DFSC 1316: digital forensic and information assurance fundamentals I

3.1. NETWORK FUNDAMENTALS

*Reference book: *TCP/IP Protocol Suite* by Behrouz A. Forouzan.

A Short Video from CSI: Cyber

- Criminal Scene Investigation (CSI): Cyber Season 1 E06 (from 1 minute)

https://www.youtube.com/watch?v=tEv6hBpIoQY

History of the Internet

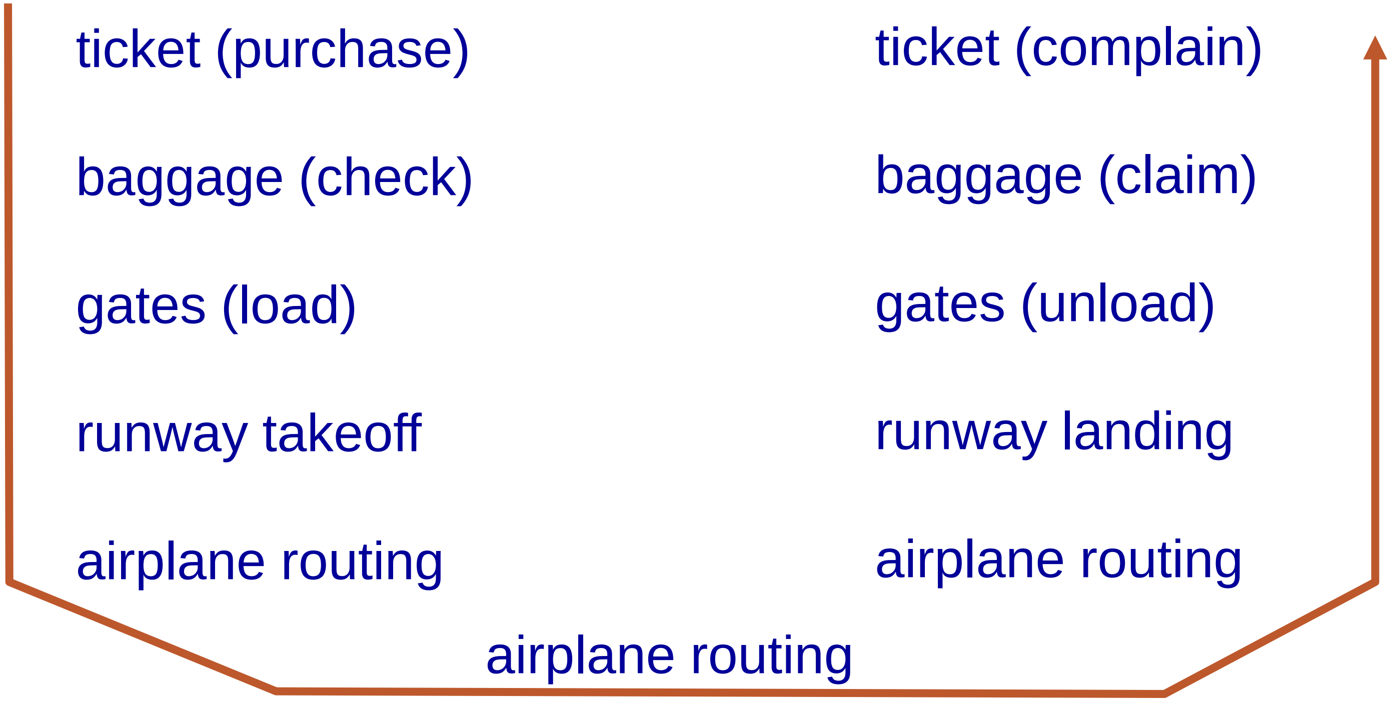
- Early 1960s, the concept of “packet switching” is proposed by Leonard Kleinrock at MIT.
- Late 1960s and early 1970s, the Advanced Research Projects Agency Network (ARPANET) was proposed, designed, and deployed, lead by Defense Advanced Research Projects Agency (DARPA) and US Department of Defense (DoD).
- First packet was sent from UCLA to SRI (Stanford Research Institute), Oct 29, 1969.

History of the Internet

- Early 1980s, the access to the ARPANET was expanded with multiple agencies joined, NSFNET.
- Late 1980s, Internet Service Providers (ISPs) began to emerge.
- 1990, ARPANET was decommissioned.
- Mid 1990s, Internet began to drastically expand and generate revolutionary impact to our society.

