Computer Network(CSC 503)

Shilpa Ingoley

Lecture 6

Module		Content	Hrs
1		Introduction to Networking	4
	1.1	Introduction to computer network, network application, network software and hardware components (Interconnection networking devices), Network topology, protocol hierarchies, design issues for the layers, connection oriented and connectionless services	
	1.2	Reference models: Layer details of OSI, TCP/IP models. Communication between layers.	

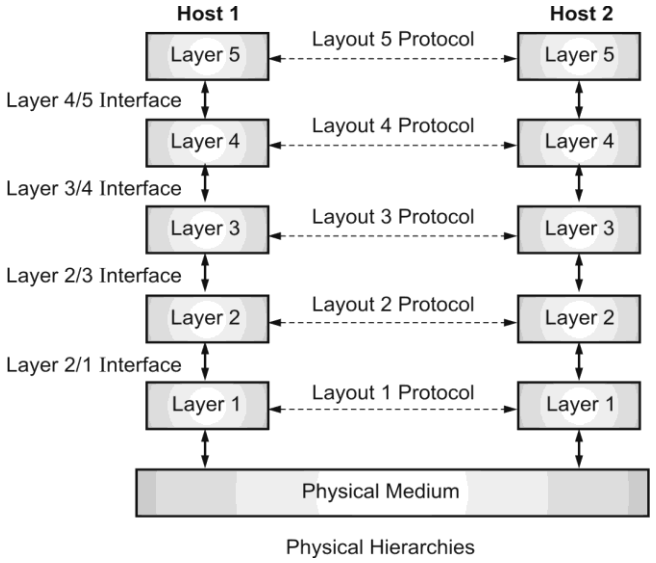
Protocol

- A **protocol** is simply defined as a **set of rules and regulations** for data communication
- Networks are needed to **follow** these **protocols to transmit data** successfully.
- There are **three aspects of protocols** :
  - **Syntax : - data format or structure** that is needed to be **sent or received**.
  - **Semantics :** It is used to explain **exact meaning** of each of **sections** of bits that are usually transferred.
  - **Timings :** It is used to explain **exact time** at which **data** is generally **transferred** –transmission rate/speed ,duration.

Protocol Hierarchy

- **Necessity for Layering :** To **reduce their design complexity**
- A **set of layers and protocols is called as a network architecture**.
- **Purpose of Layer :**
- A **list of the protocols used by a certain system**, protocol(s) per layer, is called as **protocol stack**
- The **layers in the same levels are called peers** and **have a set of protocols for communication**.

- The **dotted arrows** depict **virtual communication** between peer layers
- The solid arrows represent the **physical communications** between the adjacent layers.



Between each pair of adjacent layers is an **interface**. The interface defines which primitive operations and services the lower layer makes available to the upper one.

Fig : Layer, Protocol and Interface

Design Issues for the layers

(1) Reliability
(2) Internetworking
(3) Scalability
(4) Addressing
(5) Error control
(6) Flow control
(7) Congestion
(8) Resource allocation
(9) Protocol layering
(10) Statistical multiplexing
(11) Routing
(12) Security
(13) Quality of service
(14) Confidentiality, Integrity and Availability

Design Issues of layers

1. Reliability

- Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not distorted.

2. Scalability

- Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

3. Addressing

- At a particular time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.

Contd…

4. Error Control

- Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

5. Flow Control

- If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

Contd…

6. Statistical Multiplexing

- It is not feasible to allocate a dedicated path for each message while it is being transferred from the source to the destination. So, the data channel needs to be multiplexed, so as to allocate a fraction of the bandwidth or time to each host.

7.Routing

- There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems

8. Security

- A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

Connection oriented and connection less services

1.Connection oriented

- The **connection oriented service** first **establishes** the **virtual connection** between the source and the destination, **then transfers all data packets** belonging to the same message through same dedicated established connection and after all packets of a message is transferred it **releases the connection**.

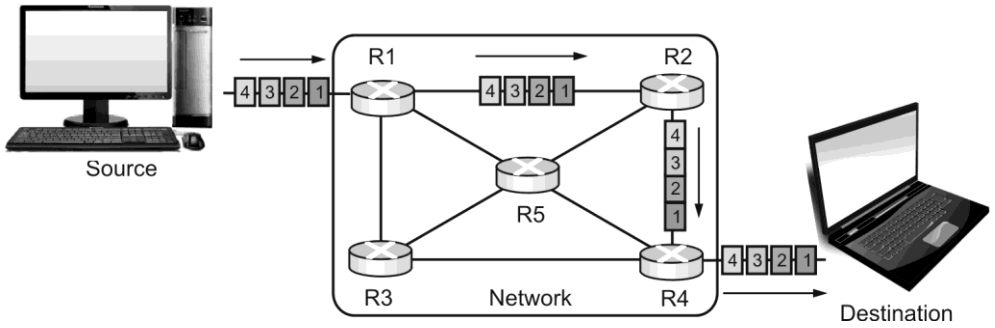
Ex: Telephone system

- When the connection is established a sequence of packets from source to the destination can be sent one after another on the same path and in sequential order.
- When all packets of message have been delivered, the connection is terminated
- As connection-oriented service provides **acknowledgement** at each action, it provides **reliability** in the service.
- The destination sends the **acknowledgement for received** packet it provides **reliability** in the service. There are **fewer** chances of **packet loss** as they travel a predefined path.
- As the virtual path is predefined there are rare or no chances of **congestion,** no delay in the transmission of packets as there is a dedicated path for it.

