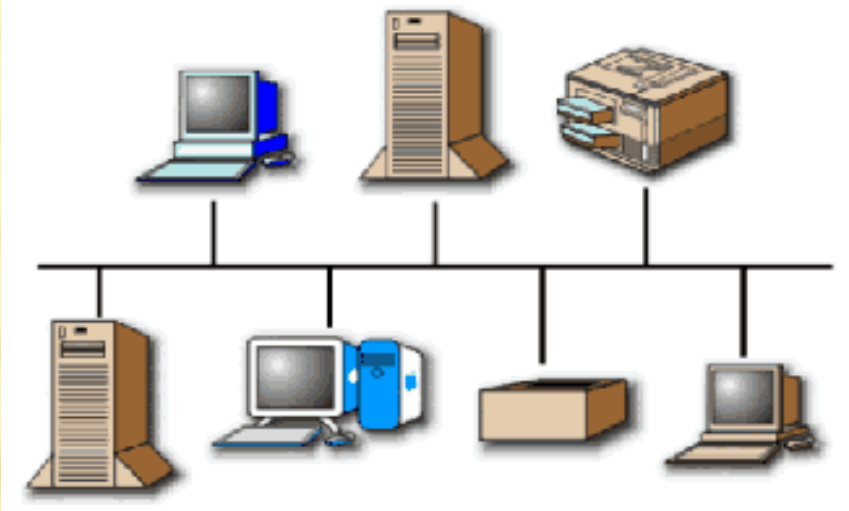
BASICS OF NETWORKING

What is a Computer Network?

A network is a collection of computers, printers, routers, switches, and other devices that are able to communicate with each other over some transmission media.



Types of Networks

There are two basic types of networks currently in existence:

A *Local Area Network* (LAN)

A *Wide Area Network* (WAN)

Local Area Networks (LAN)

A *Local Area Network* (LAN) is a group of computers and network communication devices within a limited geographic area, such as an office building. No third party involvement here. They are characterized by the following:

- High data transfer speeds
- Generally less expensive technologies
- Limited geographic area

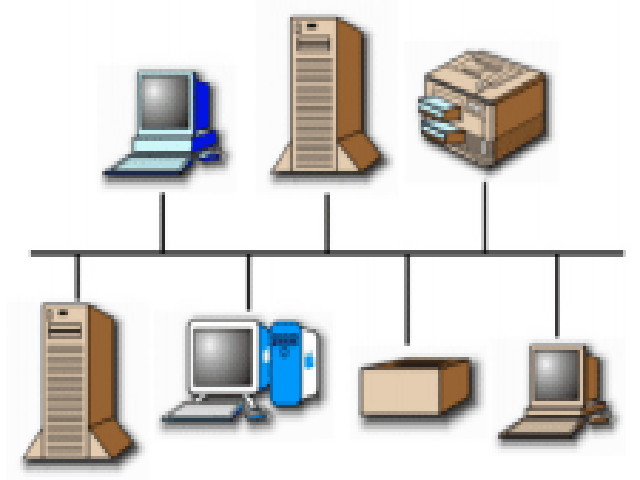
Wide Area Networks (WAN)

A *Wide Area Network* (WAN) interconnects LANs. It is not restricted to a particular geographic area and may be interconnected around the world. Third party network is involved. They are characterized by the following:

- Multiple interconnected LANs
- Generally more expensive technology
- More sophisticated to implement than LANs
- Exist in an unlimited geographic area
- Less error resistance due to transmission travel distances

Common LAN Topologies

Bus Architecture

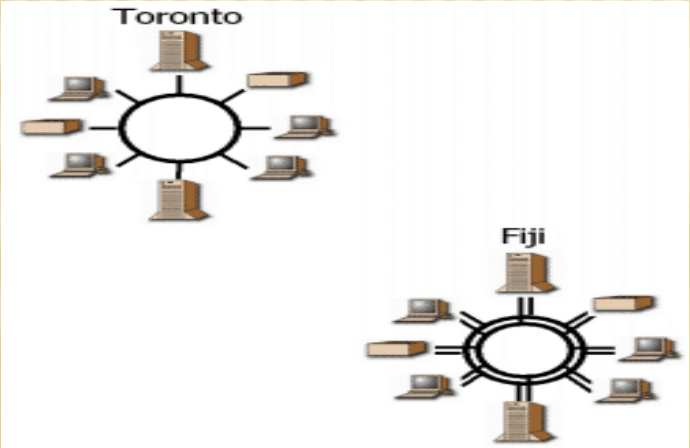


In a bus topology:

- a single cable connects each workstation in a linear, daisy-chained fashion.

- signals are broadcasted to all stations, but stations only act on the frames addressed to them.

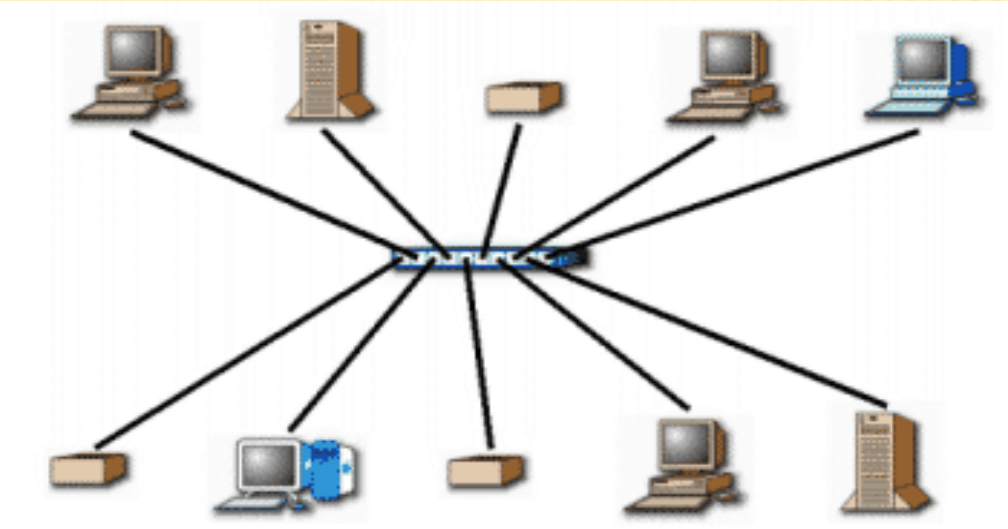
Ring Architecture



- In a ring topology:

- Unidirectional links connect the transmit side of one device to the receive side of another device.
- Devices transmit frames to the next device (downstream member) in the ring.

Star Topology



In a star topology, each station is connected to a central hub or concentrator that functions as a multi-port repeater. Each station broadcasts to all of the devices connected to the hub. Physical LAN topologies are usually characterized as either bus or ring.

LAN Transmission Methods

LAN transmission methods fall into 3 main categories:

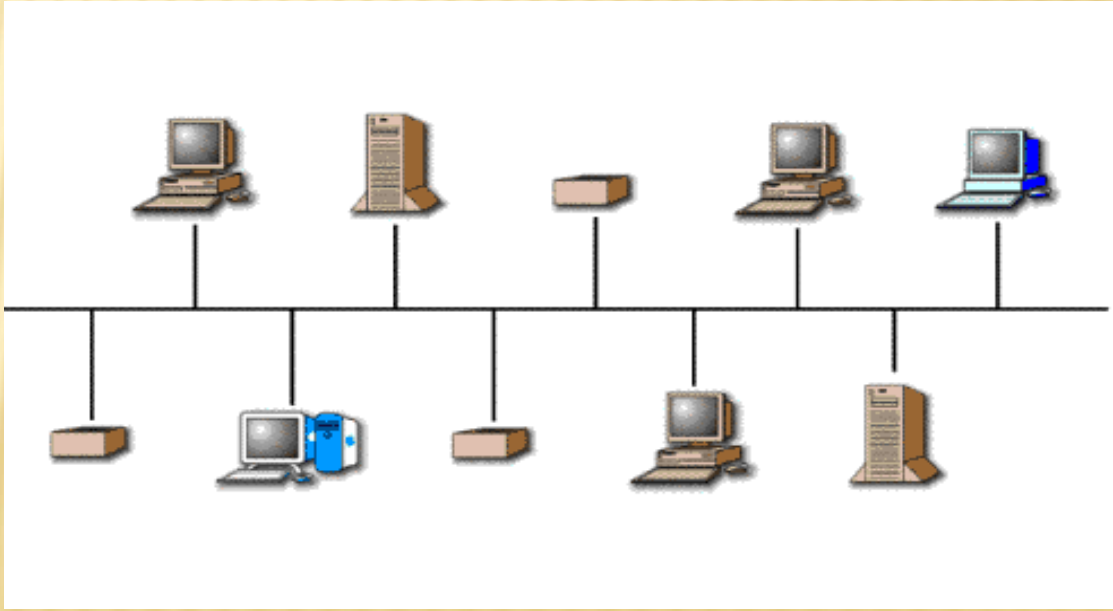
- **Unicast transmission**
- **Multicast transmission**
- **Broadcast transmission**

Unicast Transmission

In unicast transmissions, a single data packet is sent from a source to a single destination on the network.

Unicast Process

- The source addresses the packet with the destination address.
- The packet is sent into the network.
- The network delivers the packet to the destination.

