Wollo University
Kombolcha Institute of Technology
Department of Software Engineering

Data Communication and Computer Networks

Chapter 04:

NETWORK PROTOCOLS

4.1 Rules and Network Protocols

- A network protocol defines rules and conventions for communication between network devices.
- Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received.
- Some protocols also support message acknowledgment and data compression designed for reliable and/or high-performance network communication.

Network Protocols…

protocols are fundamental to all data communications

Characteristics

- The concepts of distributed processing and computer networking imply that entities in different systems need to communicate.
- We use the terms *entity* and *system* in a very general sense.
  - Examples of entities are
    - ✓ user application programs,
    - ✓ file transfer packages,
    - ✓ data base management systems,
    - ✓ electronic mail facilities, and
    - ✓ terminals.
  - Examples of systems are
    - ✓ computers,
    - ✓ terminals, and
    - ✓ remote sensors

Protocols…

- Note that in some cases the entity and the system in which it resides are coextensive (e.g., terminals)
- In general, an entity is anything capable of sending or receiving information; and
- a system is a physically distinct object that contains one or more entities.
- For two entities to successfully communicate, they must "speak the same language."
- What is communicated, how it is communicated, and when it is communicated must conform to some mutually acceptable set of conventions between the entities involved.

Protocols…

- The set of conventions is referred to as a protocol, which may be defined as
  - ✓ a set of rules governing the exchange of data between two entities.
- A Network *protocol* is a set of rules that enables effective communications to occur.
- Network protocols are layered such that each one relies on the protocols that underlie it
- Sometimes referred to as a **protocol stack**

The key elements of a protocol are

- **Syntax**: Includes such things as data format, coding, and signal levels.
- **Semantics**: Includes control information for coordination and error handling.
- **Timing**: Includes speed matching and sequencing

Cont…

Network protocols provide the following services:

- addressing and routing information,
- error checking,
- requesting retransmissions, and
- Establishing rules for communicating in a particular networking environment.

- These services are also called link services.

Cont…

- Modern protocols for computer networking all generally use packet switching techniques to send and receive messages in the form of *packets.*
  - ***Packet switching***, using the Internet protocol (IP), accepts data packets from multiple users at many different cell sites and routes them to the next appropriate router on the network.
  - ***Packets*** are messages subdivided into pieces that are collected and re-assembled at their destination.
  - **The Internet and most other data networks work by organizing data into small pieces called** *packets.*

Characteristics of Protocols

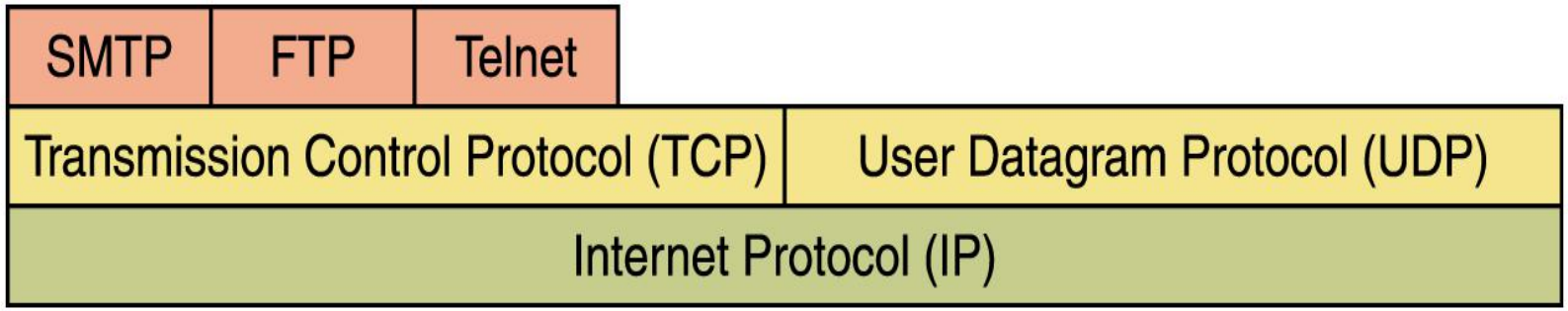
Three basic characteristics that distinguish one type of protocol from another are:

1. **simplex vs. duplex**:
   - A simplex connection allows only one device to transmit on a network.
   - Conversely, duplex network connections allow devices to both transmit and receive data across the same physical link.
2. **connection-oriented or connectionless:**
   - A connection-oriented network protocol exchanges (a process called a *handshake*) address information between two devices that allows them to carry on a conversation (called a *session*) with each other.
   - Conversely, connection-less protocols deliver individual messages from one point to another without regard for any similar messages sent before or after (and without knowing whether messages are even successfully received).

Characteristics of Protocols…

3. **layer**:

- Network protocols normally work together in groups (called *stacks* because diagrams often depict protocols as boxes stacked on top of each other).



