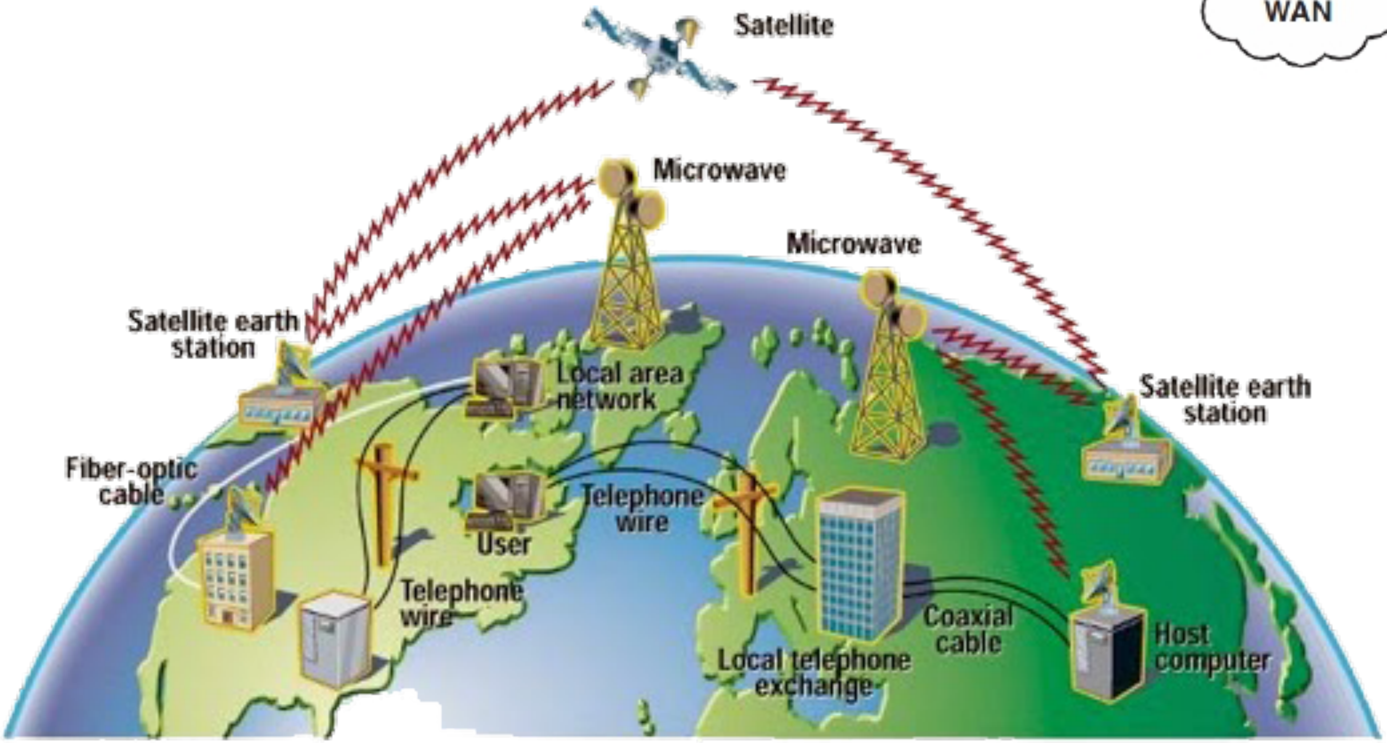
LAN



WAN

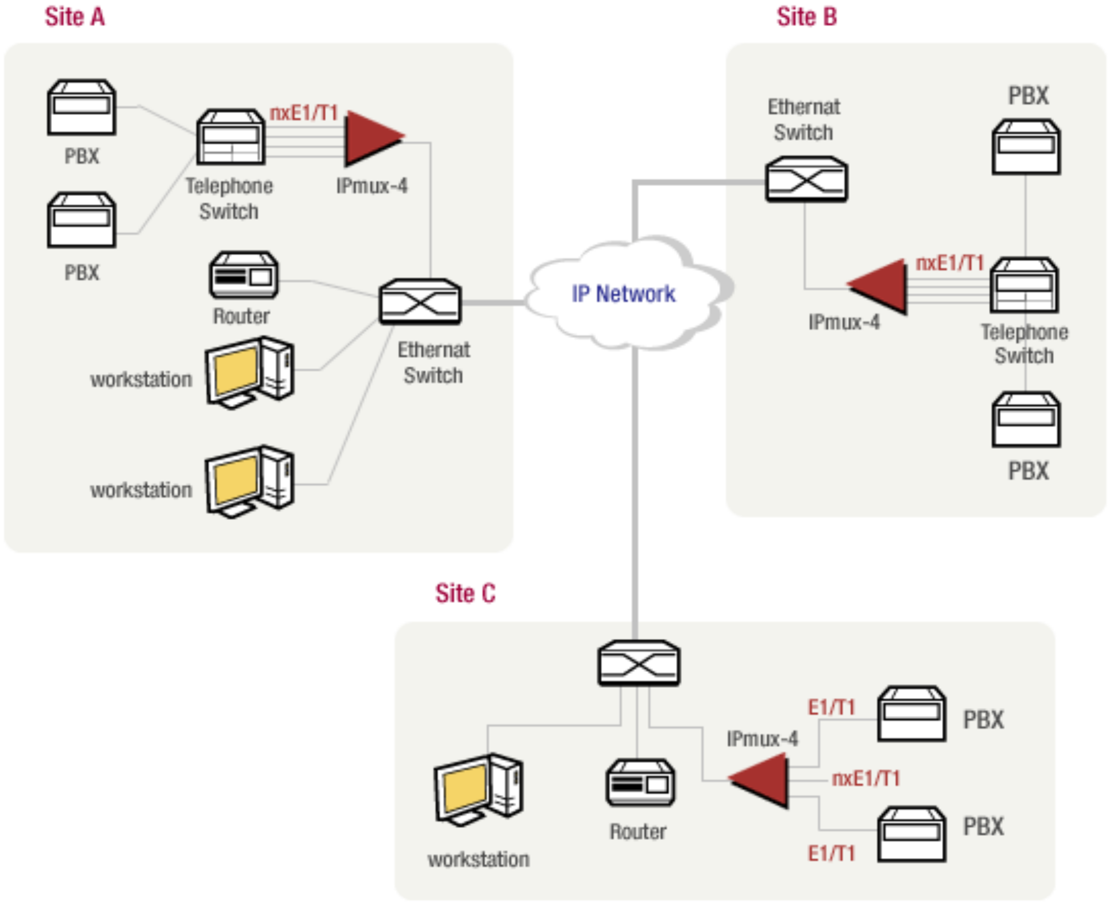


Ethernet
LAN
Ethernet
Wireless
LAN
WAN
DSL,
Cable,
Satellite
Router

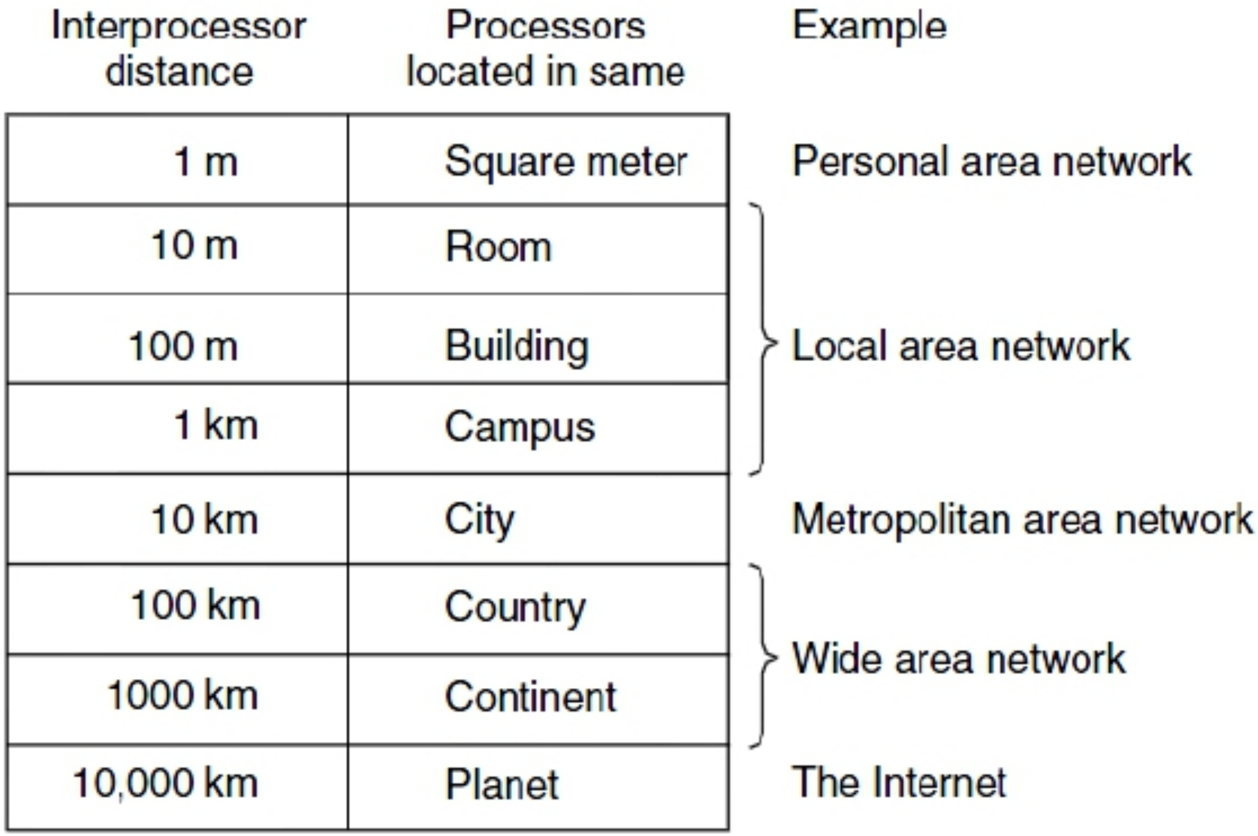


Satellite
Microwave
Microwave
Satellite earth station
Local area network
Satellite earth station
Fiber-optic cable
Telephone wire
User
Telephone wire
Coaxial cable
Host computer
Local telephone exchange

MAN


Site A
PBX
PBX
Telephone Switch
nxE1/T1
IPmux-4
Router
Ethernat Switch
workstation
workstation
IP Network
Site B
Ethernat Switch
PBX
nxE1/T1
IPmux-4
Telephone Switch