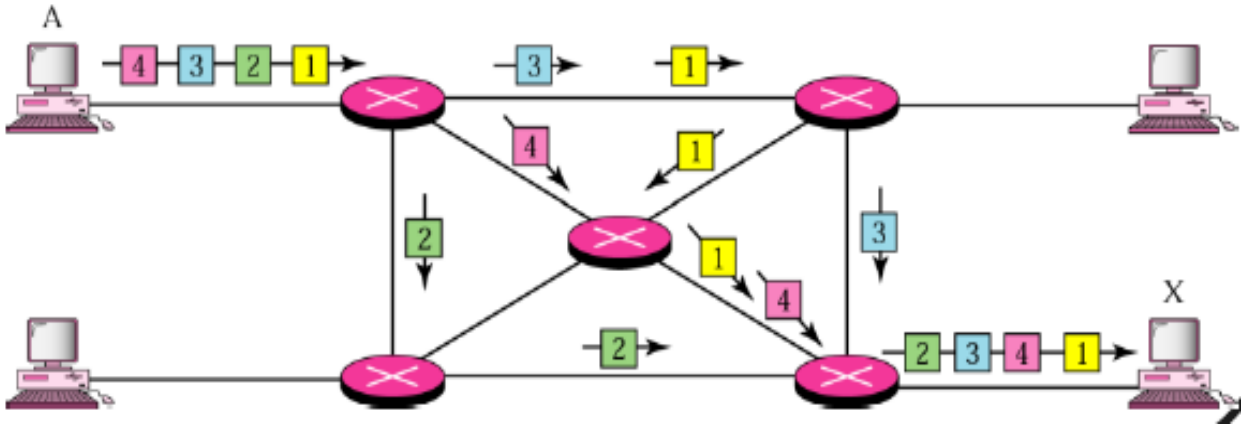
Contd…

2.Connection Less

- Connectionless service is also termed as **datagram service**
- It sends the data, but does not establish and verify a connection between hosts before sending data.
- Treats each datagram/packet independently, the packets in a message may or may not travel the same path to their destination.
- **Ex: postal system**
- Each datagram may travel a **different path**



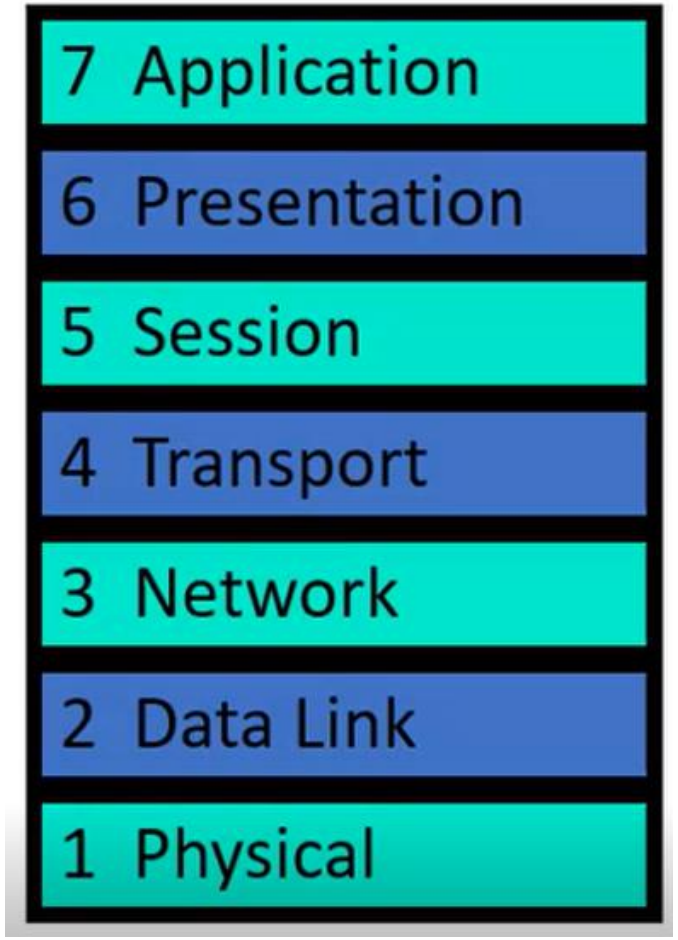
Connection Oriented Service



Connectionless Services

Introduction OSI

- OSI reference model was **developed by** the **International Organization for Standardization** (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- The **Open System Interconnection Reference Model** (OSI Reference Model or **OSI Model**) is an abstract description for layered communications and computer network protocol design.
- It divides network architecture into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data Link, and Physical Layers. It is therefore often referred to as the **OSI Seven Layer Model**.



