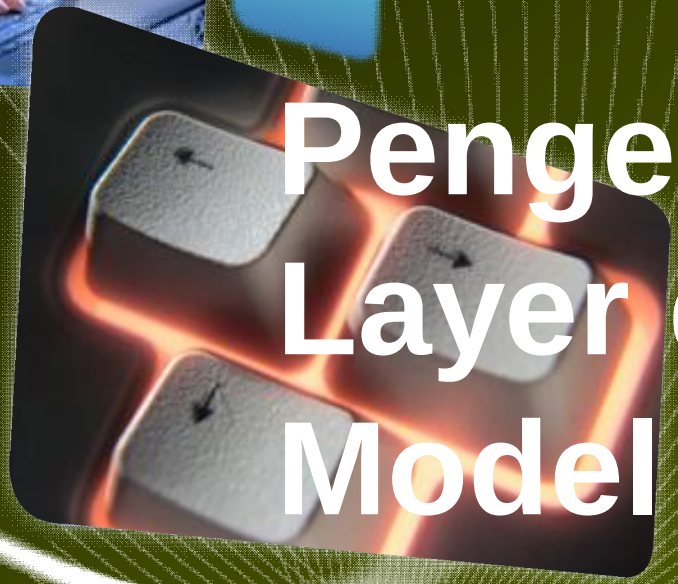


INSTITUT TEKNOLOGI TELKOM

Pengenalan OSI Layer dan TCP/IP Model

The Elements of Communication

- **Communication begins with a message, or information, that must be sent from one individual or device to another using many different communication methods.**
- **All of these methods have 3 elements in common:**
  - message source, or sender
  - destination, or receiver
  - a channel

Communicating The Messages

- **Data is divided into smaller parts during transmission - Segmentation**
- **The benefits of doing so:**

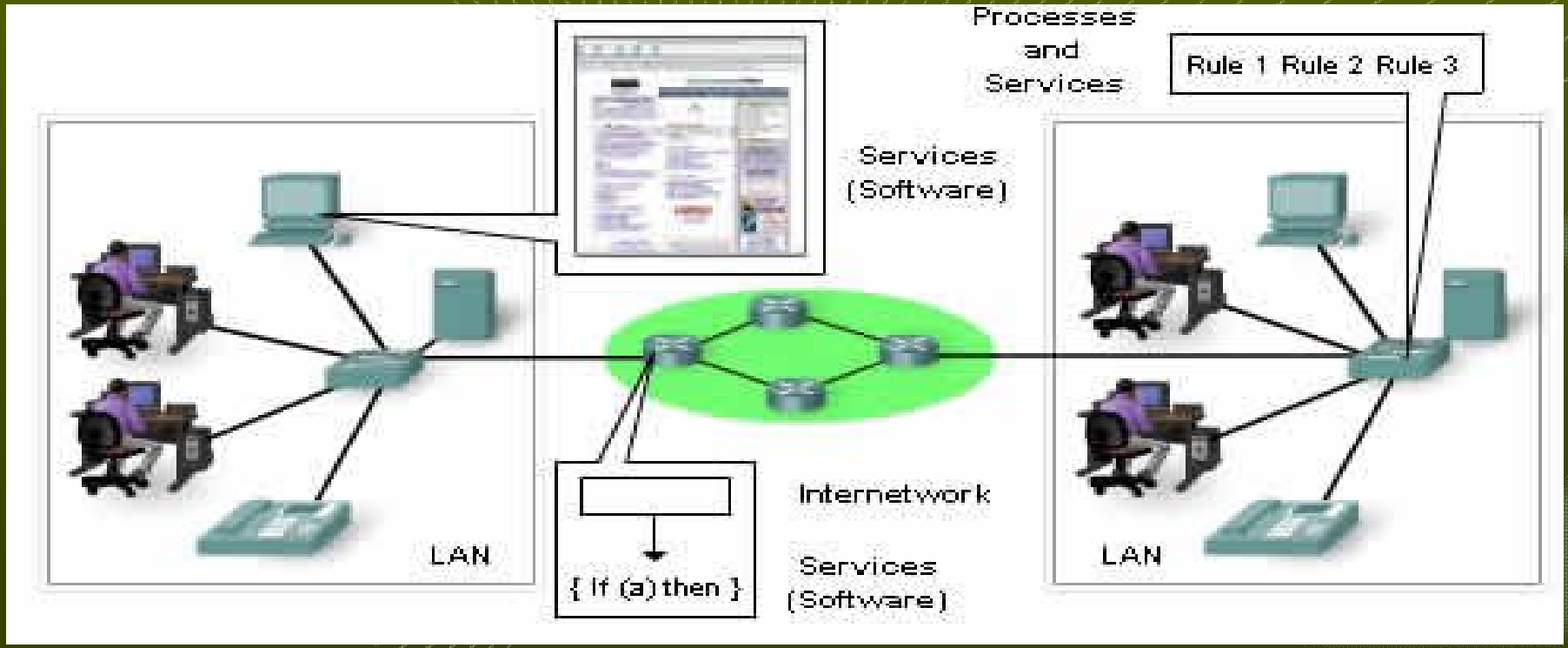
  - Many **different conversations can be interleaved** on the network. The process used to interleave the pieces of separate conversations together on the network is called **multiplexing**.

  - **Increase the reliability** of network communications. The separate pieces of each message need not travel the same pathway across the network from source to destination

- Downside of segmentation and multiplexing - level of complexity is added (process of addressing, labeling, sending, receiving and etc are time consuming)
- Each segment of the message must go through a similar process to ensure that it gets to the correct destination and can be reassembled into the content of the original message
- Various types of devices throughout the network participate in ensuring that the pieces of the message arrive reliably at their destination

Components of the Network

- Devices (PCs, intermediary devices)
- Media (Cable or wireless)
- Services and processes (Software)



End Devices and Their Roles

- In the context of a network, end devices are referred to as hosts.
- A host device is either the sender or receiver
- To distinguish one host from another, each host on a network is identified by an address.
- A host (sender) uses the address of the destination host to specify where the message should be sent.
- Software determines the role of a host. A host can be a client, server or both

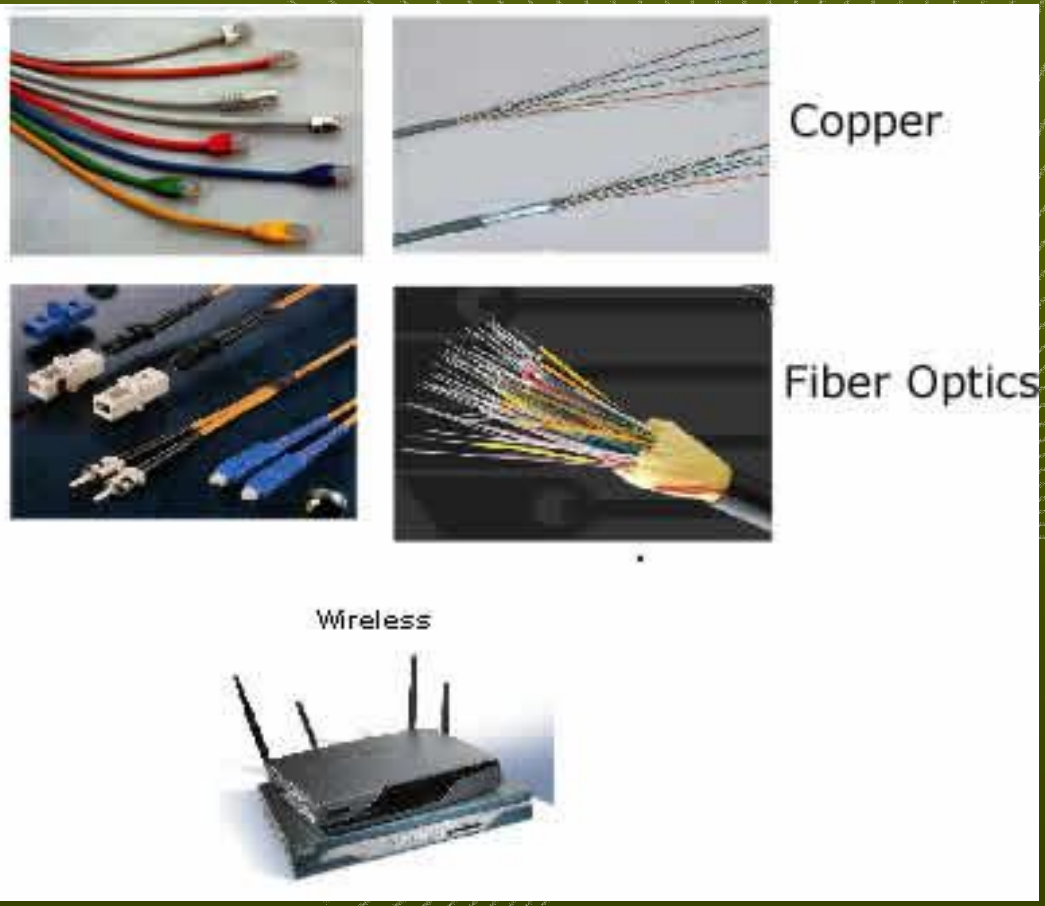
Intermediary Devices and Their Roles

- **Examples:**
  - **Network Access Devices (Hubs, switches, and wireless access points)**
  - **Internetworking Devices (routers)**
  - **Communication Servers and Modems**
  - **Security Devices (firewalls)**

