THE OSI & TCP/IP MODELS

CMP 1103 : Information & Communication Technology
Mark Kagarura
Makerere University
markkagarura@gmail.com

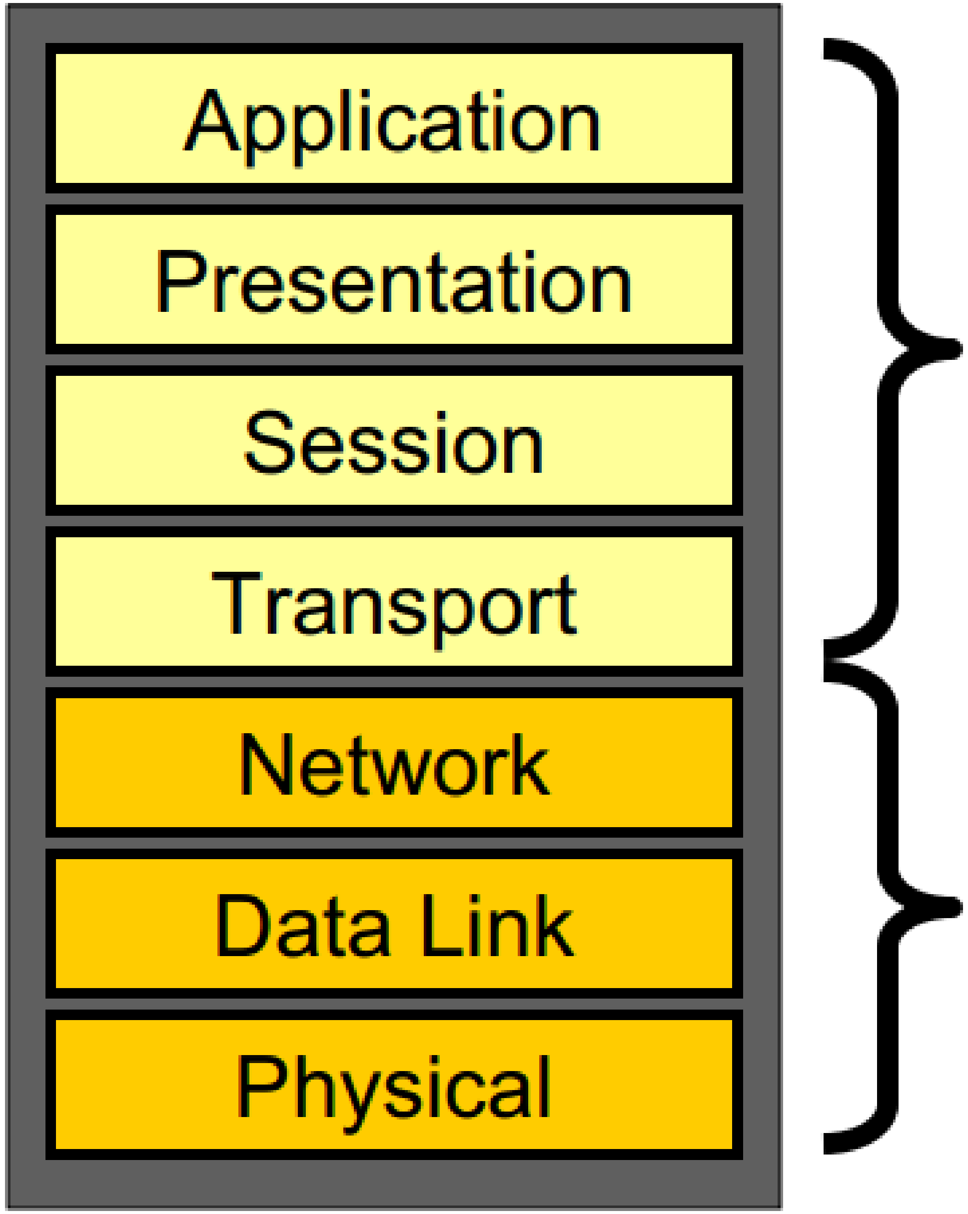
The OSI Model

- OSI stands for Open Systems Interconnection
  - Created by International Standards Organization (ISO) in 1984
- Framework and reference model created to explain how different networking technologies work together and interact
  - The OSI model is a reference tool for understanding data communications between any two networked systems
- Provides a set of design standards for equipment manufacturers to enable inter-communications
- Divides the communications processes into seven layers. Each layer both performs specific functions to support the layers above it and offers services to the layers below it.
  - The three lowest layers focus on passing traffic through the network to an end system.
  - Top four complete the network