Contd…

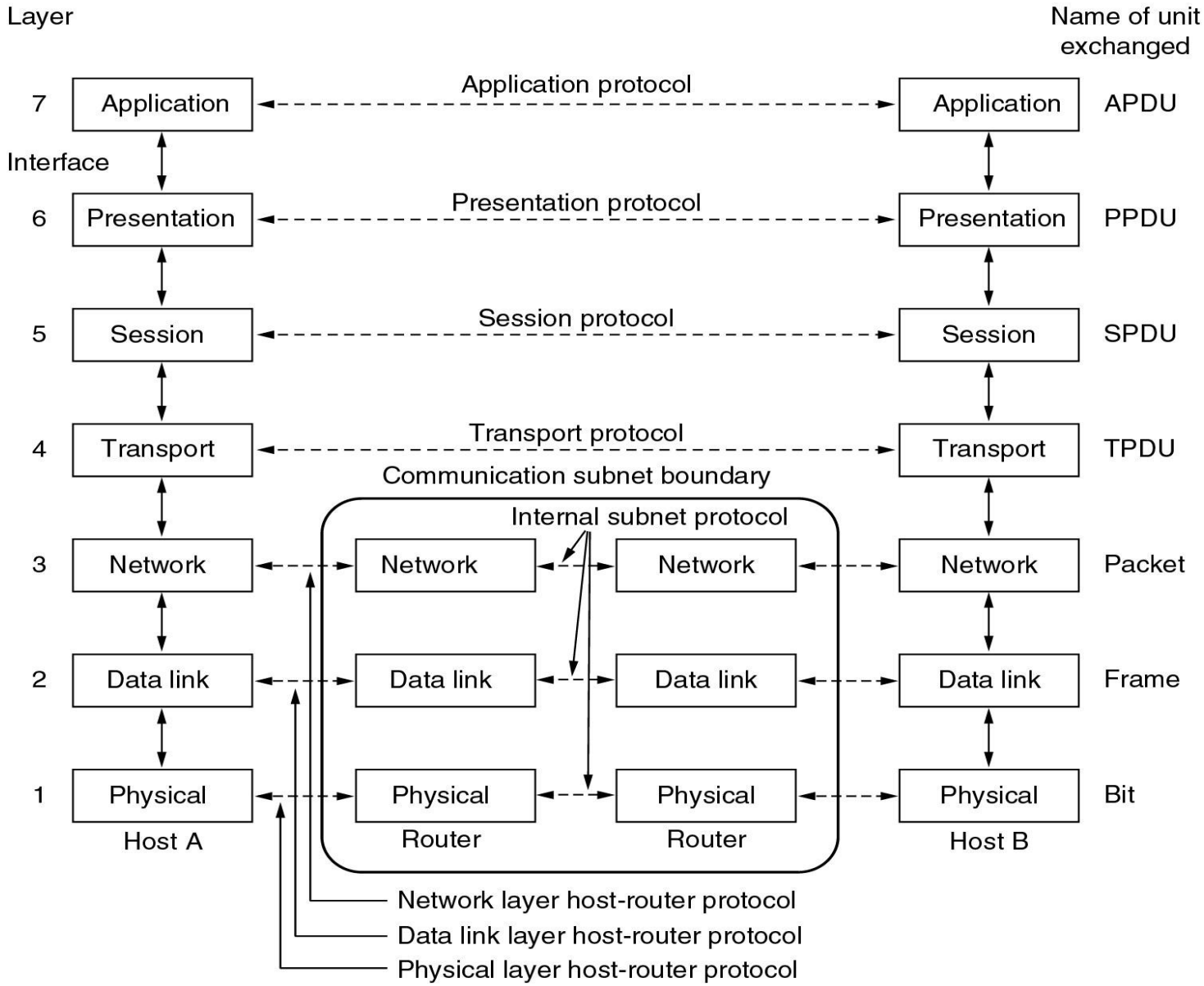
- The benefits of the layered models are modularity and clear interfaces
- In reality, no data are directly transferred from layer n on one machine to layer n on another machine.
- Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which actual communication occurs.
- Virtual communication is shown by dotted lines and physical communication by solid lines.

The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

Reference Models

The OSI reference model.



How Data Flows through the OSI Layers

- Each layer adds (or encapsulates) some form of header or trailer. (Layer 2, the Data Link layer, is responsible for adding a trailer) as the data flow from Device A to Device B.
- When the end system receives the unstructured bit stream from the physical wire, each layer removes the header information applicable to it until the application receives the data.
- Eg: An email is sent from Device A to Device B

1. An application, such as an email program, creates data that will be sent by an end user, such as an email message. The Application layer (layer 7) places a header (encapsulation) field that contains information such as screen size and fonts,

and passes the data to the Presentation layer (layer 6).

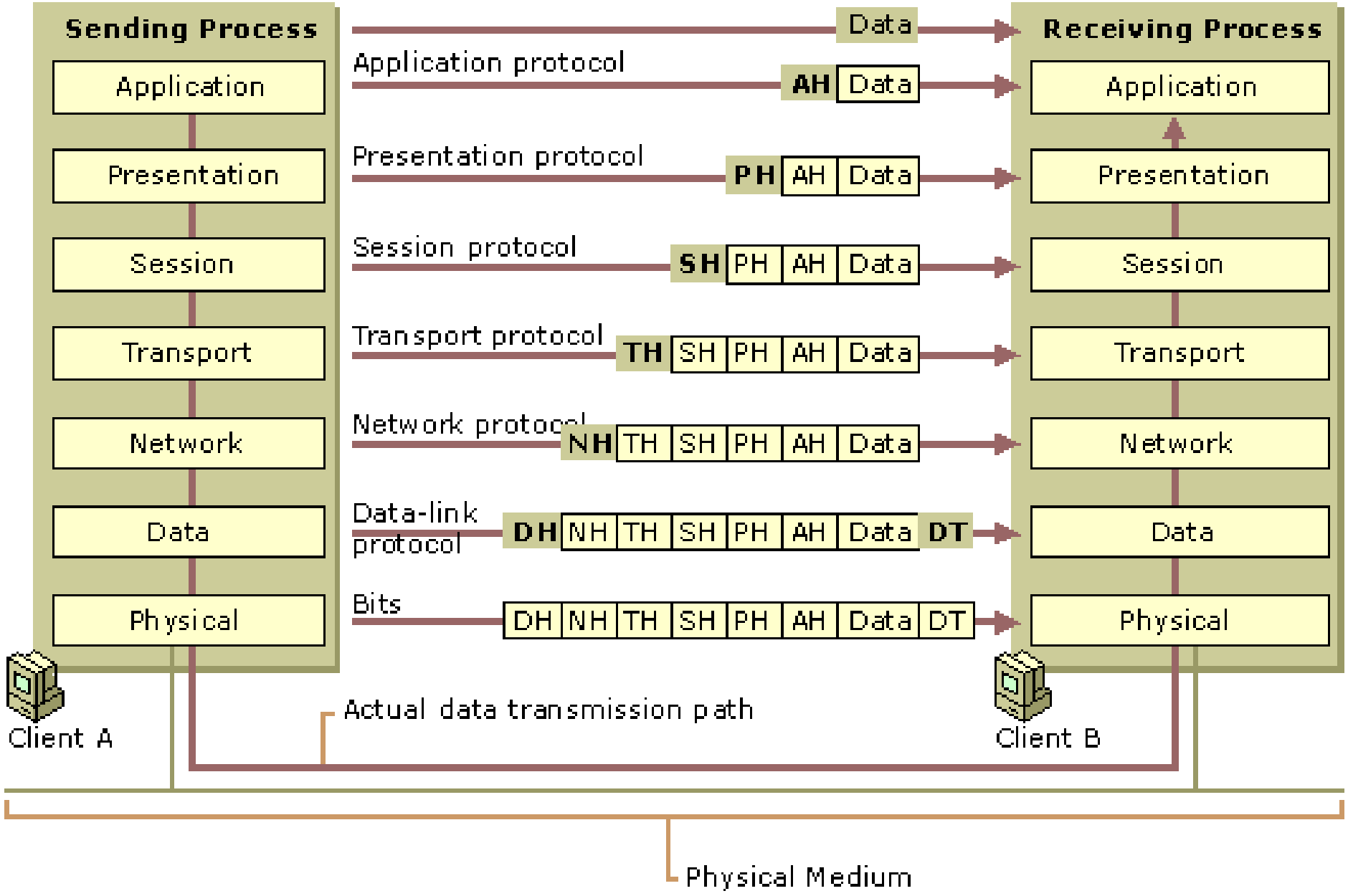
Contd...