- **Processes running on the intermediary network devices perform these functions:**
  - Regenerate and retransmit data signals
  - Maintain information about what pathways exist through the network and internetwork
  - Notify other devices of errors and communication failures
  - Direct data along alternate pathways when there is a link failure
  - Classify and direct messages according to QoS priorities
  - Permit or deny the flow of data, based on security settings

Network Media

- **Communication across a network is carried on a medium**

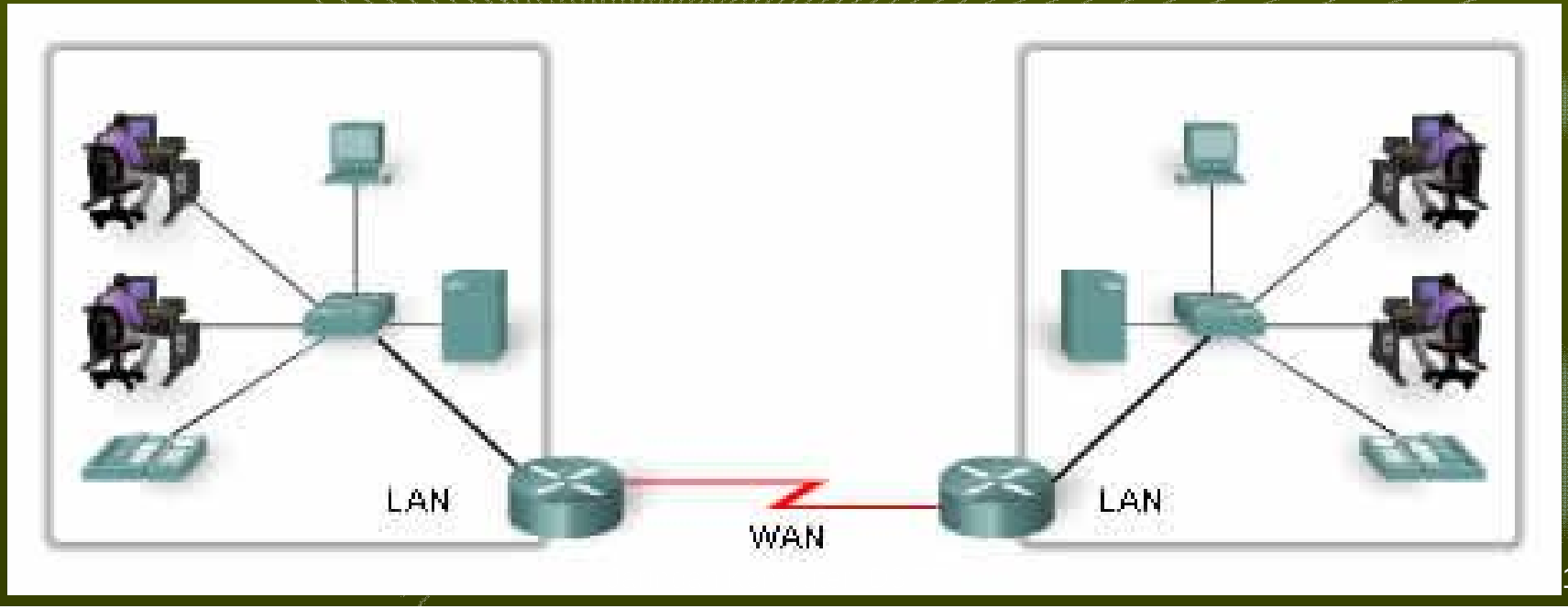


•3 types of Media:
- Metallic wires within cables
- Glass or plastic fibers (fiber optic cable)
-Wireless transmission

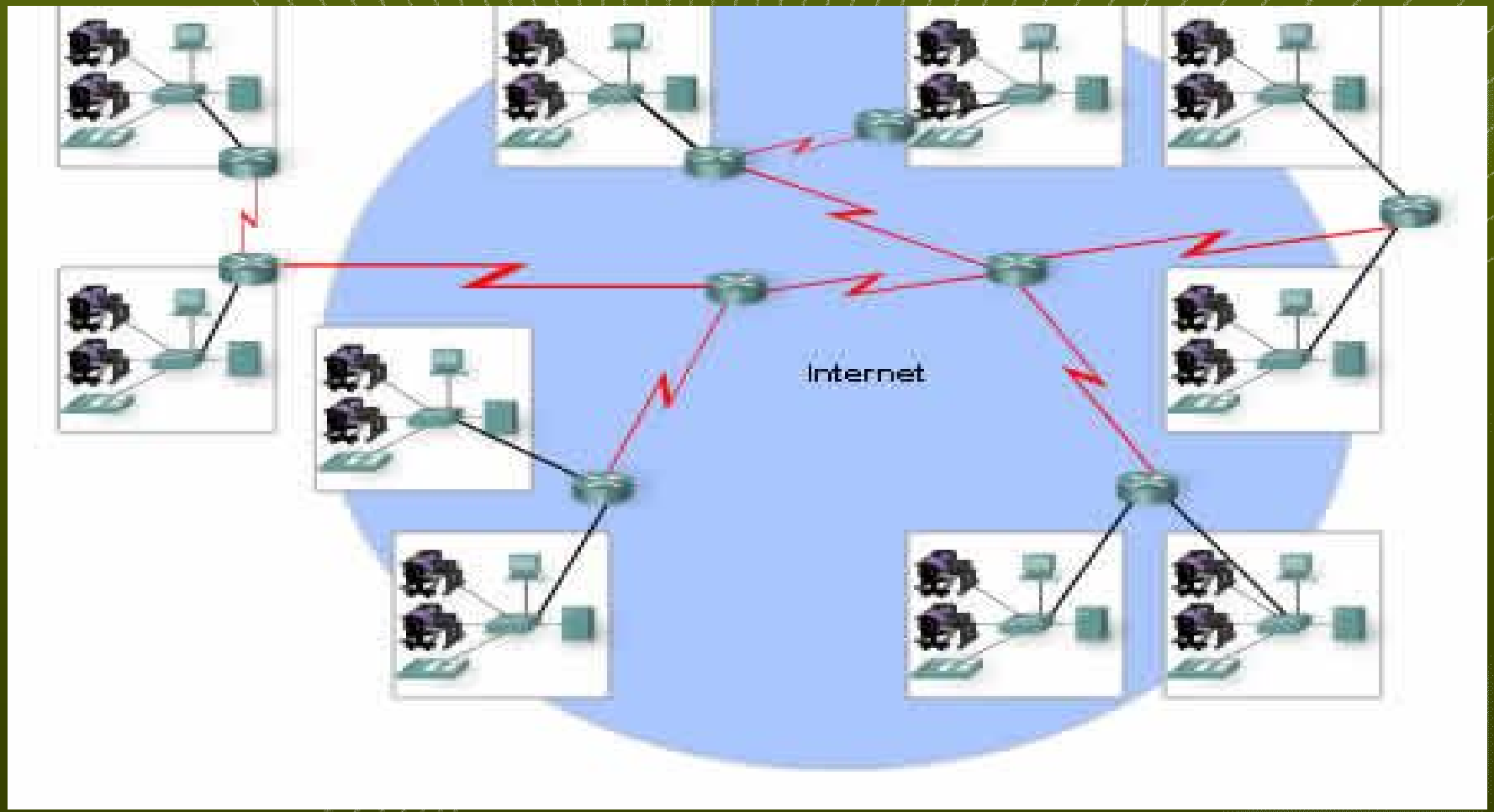
- **The signal encoding is different for each media type.**
  - Metallic wires, the data is encoded into electrical impulses
  - Fiber optic - pulses of light, within either infrared or visible light ranges.
  - Wireless transmission, electromagnetic waves
- **Criteria for choosing a network media are:**
  - The **distance** the media can successfully carry a signal.
  - The **environment** in which the media is to be installed.
  - The **amount** of data and the **speed** at which it must be transmitted.
  - The **cost** of the media and installation

LAN, WAN, Internetworks

- Local Area Network (LAN) - An individual network usually spans a single geographical area, providing services and applications to people within a common organizational structure, such as a single business, campus or region
- Wide Area Network (WAN)- Individual organizations usually lease connections through a telecommunications service provider network. These networks that connect LANs in geographically separated locations are referred to as Wide Area Networks.