PBX
Site C
workstation
Router
IPmux-4
E1/T1
nxE1/T1
E1/T1
PBX
PBX

Network classification



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

Intranet VS Internet

- ***Intranet:*** is a private network that is contained within an enterprise
  - It may consist of many interlinked local area networks and also use leased lines in the wide area network
- ***Internet:*** is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers)

Hardware and Network Peripherals

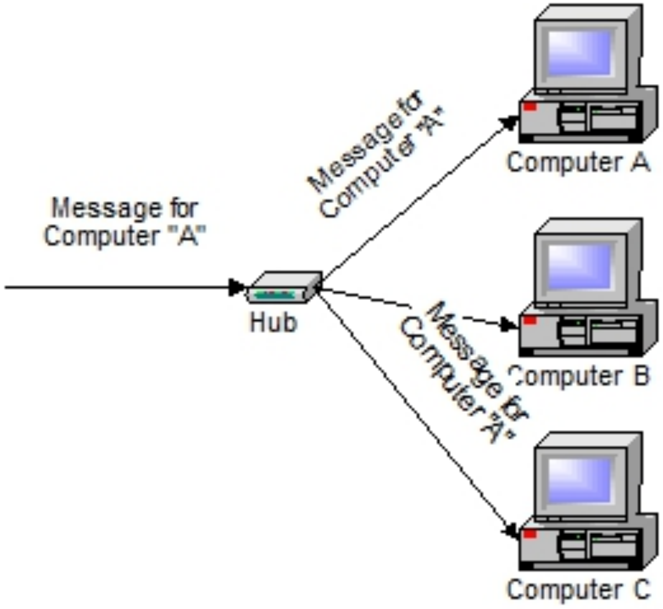
- Network Interface Card (NIC)
- Hub
- Bridge
- Switch
- Router