The OSI Reference Model

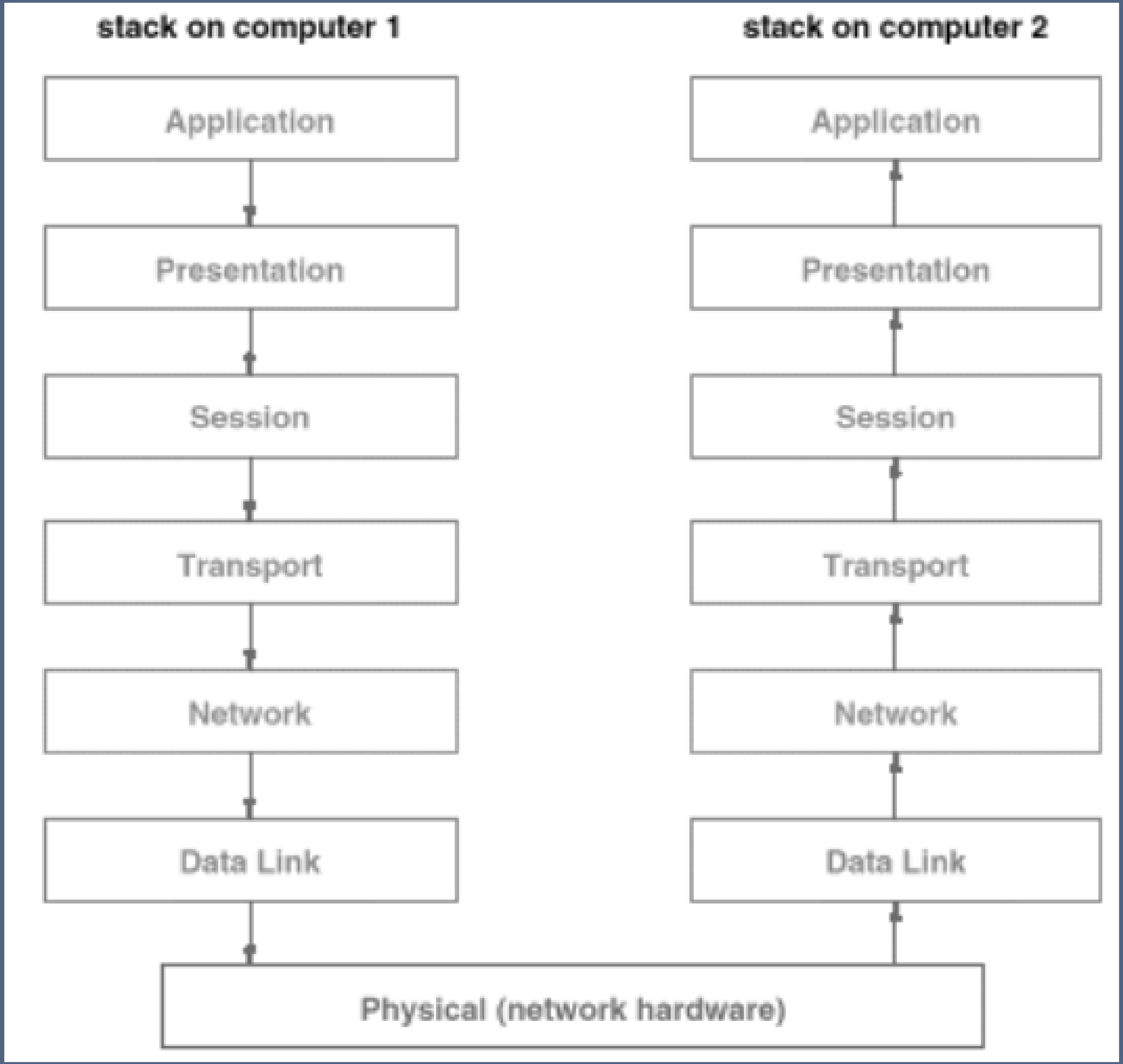
- Principles for the layered Communication (OSI)
  - Layers created for different abstractions
  - Each layer performs well-defined function
  - Function of layer chosen with definition of international standard protocols in mind
  - Minimize information flow across interfaces between boundaries
  - Number of layers optimum
- OSI Reference Model Layers
  - Physical, Data link layer, Network layer, Transport layer, Session layer, Presentation layer, Application layer

Layer	No.	Sender	Role	Receiver
Application	7	Dictates or Writes a Message	Manager	Reads Message
Presentation	6	Proofreads, Corrects and Prepares the Message	Assistant	Alerts Manager of Incoming Message
Session	5	Provides Address. Puts in Envelope	Secretary	Opens Message. Reads it
Transport	4	Drives Letter to Post Office	Driver	Picks up Message from Post Office
Network	3	Takes Letter and Puts in Right Compartment	Intake & Sorting	Sorts Messages
Data Link	2	Pack letter for Individual	Packaging	Unpacks Packages from Various Sources
Physical	1	Delivers letters & packages	Mail Carrier	Picks up letters & packages



