# COMPUTER NETWORK

**By:**
Dr. Ankush Agarwal

# Outline

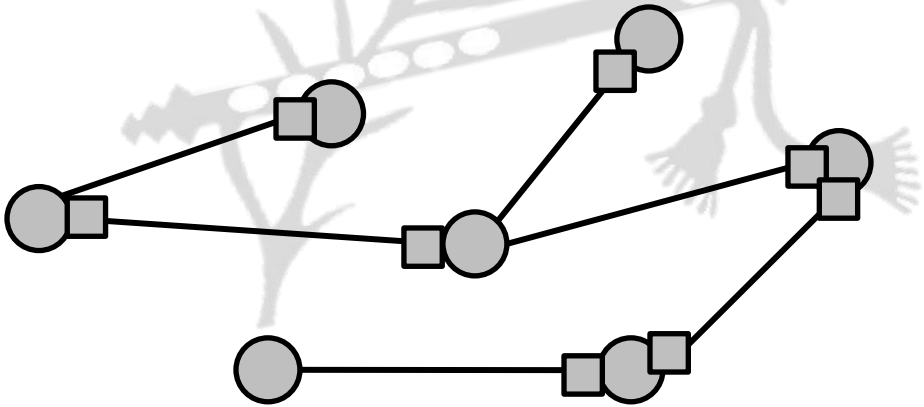
- **Introduction Concepts:**
  - Goals and Applications of networks
  - Network structure and architecture
  - The OSI reference model and services
  - Network topology design
  - Physical Layer Transmission Media
  - Line coding scheme
  - Switching methods (circuit switching, Packet switching)
  - TDM

# INTRODUCTION CONCEPTS

# Introduction

Network

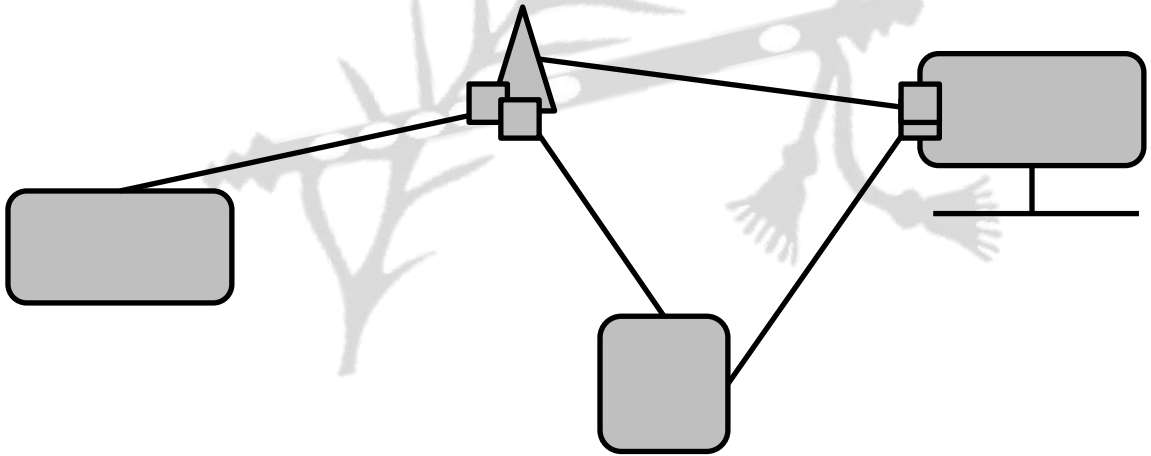
- It is defined as a medium which is responsible for carrying the data from one node to another
- Eg: intranet, internet, PAN, etc



# Introduction

Computer Network

- A computer network is comprised of nodes and links
- A node is the end point whereas links are the medium
- It is defined as a network through which one system can communicate with the other system



# Goals of network

The main goals of network are:

- Resource sharing
  - Eg: printer on network, shared drives, etc
- High reliability
  - Eg: alternative sources, multiple copies, etc
- Increase system utilization
  - Eg: load sharing, pooling, etc
- Powerful communication medium
  - Eg: update is reflected immediately

# Application of network

The main applications of network are:

- Accessing web
- File transfer
- File sharing
- Remote procedure call
- Remote method invocation, etc

# Network architecture

- Network architecture is the design of a computer network
- It is a framework for the specification of a network's physical components and their functional organization
- It also defines the set of rules which are followed during communication (also known as protocols)
- Network architecture refers to the way network devices and services are structured to serve the connectivity needs of client devices
- A architecture defines how the computers should get connected to get the maximum advantages of a computer network such as better response time, security, scalability, etc