Internetworks - A global mesh of interconnected networks for communication. Ex: Internet



- **The term intranet is often used to refer to a private connection of LANs and WANs that belongs to an organization, and is designed to be accessible only by the organization's members, employees, or others with authorization.**

Network Representations

Desktop Computer

Laptop

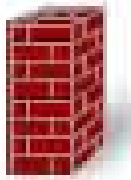
Server

IP Phone

LAN Media

Wireless Media

LAN Switch



Firewall

Router

Wireless Router

Cloud

WAN Media

- Network Interface Card - A NIC, or LAN adapter, provides the physical connection to the network at the PC or other host device. The media connecting the PC to the networking device plugs directly into the NIC.

- Physical Port - A connector or outlet on a networking device where the media is connected to a host or other networking device.

- Interface - Specialized ports on an internetworking device that connect to individual networks. Because routers are used to interconnect networks, the ports on a router are referred to network interfaces.

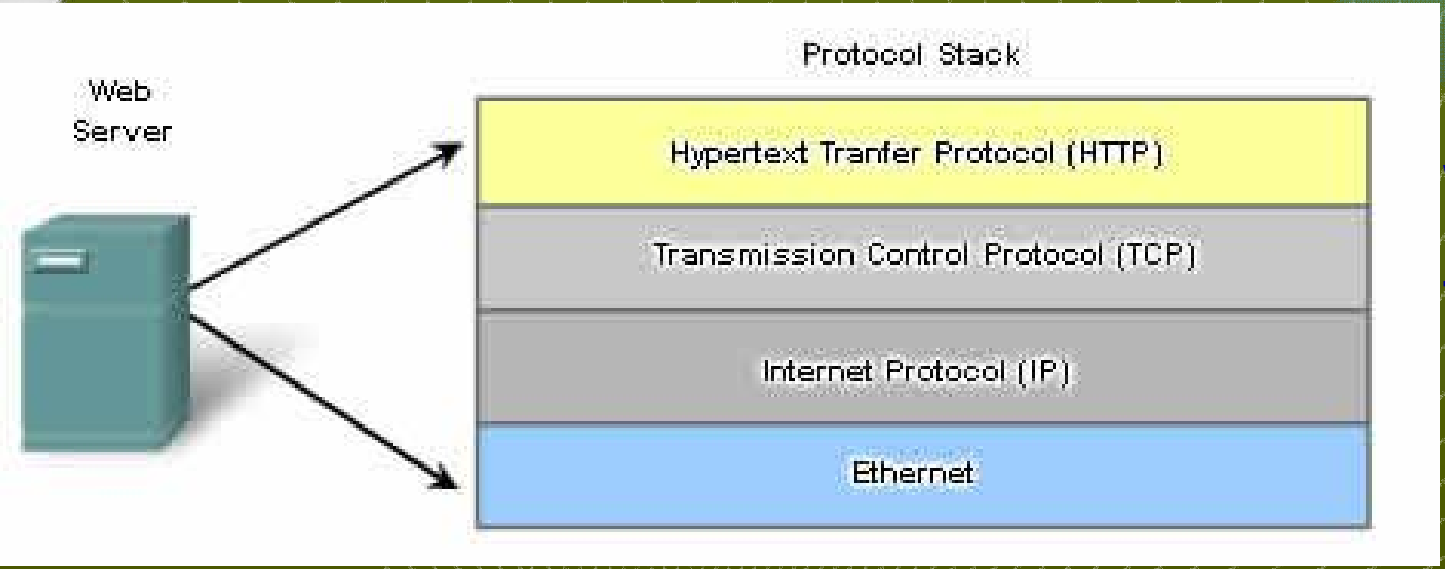
Rules that Govern Communications

- **Communication in networks is governed by pre-defined rules called protocols.**
- **A group of inter-related protocols that are necessary to perform a communication function is called a protocol suite. These protocols are implemented in software and hardware that is loaded on each host and network device**
- **Networking protocols suites describe processes such as:**
  - The format or structure of the message
  - The process by which networking devices share information about pathways with other networks
  - How and when error and system messages are passed between devices
  - The setup and termination of data transfer sessions
- **Individual protocols in a protocol suite may be vendor-specific and proprietary.**

Protocol Suites & Industry Standard

- Many of the protocols that comprise a protocol suite reference other widely utilized protocols or industry standards
- Institute of Electrical and Electronics Engineers (IEEE) or the Internet Engineering Task Force (IETF)
- The use of standards in developing and implementing protocols ensures that products from different manufacturers can work together for efficient communications

The Interaction of Protocols



Will learn more in TCP/IP model

- **Application protocol – HTTP. HTTP defines the content and formatting of the requests and responses exchanged between the client and server**
- **Transport Protocol – TCP. TCP divides the HTTP messages into smaller segments. It is also responsible for controlling the size and rate of message exchange.**
- **Internetwork Protocol – IP. It encapsulating segments into packets, assigning the appropriate addresses, and selecting the best path to the destination host.**
- **Network Access Protocol – Protocols for data link management and the physical transmission of data on the media.**

Using Layer Models

- To visualize the interaction between various protocols, it is common to use a layered model.
- Benefits of doing so:

  - Assists in protocol design, because protocols that operate at a specific layer have defined information that they act upon and a defined interface to the layers above and below.
  - Fosters competition because products from different vendors can work together.
  - Prevents technology or capability changes in one layer from affecting other layers above and below.
  - Provides a common language to describe networking functions and capabilities.

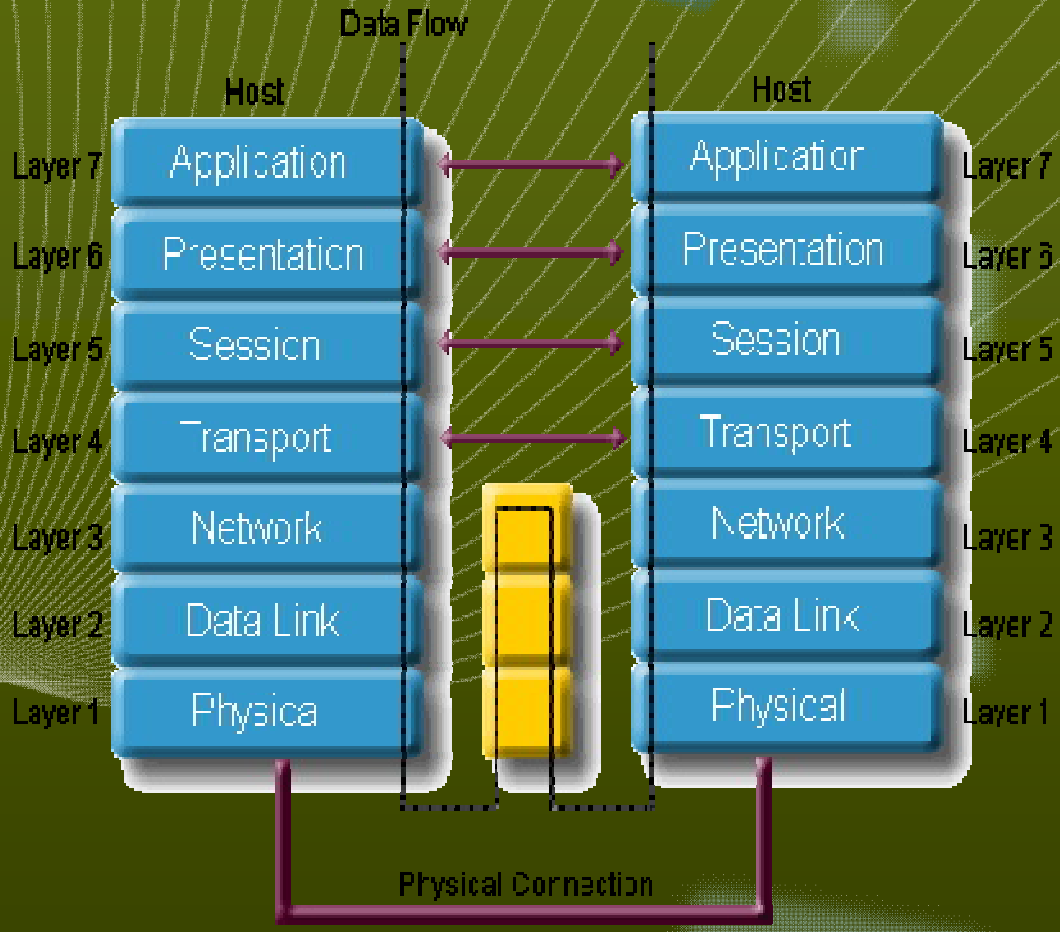
Protocol & Reference Model

- 2 types of networking models
- A protocol model provides a model that closely matches the structure of a particular protocol suite. The hierarchical set of related protocols in a suite typically represents all the functionality required to interface the human network with the data network. Ex: TCP/IP model
- A reference model provides a common reference for maintaining consistency within all types of network protocols and services. A reference model is not intended to be an implementation specification or to provide a sufficient level of detail to define precisely the services of the network architecture. The primary purpose of a reference model is to aid in clearer understanding of the functions and process involved