NIC

- provides the physical interface between computer and cabling
  - prepares data, sends data, and controls the flow of data
  - It can also receive and translate data into bytes for the CPU to understand
- The following factors should be taken into consideration when choosing a NIC:
  - Preparing data
  - Sending and controlling data
  - Configuration
  - Drivers
  - Compatibility
  - Performance

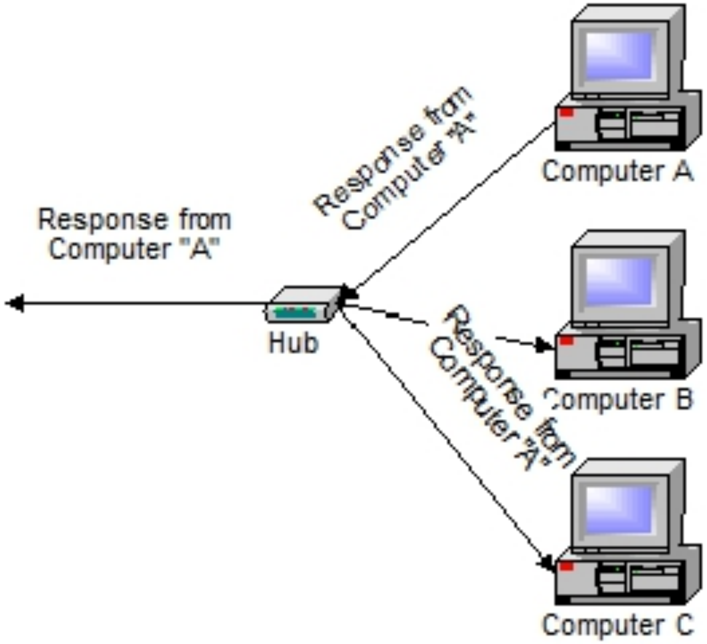
Hub

- A **hub** is typically the least expensive, least intelligent, and least complicated of network devices. Its job is very simple – anything that comes in one port is sent out to the others
- If a message comes in for computer “A”, that message is sent out all the other ports, regardless of which one computer “A” is on



Hub

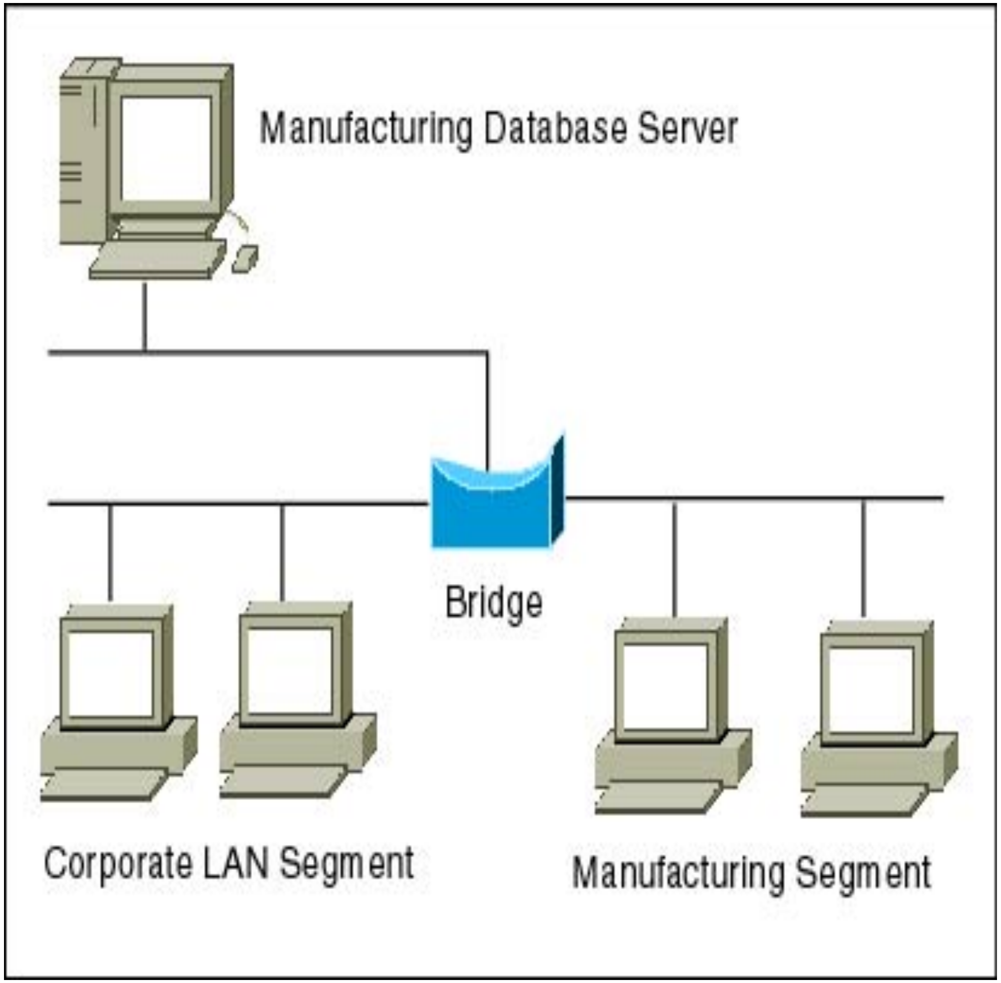
- And when computer “A” responds, its response also goes out to every other port on the hub
- Every computer connected to the hub “sees” everything that every other computer on the hub sees
- The computers themselves decide if they are the targeted recipient of the message and when a message should be paid attention to or not