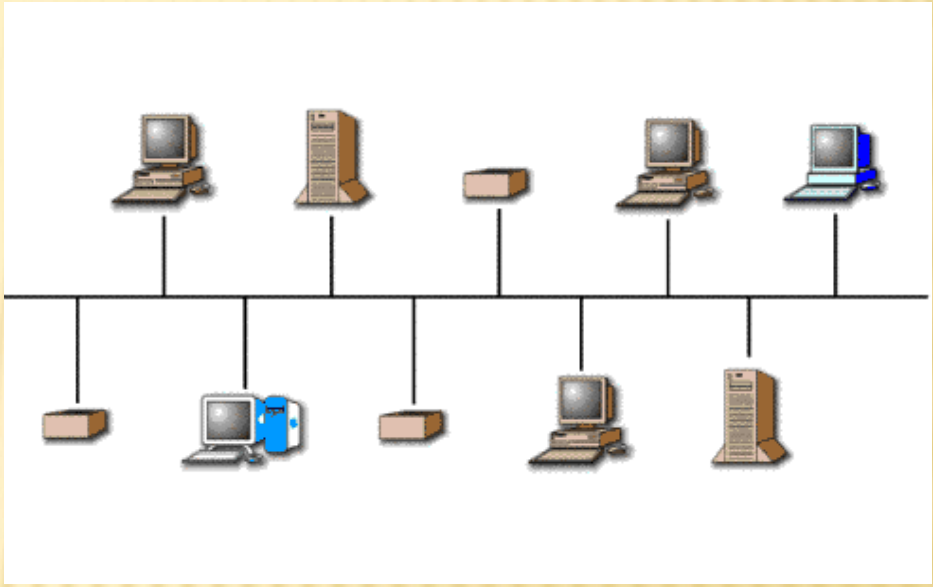


Multicast Transmission

In multicast transmissions, a single data packet is copied and sent to specific destinations on the network

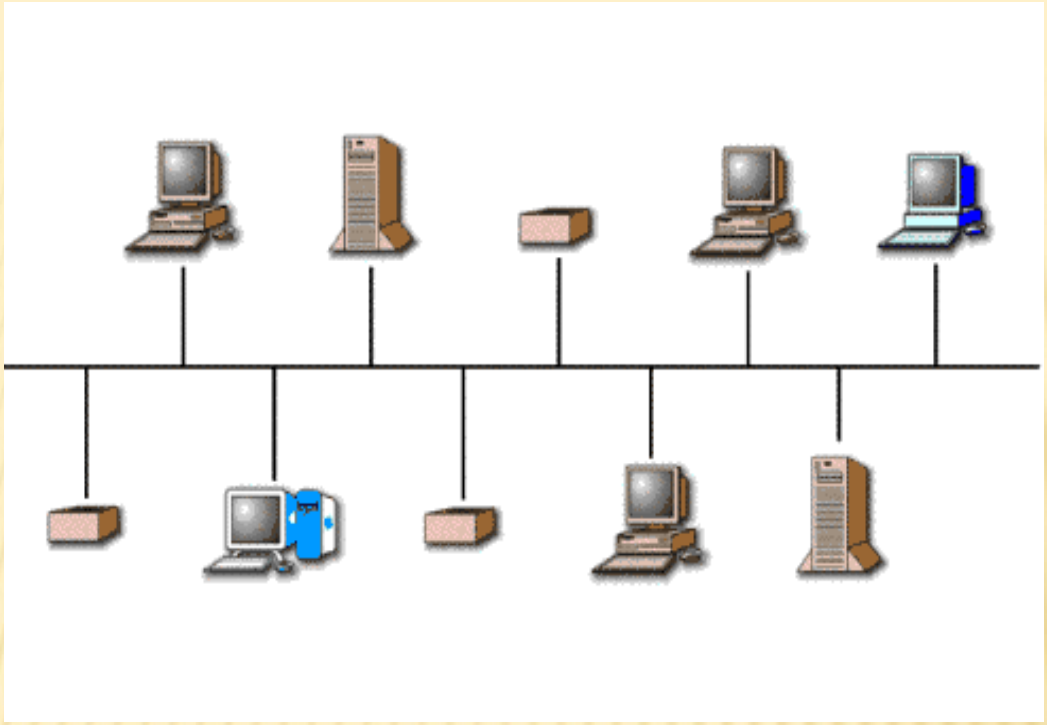
Multicast Process

- The source addresses the packet using a multicast address.
- The packet is sent into the network.
- The network copies the packet.
- A copy is delivered to each destination that is included in the multicast address.



Broadcast Tranmission

In Broadcast transmissions, a single data packet is copied and sent to all the devices in the network



Broadcast Process

- The source addresses the packet with the broadcast address.
- The packet is sent into the network.
- The network copies the packet.
- The packet copies are delivered to all destinations on the network.

LAN Infrastructure Devices

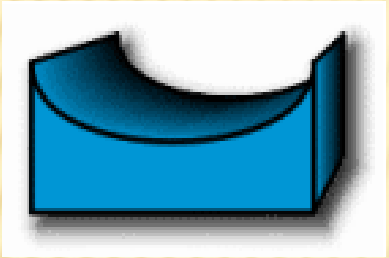
There are numerous devices associated with data information flow across a LAN. When adjoined, they create the infrastructure of a functional LAN. These devices include:

- **Repeaters**
- **Bridges**
- **Hubs**
- **Switches**
- **Routers**

Repeaters

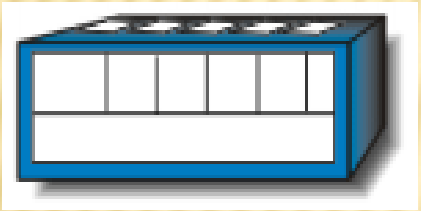
Repeaters, located within the physical layer of a network, regenerate and propagate signals from one to another. They do not change any information being transmitted, and they cannot filter any information. Repeaters help to extend the distances of networks by boosting weak signals.

Bridges



Bridges are intelligent repeaters. They regenerate transmitted signals, but unlike repeaters, they can also determine destinations.

Hubs



Hubs connect all computer LAN connections into one device. They are nothing more than multiport repeaters. Hubs cannot determine destinations; they merely transmit to every line attached in a half-duplex mode.

Routers

Routers are a step up from bridges. They are able to route and filter information to different networks. Some routers can automatically detect problems and redirect information around the problem area. These are called "intelligent routers."

Switches

Switches connect all computer LAN connections, the same as hubs do. The difference is that switches can run in full-duplex mode and are able to direct and filter information to and from specific destinations.

WAN

WAN Infrastructure

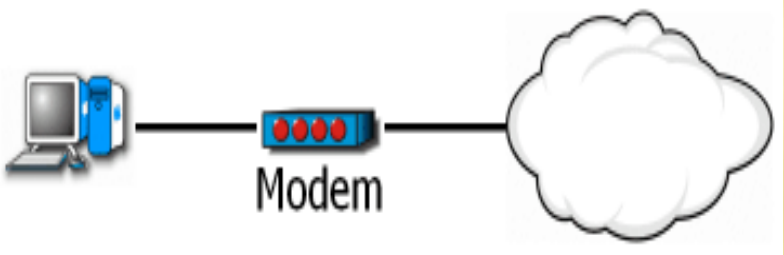
As with LANs, there are numerous devices associated with data information flow across a WAN. Together, these devices create the infrastructure of a functional WAN. These devices include:

- **Router**
- **ATM Switch**
- **Modem and CSU/DSU**
- **Communication Server**
- **Multiplexer**
- **X.25/Frame Relay Switches**

ATM Switches

ATM Switches provide high-speed transfer between both LANs and WANs.

Modem (modulator / demodulator)



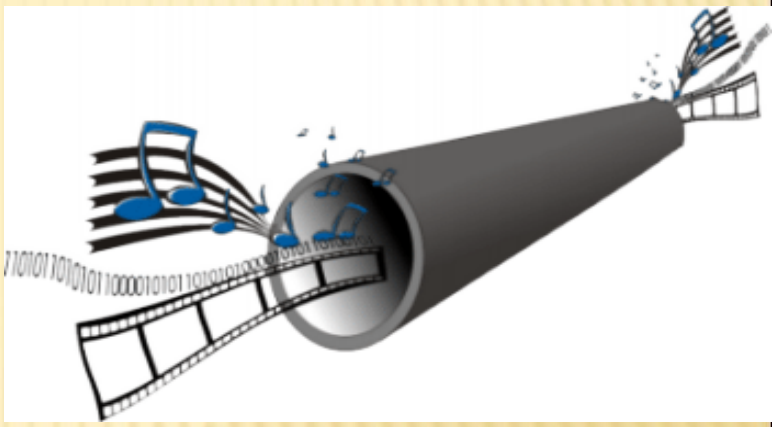
Modems convert digital and analog signals. At the source, modems convert digital signals to a form suitable for transmission over analog communication facilities (public telephone lines). At the destination, modems convert the signal back to a digital format.

CSU/DSU (Channel Service Unit / Data Service Unit)

CSUs/DSUs are similar to modems, however they send data in digital format across digital telephone loops. They are usually in a physical box, but they may come in two separate units: CSUs or DSUs.

Multiplexers

A Multiplexer combines multiple signals for transmission over a single circuit. This allows for the transfer of various data simultaneously, such as video, sound, text, etc.



Communication Servers

Communication Servers are typically dial in/out servers that allow users to dial in from remote locations and attach to the LAN.

X.25 / Frame Relay Switches

X.25 and Frame Relay Switches connect private data over public data circuits using digital signal. These units are very similar to ATM switches, but the transfer rate of data is not comparable.