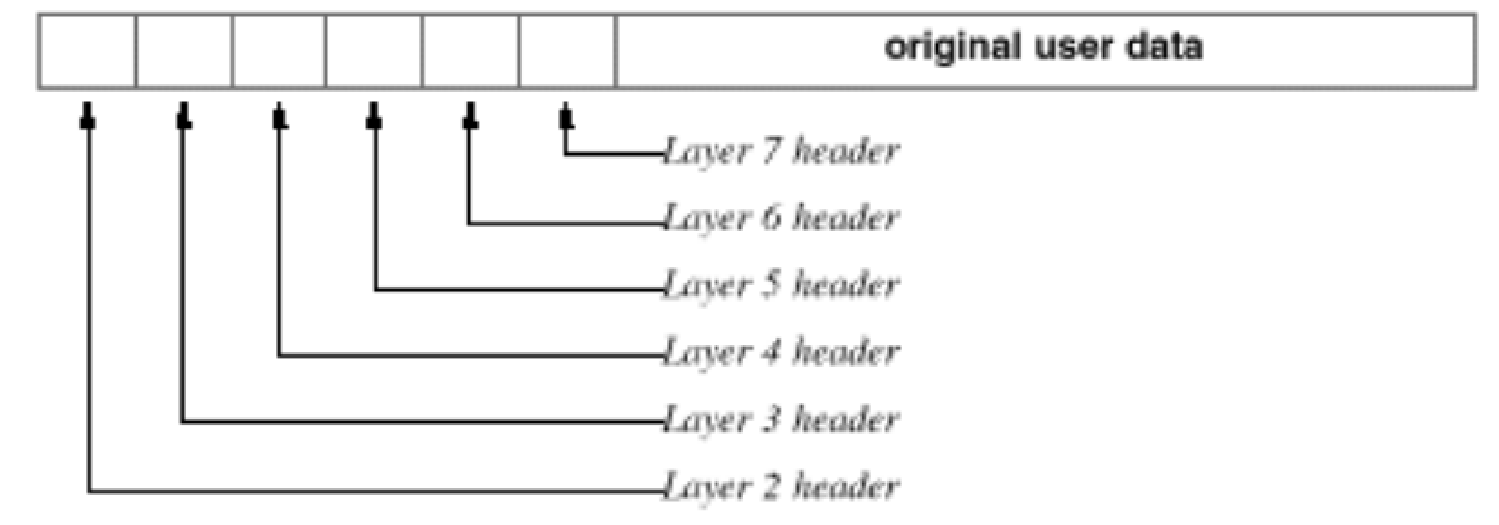
Host Layers: Used whenever a message passes from or to a user

Media Layers: Used whenever any message passes through the host device


stack on computer 1
stack on computer 2
Application
Presentation
Session
Transport
Network
Data Link
Application
Presentation
Session
Transport
Network
Data Link
Physical (network hardware)

How Data Moves Through the OSI Model

- Each layer except Physical adds its own header to data from OS
  - – Header (in front of previous) contains information that describes what each layer of the OSI Model should do with the data
- Data Link layer also adds a trailer (or tailer)
  - – Trailer contains additional information for error correction



Data in the OSI Model

Data	• Application, Presentation, and Session layers
Segment	• Transport layer
Packet	• Networking layer
Frame	• Data Link layer
Bits	• Physical layer

Encapsulation:

- Data > segment >packet > frame >bits

De-encapsulation:

- Bits > frame >packet > segment> data

Protocols

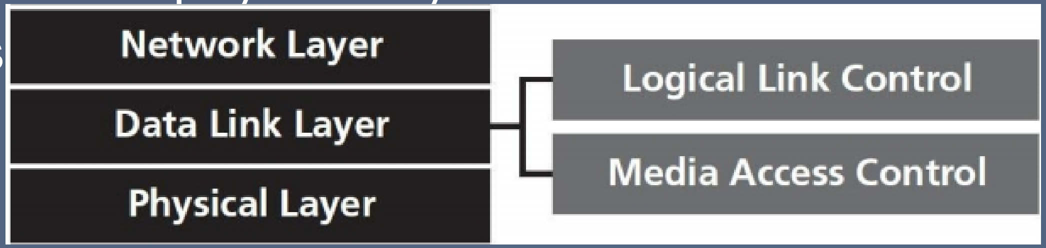
- Define a set of rules for communication
  - Specify the Meaning and Format of messages
  - Define exchange rules
  - Exception handling e.g.
    - duplicities and
    - bit corruption (checksum errors,
    - lost information and
    - out of order packets
  - Other functions
    - Identify different sources/destinations
    - Separate applications
    - Handle multiple instances of the same application on one machine
  - A family of protocols shares all these tasks
    - Protocol suite/stack
    - Assign functions to different protocols (layers)

1. Physical Layer

- Defines optical, electric and mechanical characteristics: voltage levels, timing of voltage changes, physical data rates, transmission distances and physical connections
  - Deals with all aspects of physically moving data from one computer to next
  - Converts data from upper layers to 1s and 0s for transmission over media
  - Defines how data is encoded onto the media used to transmit the data
- Device examples:
  - Hub, RS232, RJ45, RJ11, Ethernet cables, 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
  - Components, adapters, NICs, SCSI, pinouts, panels, connectors

2. Data Link Layer

- Provides error-free transmission line for upper layers between adjacent nodes or computers
  - Responsible for moving frames from node to another.
  - It may perform error control and channel access
- Channel access (control shared communication channel)
  - Requires physical address or MAC to send device's data on network
  - Allows device access the network to send/receive messages (frames)
    - avoid collisions on a network segment, plus filter and forward traffic.
    - Can move frames from one adjacent computer to another, but not across routers
- Data Framing
  - Breaking information into frames and using services of physical layer
  - Ensuring uniqueness and correctness of frames
  - Flow control between sender and receiver