Response from Computer "A"
Response from Computer "A"
Computer A
Hub
Response from Computer "A"
Computer B
Computer C

Bridge

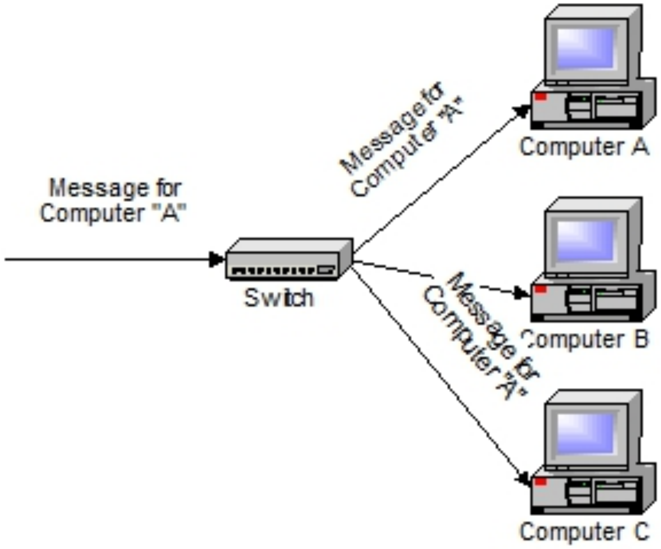
- joins multiple similar topologies segments, and divides network segments
- For example, with 200 people on one Ethernet segment, the performance will be mediocre, because of the design of Ethernet and the number of workstations that are fighting to transmit. If you divide the segment into two segments of 100 workstations each, the traffic will be much lower on either side and performance will increase.

Bridge


Manufacturing Database Server
Bridge
Corporate LAN Segment
Manufacturing Segment

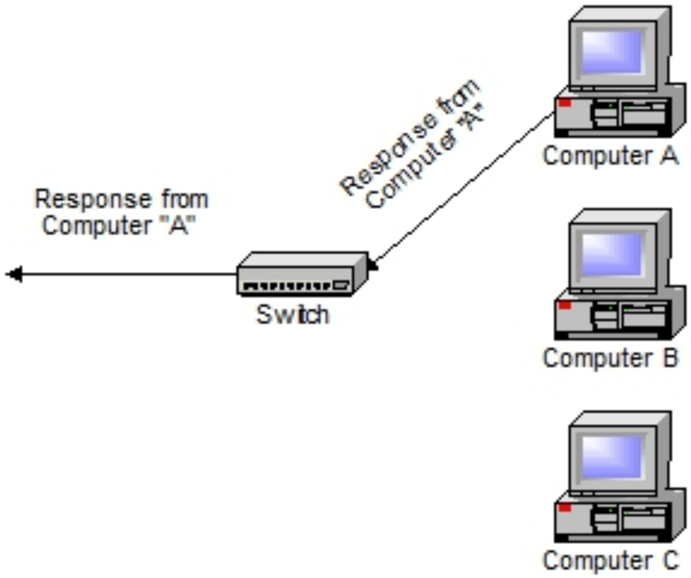
Switch

- A **switch** does essentially what a hub does, but more efficiently
- By paying attention to the traffic that comes across it, it can “learn” where particular addresses are
- Initially, a switch knows nothing and simply sends on incoming messages to all ports



Switch

- Even by accepting that first message, however, the switch has learned something
- It knows on which connection the sender of the message is located
- Thus, when machine "A" responds to the message, the switches only need to send that message out to the one connection

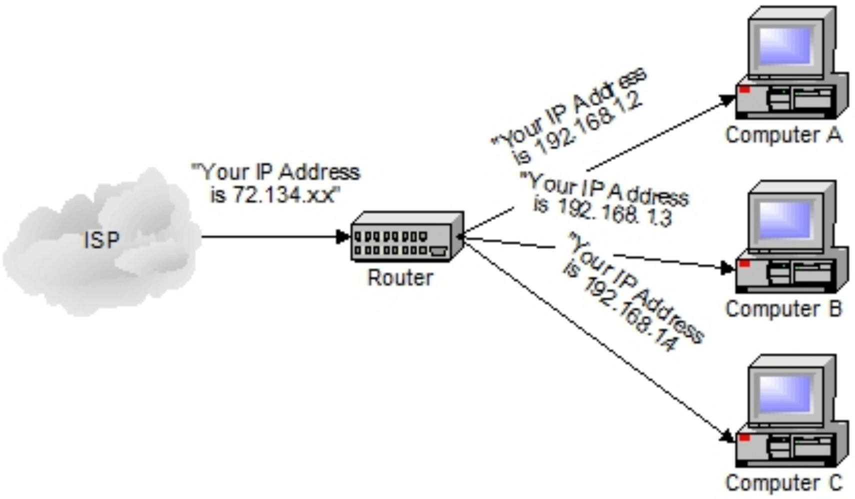


Router

- A **router** is the smartest and most complicated of the bunch
- A router is essentially a piece of networking hardware with two built-in network addresses, one for the LAN and one for the WAN. The purpose is to allow messages to be sent from one network to another
- Routers come in all shapes and sizes – from the small, four-port broadband routers that are very popular right now to the large industrial strength devices that drive the internet itself
- As far as simple traffic routing is concerned, a router operates exactly as a switch

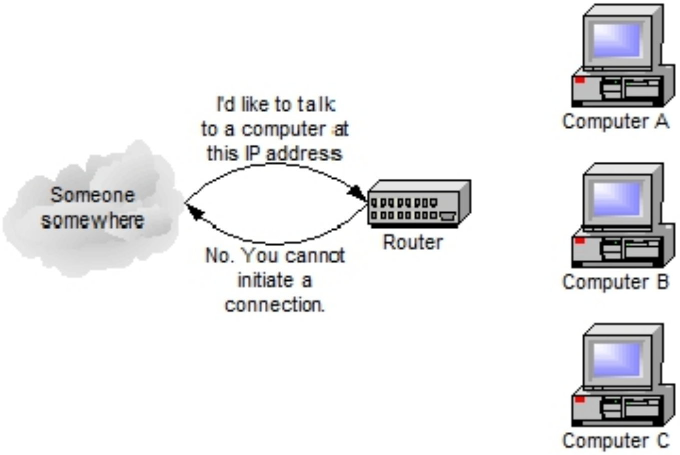
What Else Can a Router Do?