Local Area Network Cabling

The earliest LANs used coaxial cables. Over time, the twisted pair cables used in telephone systems were improved to carry higher frequencies and support LAN traffic. More recently, fiber optic cables have emerged as a high-speed cabling option.
Local Area Networks use four types of cables:

- **Coaxial**
- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**
- **Fiber Optic**

Ethernet

Ethernet was developed by Xerox in 1970. It was implemented through thicknet cable running at 10 Mbps.

Ethernet is a connection media access method that allows all hosts on a network to share the same bandwidth of a link.

Ethernet actually just refers to the LAN implementations that includes three principal categories.

- Ethernet / IEEE 802.3---operates at 10 Mbps on coaxial cable and twisted pair cable.
- 100-Mbps Ethernet---(also known as Fast Ethernet) operates at 100 Mbps over twisted-pair cable.
- 1000-Mbps Ethernet---(also known as Gigabit Ethernet) operates at 1000 Mbps (1 Gbps) over fiber and twisted-pair cables.

Basic Operation

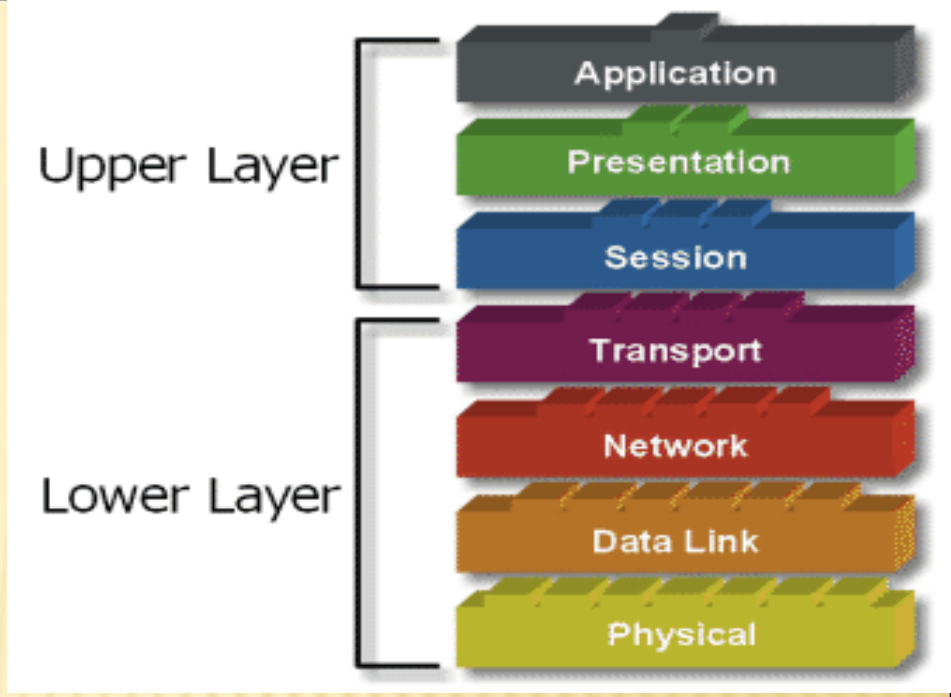
Ethernet and IEEE 802.3 operation involves three basic components:

- **Transmission**
- **Media access**
- **Collision handling**

OSI Model

OSI Network Model

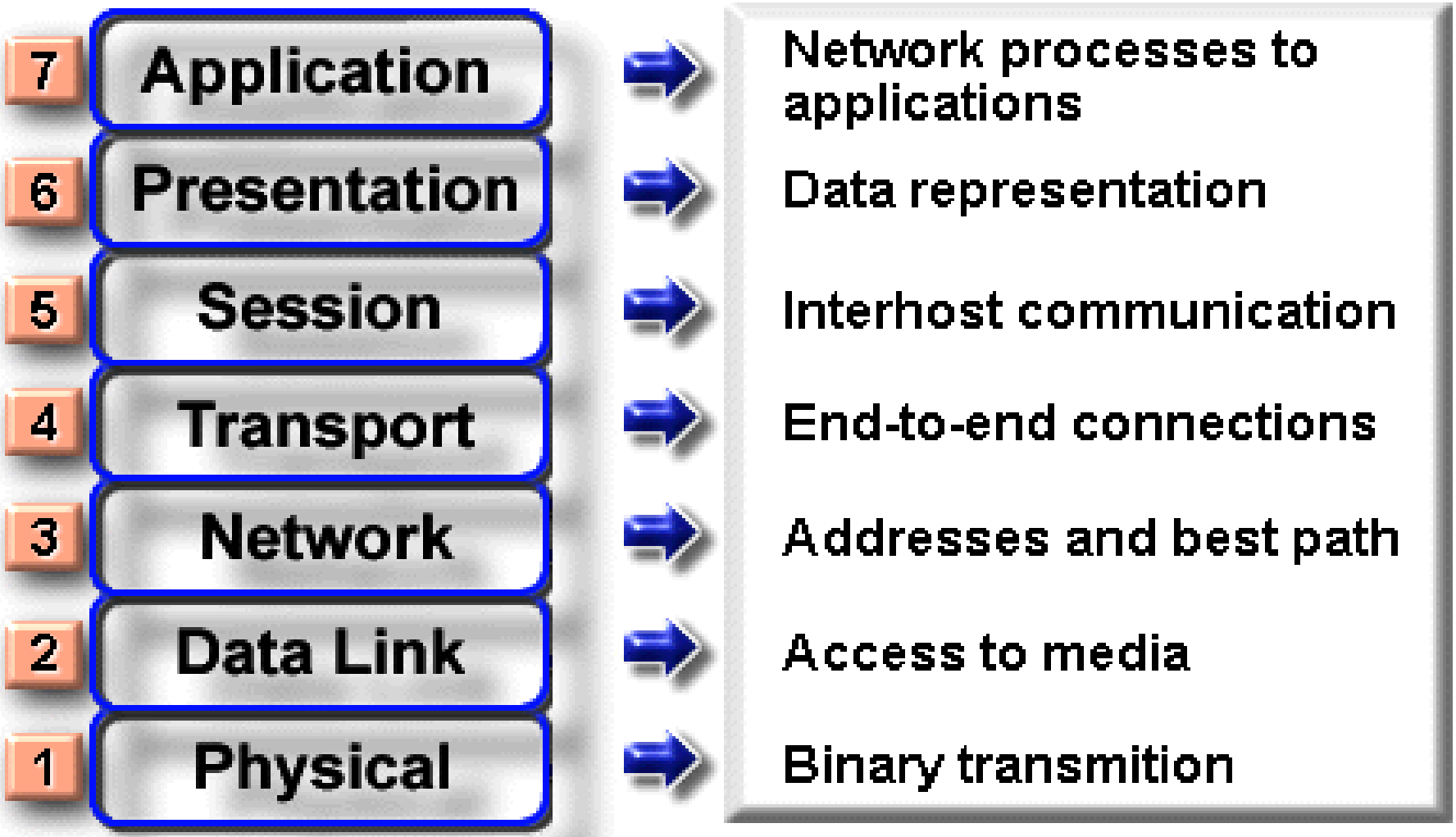
There are 7 layers in the OSI model. Each layer is responsible for a particular aspect of data communication. For example, one layer may be responsible for establishing connections between devices, while another layer may be responsible for error checking during transfer.



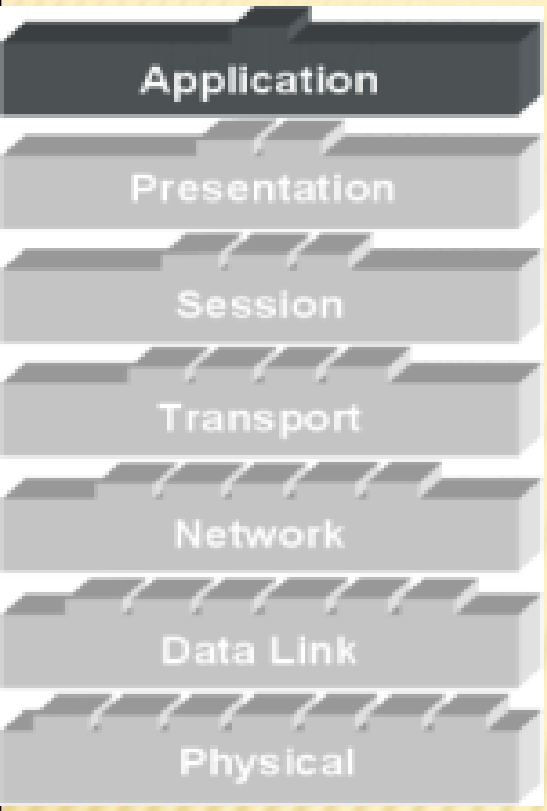
The layers of the OSI model are divided into two groups: the upper layer and lower layer. The upper layers focus on user applications and how files are represented on the computers prior to transport. For the most part, network engineers are more concerned with the lower layers. It's the lower layers that concentrate on how the communication across a network actually occurs.