2. Data Link Layer

- Error control: Error free transmission over the link
  - Error detection: Several (other) data links may exist between end points
    - Higher layers may also have error control functions
    - Error-detecting codes e.g. CRC (cyclic redundancy check) to verify integrity
  - Error Correction: Uses error-correcting codes e.g. block codes
  - Positive acknowledgment
  - Retransmission after timeout
- Protocols defined include
  - Ethernet Protocol and
  - Point-to-Point Protocol (PPP)
- Device example: Switch, Network interface cards , Ethernet and Token Ring switches, Bridges

3. Network Layer

- **Responsible for moving packets (data) from one end of the network to the other, called end-to-end communications - r**
- Routing of data packets from source host to destination host
- Controlling network congestion
- Internetworking - multiple heterogeneous networks. The IP addresses enable global network set up/interconnection.
  - – Addressing issues- L2 networks (Ethernet,
  - – Packet sizes (manages different)
  - – Protocol differences (gateways do protocol translation)

3. Network Layer

- Fragmentation and re-assembly
  - The network layer accomplishes change of packets sizes to fit layer 2 via a process known as **fragmentation**.
  - All reassembly of fragmented packets happens at the network layer of the final destination system.
- Device example: Router

  Routing is the ability of various network devices and their related software to move data packets from source to destination
    - Requires logical addresses such as IP addresses
  - Routers /networked systems make routing decisions at the network layer
  - Routing protocols used to learn of other networks present and to calculate the best way to reach each network based on a variety of criteria (such as the path with the fewest routers).

4. Transport Layer

- Provides for reliable exchange of information between end systems:
  - Ensures error free data stream, in-sequence delivery without loss or duplication
- Reliability of the transport of sent data (QoS Management)
  - Provides acknowledgment of successful transmissions
  - Requests retransmission if some packets don't arrive error-free
    - Uses Acknowledgements and timeouts
    - connection-oriented data stream
- Provides flow control and sequencing
  - Orders segments (sequencing) for correct reassembly at destination
  - breaks data from higher layers it into segments to lower-layers for TX
  - Reassembles data segments into data that higher-level protocols/applications
- Uses port addressing
  - E.g 80: HTTP, 23 Telnet etc