2. The Presentation layer places layer 6 header information(PH) and will then pass the new data to the Session layer (layer 5).
3. The Session layer follows the same process by adding layer 5 header information(SH).
4. The Transport layer places layer 4 information in the header(TH), and passes it to the Network layer (layer 3).
5. The Network layer places layer 3 header information(NH), such as the source and destination address so the Network layer can determine the best delivery path for the packets, and passes this data to the Data Link layer (layer 2).

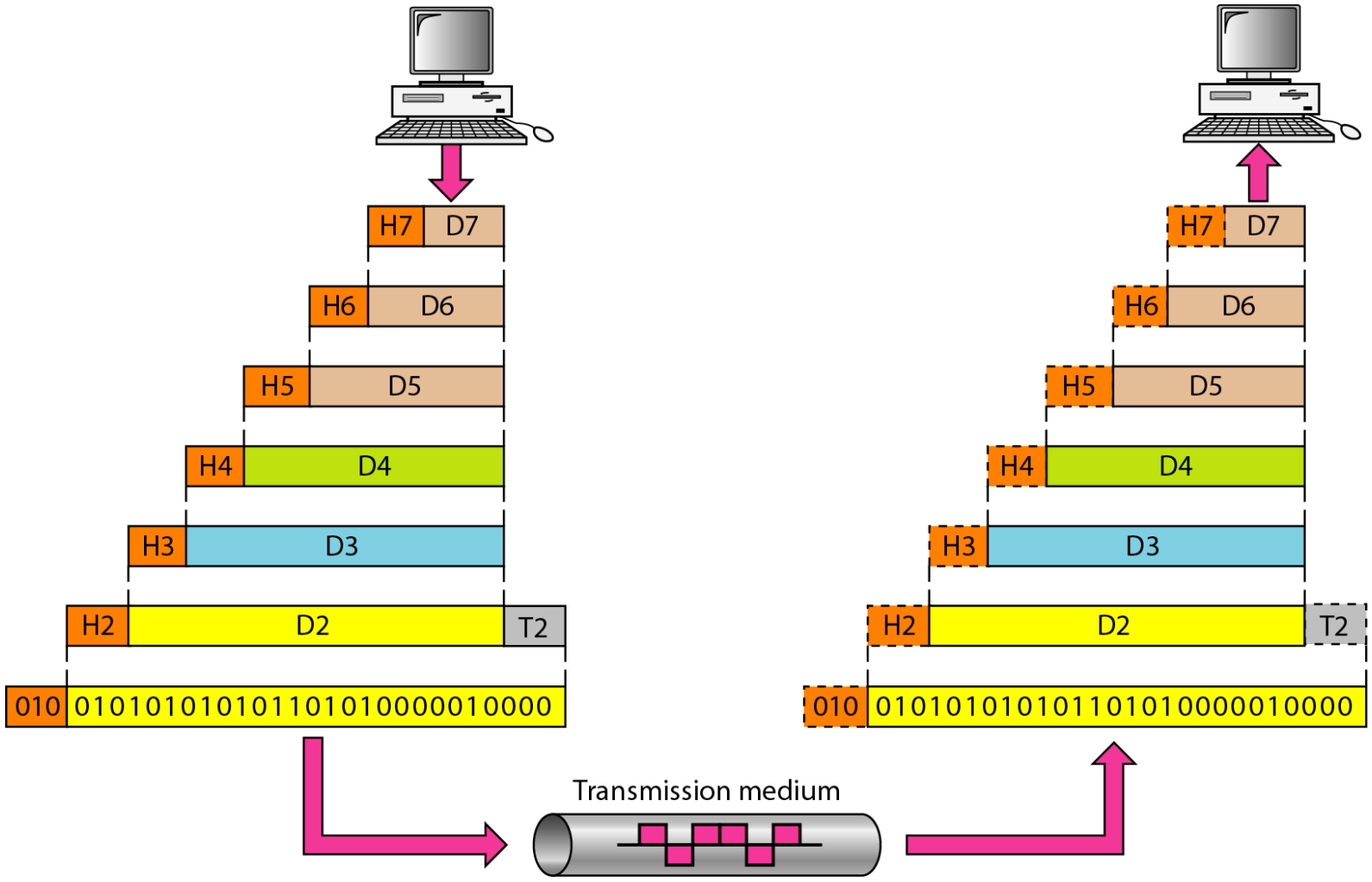
Contd…

6. The Data Link layer places layer 2 header(DH) and trailer information(DT) such as a Frame Check Sequence (FCS) to ensure that the information is not corrupt, and passes this new data to the Physical layer (layer 1) for transmission across the media.
7. The bit stream is then transmitted as ones and zeros on the Physical layer.
8. Steps 1 through 7 occur in reverse order on the destination device. Device B collects the raw bits from the physical wire and passes them up the Data Link layer. The Data Link layer removes the headers and trailers and passes the remaining information to the Network layer and so forth until data is received by the Application layer. Eventually, Device B will receive an email notification displaying a message to indicate that a new email message has been received.