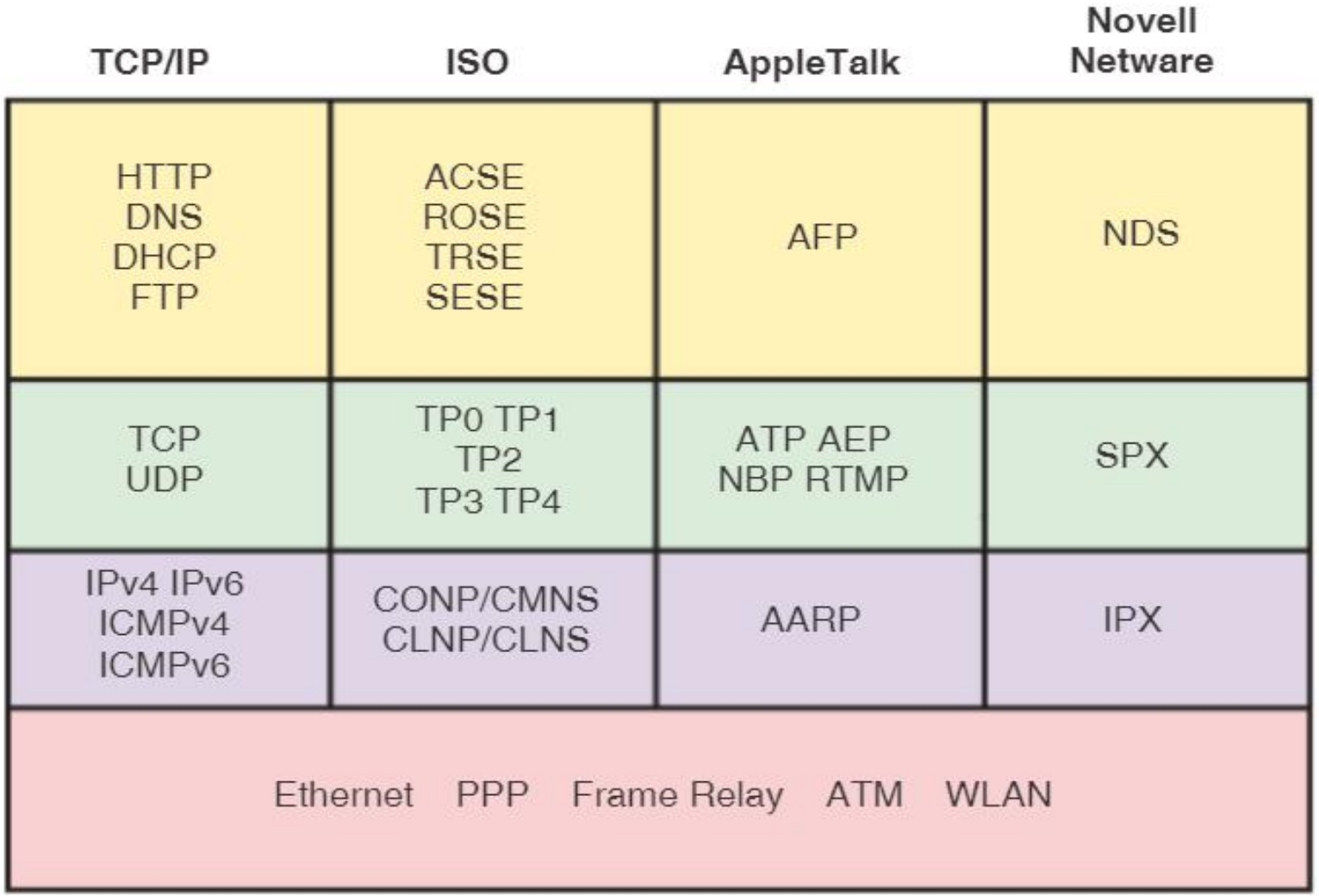
- Some protocols function at lower layers closely tied to how different types of wireless or network cabling physically works.
- Others work at higher layers linked to how network applications work, and some work at intermediate layers in between.

- If a protocol is not rigidly observed by a particular manufacturer, their equipment or software may not be able to successfully communicate with products made by other manufacturers.
- In data communications, for example, if one end of a conversation is using a protocol to govern one-way communication and the other end is assuming a protocol describing two-way communication, in all probability, no data will be exchanged.
- some protocols are proprietary. Proprietary, in this context, means that one company or vendor controls the definition of the protocol and how it functions.

- Some proprietary protocols can be used by different organizations with permission from the owner.
- Others can only be implemented on equipment manufactured by the proprietary vendor. Examples of proprietary protocols are *AppleTalk* and *Novell Netware*.
- Several companies may even work together to create a proprietary protocol.
- It is not uncommon for a vendor (or group of vendors) to develop a proprietary protocol to meet the needs of its customers and later assist in making that proprietary protocol an open standard.

- For example, Ethernet was a protocol originally developed by Bob Metcalfe at the XEROX Palo Alto Research Center (PARC) in the 1970s. In 1979, Bob Metcalfe formed his own company, 3COM, and worked with Digital Equipment Corporation (DEC), Intel, and Xerox to promote the "DIX" standard for Ethernet.
- In 1985, the Institute of Electrical and Electronics Engineers (IEEE) published the IEEE 802.3 standard that was almost identical to Ethernet. Today, 802.3 is the common standard used on local-area networks (LANs).
- Another example, most recently, Cisco opened the EIGRP routing protocol as an informational RFC to meet the needs of customers who desire to use the protocol in a multivendor network.

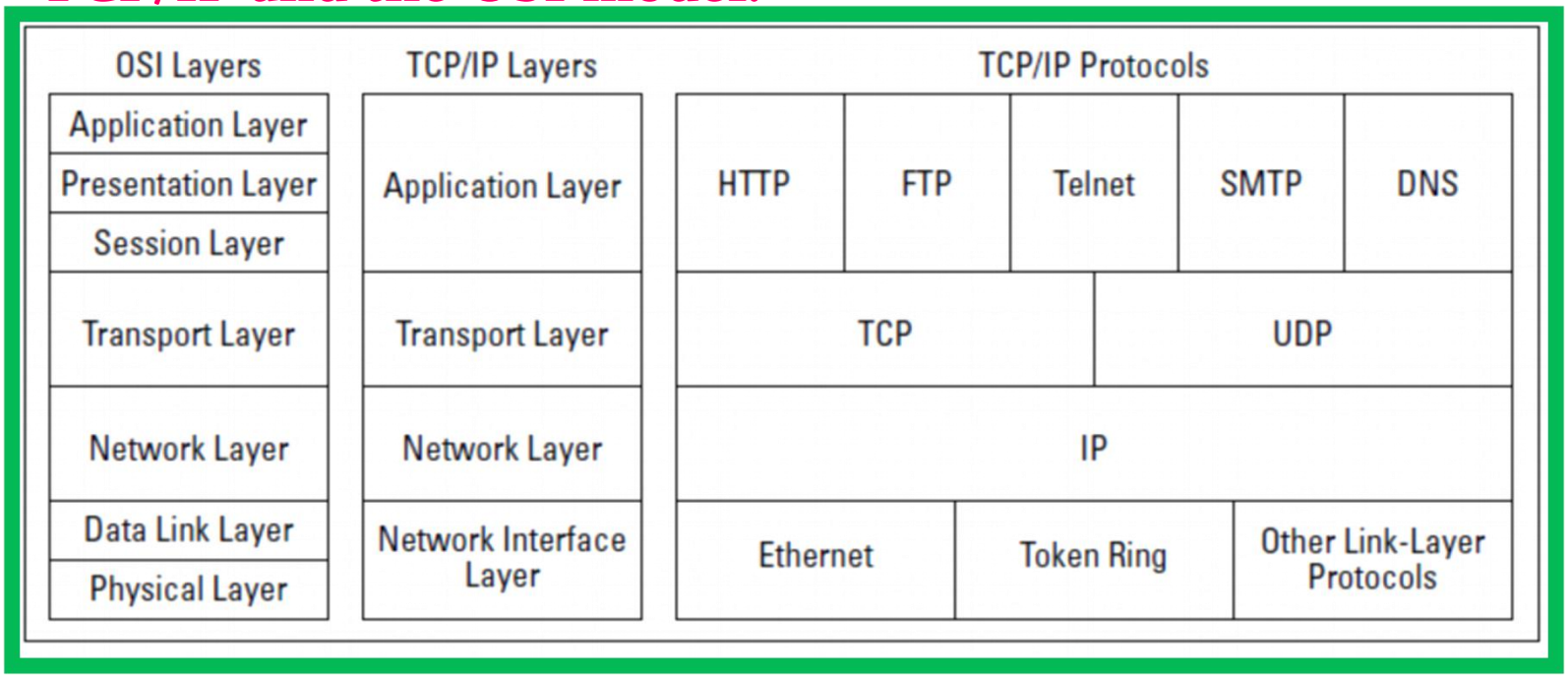
Protocol Suites and Industry Standards



TCP/IP Protocol suites…

- TCP/IP can run over a wide variety of Network Interface layer protocols, including Ethernet, as well as other protocols, such as Token Ring and FDDI (an older standard for fiber-optic networks).