  Ex: OSI model

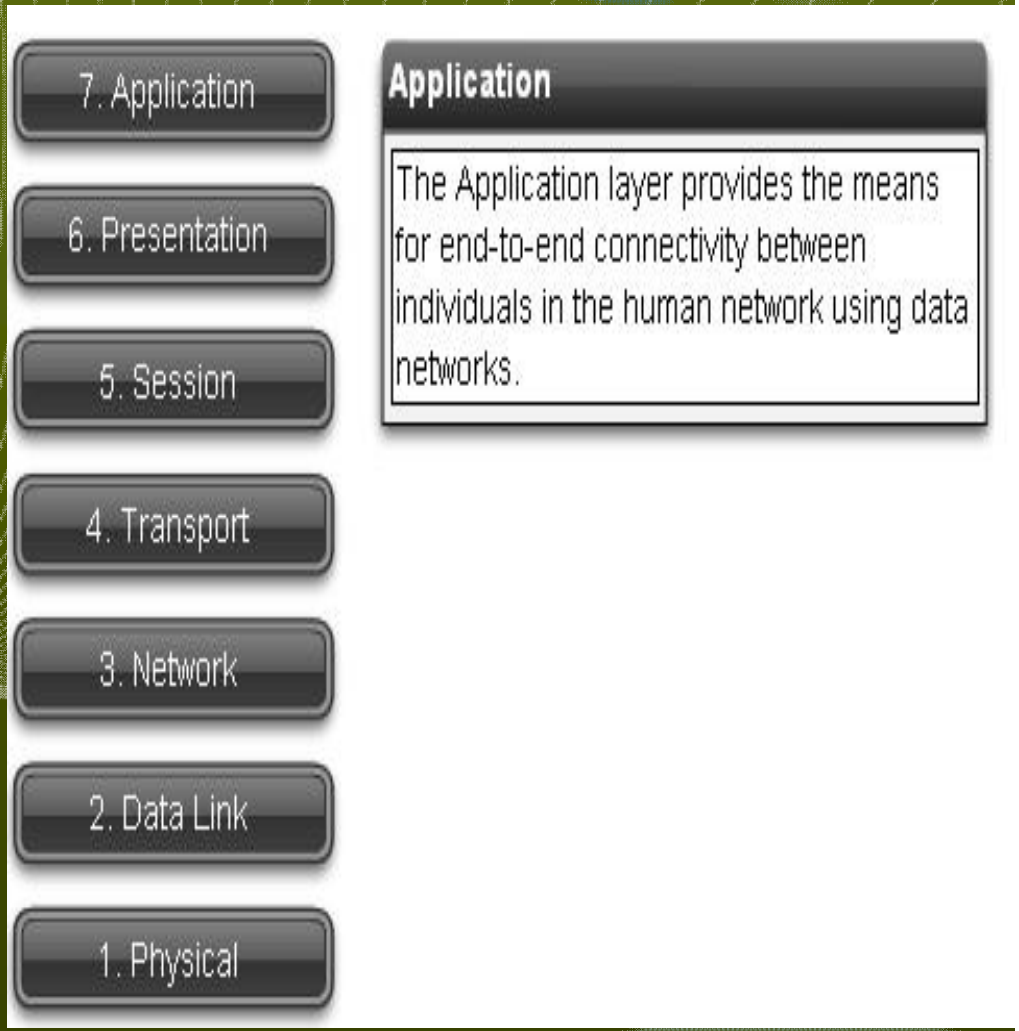
The OSI Reference Model

- The OSI reference model is the primary model for network communications.
- Allows you to view the network functions that occur at each layer.
- It is a framework that you can use to understand how information travels throughout a network
- 7 layers -- each of which illustrates a particular network function.



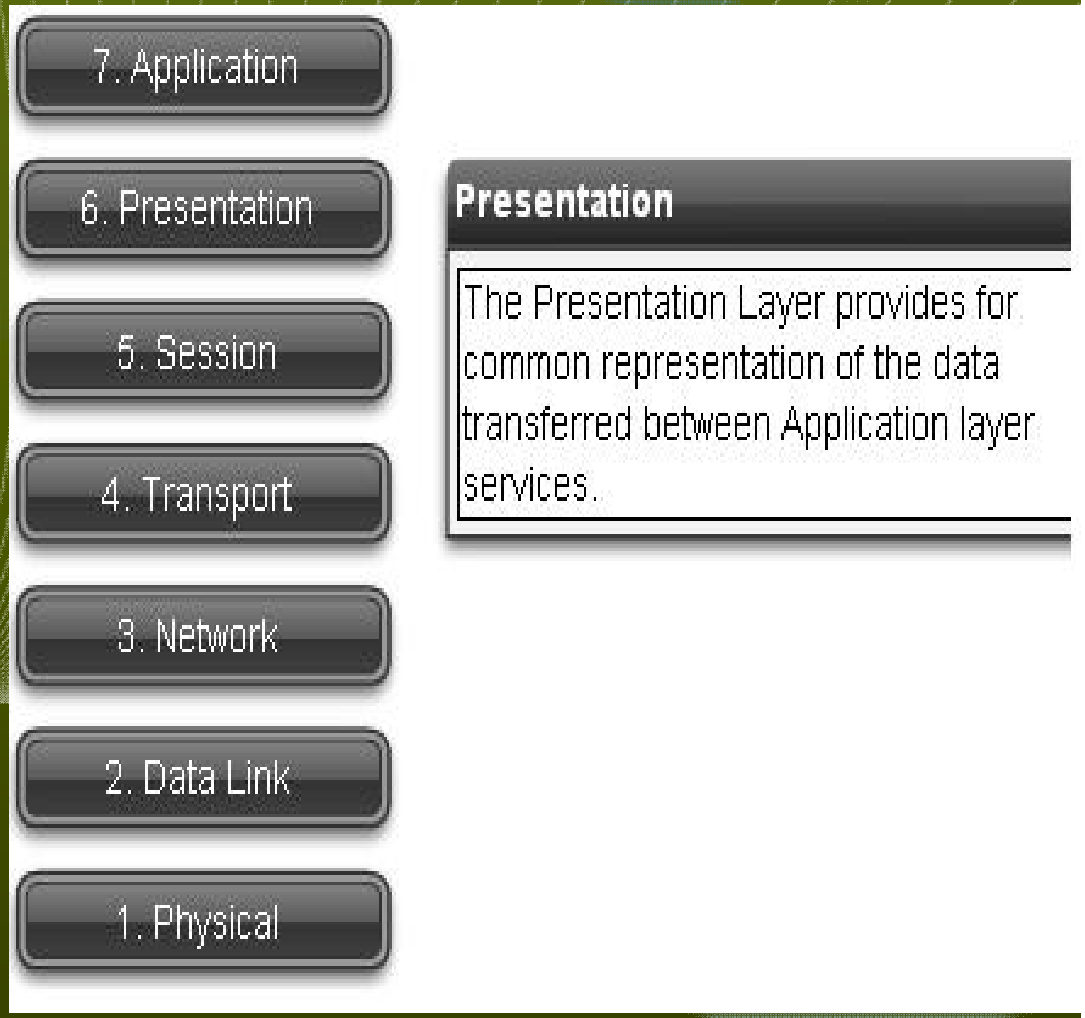
OSI – The Application Layer

- Provides network services to the user's applications.
- It does not provide services to any other OSI layer
- ***Think of any network application you use daily