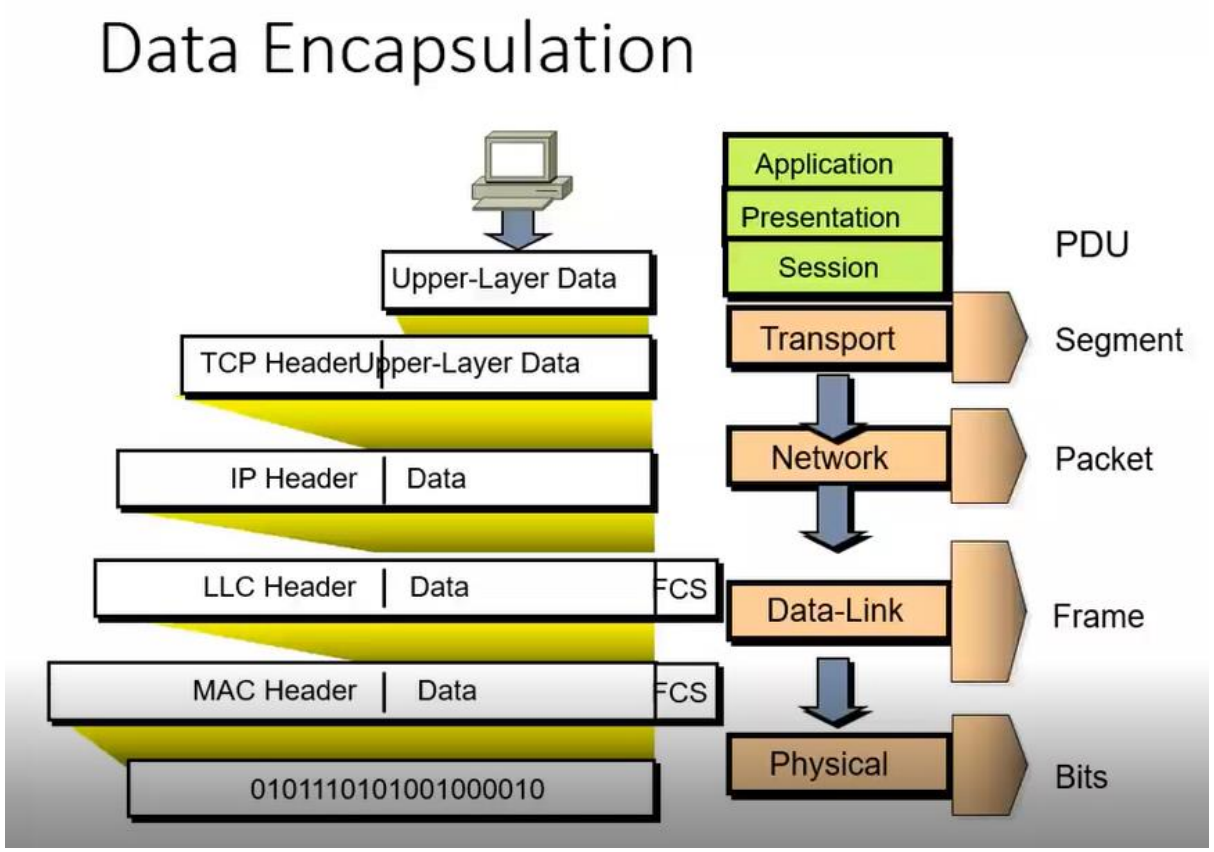
Contd...


Sending Process
Application
Presentation
Session
Transport
Network
Data
Physical
Data
Application protocol
AH
Data
Presentation protocol
PH
AH
Data
Session protocol
SH
PH
AH
Data
Transport protocol
TH
SH
PH
AH
Data
Network protocol
NH
TH
SH
PH
AH
Data
Data-link protocol
DH
NH
TH
SH
PH
AH
Data
DT
Bits
DH
NH
TH
SH
PH
AH
Data
DT
Receiving Process
Application
Presentation
Session
Transport
Network
Data
Physical
Client A
Client B
Actual data transmission path
Physical Medium