TCP/IP and the OSI model.



TCP/IP Protocol suites…

- The Application layer of the TCP/IP model corresponds to the upper three layers of the OSI model — that is, the
  - Session,
  - Presentation, and
  - Application layers
- Many protocols can be used at this level. A few of the most popular are HTTP, FTP, Telnet, SMTP, DNS, and SNMP.
- The three most important protocols in the TCP/IP suite: IP, TCP, and UDP.

4.3 Layered Models

The Benefit of Using Layered Models

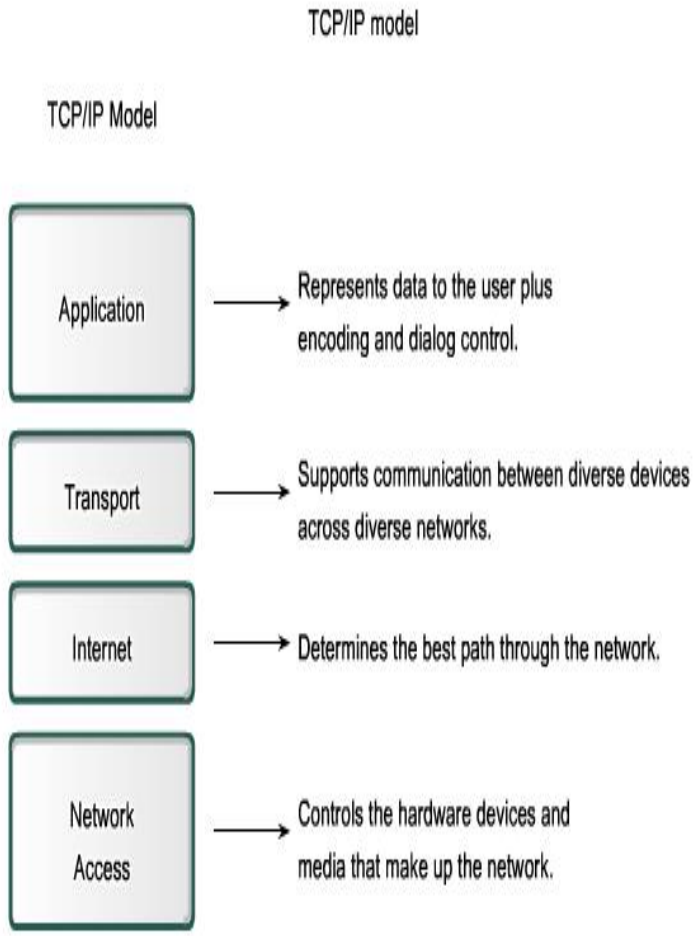
- To visualize the interaction between various protocols, it is common to use a **layered model.**
- A layered model depicts the operation of the protocols occurring within each layer, as well as the interaction with the layers above and below it.
- There are benefits to using a layered model to describe network protocols and operations.
- Using a layered model:
  - ✓ ***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 and Reference model

- There are two basic types of networking models: protocol models and reference 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.
- The TCP/IP model is a protocol model because it describes the functions that occur at each layer of protocols within the TCP/IP suite.
- 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.

4.4 TCP/IP (DoD)Model

- The first layered protocol model for internetwork communications was created in the early 1970s and is referred to as the Internet model.
- It defines four categories of functions that must occur for communications to be successful.
- The architecture of the TCP/IP protocol suite follows the structure of this model.
- Because of this, the Internet model is commonly referred to as the TCP/IP model.



Layers Function

- **The *Process/Application* layer** defines protocols for
  - ✓ node-to-node application communication and also
  - ✓ controls user-interface specifications.
- **The transport (*Host-to-Host) layer*** parallels the functions of the OSI's Transport layer, defining protocols for setting up the level of transmission service for applications.
- **The *Internet layer*** corresponds to the OSI's Network layer, designating the protocols relating to the logical transmission of packets over the entire network.
- The equivalent of the Data Link and Physical layers of the OSI model, the **Network Interface (*Network Access)* layer** oversees hardware addressing and defines protocols for the physical transmission of data.

The process/Application layer

- *Telnet* - allows a user on a remote client machine, called the Telnet client, to access the resources of another machine, the Telnet server.

Telnet makes client machine appear as though it were a terminal directly attached to the server.

- *File Transfer Protocol (FTP)* - is the protocol that actually lets us transfer files, and it can accomplish this between any two machines using it.
  - ✓ Usually users are subjected to authentication
- *Network File System (NFS)* - a protocol specializing in file sharing allowing two different types of file systems to interoperate.
- *Simple Mail Transfer Protocol (SMTP)* - uses a spooled, or queued method of mail delivery.
  - ✓ POP3 is used to receive mail.

The process/Application layer…

- *Simple Network Management Protocol (SNMP)* -collects and manipulates valuable network information. This protocol stands as a watchdog over the network, quickly notifying managers of any sudden turn of events.
- *Domain Name Service (DNS)* – resolves hostnames—specifically, Internet names, such as www.wu.edu.et to the IP address 10.172.76.1
- *Dynamic Host Configuration Protocol (DHCP)* - gives IP addresses to hosts. It allows easier administration and works well in small-to-even-very large network environments