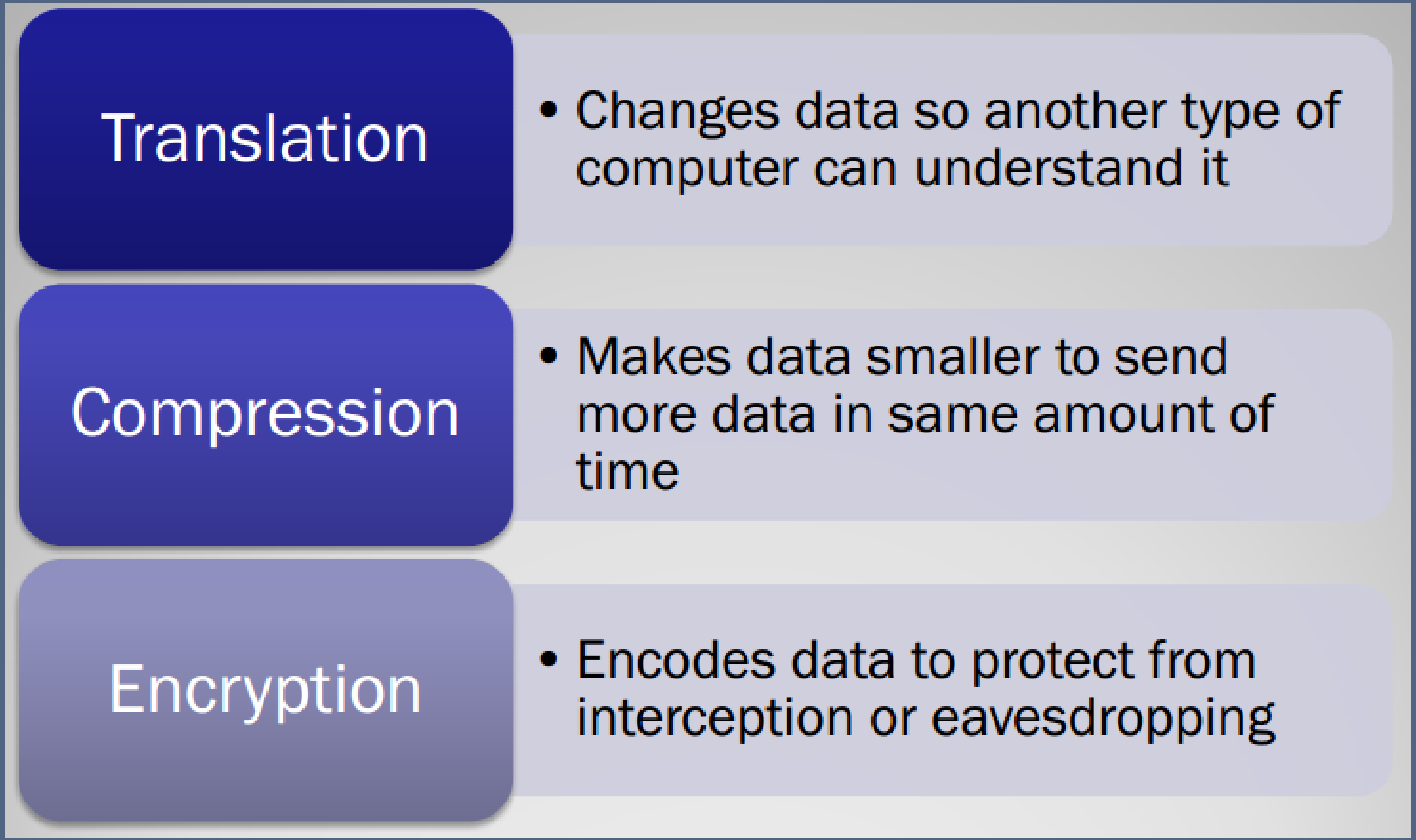
5. Session Layer

- Establishes, maintains and ends sessions across the network
- Responsible for managing the dialog between networked devices
  - Manages who can transmit data at a certain time and for how long
  - Establishes, manages, and terminates connections
  - Provides duplex, half-duplex, or simplex communications between devices
  - Responsible for name recognition (identification) so only the designated parties can participate in the session
- Synchronization: Data checkpoints
  - Provides synchronization services by planning check points in the data stream (check points for retransmission)

6. Presentation Layer

- The layer, is responsible for how an application formats the data to be sent out onto the network.
  - The presentation layer basically allows an application to read (or understand) the message.
- Functionality examples of presentation layer include:
  - Encryption and decryption of a message for security
  - Compression and expansion of a message so that it travels efficiently
  - Graphics formatting
  - Content translation/ System-specific translation

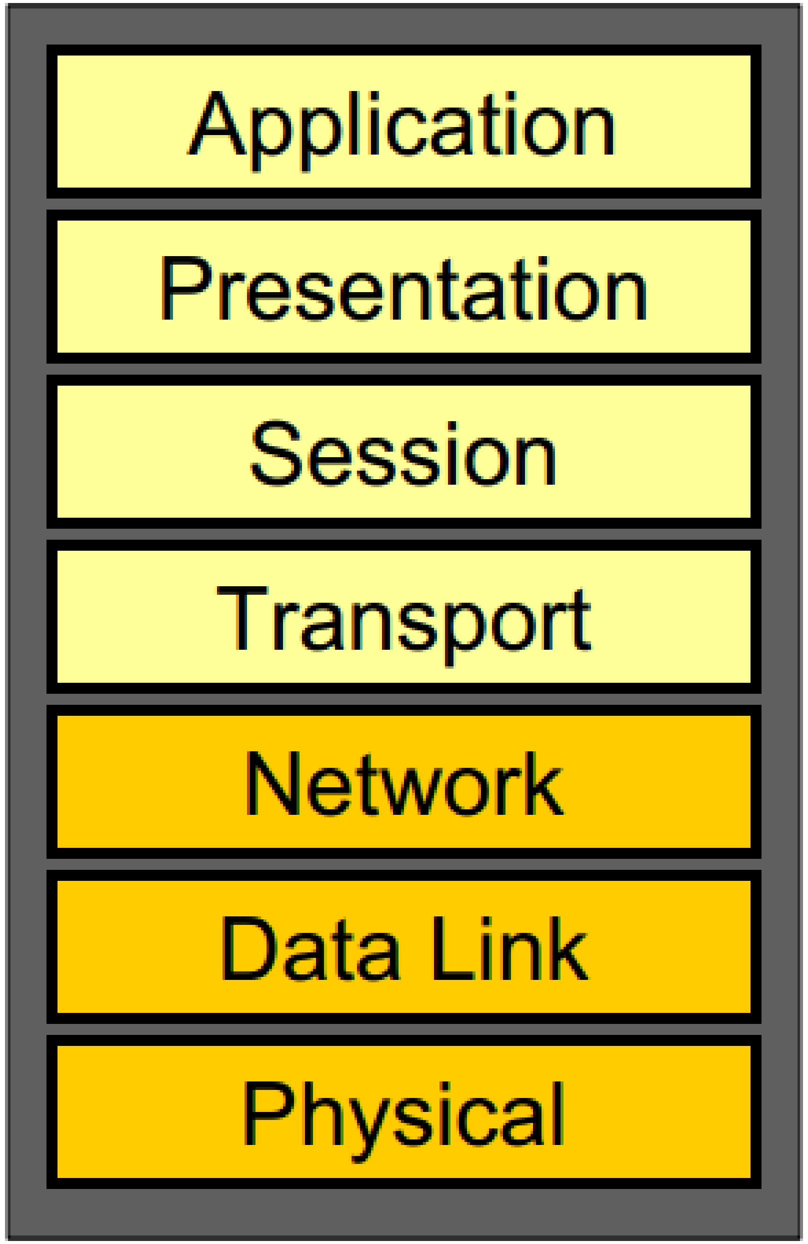
6. Presentation Layer



7. Application Layer

- Allows access to network services that support applications
  - Used for applications that run over the network (What the user “sees or does”)
  - Services that directly support user applications (e.g. file transfer, email)
- Functionality examples of application layer include:
  - Support for file transfer ;
  - Ability to print on a network
  - Electronic mail/Electronic messaging POP3 (Post Office Protocol version 3) to read e-mails and SMTP (Simple Mail Transport Protocol) to send e-mails
  - Browsing the World Wide Web HTTP (Hyper-Text Transport Protocol)