Why Layered Network?

- An analogy



ticket (purchase)

baggage (check)

gates (load)

runway takeoff

airplane routing

airplane routing

ticket (complain)

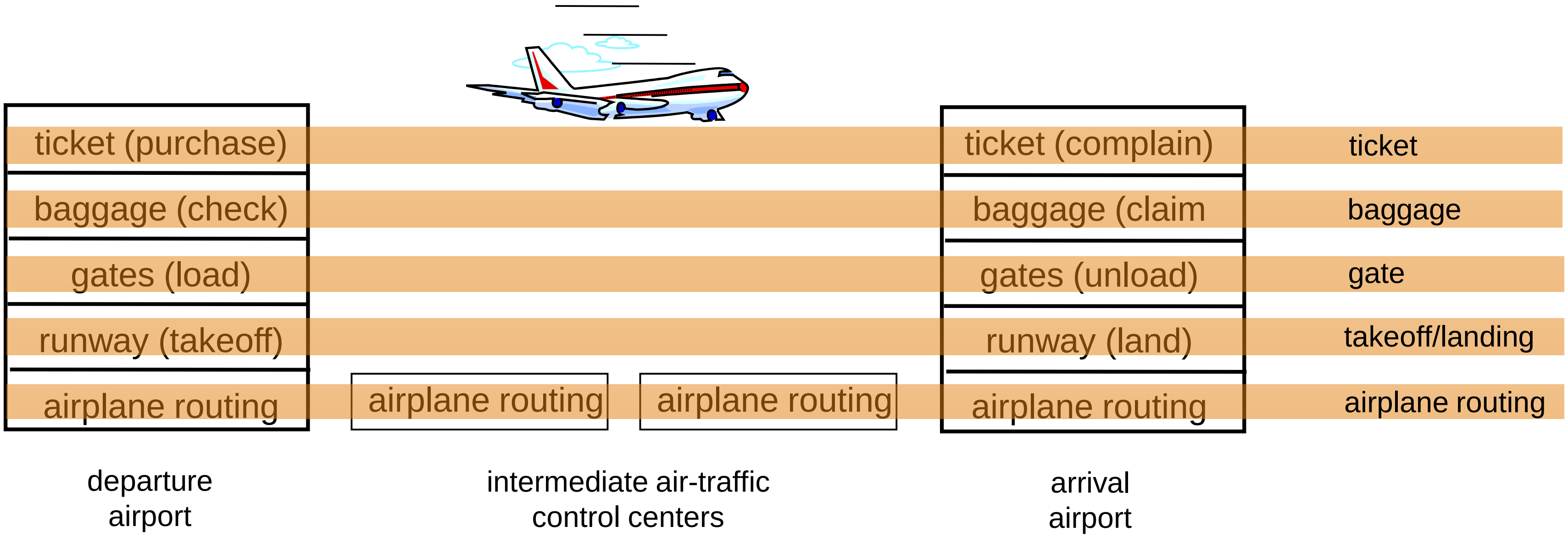
baggage (claim)

gates (unload)

runway landing

airplane routing

Why Layered Network?



layers: each layer implements a service

- via its own internal-layer actions
- relying on services provided by layer below

Layered Network Architecture

- Communication is a complex task
  - Discussion: how to establish a communication between two parties?