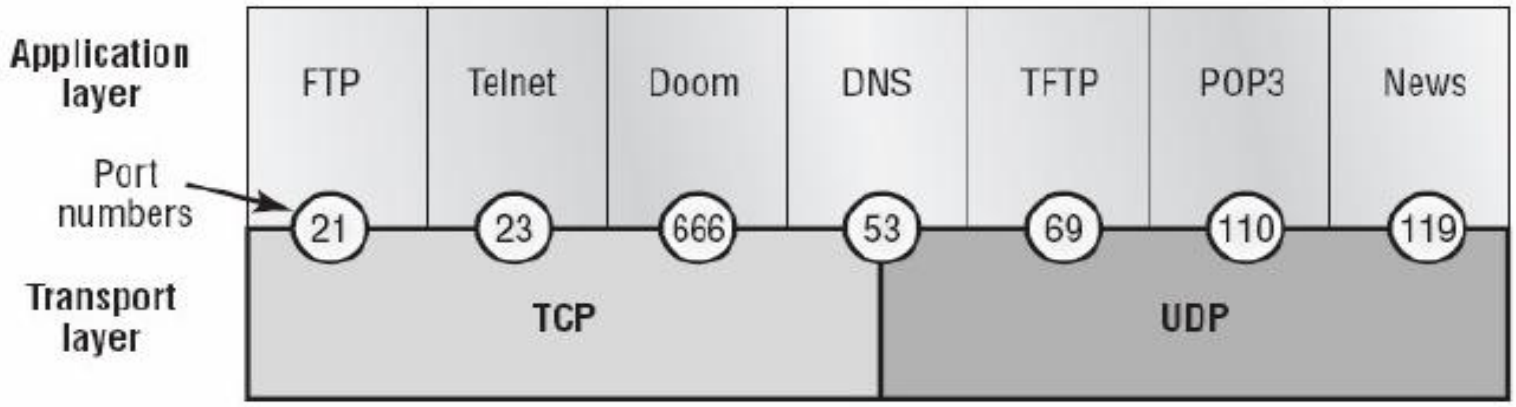
The Host-to-Host Layer

- *Transmission Control Protocol (TCP)* - takes large blocks of information from an application and breaks them into segments.
  - ✓ It numbers and sequences each segment so that the destination's TCP protocol can put the segments back into the order the application intended.
  - ✓ Uses three way handshaking and it is connection-oriented Protocol
- *User Datagram Protocol (UDP)* - does not sequence the segments and does not care in which order the segments arrive at the destination.
  - ✓ But after that, UDP sends the segments off and forgets about them.
  - ✓ It doesn't follow through, check up on them, or even allow for an acknowledgment of safe arrival—complete abandonment.
  - ✓ It is connectionless Protocol
  - ✓ TCP for reliability and UDP for faster transfers.

Port Numbers

- TCP and UDP must use *port numbers* to communicate with the upper layers, because they're what keeps track of different conversations crossing the network simultaneously.
- These port numbers identify the source and destination application or process in the TCP segment.
- There are 2^16 = 65536 ports available.
- Well-known ports - The port numbers range from 0 to 1023.
- Registered ports - The port numbers range from 1024 to 49151.
- Registered ports are used by applications or services that need to have consistent port assignments.
- Dynamic or private ports - The port numbers range from 49152 to 65535.
- These ports are not assigned to any protocol or service in particular and can be used for any service or application.
- If a port is closed/blocked, you cannot communicate with the computer by the protocol using that port.
- Eg. If port 25 is blocked you cannot send mail.
- Firewalls by default block all ports.
- You should know the port numbers of different protocols!!

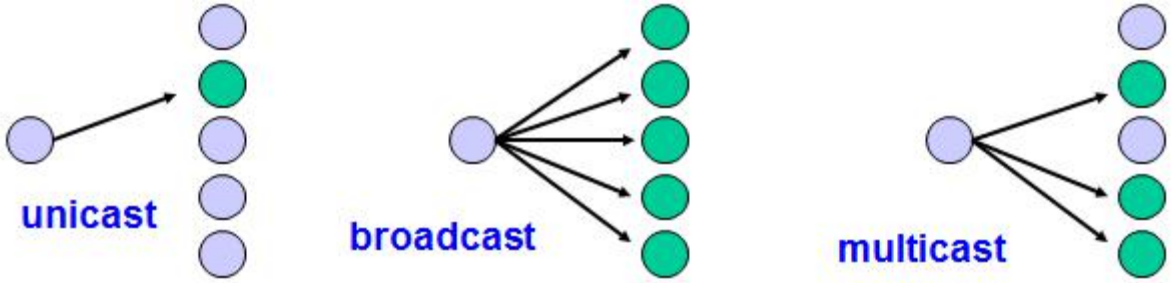
Port Numbers…



TCP Ports	UDP Ports
Telnet 23	SNMP 161
SMTP 25	TFTP 69
HTTP 80	DNS 53
FTP 21	POP3 110
DNS 53	
HTTPS 443	
SSH 22	

The Internet Protocol

- *Internet Protocol (IP)*-essentially is the Internet layer.
  - ✓ The other protocols found here merely exist to support it.
  - ✓ It can do this because all the machines on the network have a software, or logical, address called an IP address.
- IP supports the following services:
  - one-to-one (unicast)
  - one-to-all (broadcast)
  - one-to-several (multicast)



- *IP multicast also supports a many-to-many service.*
- *IP multicast requires support of other protocols (IGMP (Internet Group Management Protocol), multicast routing)*

The Internet Protocol

- *Internet Control Message Protocol (ICMP)*-works at the Network layer and is used by IP for many different services.
  - ✓ ICMP is a management protocol and messaging service provider for IP.

  The following are some common events and messages that ICMP relates to:

  - ✓ **Destination Unreachable :**If a router can't send an IP datagram any further, it uses ICMP to send a message back to the sender, advising it of the situation.
  - ✓ **Buffer Full :**If a router's memory buffer for receiving incoming datagrams is full, it will use ICMP to send out this message until the congestion abates.

Cont…

- ✓ **Hops:** Each IP datagram is allotted a certain number of routers, called hops, to pass through. If it reaches its limit of hops before arriving at its destination, the last router to receive that datagram deletes it. The executioner router then uses ICMP to send an obituary message, informing the sending machine of the demise of its datagram.
- ✓ **Ping:**(Packet Internet Groper) uses ICMP echo messages to check the physical and logical connectivity of machines on a network.
- ✓ **Traceroute :**Using ICMP timeouts, Traceroute is used to discover the path a packet takes as it traverses an internetwork.

Cont…

- *Address Resolution Protocol (ARP)* -finds the hardware address of a host from a known IP address.

ARP interrogates the local network by sending out a broadcast asking the machine with the specified IP address to reply with its hardware address.

- *Reverse Address Resolution Protocol (RARP)*-discovers the identity of the IP address for diskless machines by sending out a packet that includes its MAC address and a request for the IP address assigned to that MAC address.

✓ A designated machine, called a *RARP server*, responds with the answer, and the identity crisis is over.