Network Components



Routers, Layer 3 switches

Switches, Bridges

NICs, Cables, Hubs, Repeaters

Protocols

Application	NNTP, SIP, SSI, DNS, FTP, Gopher, HTTP, NFS, NTP, SMPP, SMTP, DHCP, SNMP, Telnet, Netconf
Presentation	MIME, XDR, TLS, SSL
Session	Named Pipes, NetBIOS, SAP, SIP, L2TP, PPTP
Transport	TCP, UDP, SCTP, DCCP
Network	IP (IPv4, IPv6), ICMP, IPsec, IGMP, IPX, AppleTalk
Data Link	ATM, SDLC, HDLC, ARP, CSLIP, SLIP, PLIP, IEEE 802.3, Frame Relay, ITU-T G.hn DLL, PPP, X.25
Physical	EIA/TIA-232, EIA/TIA-449, ITU-T V-Series, I.430, I.431, POTS, PDH, SONET/SDH, PON, OTN, DSL, IEEE 802.3, IEEE 802.11, IEEE 802.15, IEEE 802.16, IEEE 1394, ITU-T G.hn PHY, USB, Bluetooth

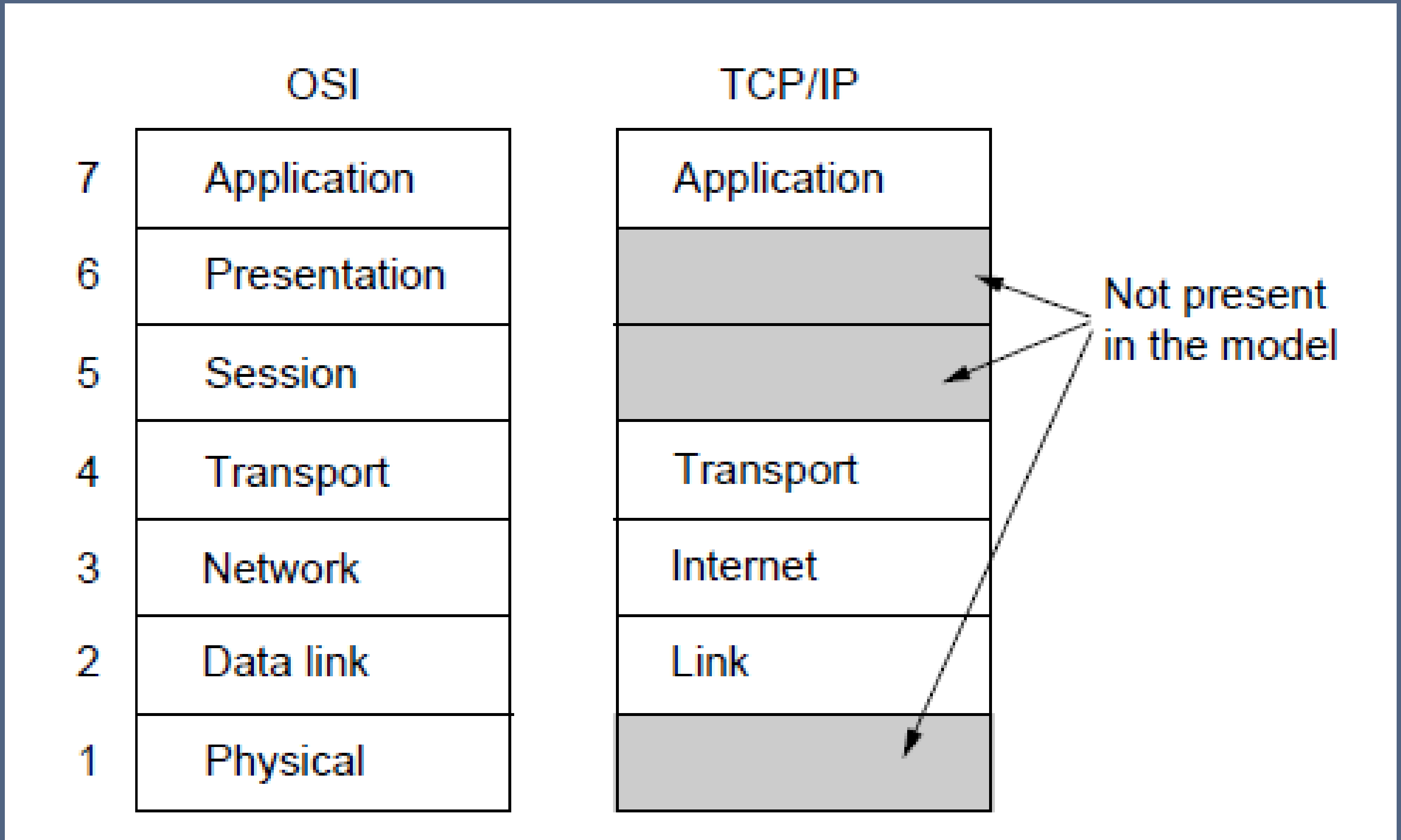
TCP/IP Reference Model

- TCP/IP reference model
- Comparison of OSI and TCP/IP
- Critique of OSI model and protocols
- Critique of TCP/IP model