- **ALL People Seem to Need Data Processing (Layer 7 to 1)**
- **Please Do Not Take Sausage Pizzas Away (Layer 1 to 7)**

Layer Functions



The Application Layer

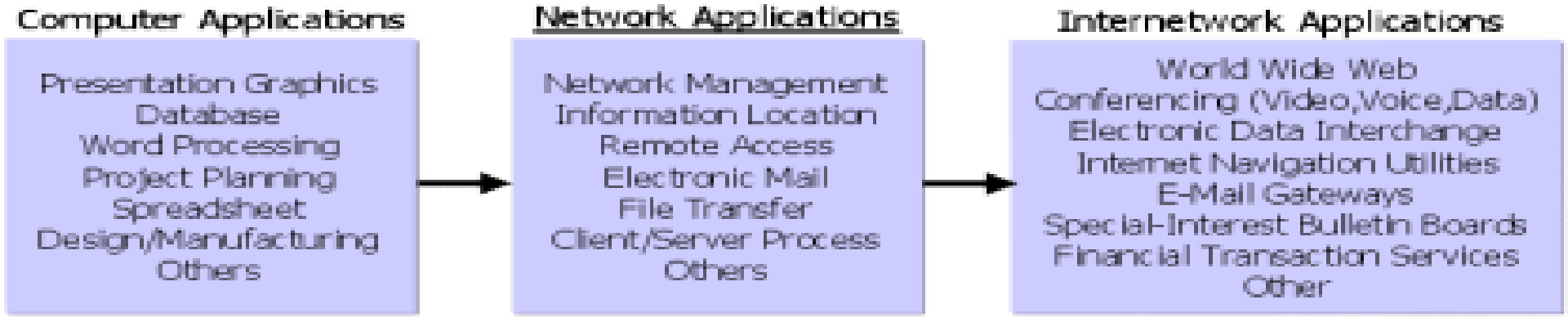


The Application Layer is the highest layer in the protocol stack and the layer responsible for introducing data into the OSI stack. In it resides the protocols for user applications that incorporate the components of network applications.

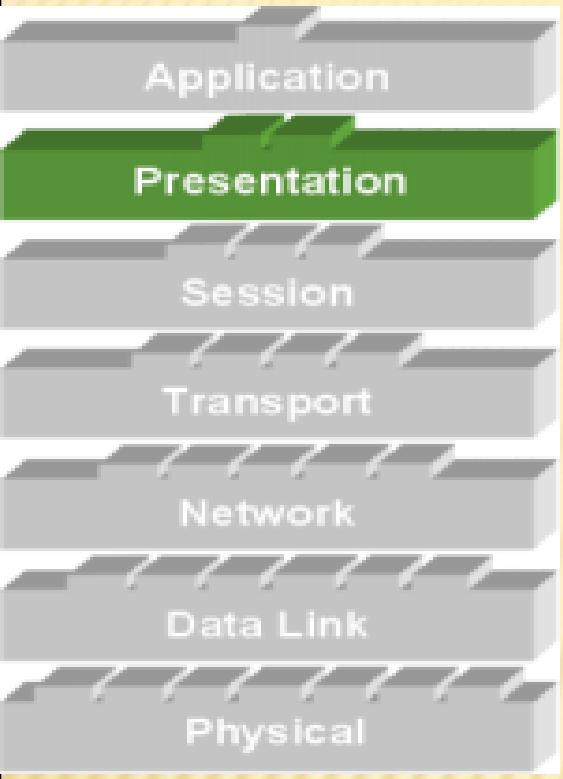
Classification of Applications

Computer applications
Network applications
Internetwork applications

Examples: Telnet, FTP, HTTP, WWW Browsers, NFS, SMTP, POP, TFTP .



Presentation Layer

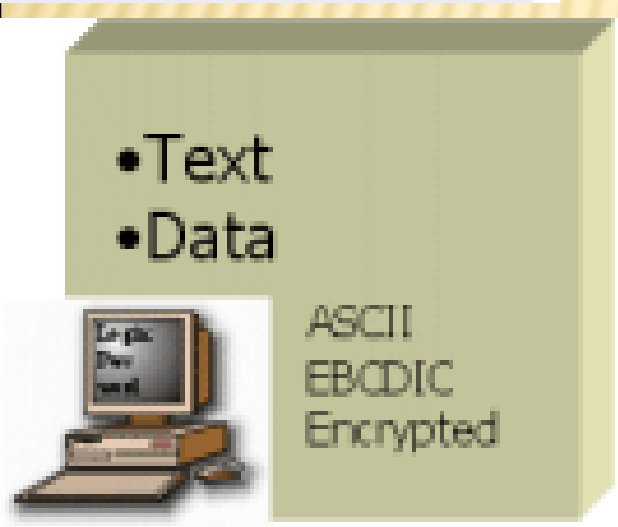


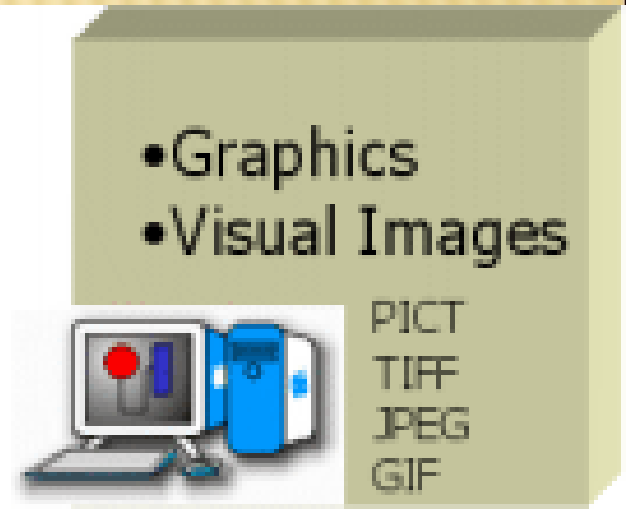
The Presentation Layer manipulates the representation of data for transfer to applications on different devices.

The Presentation Layer is responsible for the following services:

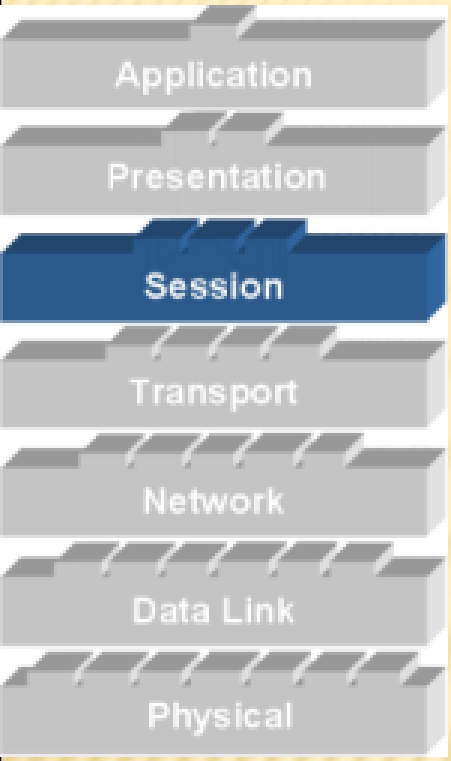
- **Data representation**
- **Data security**
- **Data compression**

Data Representation





Session Layer



The Session Layer establishes, manages, and terminates sessions (different from connections) between applications as they interact on different hosts on a network.
Its main job is to coordinate the service requests and responses between different hosts for applications.
Examples: NFS, SQL, RPC, ASP

Three different communication modes exists for data transfer within a session connection:

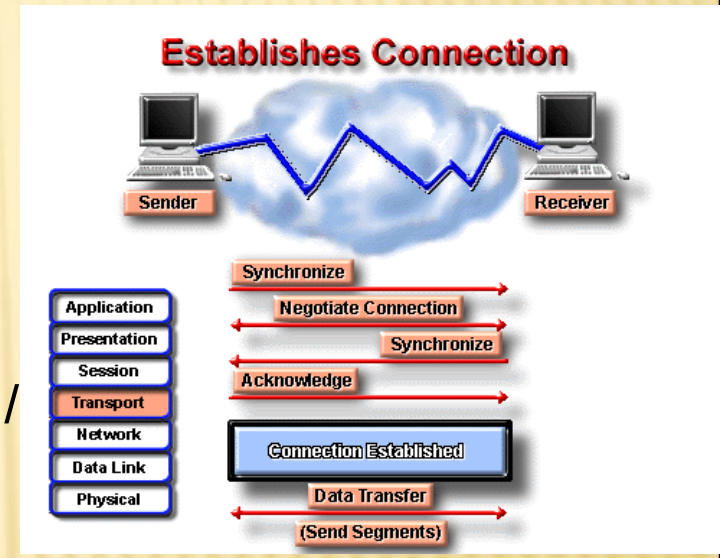
- **Single-duplex**

- **Half-duplex**

- **Full-duplex**.

Transport Layer

The basic roles of the Transport Layer are to establish end-to-end connections from one computer to another on the network and provide reliable "transport" of data between devices.



Basic Transport Layer Services:

Resource Utilization (multiplexing)
Connection Management (establishing)
Flow Control (Buffering / Windowing)
Reliable Transport (positive acknowledgment /

Flow Control

Once the connection has occurred and transfer is in progress, congestion of the data flow can occur at a destination for a variety of reasons. Possible options include:

The destination can become overwhelmed if multiple devices are trying to send it data at the same time.

It may become overwhelmed if the source is sending faster than it can physically receive.