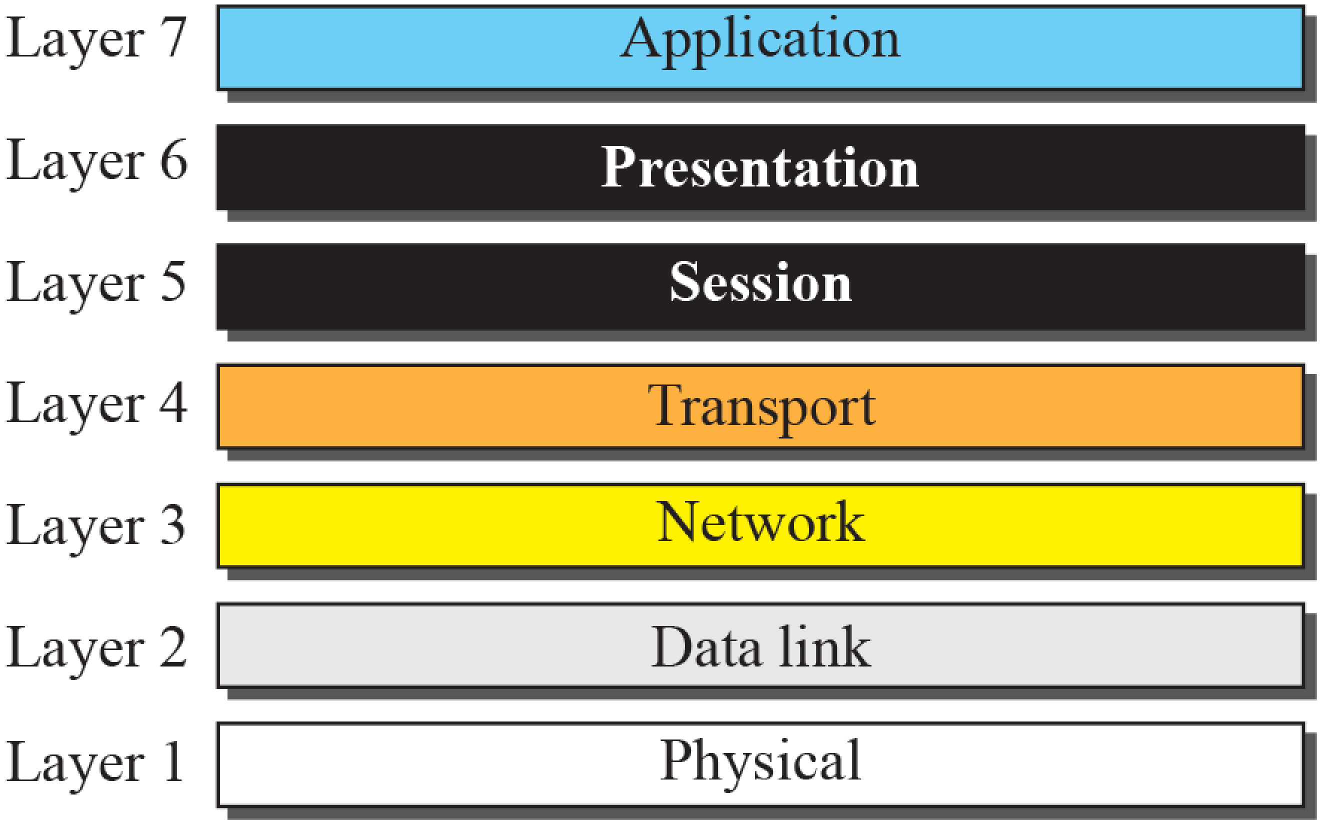
- Each layer only accomplish a part of the task.

- Collaboration of all layers make the communication efficient and effective.

ISO-OSI Model

- ISO: International Standards Organization.
- OSI: Open Systems Interconnection.
- Introduced in 1978 and revised in 1984.
- Formulates the communication process into structured layers.
- There are seven layers in the model.
- The model acts as a frame of reference in the design of communications and networking products.