4.5 The OSI Reference Model

- The OSI model presents a layered approach to networking.
- Each layer of the model handles a different portion of the communications process.
- By separating such communications into layers, the OSI model simplified how network hardware and software work together, as well as eased troubleshooting woes by providing a specific method for how components should function.
- The OSI Reference Model divides networking into seven layers, as shown in figure depicted below.
- Open system interconnection (OSI) model is a framework for defining standards for linking heterogeneous computer systems, located anywhere.

The OSI Reference Model…

- The OSI model is a theoretical ***blueprint*** that helps us understand how data gets from one user's computer to another.
- It is also a model that helps develop standards so that all of our hardware and software talks nicely to each other.

Why use a reference model?

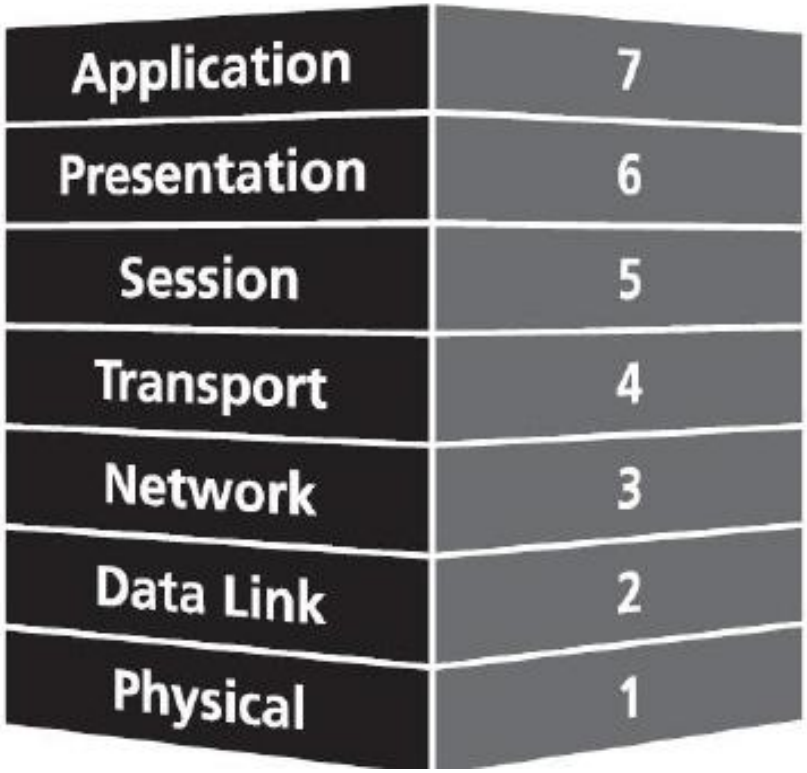
– Serves as an outline of rules for how protocols can be used to allow communication between computers.

– Each layer has its own function and provides support to other layers.

- Other reference models are in use.
  - Most well known is the TCP/IP reference model.

OSI Reference Models

All layers work together in the correct order to move data around a network



Two Sets of Layers

1. Application
    1. Session
    2. Presentation
    3. Application
2. Data Transport
    1. Physical
    2. Data Link
    3. Network
    4. Transport