- **DHCP**: Dynamic Host Configuration Protocol
  - the way dynamic IP addresses are assigned
  - router asks ISP server for an IP address
  - local computers ask the router for an IP address


ISP
"Your IP Address is 72.134.xx"
Router
"Your IP Address is 192.168.12
"Your IP Address is 192.168.1.3
"Your IP Address is 192.168.14
Computer A
Computer B
Computer C

What Else Can a Router Do?

- **NAT** – Network Address Translation – is the way that the router *translates* the IP addresses of packets that cross the internet/local network boundary
- When the router passes packets to and from the internet, it replaces the local IP address with the internet IP address assigned by the ISP, and vice-versa
- A side effect of NAT is that machines on the internet can not initiate communications to local machines – they can only respond to communications initiated by those local machines
- The net effect is that the router then also acts as a firewall

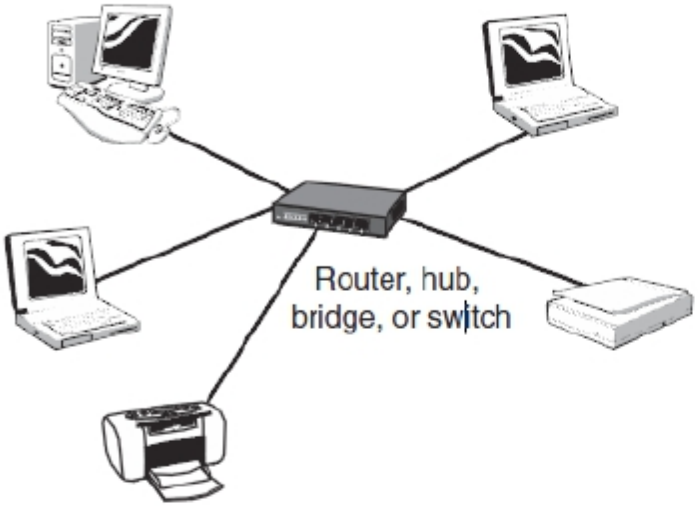

I'd like to talk to a computer at this IP address
Someone somewhere
No. You cannot initiate a connection.
Router
Computer A
Computer B
Computer C

Network Topology

- A *topology* is a way of “laying out” the network
  - Star
  - Ring
  - Bus
  - Cellular

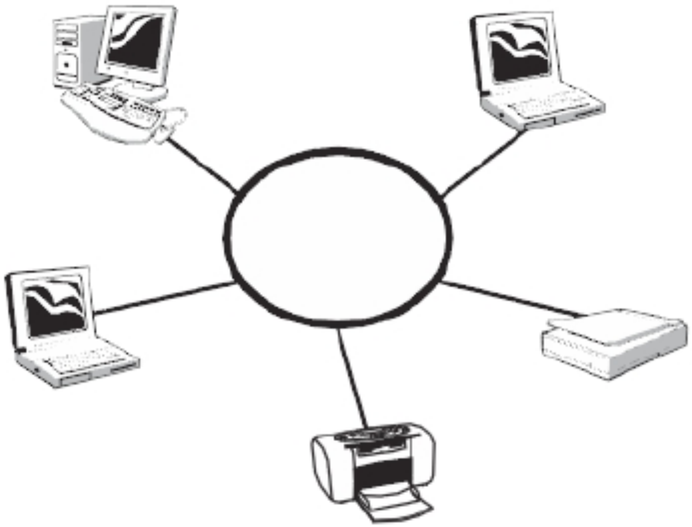
Star Topology

- **Star**—The *star* topology employs a central connection point, called a *router, hub, bridge*, or *switch*
- The computers on the network radiate out from this point



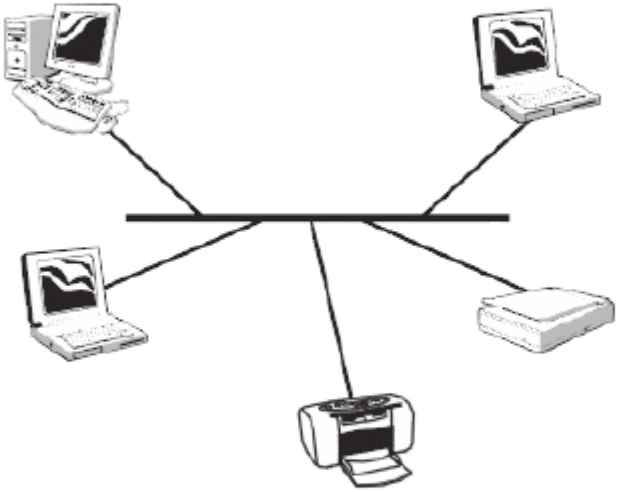
Ring Topology

- The *ring* topology connects the computers through a wire or cable
- Data packet travels around the ring
- Each computer examines the destination address
- If the computer sees its address, it copies the data
- Otherwise it passes it along
- When it reaches the source again, the packet is discarded