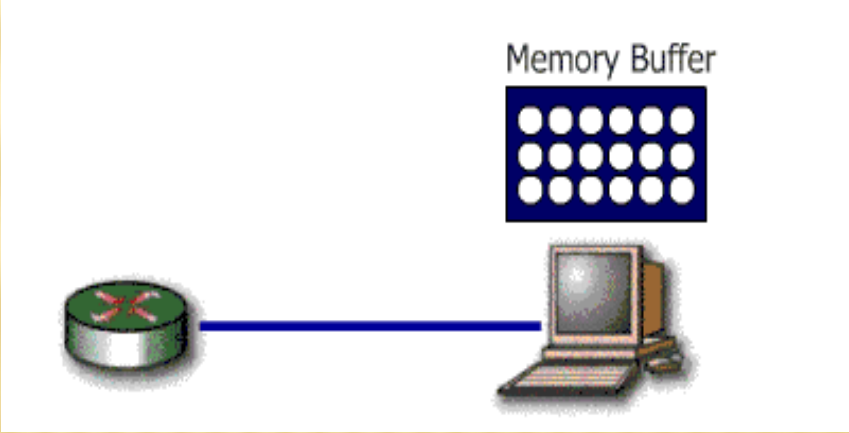
Congestion Prevention

The Transport Layer is responsible for providing flow control to alleviate the issue of congestion and provide reliability in the data transfer. Two main methods for flow control include

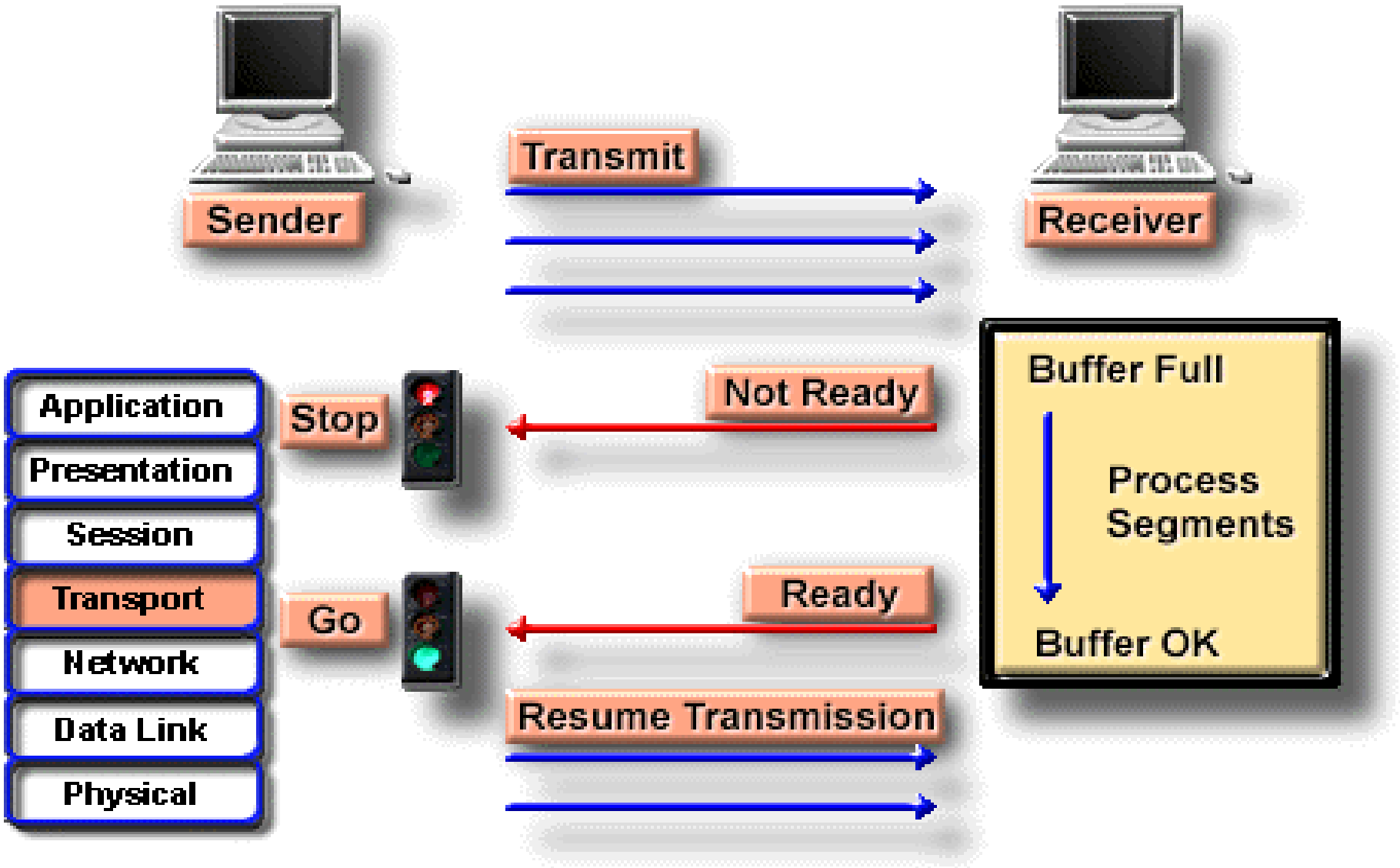
- **Buffering**
- **Windowing**

Buffering

Buffering is a form of data flow control regulated by the Transport Layer. It is responsible for ensuring that sufficient buffers are available in the destination for the processing of data and that is data transmitted at a rate that does not exceed what the buffer can handle.

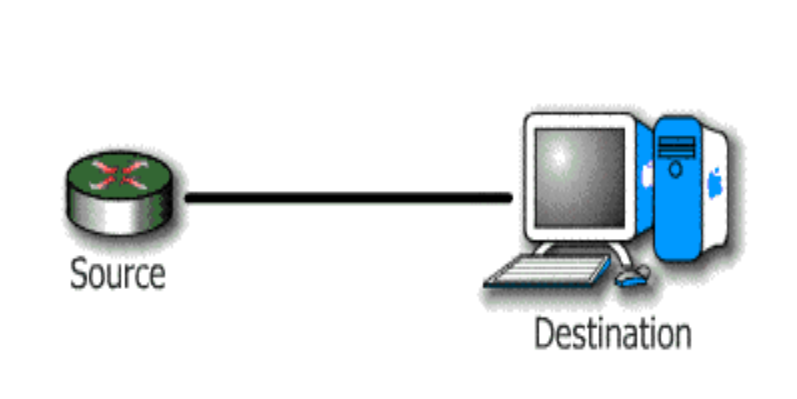


Sends Segments with Flow Control

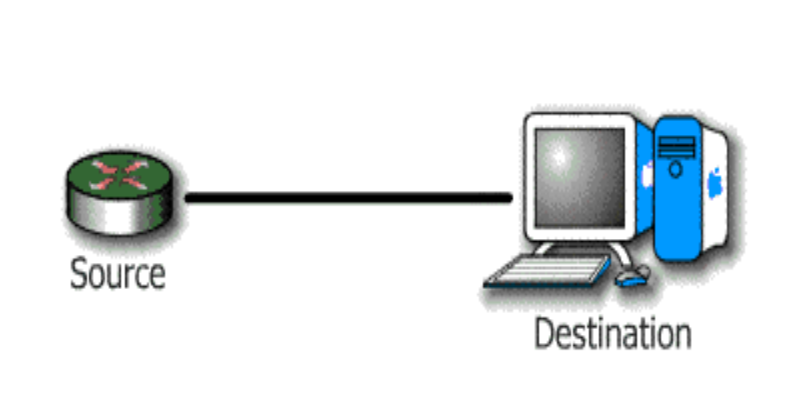


Windowing

Windowing is a flow control scheme in which the source computer will monitor and make adjustments to the amount of information sent based on successful, reliable receipt of data segments by the destination computer. The size of the data transmission, called the "window size", is negotiated at the time of connection establishment. It is determined by the amount of memory or buffer that is available.