Seven Layers of the OSI Model



Layer 7 Application

Layer 6 Presentation

Layer 5 Session

Layer 4 Transport

Layer 3 Network

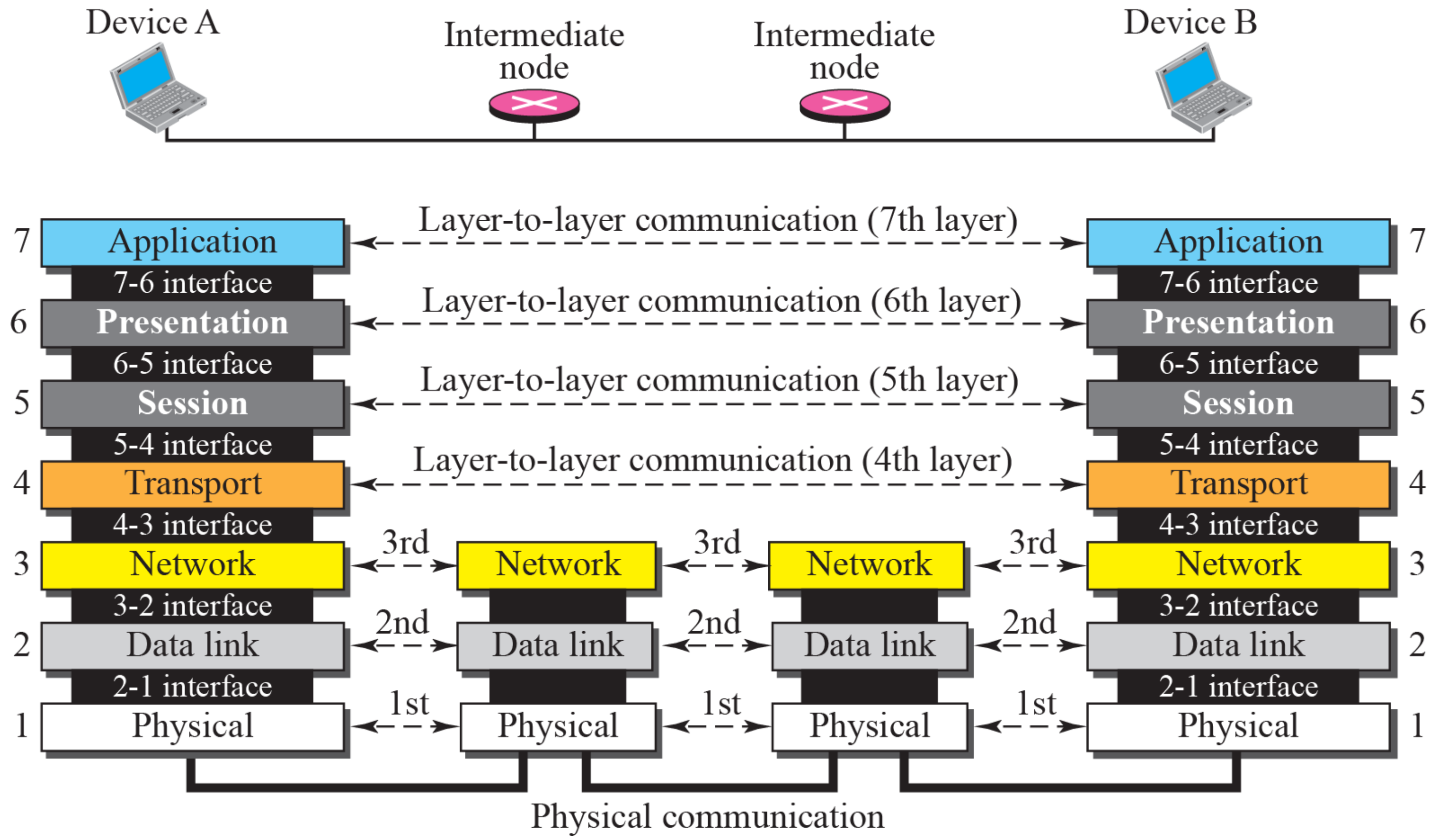
Layer 2 Data link

Layer 1 Physical

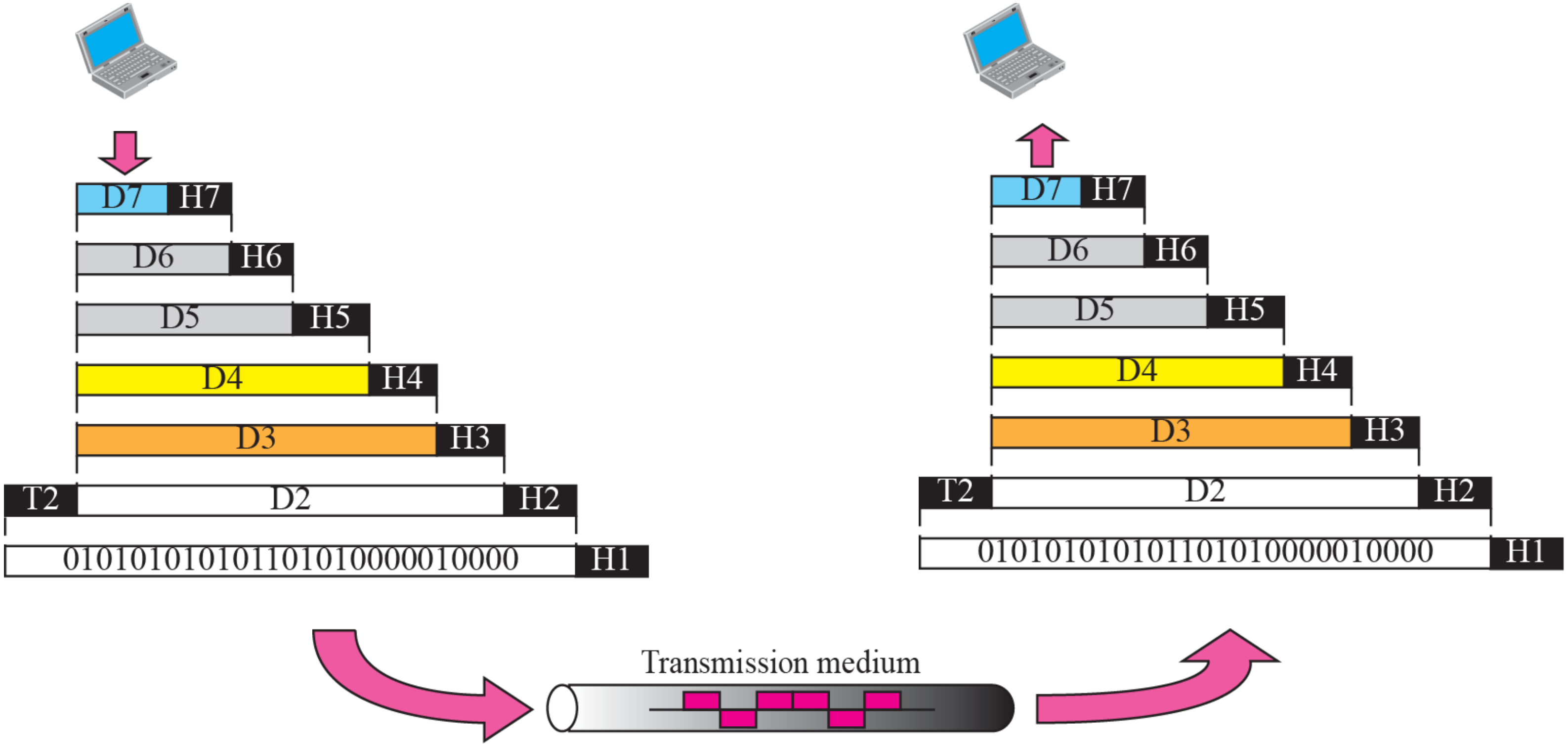
Function of Layers

- Each layer deals with one aspect of networking
  - Layer 1 deals with the communication media
- Each layer communicates with the adjacent layers
  - In both directions
  - Ex: Network layer communicates with:
    - Transport layer
    - Data Link layer
- Each layer formats the data packet
  - Ex: Adds or deletes addresses

Communication between Layers



Message with OSI Model



1. Physical Layer