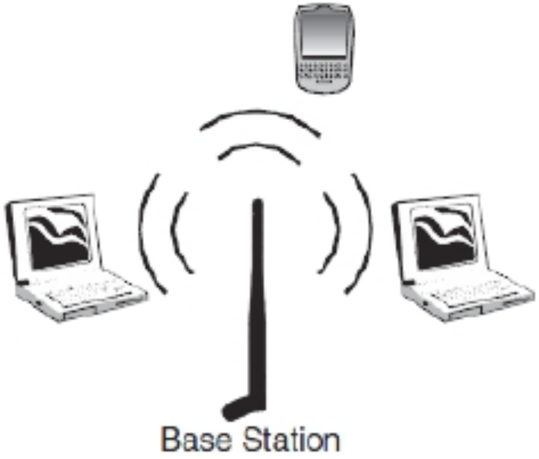
Bus Topology

- Consists of a wire with taps along its length to which computers connect
- It is also a broadcast network because all nodes receive the traffic
- Sending node transmits the packet in both directions
- Receiving node copies the packet if the destination address matches its address
- Packets terminates at the ends of the bus
- Must have a collision detection procedure



Cellular Topology

- Cellular networks use broadcast protocols
- All nodes are capable of receiving transmissions on a control channel from a central site
- A wireless control node (called the base station) uses this common channel to direct a node to lock onto a specific (user) channel for its connection

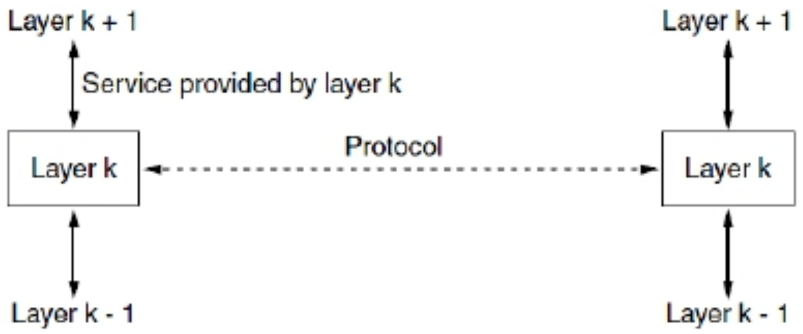


What Is a Protocol

- An agreement between the communicating parties on how communication is to proceed
- Similar to a chosen language when humans speak
- Different protocols are built with different situations in mind
- On the Internet we commonly use TCP/IP along with a variety of protocols like HTTP, FTP, SMTP, POP, etc.

Services & Protocols

- A *service* is a set of primitives (operations) that a layer provides to the layer above it
- A *protocol*, in contrast, is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer
- Entities use protocols to implement their service definitions



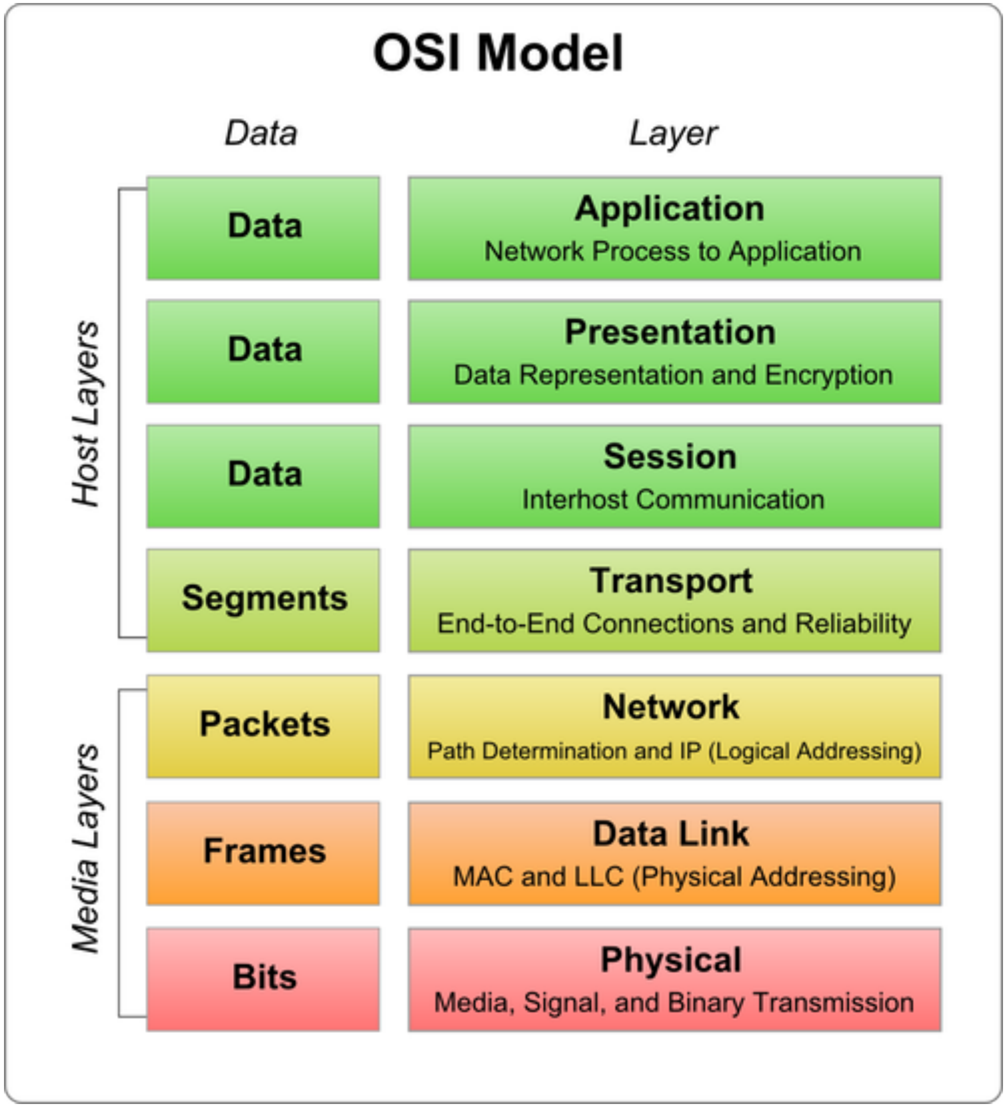
OSI Reference Model

- Based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983)
- It was revised in 1995 (Day, 1995)
- Called **OSI** (**Open Systems Interconnection**) Reference Model because it deals with connecting open systems