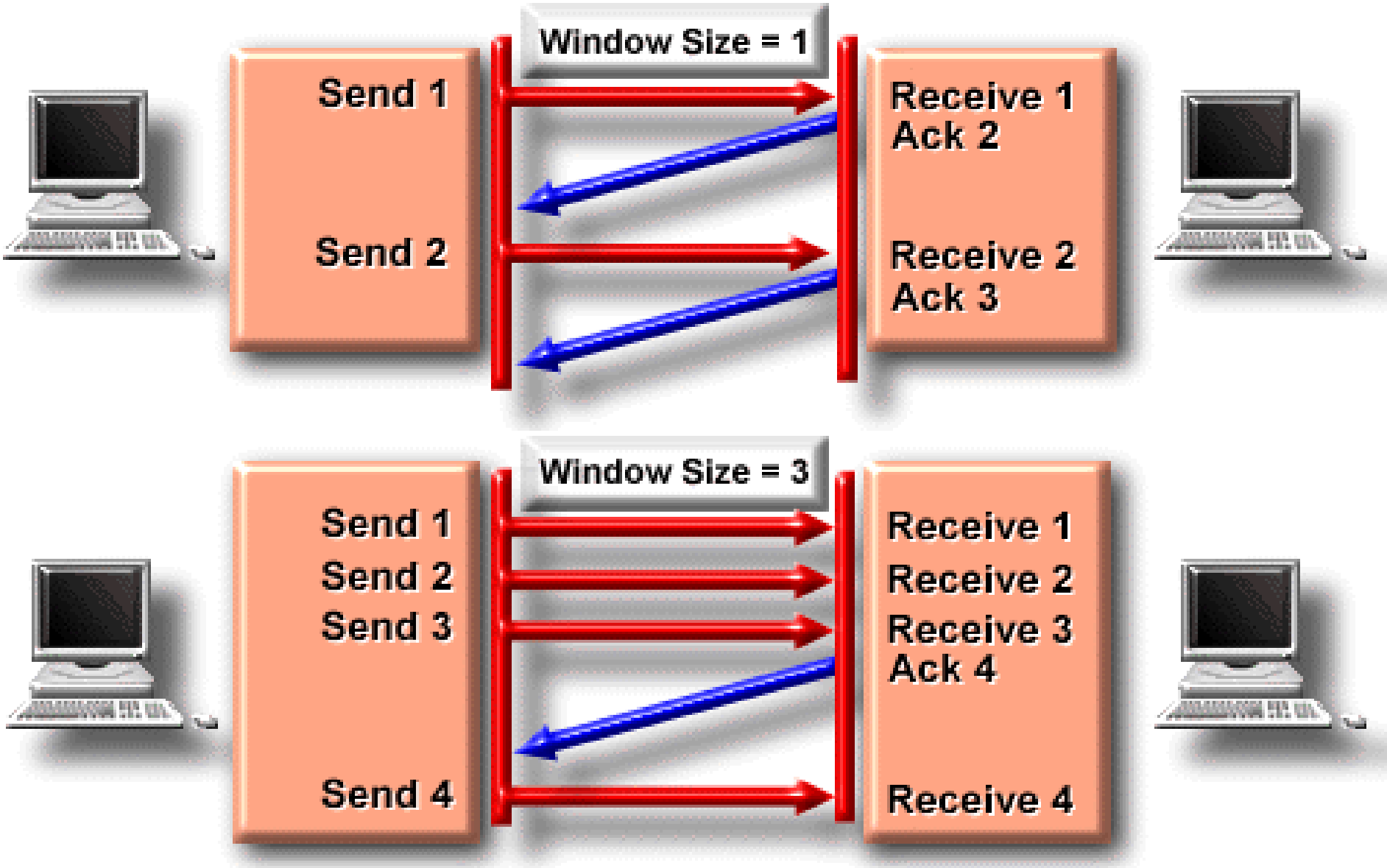


Given a window size of 3, the source (in this case a router) sends 3 data segments to the destination. The destination sends an acknowledgement asking for the next set of data segments.



If the destination does not receive all three of the negotiated data segments, for example, due to a buffer overflow, it sends no acknowledgment. Since the source does not receive an acknowledgment, it knows the data segments should be retransmitted

Reliability with Windowing

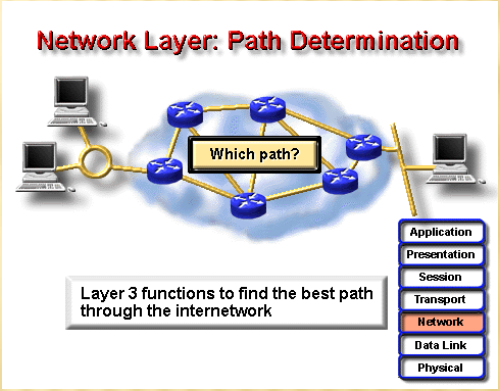


Network Layer

The Network Layer is the 3rd layer in the OSI model and is responsible for identifying computers on a network. This layer works closely with layer 2 to translate data packets from a logical address (similar to an IP address) into hardware based MAC addresses.

This layer is concerned with 2 functions:

- Routing
- Fragmentation / Reassembly



Two types of packets are used at the Network layer:

Data packets: Used to transport user data through the internetwork. Protocols used to support data traffic are called routed protocols. Eg. IP and IPX.

Route update packets: Used to update neighboring routers about the network connected to all routers within the internetwork. Protocols that send route updates are called routing protocols. Eg. RIP, EIGRP, OSPF

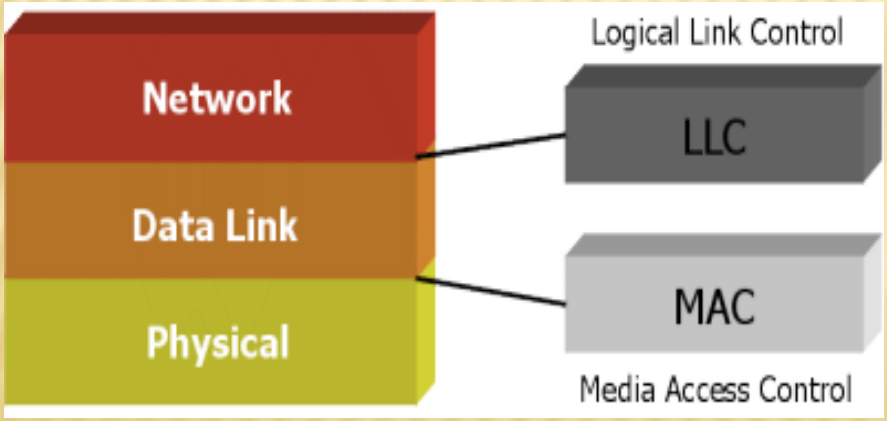
Data Link / Physical Layer

LAN and WAN protocols occupy the bottom two layers of the OSI model. These two layers, Physical Layer and Data Link Layer, work very closely together to ensure data transfer across the physical network. Examples: HDLC, Frame Relay, PPP, ATM, FDDI, IEEE 802.3/802.2

To accomplish accurate delivery, the Data Link Layer provides the following services:

1. Machine address determination of both sending and receiving machines
2. Formatting of Network Layer "packets" into frames with machine addresses attached
3. Sequencing and resequencing of frames transmitted out of sequence

Data Link Sublayers



Logical Link Control (LLC) responsible for identifying Network layer protocols and encapsulating them.

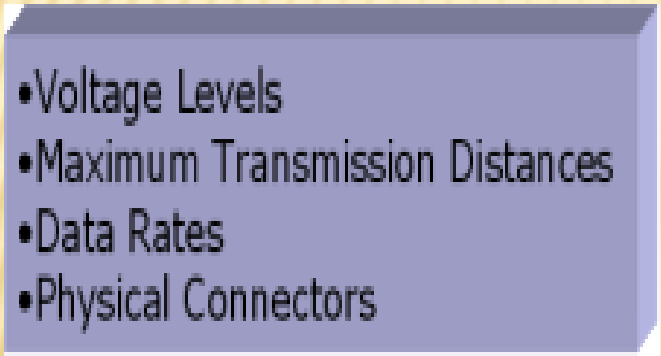
Media Access Control (MAC) defines how packets are placed on media

Physical Layer

The Physical Layer is the lowest layer in the OSI model and is concerned with how the physical structure of the network enables transmission of data. It is responsible for defining the mechanical and electrical specifications for the transmission medium within a connection, as well as the transformation or encoding of data into “bits”.

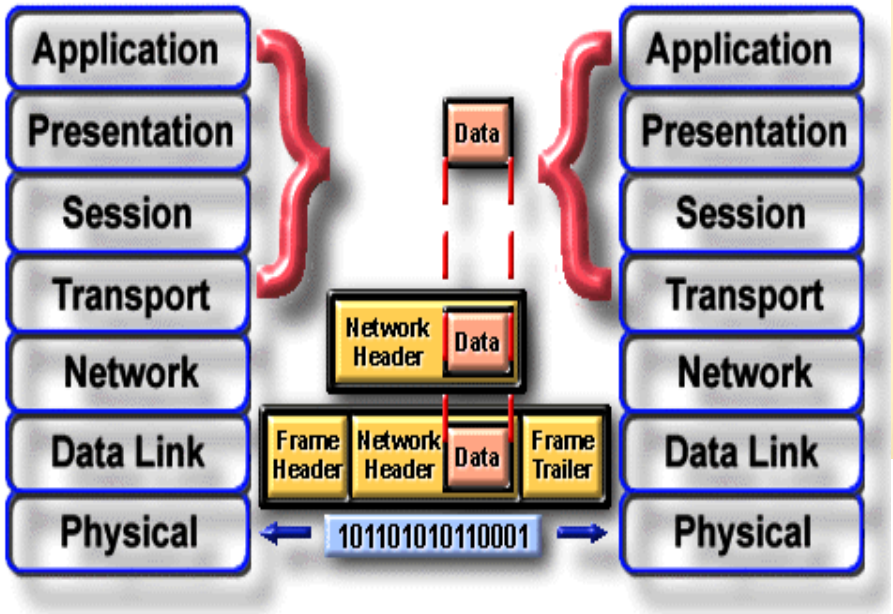
Examples:EIA/TIA-232, V.35, EIA/TIA-449, RJ-45, Ethernet, 802.3

Protocols



Protocols defined at the Physical Layer standardize physical connections. Specifications include voltage levels, maximum transmission distances, data rates, and physical connectors.