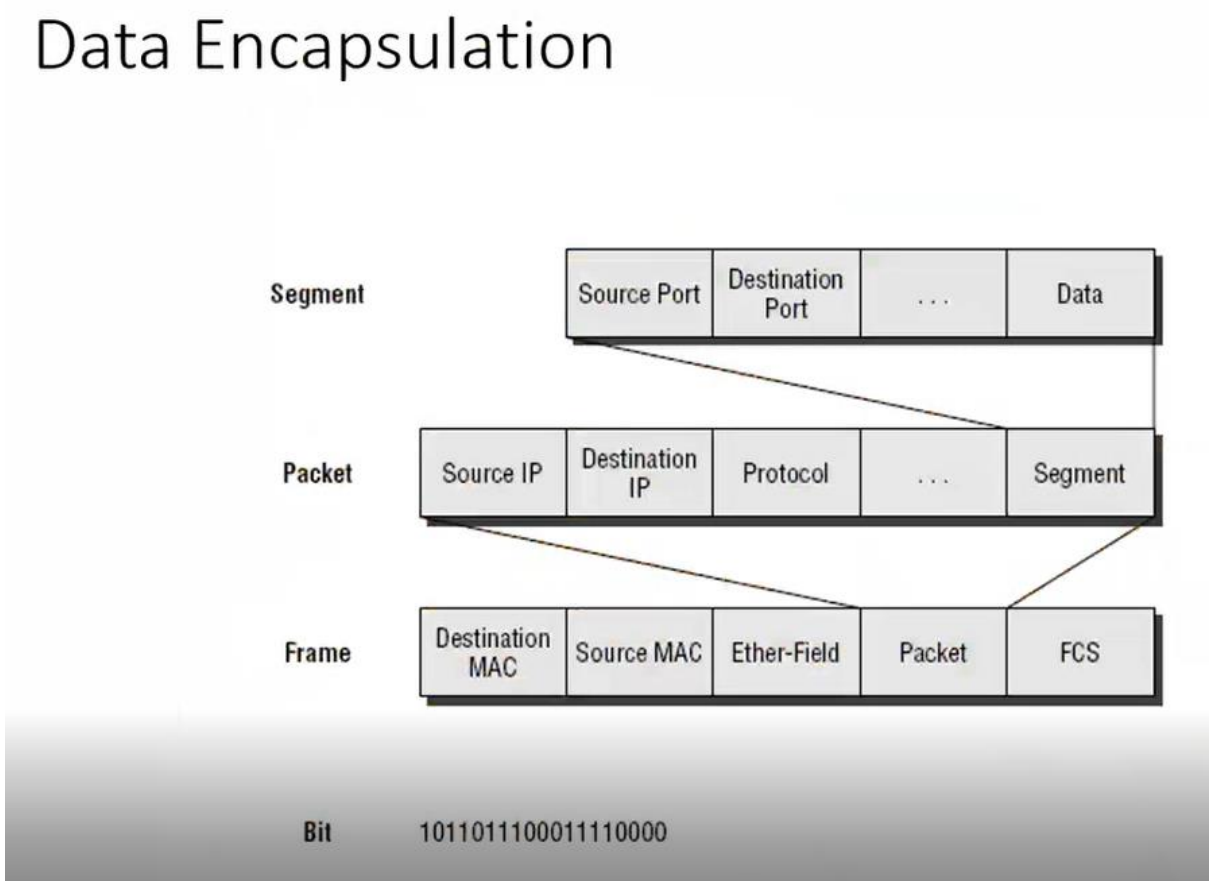
Contd…


H7
D7
H6
D6
H5
D5
H4
D4
H3
D3
H2
D2
T2
010
0101010101011010100000010000
Transmission medium
H7
D7
H6
D6
H5
D5
H4
D4
H3
D3
H2
D2
T2
010
0101010101011010100000010000

Data Encapsulation



Data Encapsulation



Physical layer

It provides the hardware means of sending and receiving data on a carrier.

Functions

1. **Representation of Bits**: Data in this layer consists of stream of bits. The bits must be encoded into signals for transmission. It defines the type of encoding i.e. how 0's and 1's are changed to signal.
2. **Data Rate**: This layer defines the rate of transmission which is the number of bits per second.
3. **Synchronization**: It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.
4. **Interface**: The physical layer defines the transmission interface between devices and transmission medium.

Contd...

5. **Line Configuration**: This layer connects devices with the medium: Point to Point configuration(dedicated link between 2 devices) and Multipoint configuration(shared link between more than 2 devices)
6. **Topologies**: Devices must be connected using the following topologies: Mesh, Star, Ring and Bus.
7. **Transmission Modes**: Physical Layer defines the direction of transmission between two devices: Simplex(signals can flow only in one direction), Half Duplex(signals can flow in both directions not at the same time). Full Duplex(signals can flow in both directions at the same time).

Data Link Layer

- When sending data to the physical layer it puts a header(MAC address) and a frame check sequence(trailer).
- When obtaining data from the Physical layer, the Data Link layer checks for physical transmission errors and packages bits into data "frames".
- **The data link layer provides error-free transfer of data frames from one node to another over the physical layer.**
- The data link layer is divided into two sub layers:
  - The Media Access Control (MAC) layer
  - The Logical Link Control (LLC) layer.

Contd…

Data Link Layer Functions

1. **Framing:** Divide the stream of bits received from network layer into data units called frames
2. **Physical Addressing:** The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.
3. **Flow Control:** A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.

Contd…

4. Error Control:

- Add mechanisms to detect and retransmit damaged or lost frames.
- Prevent also duplication of frames.
- Error control is normally achieved through a trailer added to the end of frame.

5. Access Control: Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.

Physical and Logical Addresses

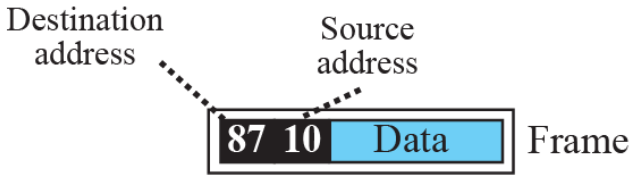
- The physical address, also known as the MAC(Media Access control) address, is the address of a node as defined by its LAN. It is included in the frame used by the data link layer.
- It is the lowest-level address. The size and format of these addresses vary depending on the network.
- For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC).
- Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below.
- Eg 07:01:02:01:2C:4B