OSI Model Layer Mnemonics

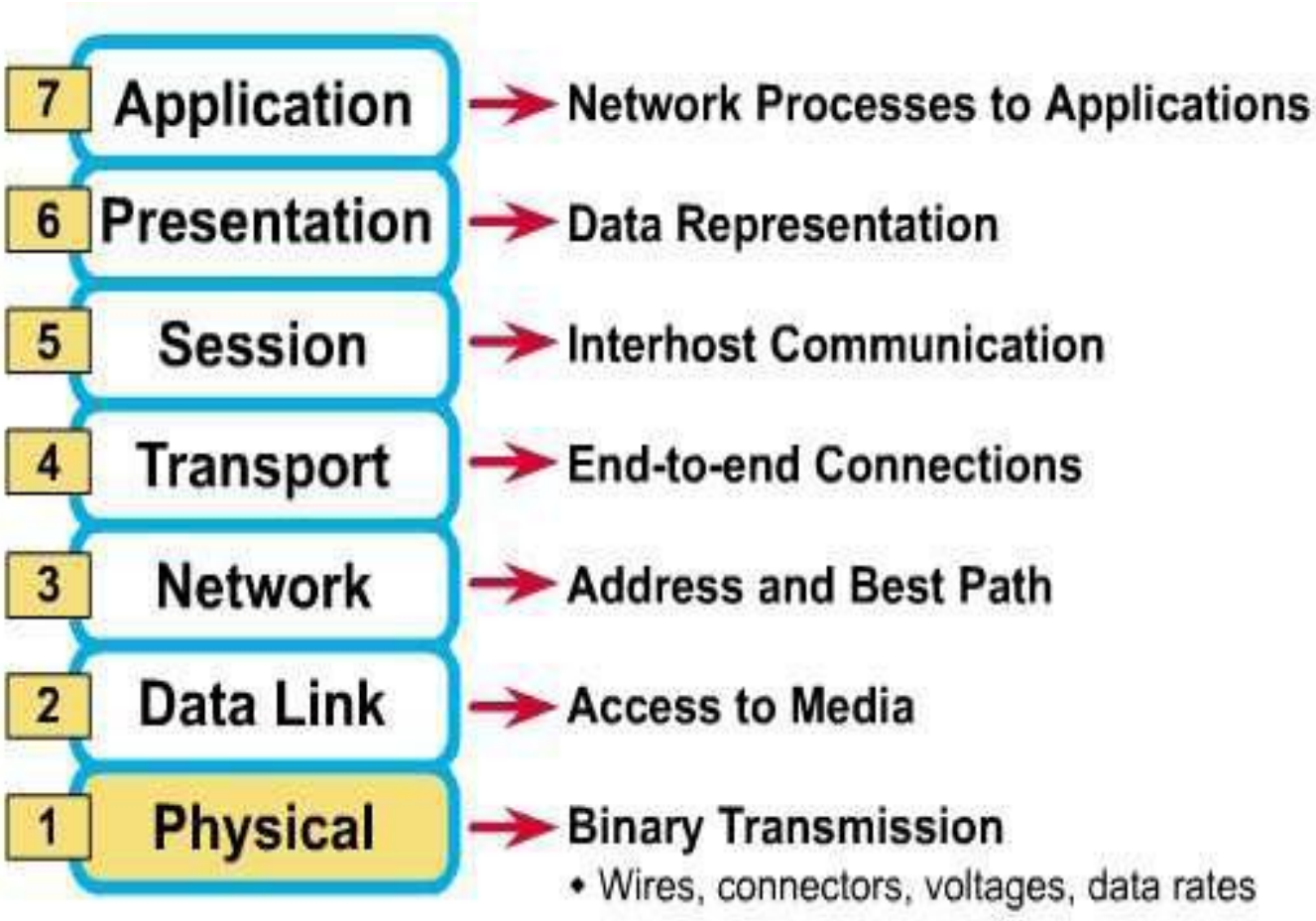
Top to Down

- All People Seem To Need Data Processing

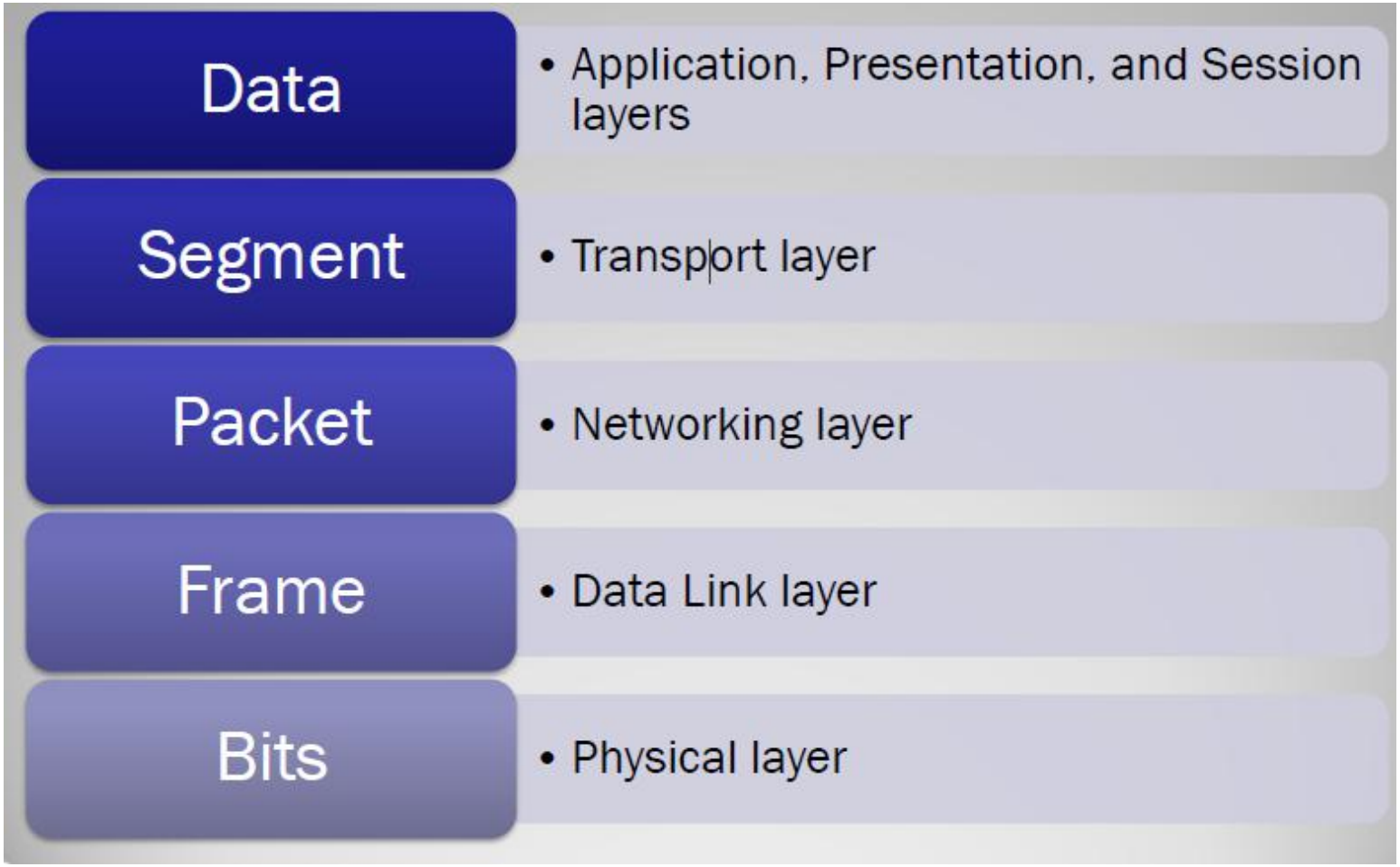
Bottom to Up

- Please Do Not Throw Salihat's Pizza Away

What Each Layer Does



How Data Is Referred to in the OSI Model



Encapsulation/De-encapsulation

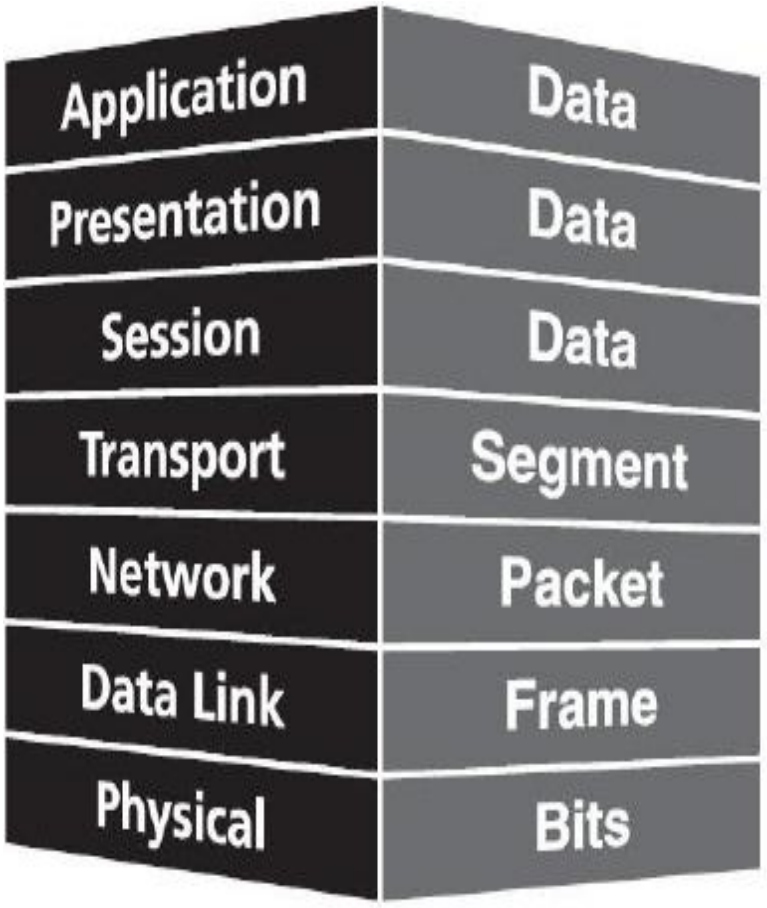
The process of moving data between layers of the OSI Model