The TCP/IP Reference Model Layers

- Link layer
- Internet layer
- Transport layer
- Application layer

The TCP/IP Reference Model



The TCP/IP reference model

The TCP/IP Reference Model

- Grandparent of all wide area computer networks *ARPANET;* It's successor Internet
- ARPANET research network sponsored by the DoD.
- Used initially leased telephone lines, When satellite and radio networks were included the new reference architecture was needed.
- Hence the ability to connect to multiple networks in a seamless way was one of the major design goals.
- This architecture latter became known as the *TCP/IP Reference Model*.
- Design criteria:
  - Network be able to survive loss of subnet hardware without existing conversations broken off.
  - Applications with divergent requirements supported ranging from file transfer to real-time speech transmission.

Link Layer

- The lowest layer, the *link layer*, describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer.
- It is not actual layer in the classical sense of the term rather is an interface between hosts and transmission links.

Internet Layer

- The *Internet Layer* holds this architecture together.
- The internet layer defines an official packet format and protocol called IP (Internet Protocol).
- **Packet routing is a major function** Plus Network Addressing.
- It permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network).
- The packets arriving in random order may be rearranged.
- Add on stuff from OSI

Transport Layer

- *Transport Layer* is designed to allow peer entities on the source and destination hosts to carry on a conversation, similarly to the OSI transport layer.
- Two end-to-end transport protocols:
  - TCP (Transmission Control Protocol) – reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.
  - UDP (User Datagram Protocol) – is unreliable connectionless protocol.

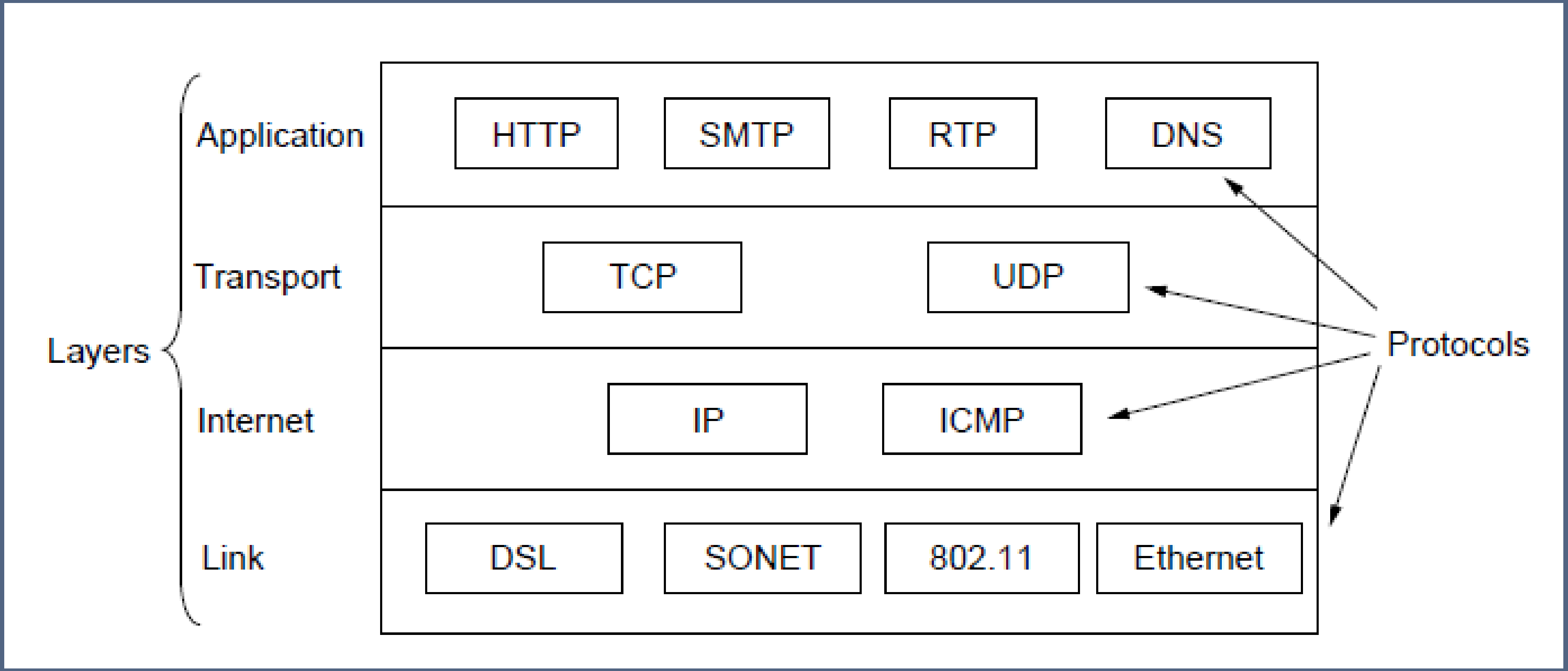
Transport Layer

- TCP (Transmission Control Protocol) –
- It segments the incoming byte stream into discrete messages
- Flow control is also managed by TCP to ensure that a fast sender cannot swamp a slow receiver.
- UDP (User Datagram Protocol) –
- is unreliable connectionless protocol.
- Applications perform their own sequencing or flow control unlike in TCP.
  - Widely used for client-server-type request-reply queries
  - prompt deliver is more important than accurate delivery e.g Speech and video