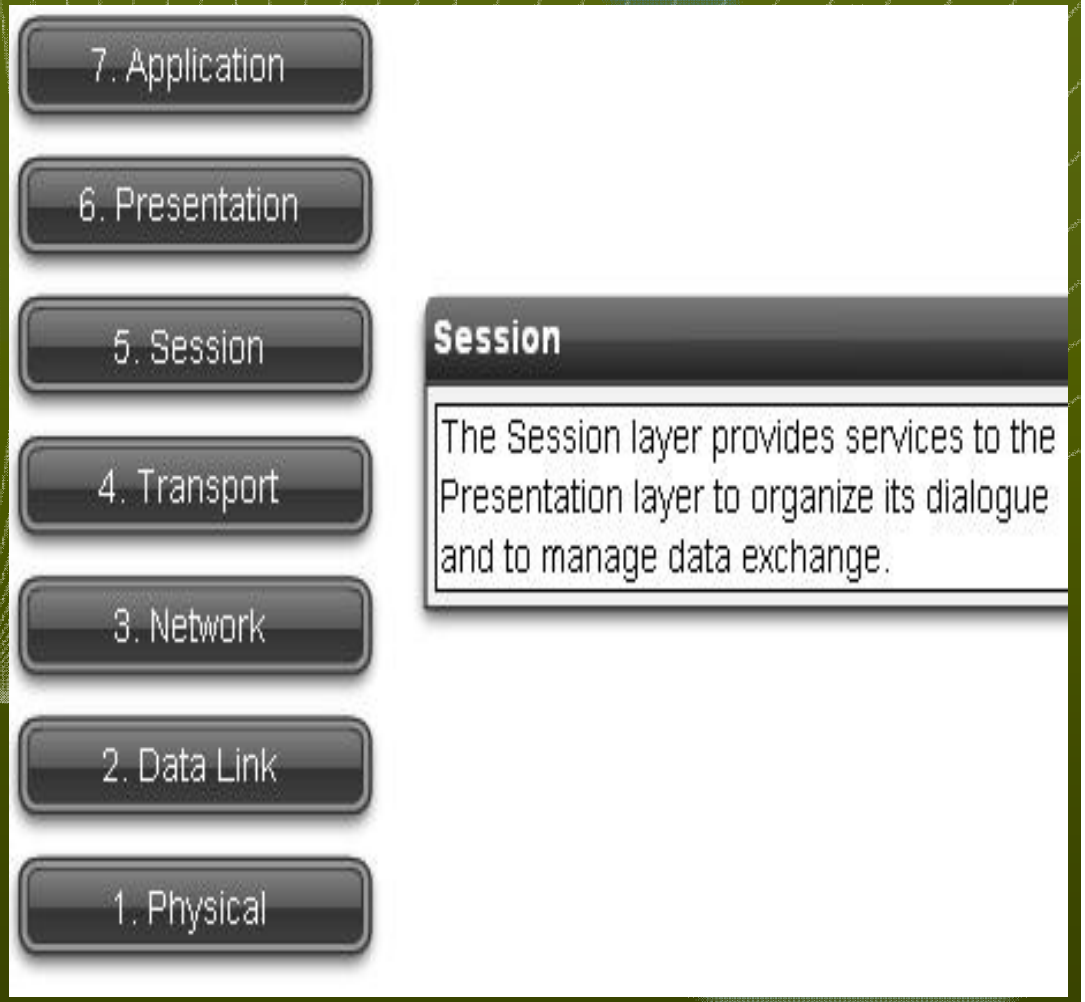
OSI – The Presentation Layer

- It ensures that the information that the application layer of one system sends out is readable by the application layer of another system.
- *** Think of any common file formats (JPEG, txt etc)



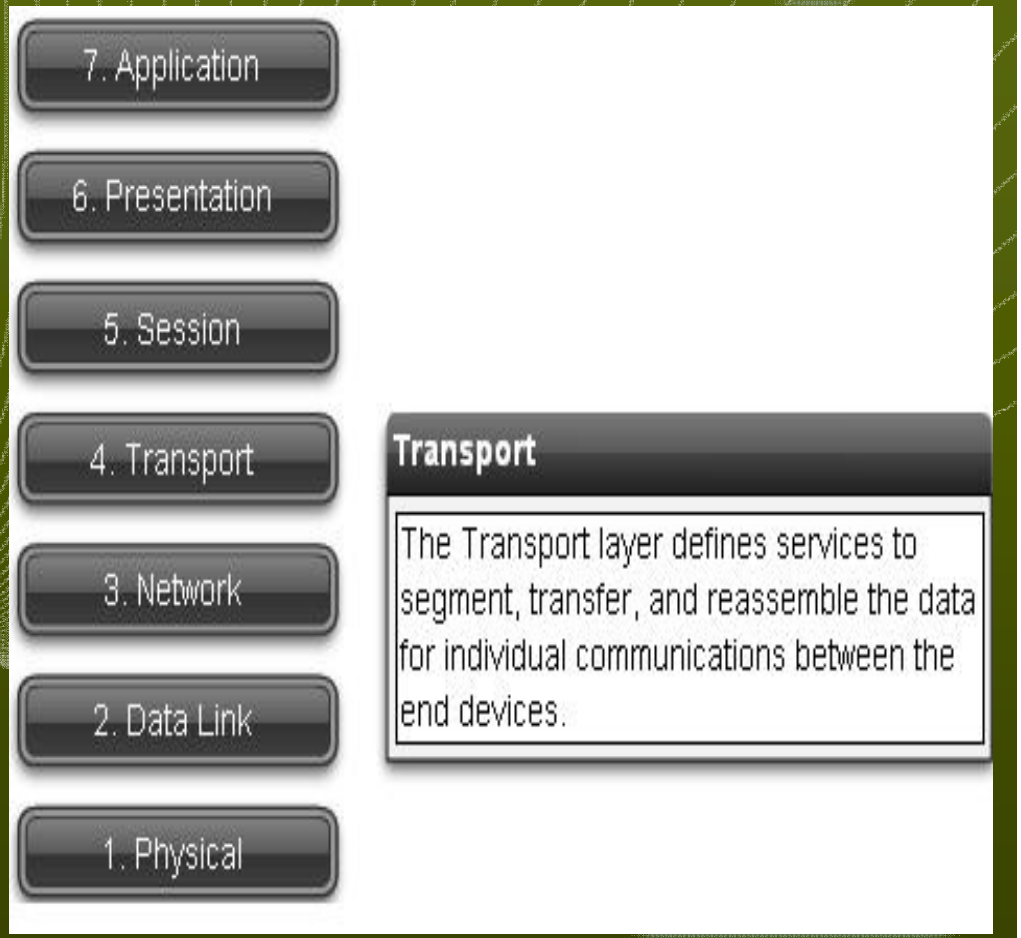
OSI – The Session Layer

- *** After you prepare your data, you need to establish the communication channels to send data
- This layer establishes, manages, and terminates sessions between two communicating hosts.
- It also synchronizes dialogue between the two hosts' presentation layers and manages their data exchange.