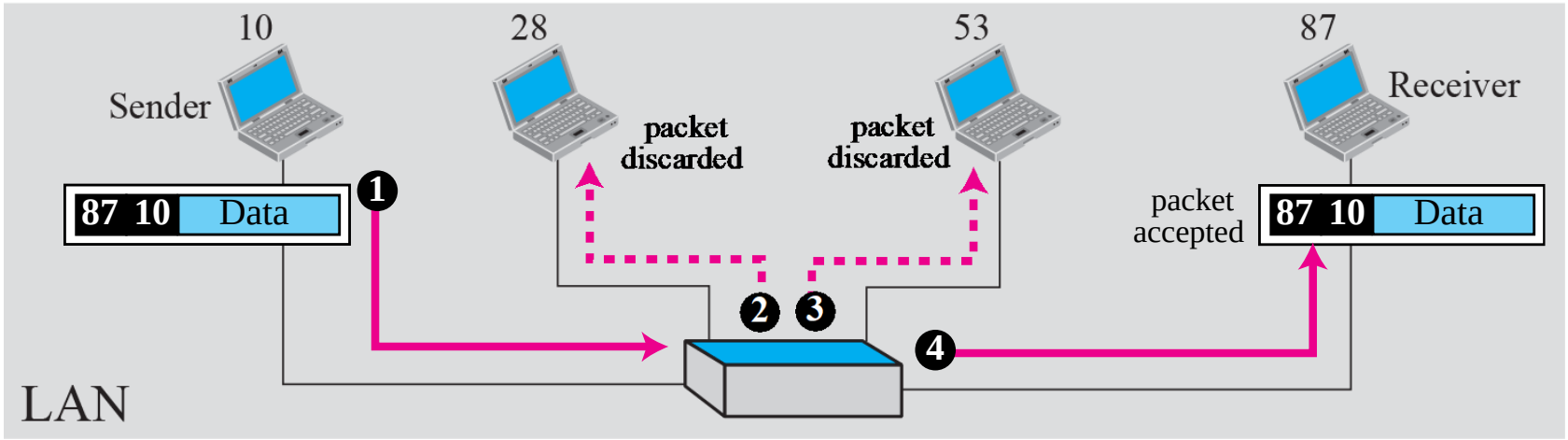
Contd…

Physical Address

- A node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a LAN. At the data link layer, this frame contains physical (link/MAC) addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection. The data link layer at the sender receives data from an upper layer. It encapsulates the data in a frame, adding a header and a trailer. The header, among other pieces of information, carries the receiver and the sender physical (link) addresses.
- The frame is propagated through the LAN. Each node with a physical address other than 87 drops the frame because the destination address in the frame does not match its own physical address. The intended destination computer, however, finds a match between the destination address in the frame and its own physical address. The frame is checked, the header and trailer are dropped, and the data part is decapsulated and delivered to the upper layer.

Physical addresses





Contd…

Logical Address

- Logical addresses are necessary for universal communications that are independent of underlying physical networks.
- **Physical addresses are not adequate in an internetwork environment.**
- A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network.
- The logical addresses are designed for this purpose.

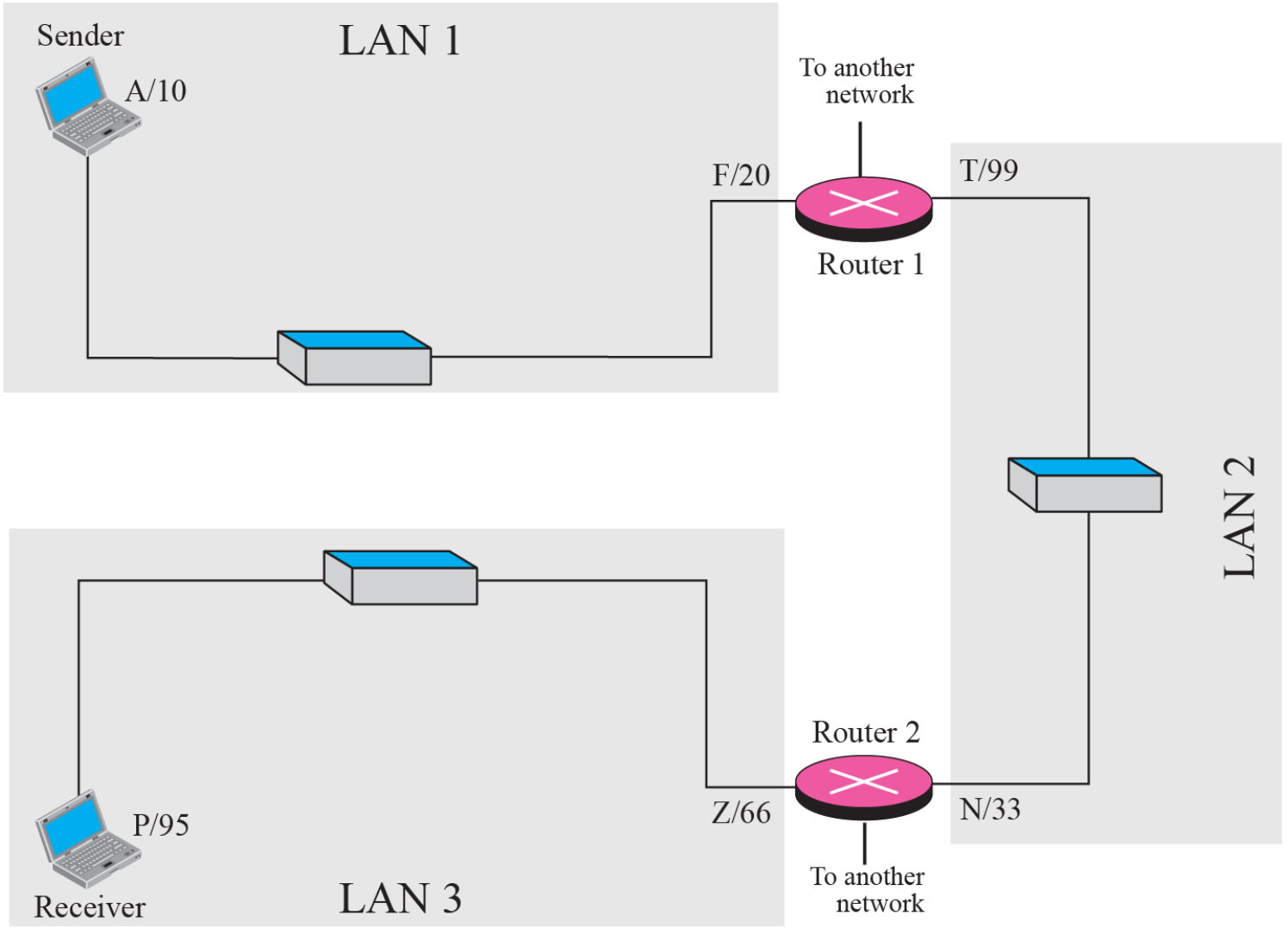
A logical address in the Internet is currently a 32- bit address that can uniquely define a host connected to the Internet.