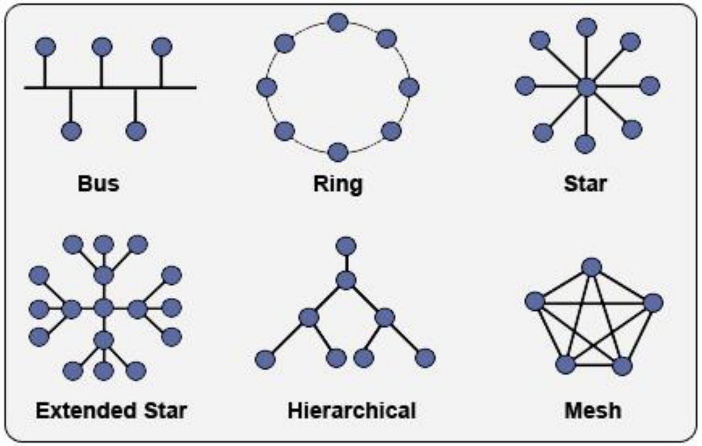
- Physical layer coordinates the functions required to transmit a bit stream over a physical medium.
  - Deals with the mechanical and electrical specifications of the interface and transmission media.
  - Defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.

Functions of Physical Layer

- Physical characteristics of interfaces and media.
  - For example, the type of transmission media.
- Representation of bits.
  - Encode and decode bits to/from electronic signals.
- Data rate.
  - Number of bits sent per second.
- Synchronization of bits.
  - Synchronize the clock at both the sender and the receiver.