Application Layer

- Applications must include any session or presentation functions that they require. Experience with the OSI model has proven this view to be correct: these layers are of little use to most applications. [see OSI model]
- Application Layer contains all the higher-level protocols.
  - TELNET - Virtual Terminal
  - FTP – File Transfer Protocol
  - SMTP – electronic mail
  - DNS – Domain Name System
  - HTTP – Hyper Text Transfer Protocol
  - RTP – Real-time Transfer Protocol
- See from OSI model

TCP/IP Protocols



The TCP/IP reference model with some protocols to look up

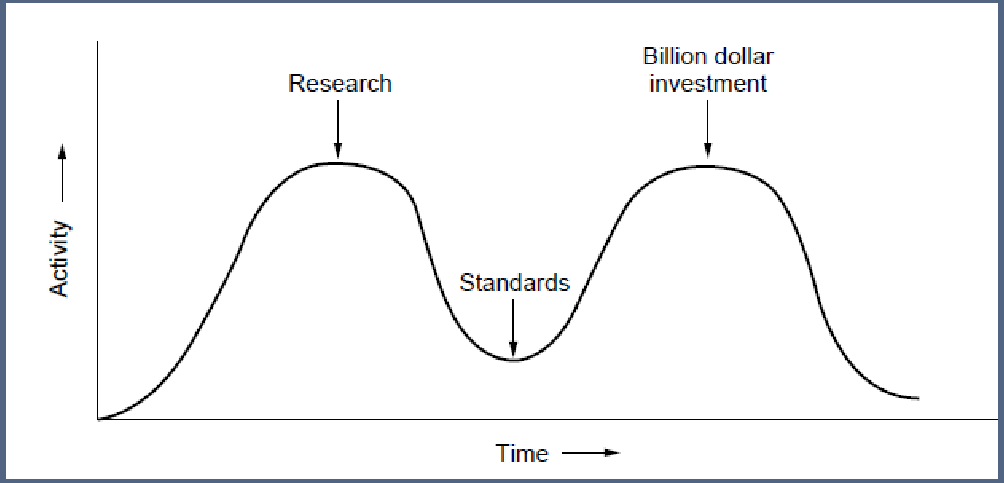
Source: Computer Networks, Fifth Edition by Andrew Tanenbaum and David Wetherall, © Pearson Education-Prentice Hall, 2011

The Comparison of TCP/IP & OSI

- The OSI reference model was devised before the corresponding protocols were invented.
  - This ordering meant that the model was not biased toward one particular set of protocols: a fact that made it quite general.
  - The downside of this ordering was that the designers did not have much experience with the subject and did not have a good idea of which functionality to put in which layer.

- With TCP/IP the reverse was true: The protocols came first, and the model was really just a description of the existing protocols.
  - There was no problem with protocols fitting the model.
  - The trouble was that the model did not fit any other protocol stacks: It was not especially useful for describing other non-TCP/IP networks.

OSI Model Limitations



Bad Timing

The apocalypse of the two elephants.

- Model Bad Technology
  - Both OSI Model and the protocols are flawed.
    - The choice of several layers was more political then technical.
      - Two of the layers (Session and Presentation) are nearly empty.
      - Two other layers (Datalink and Network) are overfull.
    - Model, its associated service definitions and protocols is extraordinary complex.
    - Some functions (addressing, flow control, and error control) reappear again and again in each layer.

OSI Model : Limitations

- Bad Implementation
  - Given enormous complexity of the OSI Model, initial implementations were:
    - Huge, Unwieldy, and Slow
- One of the first TCP/IP, part of Berkley Unix was quite good & free.
- Bad Politics
  - TCP/IP was considered (correctly) born in the US by academic institutions.
  - OSI was widely thought to be creature of European telecommunication ministries, the European Community, and later the U.S. Government.

Critique of the TCP/IP Model

- Does not distinguish clearly the concepts of services, interfaces & protocols.
- Doesn’t differentiate between the specification and the implementation.
- The link layer is really not a layer at all: It is an interface between the network & data link layers.
  - The distinction between in interface and a layer is crucial.
- TCP/IP model does not distinguish between the physical and data link layers.
  - Physical: transmission characteristics of the medium used (copper wire, fiber optics, wireless communication, etc.).
  - Data link: delimit the start and end of frames and get them from one side to the other with the desired degree of reliability.
- IP and TCP protocols were carefully thought out and well implemented, however, the other protocols were ad-hoc.
  - Example - TELNET designed for a ten-character-per second mechanical Teletype terminal and it does not know anything about graphical user interfaces and mice.