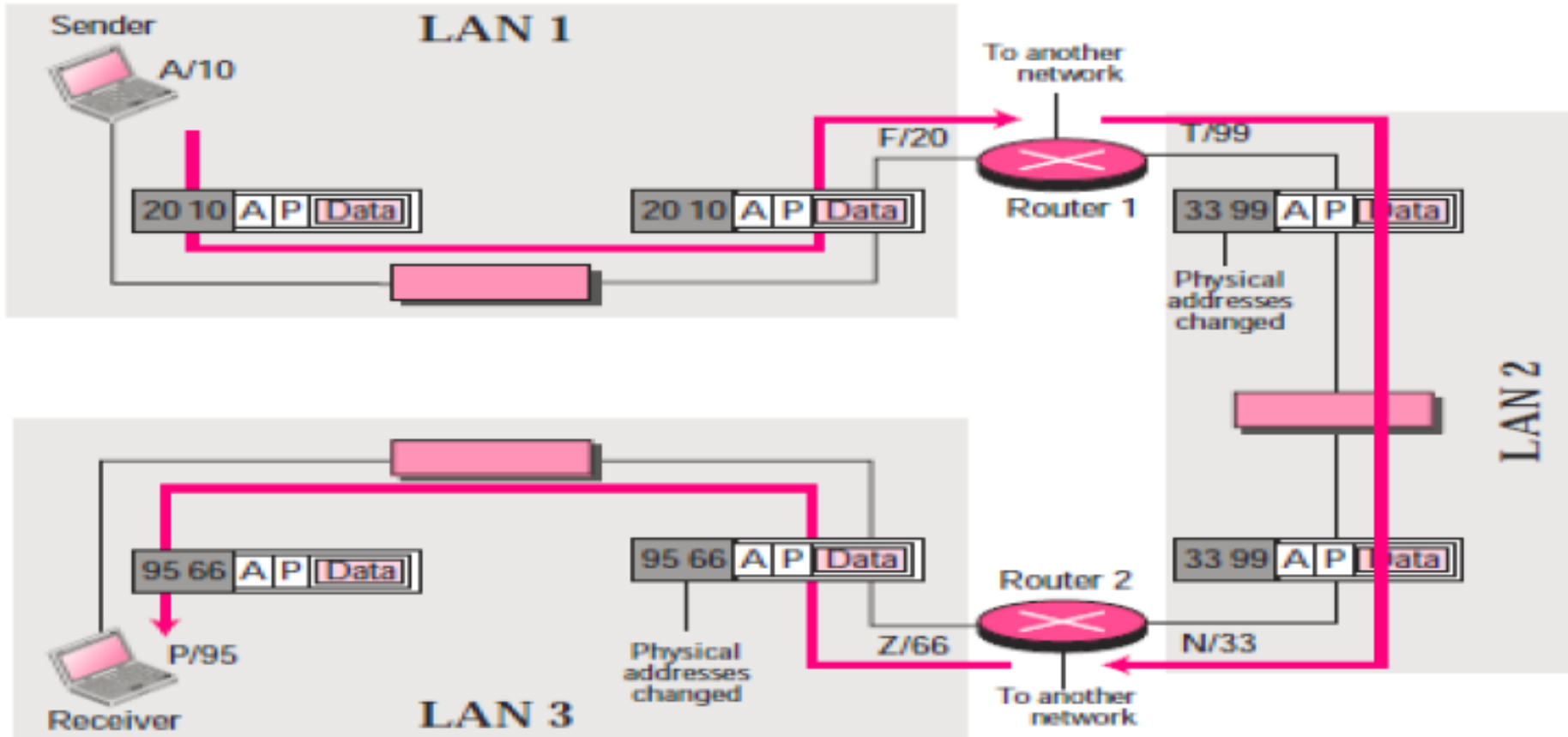
- No two hosts on the Internet can have the same IP address.
- The physical addresses will change from hop to hop,but the logical addresses remain the same

Contd…

- The Figure below shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection.
- The computer with logical address A and physical address 10 needs to send a packet to the computer with logical address P and physical address 95.
- The sender encapsulates its data in a packet at the network layer and adds two logical addresses (A and P).
- The network layer, however, needs to find the physical address of the next hop before the packet can be delivered. The network layer consults its routing table and finds the logical address of the next hop (router 1) to be F.

Example 2.5: logical addresses




Sender
LAN 1
A/10
To another network
F/20
T/99
20 10 A P Data
20 10 A P Data
Router 1
33 99 A P Data
Physical addresses changed
LAN 2
95 66 A P Data
95 66 A P Data
Router 2
33 99 A P Data
P/95
Physical addresses changed
Z/66
N/33
Receiver
LAN 3
To another network