Encapsulation:

- ✓ Data > segment > packet > frame > bits

De-encapsulation:

- ✓ Bits > frame > packet > segment > data



Layer 1: The Physical Layer

- The Physical layer manages the interface between a computer and the network medium, and instructs the driver software and the network interface as to what needs to be sent across the medium.
- Deals with all aspects of physically moving data from one computer to the next
- Converts data from the upper layers into 1s and 0s for transmission over media
- Defines how data is encoded onto the media used to transmit the data
- Defined on this layer: Cable standards, wireless standards, and fiber optic standards

The Physical Layer…

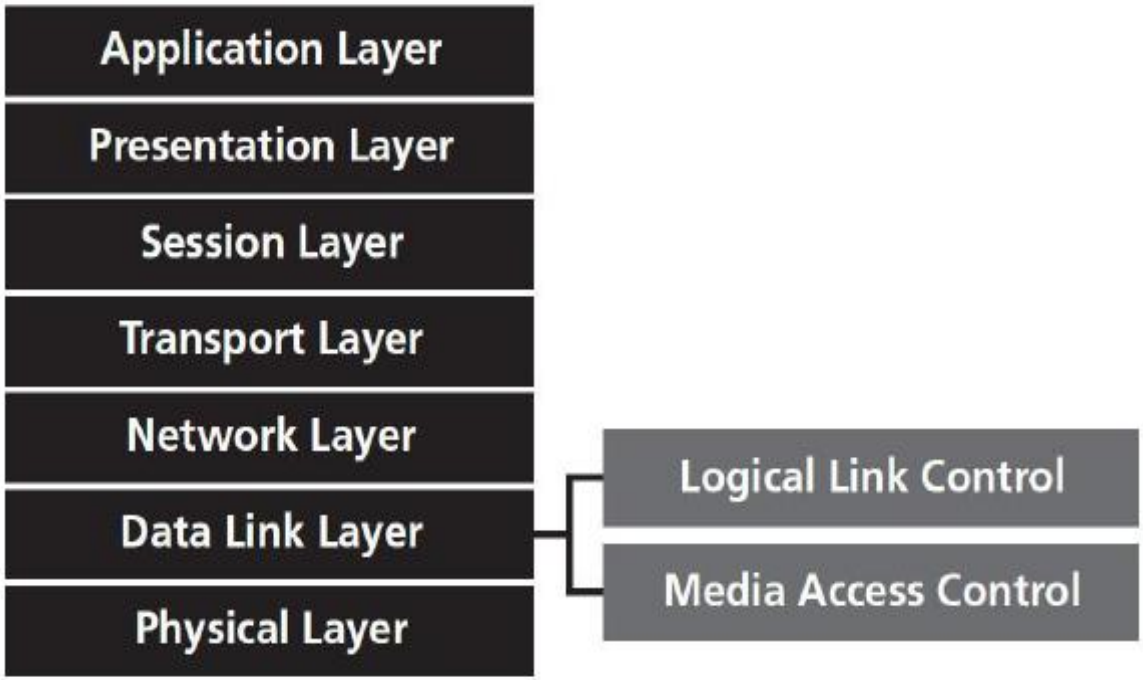
- Device example: Hub
- Used to transmit data
  - ✓Copper wiring, fiber optic cable, radio frequencies, anything that can be used to transmit data is defined on the Physical layer of the OSI Model

Layer 2:Data Link Layer

- Is responsible for moving frames from node to node or computer to computer
- Can move frames from one adjacent computer to another, cannot move frames across routers
- Encapsulation = frame
- Requires MAC address. or *physical address*
- Protocols defined include Ethernet Protocol and Point-to-Point Protocol (PPP)
- Device example: Switch
- Two sublayers: Logical Link Control (LLC) and the Media Access Control (MAC)

Data Link Layer…

Two sublayers: Logical Link Control (LLC) and the Media Access Control (MAC)



LLC and MAC Sublayers

- Logical Link Control (LLC)
  - ✓ Data Link layer addressing, flow control, address notification, error correction
- Media Access Control (MAC)
  - ✓ Determines which computer has access to the network media at any given time
  - ✓ Determines where one frame ends and the next one starts, called frame synchronization

Layer 3: Network Layer

The Network layer

- addresses messages for delivery, and
- translates logical network addresses and names into their physical equivalents.
- decides how to route transmissions between computers.

❑ To decide how to get data from one point to the next, the Network layer considers other factors, such as

- ☑ quality of service information,
- ☑ alternative routes, and
- ☑ Delivery priorities.

Network Layer…

- This layer also handles
  - ☑ packet switching,
  - ☑ data routing, and
  - ☑ network congestion control.
- Responsible for moving packets (data) from one end of the network to the other, called ***end-to-end communications .***
- Requires *logical addresses* such as IP addresses
- Device example: Router
  - Routing is the ability of various network devices and their related software to move data packets from source to destination

Layer 4: Transport Layer

- Takes data from higher levels of OSI Model and breaks it into segments that can be sent to lower-level layers for data transmission.
- Conversely, reassembles data segments into data that higher-level protocols and applications can use.
- Also puts segments in correct order (called sequencing) so they can be reassembled in correct order at destination.
- Concerned with the reliability of the transport of sent data
- May use a *connection-oriented protocol* such as TCP to ensure destination received segments

Transport Layer…

- May use a *connectionless protocol* such as UDP to send segments without assurance of delivery
- Uses port addressing
- provides acknowledgment of successful transmissions and is responsible for requesting retransmission if some packets do not arrive error-free.

Layer 5: Session Layer

- This layer allows two networked resources to hold ongoing communications, called a session, across a network. In a sense ,
  - ✓ applications on each end of the session are able to exchange data for the duration of the session.

This layer manages

- ✓ session setup,
- ✓ information or message exchanges, and
- ✓ tear-down when the session ends.

It is also responsible for

- ✓ identification so that only designated parties can participate in the session, and
- ✓ handles security services for controlling access to session information.

Session Layer…

- The Session layer furnishes synchronization services between tasks at each end of the session.
- It places checkpoints in the data stream so if communications fail, only data after the most recent checkpoint need be retransmitted.
- It also manages issues such as
  - ✓ who may transmit data at a certain time and for how long, and
  - ✓ maintains a connection through transmission of messages that keep the connection active; these messages are designed to the connection to be closed down due to inactivity.