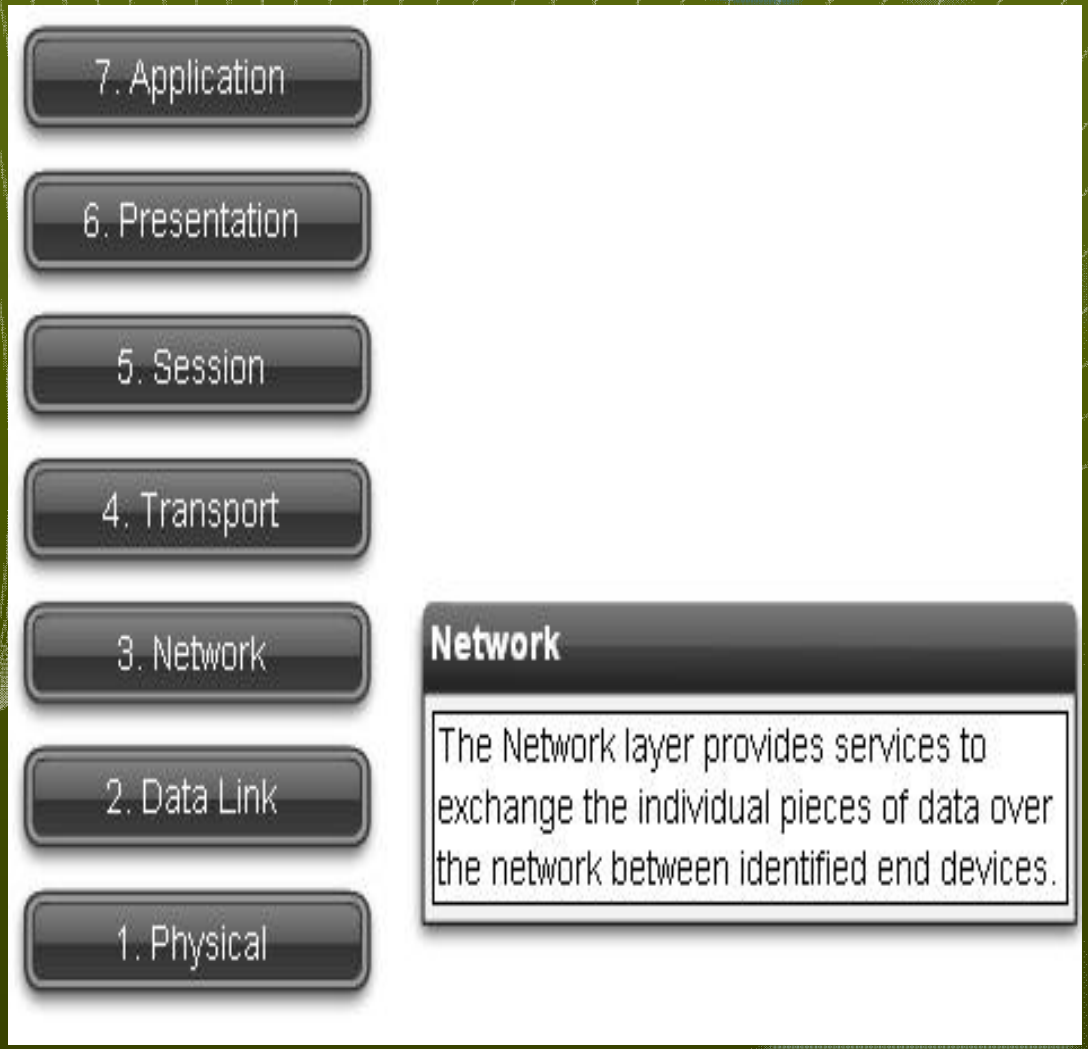
OSI – The Transport Layer

- Data will be segmented and send to destination device. Transport layer of destination device will reassemble them.
- This layer handles details of reliable transfer. (ensures that the data arrive completely)



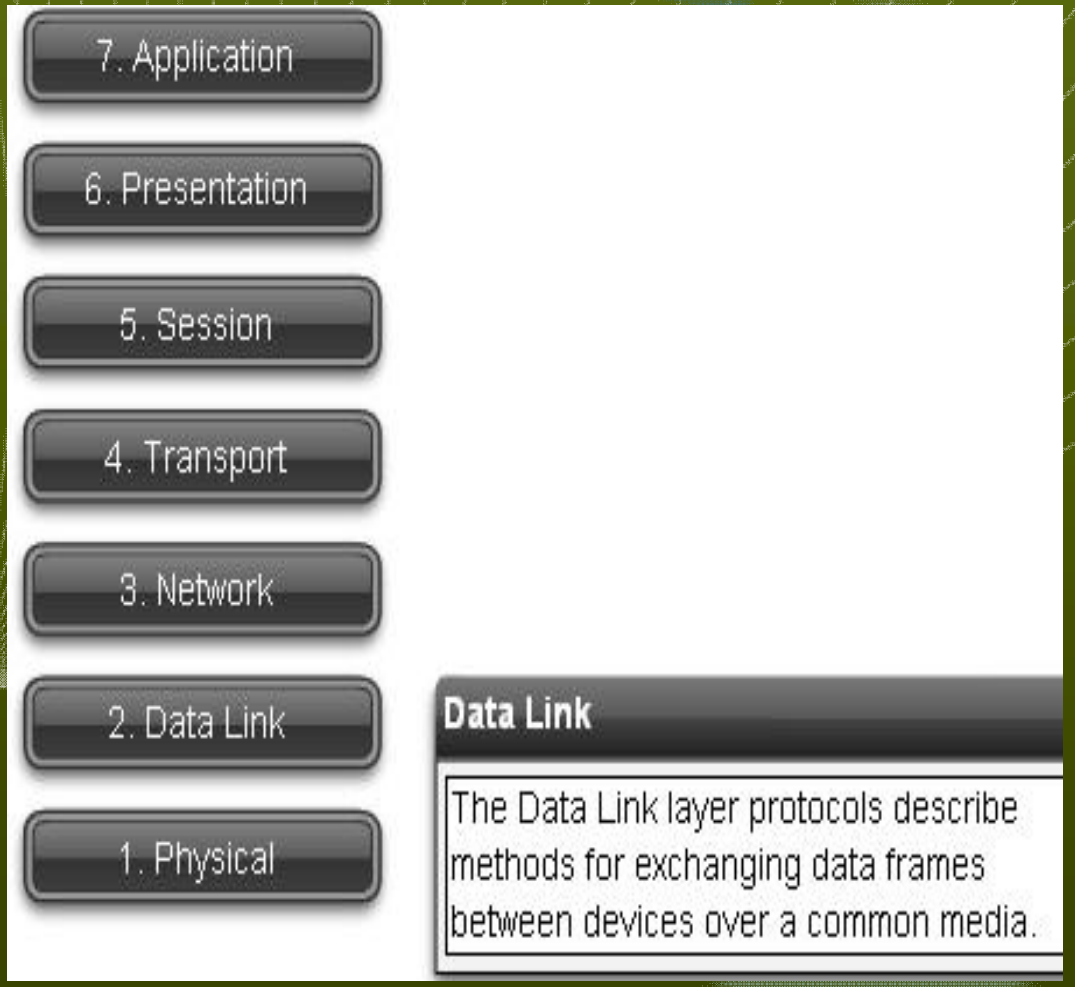
OSI – The Network Layer

- Many paths to the same destination. So, which path to follow?
- Segmented data needs address to reach the destination (network address)
- This layer handle 2 above stated issues.



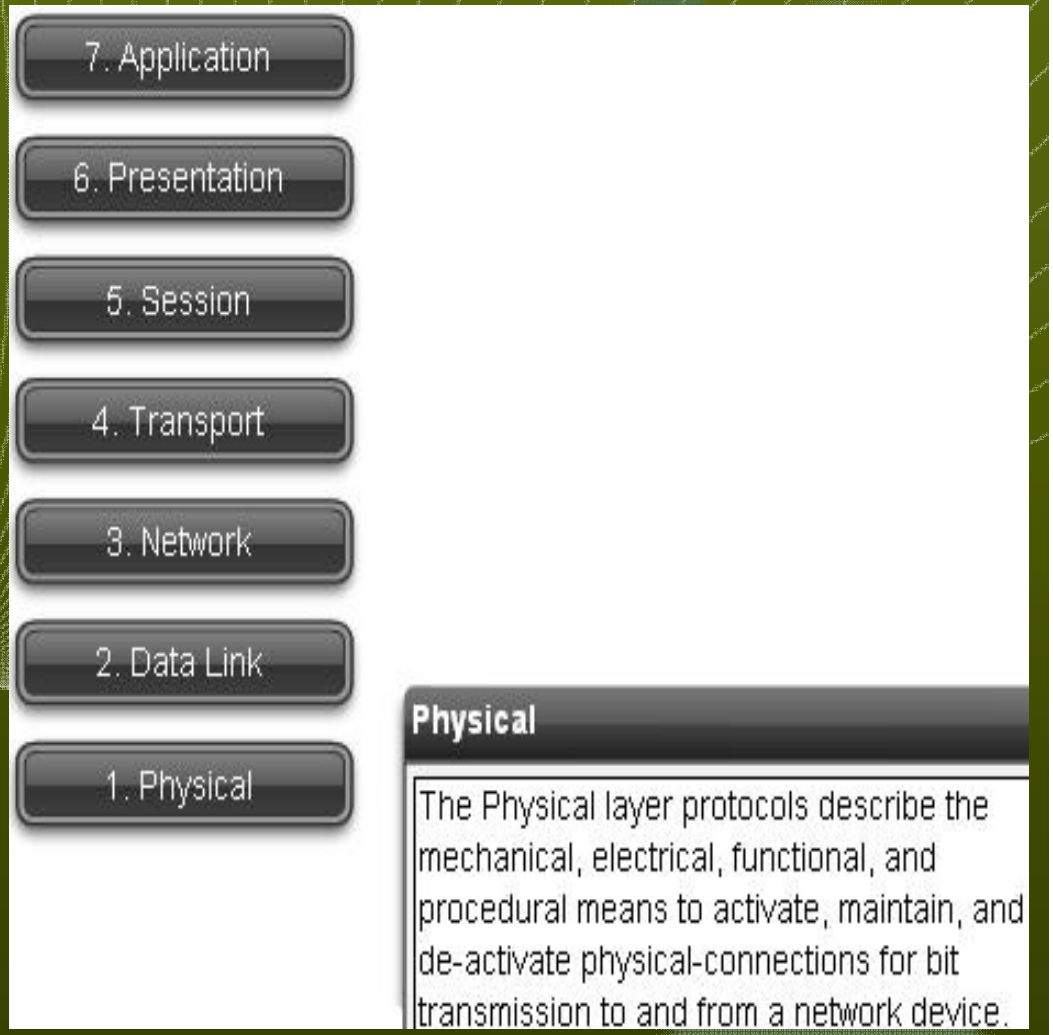
OSI – The Data Link Layer

- It provides means for exchanging data frames over a common media
- To detect and possibly correct errors that may occur in the Physical layer
- Physical Addressing, topologies and flow control