Principles of OSI Model

- The OSI model has seven layers
- The principles that were applied to arrive at the seven layers can be briefly summarized as follows:
  - A layer should be created where a 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

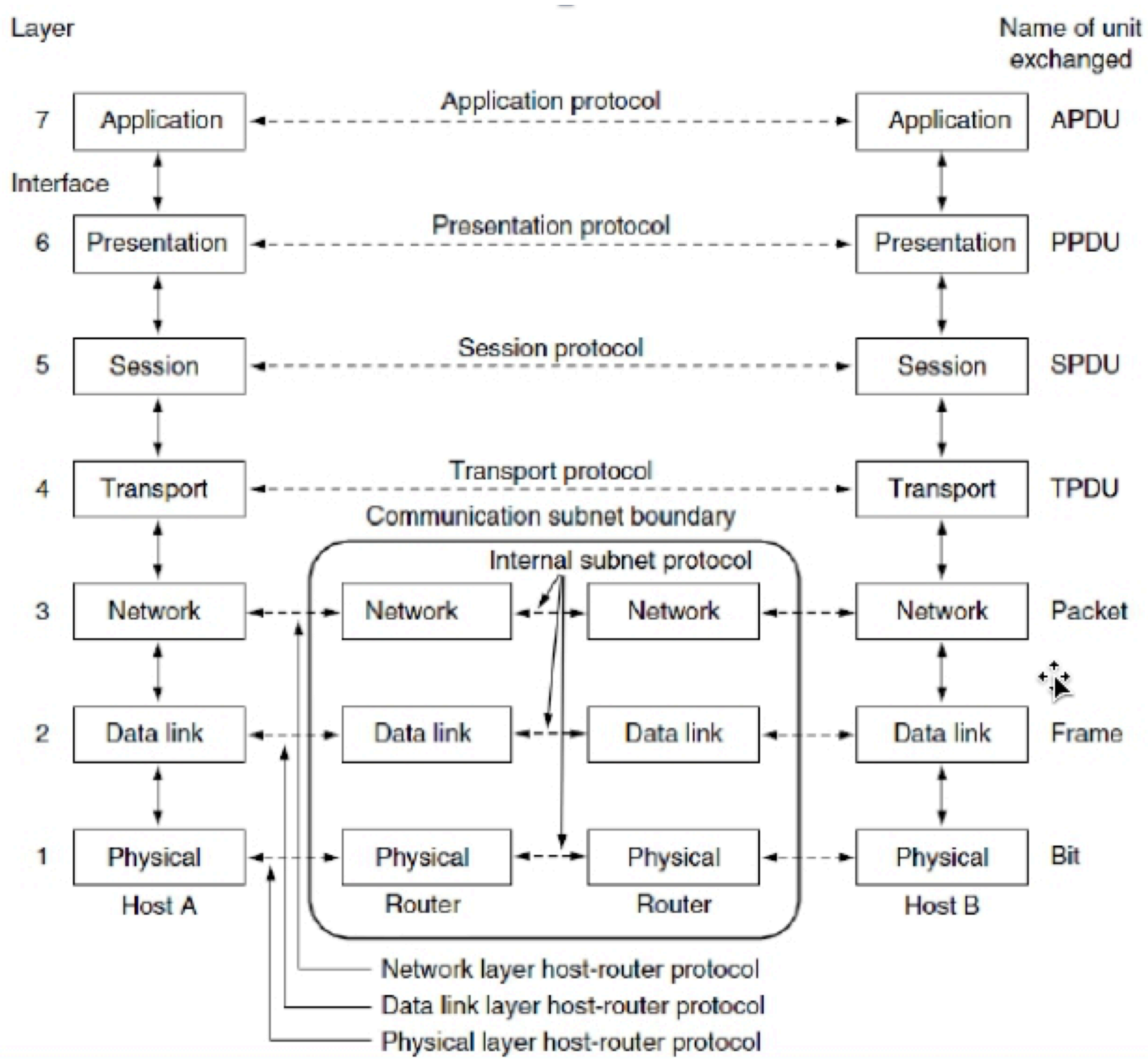
OSI Layers



OSI Model

	Data	*Layer*
Host Layers	**Data**	**Application** Network Process to Application
	Data	**Presentation** Data Representation and Encryption
	Data	**Session** Interhost Communication
	Segments	**Transport** End-to-End Connections and Reliability
Media Layers	**Packets**	**Network** Path Determination and IP (Logical Addressing)
	Frames	**Data Link** MAC and LLC (Physical Addressing)
	Bits	**Physical** Media, Signal, and Binary Transmission

OSI Layers II



Physical Layer (1)

- Concerned with transmitting raw bits over a communication channel.
- Typical questions here are
  - what electrical signals should be used to represent a 1 and a 0,
  - how many nanoseconds a bit lasts,
  - whether transmission may proceed simultaneously in both directions

Data Link Layer (2)

- Main task is to transform a raw transmission facility into a line that appears free of undetected transmission errors.
- Has the sender break up the input data into **data frames** (typically a few hundred or a few thousand bytes) and transmit the frames sequentially.
- Keeps a fast transmitter from drowning a slow receiver in data via some traffic regulation mechanism.
- Broadcast networks have an additional issue in the data link layer: how to control access to the shared channel ◊ Done by **medium access control (MAC)** sublayer.