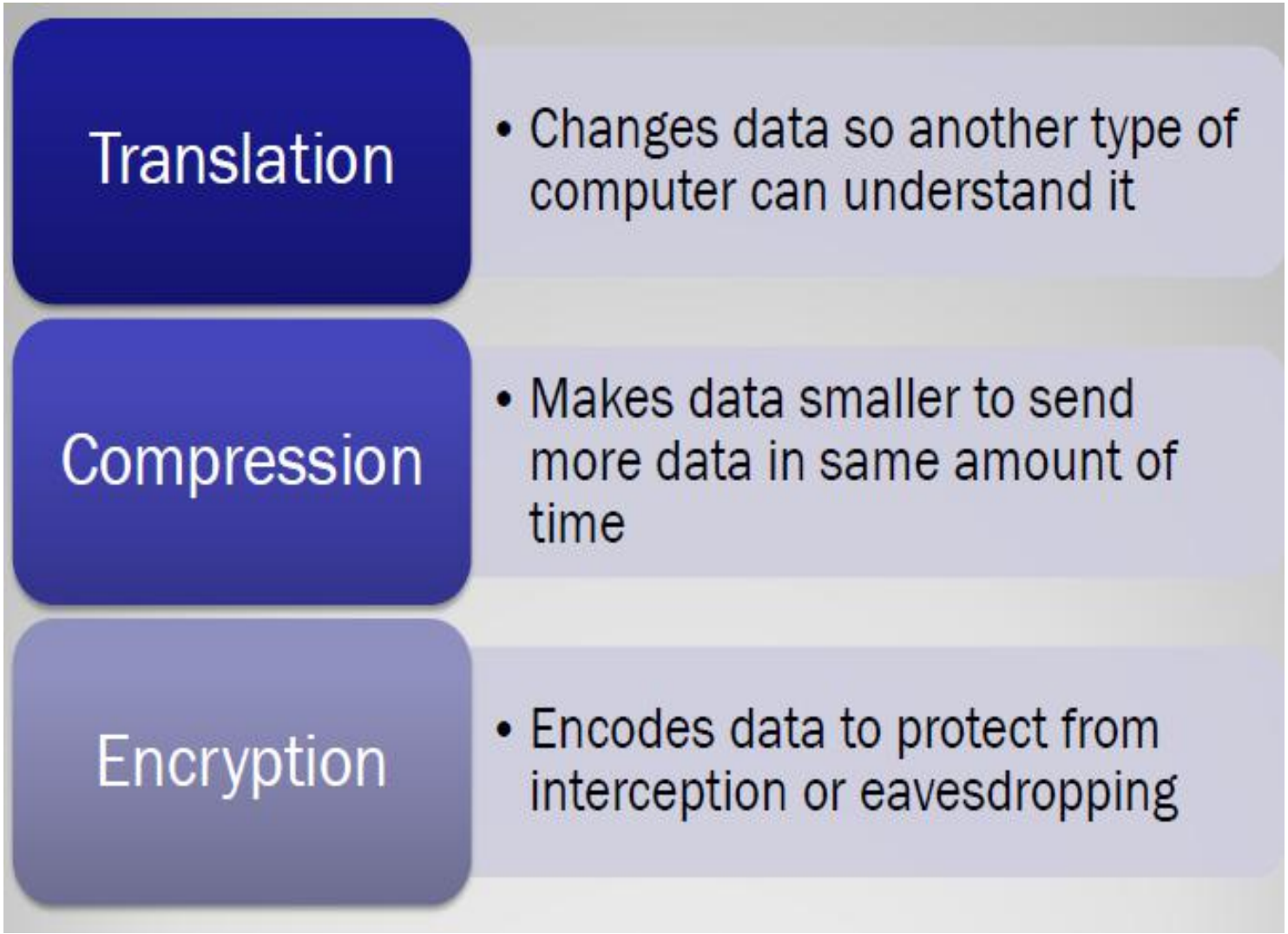
Layer 6: Presentation Layer

- This layer Concerned with how data is presented to the network
- It manages data-format information for networked communications.
- Also called the network's translator,
  - ✓ since it converts outgoing messages into a generic format that can be transmitted across a network; then, it converts incoming messages from that generic format into one that makes sense to the receiving application.
- It is also responsible for
  - ➢ protocol conversion,
  - ➢ data encryption and decryption, and
  - ➢ Graphics commands.

Presentation Layer…

- Information sent by the Presentation layer may sometimes be compressed to reduce the amount of data to be transferred (this also requires decompression on the receiving end).
- At this layer there is a special software facility known as a redirector operates.
  - ✓ The redirector intercepts requests for service and redirects requests that cannot be resolved locally to the networked resource that can handle them.
- Generally it handles three primary tasks:
  - ✓ Translation
  - ✓ Compression
  - ✓ Encryption

Presentation Layer…



Layer 7: Application Layer

- The Application layer is referred to as the top layer of the OSI Reference Model.
- This layer allows
  - **Access to network services**—such as
    - networked file transfer,
    - message handling, and
  - Database query processing—that support applications directly.

It also controls

- ✓ general network access,
- ✓ the transmission of data from sender to receiver (called ***flow control***), and
- ✓ error recovery for applications when appropriate

Application Layer…

- Contains all services or protocols needed by application software or operating system to communicate on the network.
- Examples
  - Firefox web browser uses HTTP (Hyper-Text Transport Protocol)
  - E-mail program may use POP3 (Post Office Protocol version 3) to read e-mails and
  - SMTP (Simple Mail Transport Protocol) to send e-mails

6.7. Comparing OSI Model with TCP/IP Model

1.Compare and contrast these two models with a detail discussion and Please write advantages and disadvantages for respective models?

2. List down IEEE 802 Specifications with their functions?

4.8 Overview of familiar protocols

- **DDP (Delivery Datagram Protocol)** Apple's data transport protocol that is used in AppleTalk
- **AppleTalk Protocol** used for communication with Macintosh computers
- **IP (Internet Protocol)** Part of the TCP/IP protocol suite that provides addressing and routing information
- **IPX (Internetwork Packet Exchange) and NWLink** Novell's NetWare protocol (and Microsoft's implementation of this protocol, respectively) used for packet routing and forwarding
- **NetBEUI** Developed by IBM and Microsoft, it provides transport services for NetBIOS

Some popular network protocols are…

- **APPC**(Advanced Program-to-Program Communication) protocol, developed by IBM, is a peer-to-peer protocol used in IBM's Systems Network Architecture (SNA) for use on AS/400-series computers.
- **X.25** is a set of wide-area protocols that are used in packet-switching networks.
- **HDLC** (High-level Data Link Control) is a flexible, bit-oriented data link protocol that is based on IBM's Synchronous Data Link Control (SDLC).
- **XNS** (Xerox Network System) was created by Xerox for use in Ethernet networks.

CHAPTER END

???