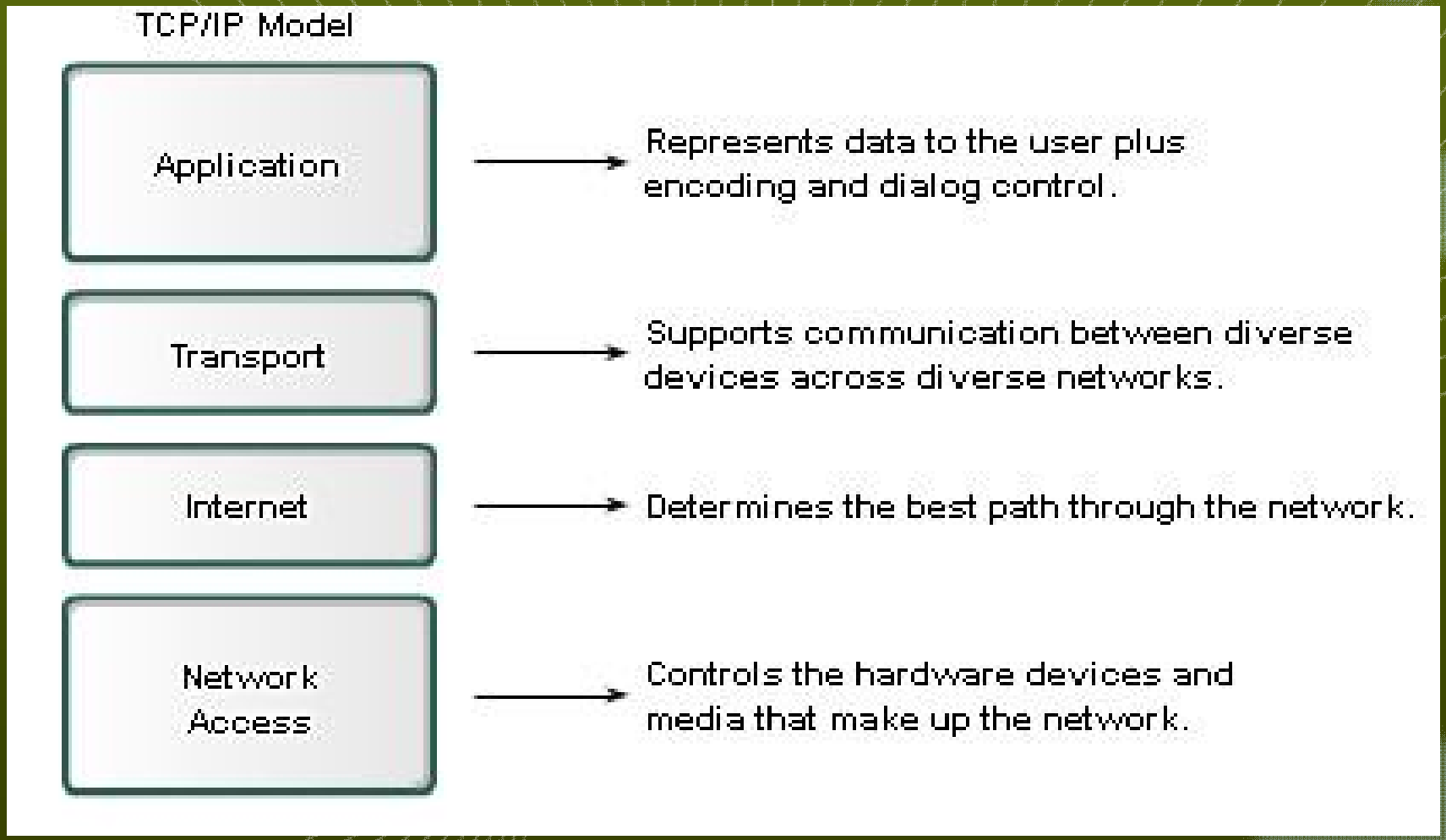


OSI – The Physical Layer

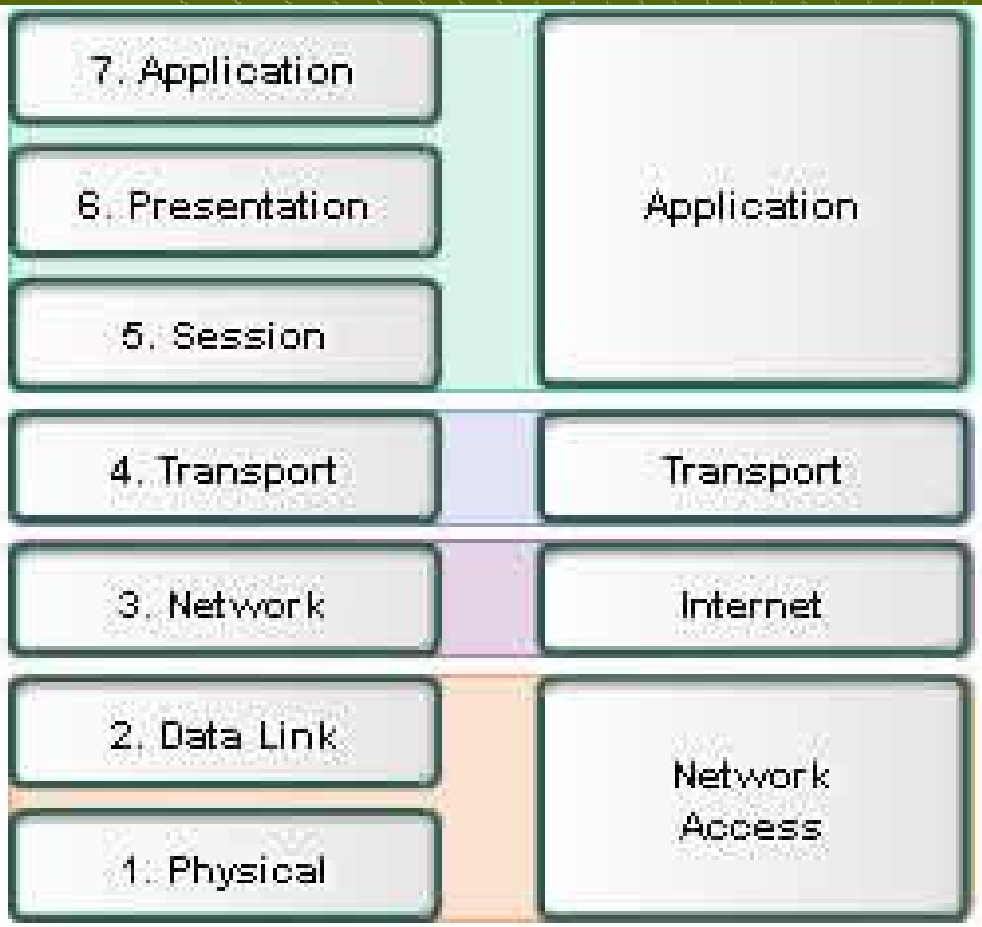
- It defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems.
- Voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other, similar, attributes defined by physical layer specifications.



TCP / IP Model


TCP/IP Model
Application
Represents data to the user plus encoding and dialog control.
Transport
Supports communication between diverse devices across diverse networks.
Internet
Determines the best path through the network.
Network Access
Controls the hardware devices and media that make up the network.

Comparison



The key parallels are in the Transport and Network layers.