Network Layer (3)

- A key design issue is determining how packets are routed from source to destination.
- Handling congestion is also a responsibility of the network layer, in conjunction with higher layers that adapt the load.
- The quality of service provided (delay, transit time, jitter, etc.) is also a network layer issue.

Transport Layer (4)

- Accepts data from above it, splits it up into smaller units if need be, passes these to the network layer, and ensures that the pieces all arrive correctly at the other end.
- Determines what type of service to provide to the session layer, and, ultimately, to the users of the network.
- Is a true end-to-end layer; it carries data all the way from the source to the destination.

Session Layer (5)

- Allows users on different machines to establish **sessions** between them.
- Sessions offer various services, including
  - **dialog control** (keeping track of whose turn it is to transmit)
  - **token management** (preventing two parties from attempting the same critical operation simultaneously)
  - **synchronization** (checkpointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery)

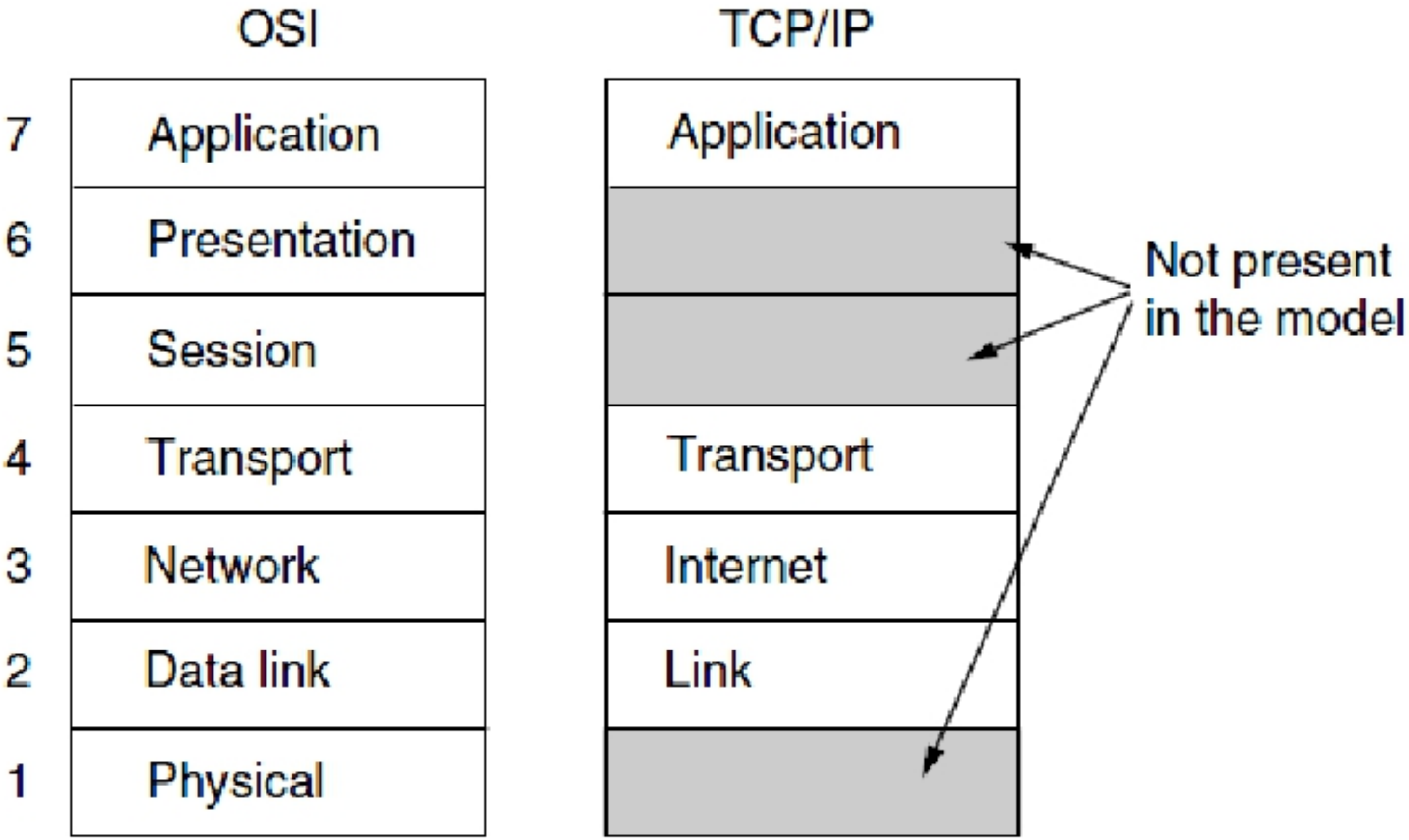
Presentation Layer (6)

- Is concerned with the syntax and semantics of the information transmitted.
- **Translation:** Networks can connect very different types of computers together. These systems have many distinct characteristics and represent data in different ways; they may use different character sets for example. The presentation layer handles the job of hiding these differences between machines.
- **Compression:** Compression (and decompression) may be done at the presentation layer to improve the throughput of data. (There are some who believe this is not, strictly speaking, a function of the presentation layer.)
- **Encryption:** Some types of encryption (and decryption) are performed at the presentation layer. This ensures the security of the data as it travels down the protocol stack.
  - Secure Sockets Layer (SSL) protocol.

Application Layer (7)

- As the "top of the stack" layer, the application layer is the only one that does not provide any services to the layer above it in the stack.
- Provides services to programs that want to use the network, and to you, the user.
- Implement the functions that are needed by users and issues the appropriate commands to make use of the services provided by the lower layers.
- Some of the most popular ones include HTTP, DNS, FTP, SMTP, DHCP, NFS, Telnet, SNMP, POP3, NNTP, and IRC.
  - Lots of alphabet soup!

OSI vs TCP/IP



	OSI	TCP/IP
7	Application	Application
6	Presentation	
5	Session	
4	Transport	Transport
3	Network	Internet
2	Data link	Link
1	Physical	

Not present in the model