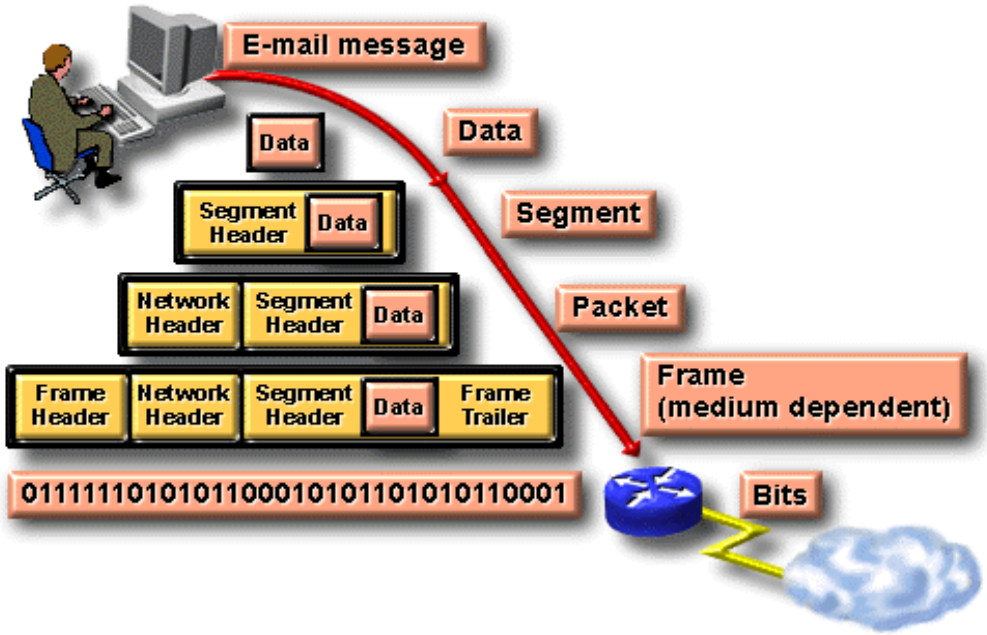
Data Encapsulation



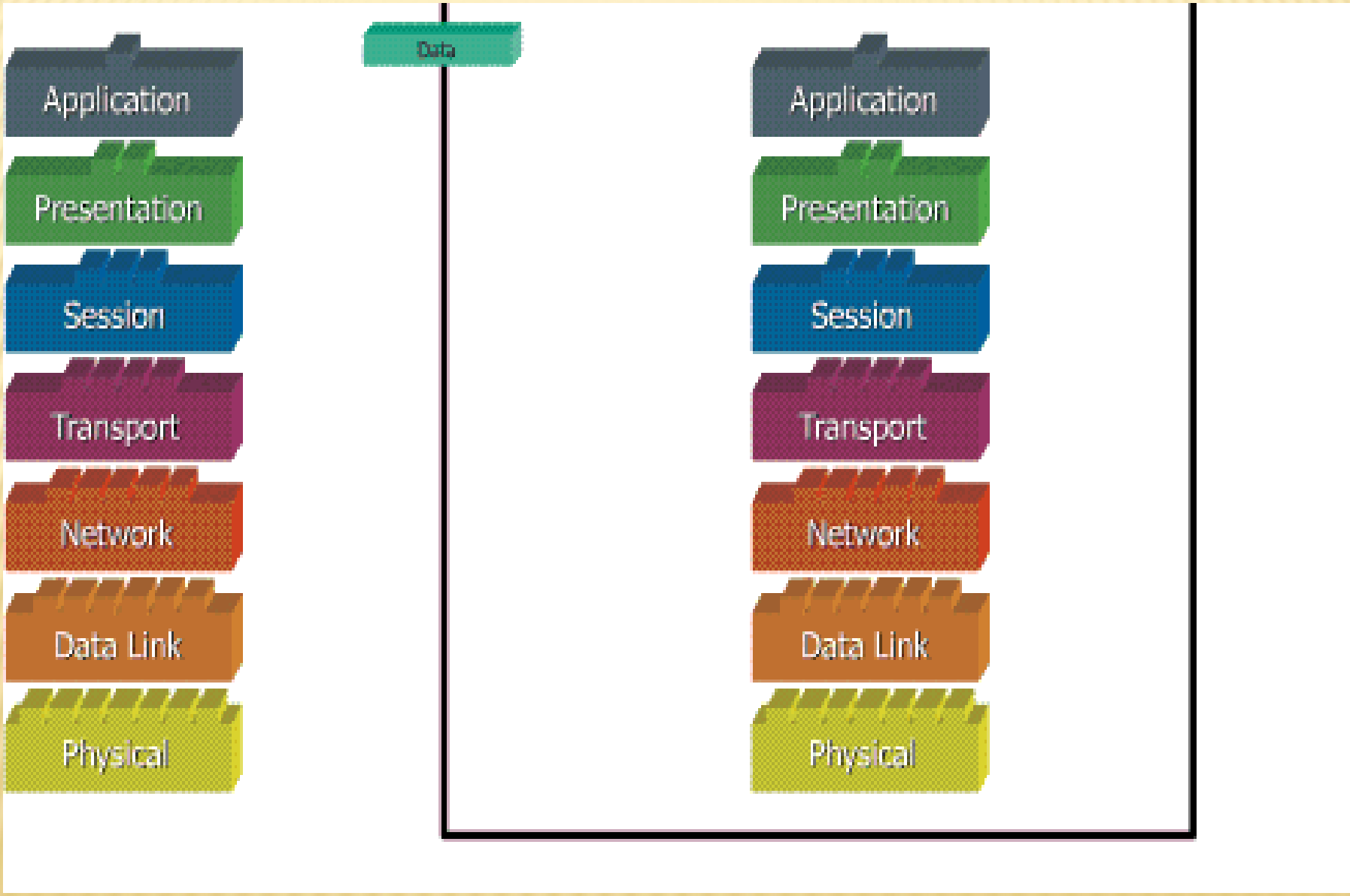
Each layer depends on the service function of the ISO/OSI layer below it. To provide this service, the lower layer uses encapsulation to put the PDU from the upper layer into its data field; then it can add whatever headers and trailers the layer will use to perform its function.

As networks perform services for users, the flow and packaging of the information changes. In this example of internetworking, five conversion steps occur:

Data Encapsulation Example

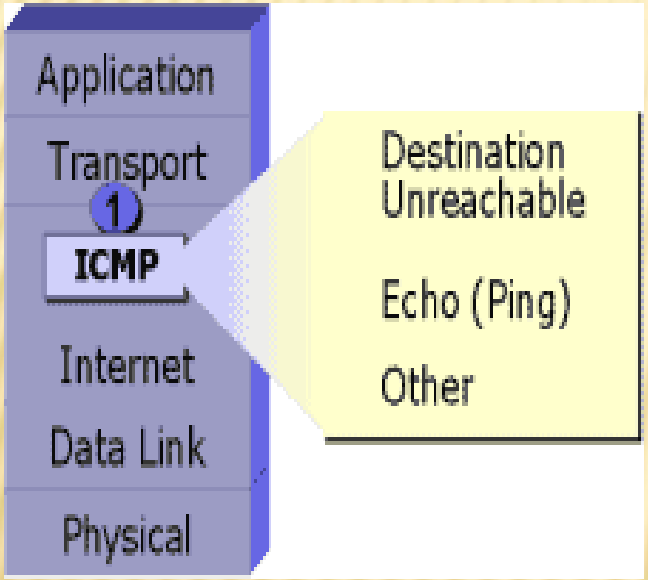


What do the 7 layers really do?



ICMP

The Internet Control Message Protocol (**ICMP**) is implemented by all TCP/IP hosts. ICMP messages are carried in IP datagrams and are used to send error and control messages.

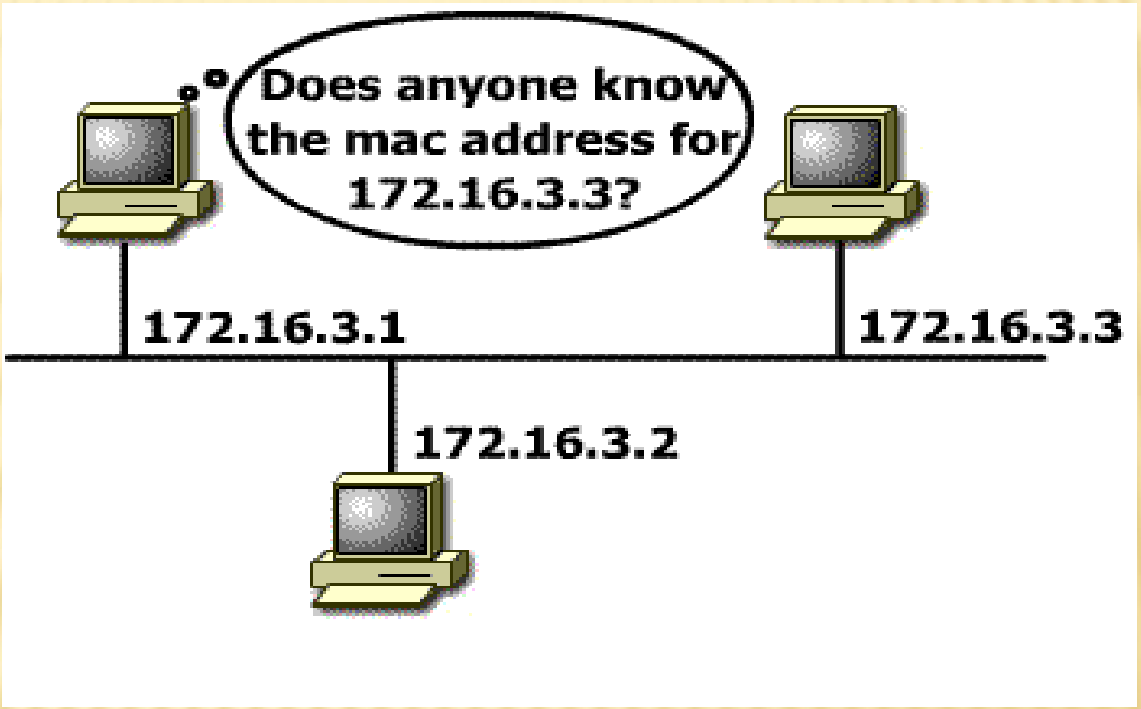


ICMP uses the following types of defined messages:

1. Destination Unreachable
2. Time Exceeded
3. Parameter Problem
4. Subnet Mask Request
5. Redirect
6. Echo
7. Echo Reply
8. Information Request
9. Information Reply
10. Address Request
11. Address Reply

Address Resolution Protocol

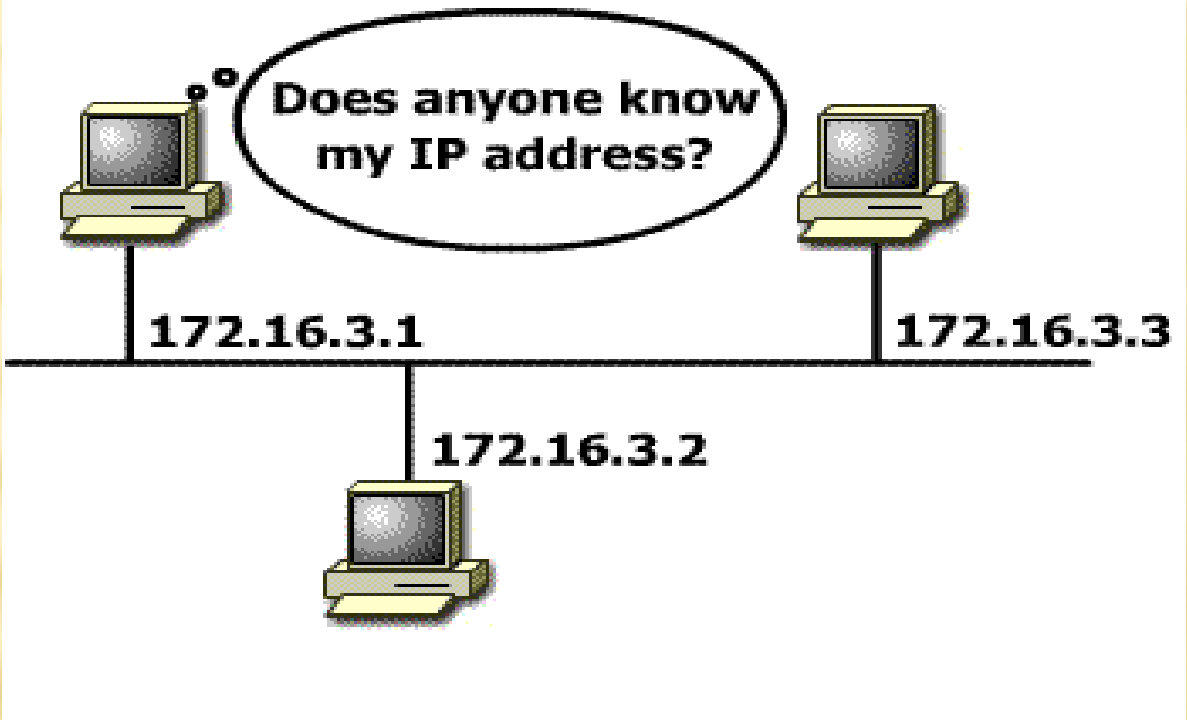
Address Resolution Protocol (**ARP**) is used to resolve or map a known IP address to a MAC sublayer address to allow communication on a multi-access medium such as Ethernet.



The term **local ARP** is used to describe resolving an address when both the requesting host and the destination host share the same media or wire.

Reverse ARP

Reverse Address Resolution Protocol (**RARP**) relies on the presence of a RARP server with a table entry or other means to respond to these requests.



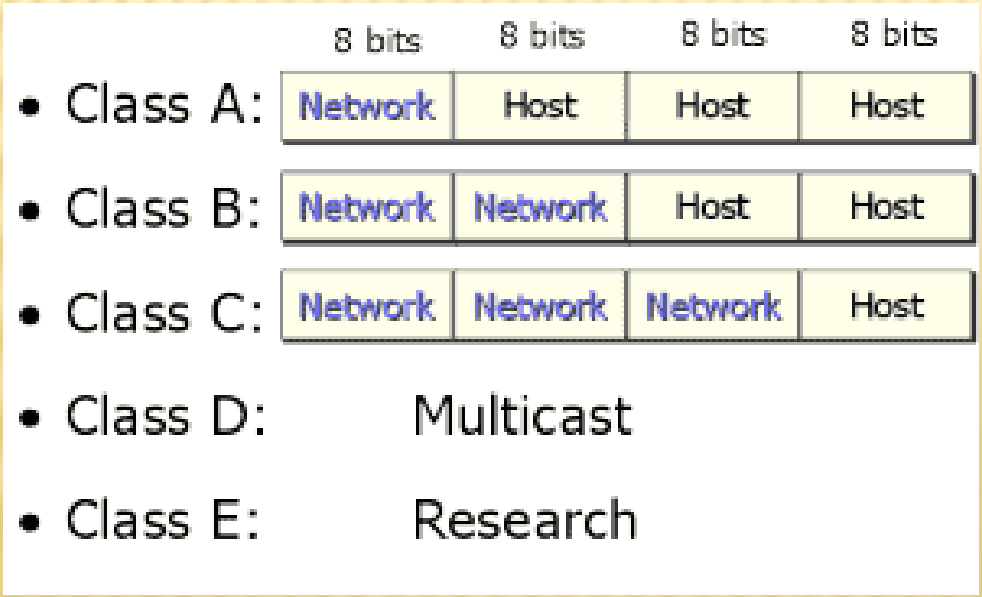
ARP and RARP are implemented directly on top of the data link layer

IP Address

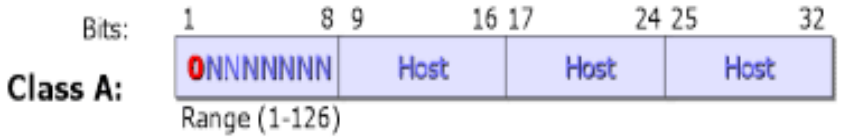
In a TCP/IP environment, end stations communicate seamlessly with servers or other end stations. This communication occurs because each node using the TCP/IP protocol suite has a unique 32-bit logical IP address.

Each IP datagram includes the source IP address and destination IP address that identifies the source and destination network and host.

When IP was first developed, there were no classes of addresses. Now, for ease of administration, the IP addresses are broken up into classes.



The bits in the first octet identify the address class. The router uses the first bits to identify how many bits it must match to interpret the network portion of the address

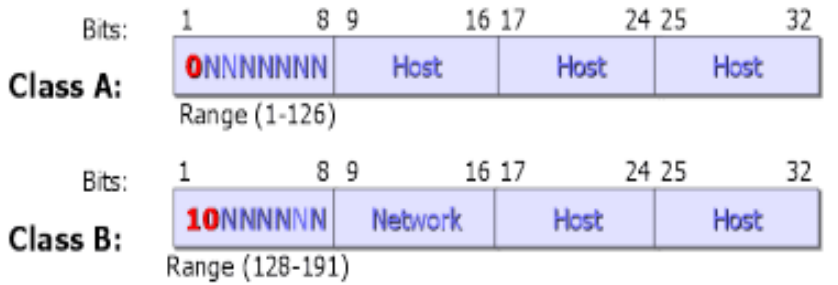


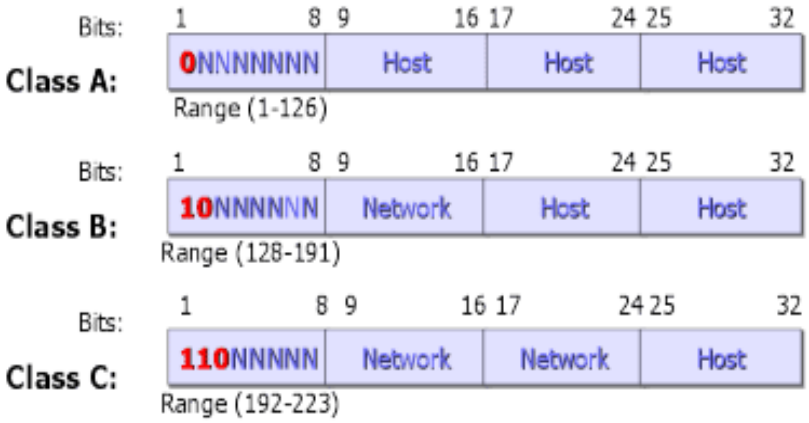
Class A addresses include the following:

- The first bit is 0.
- Range of network numbers: 1.0.0.0 to 126.0.0.0
- Number of possible networks: 127 (1-126 usable, 127 is reserved)
- Number of possible values in the host portion: 16,777,216.

Class B addresses include the following:

- The first two bits are 10.
- Range of network numbers: 128.0.0.0 to 191.255.0.0
- Number of possible networks: 16,384
- Number of possible values in the host portion: 65,536





Class C addresses include the following:

- The first three bits are 110.
- Range of network numbers: 192.0.0.0 to 223.255.255.0
- Number of possible networks: 2,097,152
- Number of possible values in the host portion: 256

Class D addresses include the following:

- Range of network numbers: 224.0.0.0 to 239.255.255.255