--Both have application layers, though they include very different services

--Both have comparable transport and network (Internet) layers

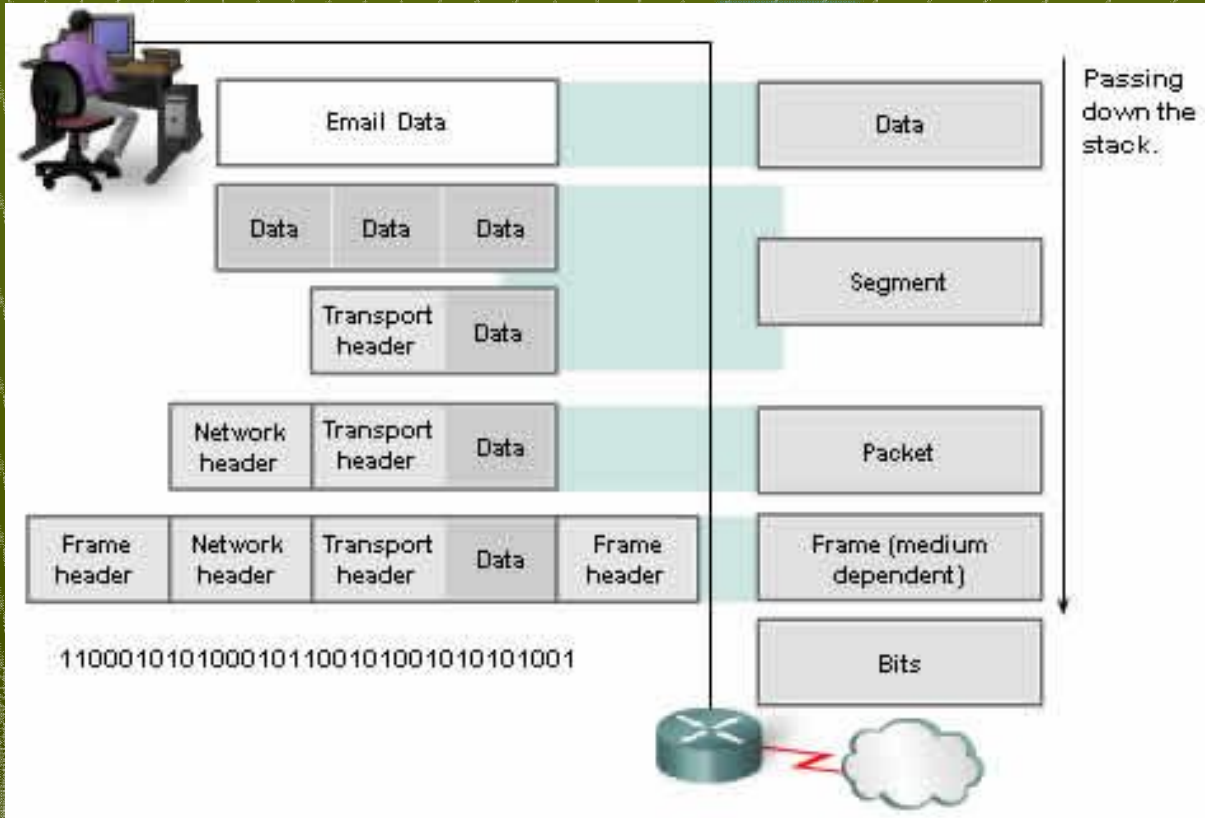
--TCP/IP combines the presentation and session layer issues into its application layer

--TCP/IP combines the OSI data link and physical layers into one layer

--TCP/IP appears simpler because it has fewer layers

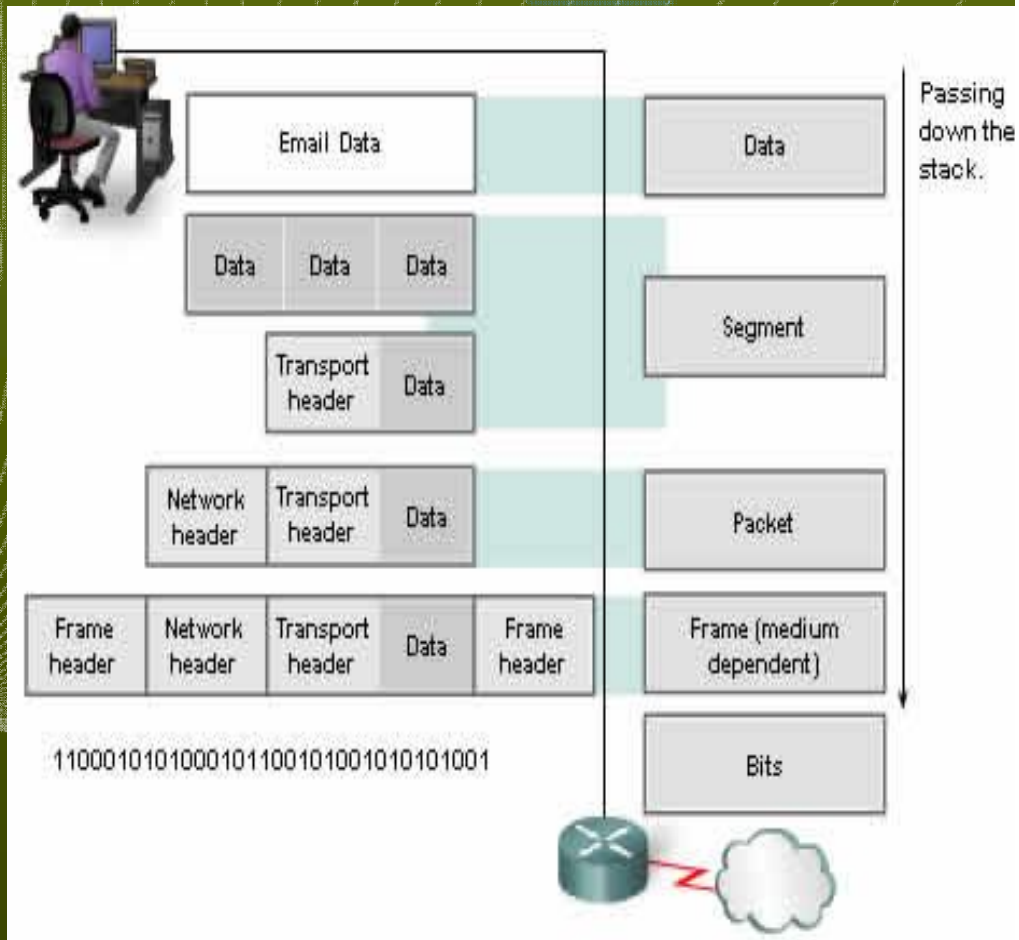
Data Encapsulation

- Build the data
- Package the data for end to end support (Segments)
- The data is put into a packet or datagram that contains a network header with source and destination logical addresses



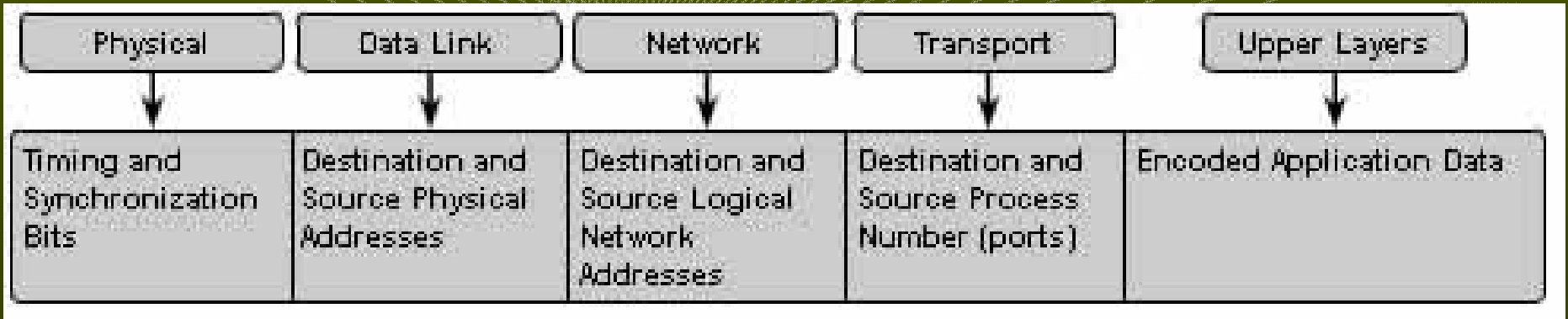
Data Encapsulation

- Each network device must put the packet into a frame.
- The frame must be converted into a pattern of 1s and 0s (bits)
- ***Data → Segments → Packet → Frames → Bits



Addressing in the Network

- There are various types of addresses that must be included to successfully deliver the data from a source application running on one host to the correct destination application running on another



Getting Data to the End Device

- The host physical address, is contained in the header of the Layer 2 PDU, called a frame.
- Layer 2 is concerned with the delivery of messages on a single local network.
- The Layer 2 address is unique on the local network and represents the address of the end device on the physical media.
- In a LAN using Ethernet, this address is called the Media Access Control (MAC) address.
- When two end devices communicate on the local Ethernet network, the frames that are exchanged between them contain the destination and source MAC addresses.
- Once a frame is successfully received by the destination host, the Layer 2 address information is removed as the data is decapsulated and moved up the protocol stack to Layer 3.

Getting the Data Through the Internetwork

- Layer 3 protocols are primarily designed to move data from one local network to another local network within an internetwork.
- Layer 3 addresses must include identifiers that enable intermediary network devices to locate hosts on different networks
- At the boundary of each local network, an intermediary network device, usually a router, decapsulates the frame to read the destination host address contained in the header of the packet, the Layer 3 PDU
- Routers use the network identifier portion of this address to determine which path to use to reach the destination host.