Functions of Physical Layer

- Line configuration.
  - Point-to-point / multipoint configuration.
- Physical topology.
  - Mesh, star, ring, and bus topology.
- Transmission mode.
  - Simplex, half-duplex, full-duplex.

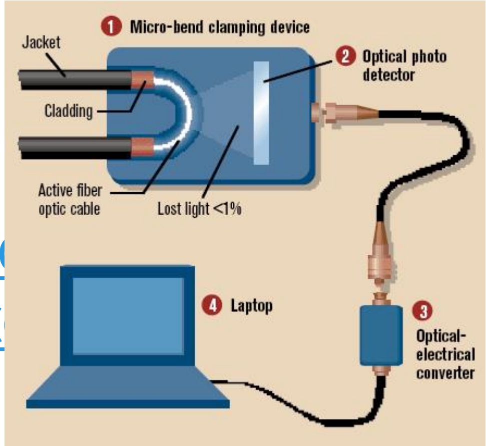


Forensic Value

- Confidentiality?
- Integrity?
- Availability?
- Authenticity?
- Non repudiation?

Physically Intercept Communications

- How to physically intercept communication on a cable?
  - Inline network tap
    - http://hackerwarehouse.com/product/lan-tap-pro/
  - Vampire tap
    - https://www.youtube.com/watch?v=WFdVkSaHRpU
  - Induction Coil
    - Theoretically possible
  - Fiber Optical Taps
    - Splitter
    - Bend coupler
    - https://www.youtube.com/watch?v=GSj-8U
    - https://www.youtube.com/watch?v=2fP-j4X



2. Data Link Layer

- Data link layer transforms the physical layer from a raw transmission to a reliable link.
  - It make the physical layer appear error-free to the upper layer (network layer).
  - Data-link-layer error control by means of retransmission.

Functions of Data Link Layer

- Framing.
  - Divide the stream of bits received from the upper layer (network layer) into manageable data units called frames.
- Physical addressing.
  - Receiver is inside of the sender's network, add receiver's address in to header.
  - Outside the sender's network, add the address of the device which connects it to the next (next hop).

Functions of Data Link Layer

- Flow control.
  - Control the flow of bit stream such that receiver will not be overwhelmed by too much information.
- Error control.
  - Detect damaged/lost frames.
  - Request retransmission.

Forensic Value

- Physical address (MAC address) is an unique identifier that reveals the host information.
  - https://aruljohn.com/mac.pl

3. Network Layer

- Network layer is to implement source-to-destination delivery of a packet usually across *multiple* networks.
- The network layer is not necessary if both sender and receive are within the same network.

Functions of Network Layer

- Logical addressing.
  - Adding logical address which is different from the data link layer address.
  - The IP address.
- Routing.
  - Route or switch packets among connected devices in multiple inter-connected networks.

Forensic Value

- IP address is the most common factor to look at when conducting network forensic.
  - Unusual IP
  - Unusual behavior
  - Unusual traffic

4. Transport Layer

- Transport layer is responsible for source-to-destination delivery of the entire message.
  - The network layer is responsible for packet delivery, whereas the transport layer oversees the whole delivery.
  - Network layer: truck line which carries freight.
  - Transport layer: owner which makes sure freight is correctly and completely delivered.

Functions of Transport Layer

- Service-point addressing.
  - Message should not only be sent to the correct device, but also to the correct process (program).
  - Service-point address (port address) to guarantee messages are delivered to the correct process.
- Segmentation and reassembly.
  - Divide message into segments.
  - Add sequence number to segments for later reassembly.
- Flow control and error control.
  - Similar concept as in data link layer.
  - Performed end to end rather than a single link.

Forensic Value

- Port number is used to identify a specific program that is running on the host.

5. Session Layer

- Not implemented, integrated into the Application layer.
- Dialog control.
  - Allows two systems to enter into a dialog.
- Synchronization.
  - Allows a process to add checkpoints into a stream of data.

6. Presentation Layer

- Not implemented, integrated into the Application layer.
- Translation.
  - Different system may use different encoding.
- Encryption.
  - Encryption and decryption are implemented here.
- Compression.
  - Data compression for more efficient data transmission.

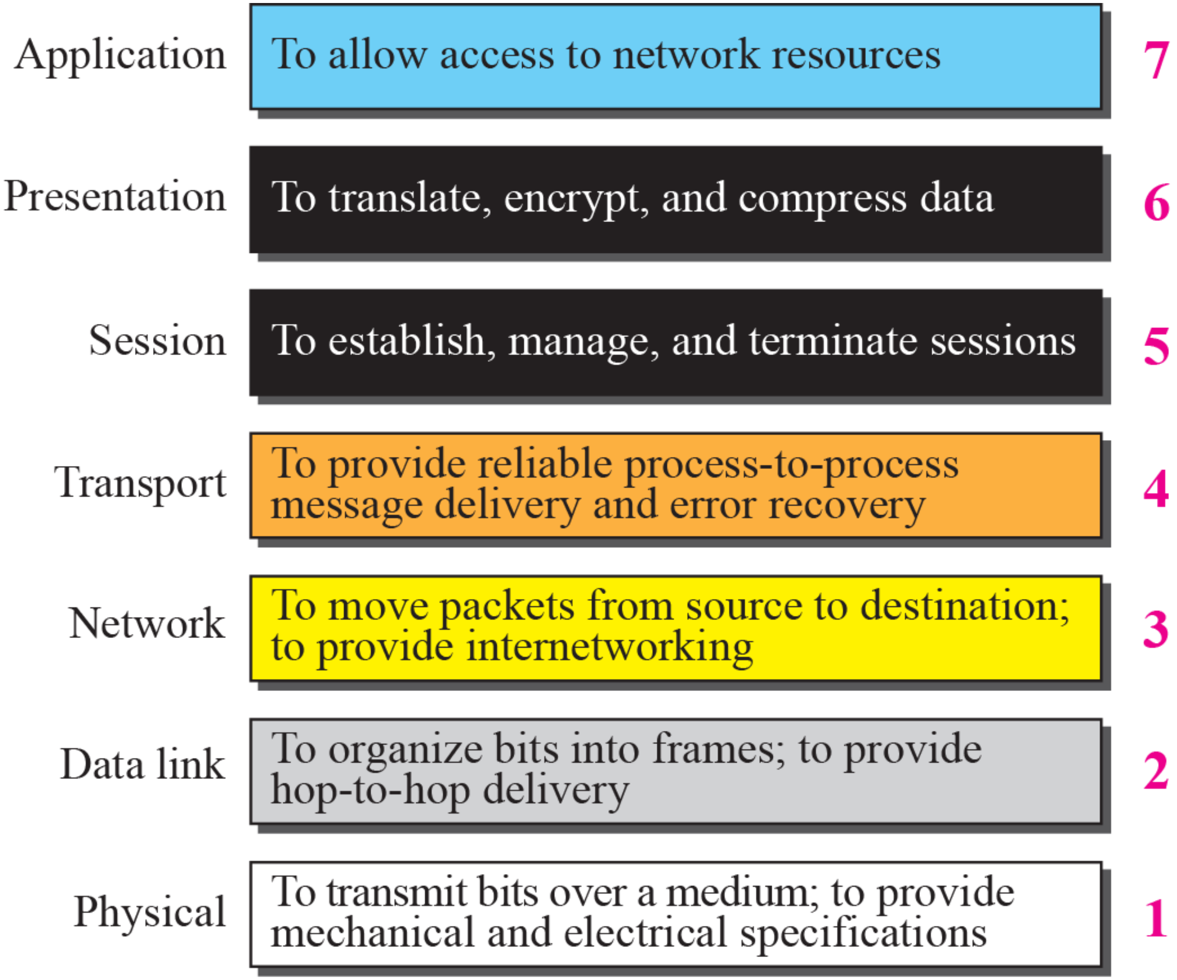
7. Application Layer

- Application layer enables the user to access the network, by providing user interfaces and support for services.
- Example of Functions
  - File transfer, access and management.
  - Email services.
  - Directory services.

Forensic Value

- Application-specific investigation
  - Email
  - tcp
  - http

Summary of 7 Layers



Application	To allow access to network resources	7
Presentation	To translate, encrypt, and compress data	6
Session	To establish, manage, and terminate sessions	5
Transport	To provide reliable process-to-process message delivery and error recovery	4
Network	To move packets from source to destination; to provide internetworking	3
Data link	To organize bits into frames; to provide hop-to-hop delivery	2
Physical	To transmit bits over a medium; to provide mechanical and electrical specifications	1