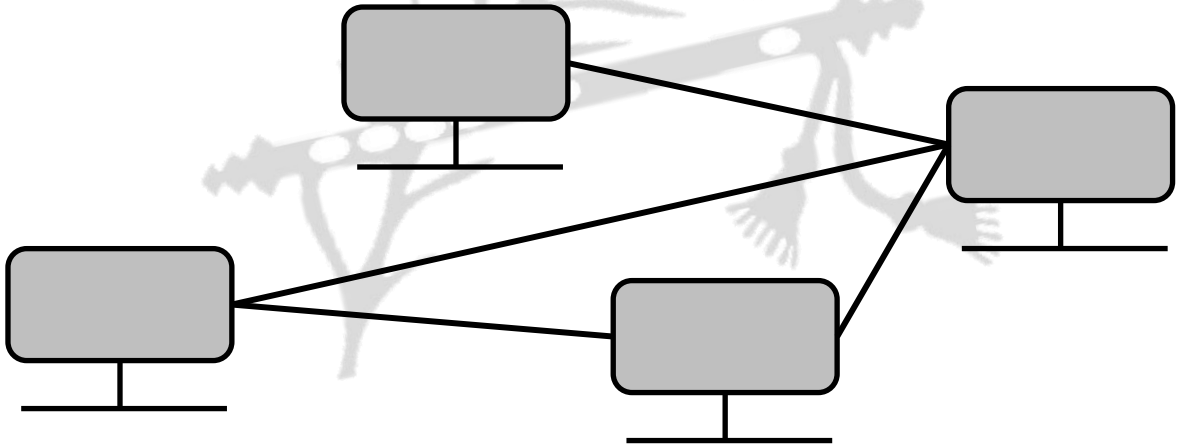
# Network architecture

The two most common network architecture are

- Peer-to-Peer
  - Known as P2P
- Client-Server
  - Known as tiered

# P2P architecture

- All the nodes in a network are inter-connected with every other nodes
- There is no one who acts as a master (also known as server) for all, rather all acts as a master independently
- It is useful for small environment



# P2P architecture

**Advantages**

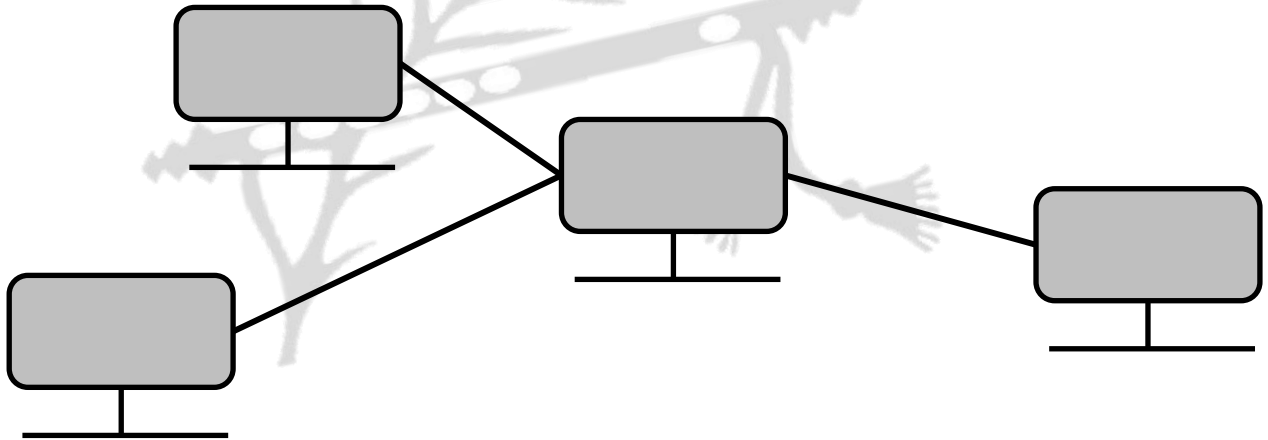
- Less costly as there is no central server
- In case of a node failure, other nodes in the network are not affected
- Installation is quite easy

**Disadvantages**

- Each computer has to take the backup of its own
- Security measures are to be taken by all the nodes independently
- Scalability is a issue

# Client-Server architecture

- All the nodes in a network are connected with the central node (known as master/server)
- The master node receive request from all the other nodes (clients) and respond their request



# Client-Server architecture

## Advantages

- Data backup is easy
- Performance is better as the response time is greatly improves
- Security is better as unauthorized access are denied by server
- Scalability is not an issue in this architecture as large number of computers can be connected with server.

## Disadvantages

- In case of server failure, the entire network is down.
- Server maintenance cost is high
- Cost is high

# Network topology

- The topology defines how the nodes in the network are connected
- It also defines the flow of data from one node to another
- There are five types of topologies defines
  - Mesh topology
  - Star topology
  - Bus topology
  - Ring topology
  - Hybrid topology

# Network topology

Mesh topology

- In this topology, each node is connected to every other node in the network
- Implementing the mesh topology is expensive and difficult
- In this type of topology, each node may send message to destination through multiple paths
- While the data is travelling, it is automatically configured to reach the destination by taking the shortest route which means the least number of hops

# Network topology

Star topology

- Each node is connected to a central device called a hub
- The hub takes a request from any node and pass it to the other node
- Data on a star topology passes through the hub, switch, or concentrator before continuing to its destination
- The hub, switch, or concentrator manages and controls all functions of the network
- The star topology reduces the chance of network failure by connecting all of the systems to a central node

# Network topology

Bus topology

- All the nodes topology are connected by one single cable
- A bus topology consists of a main run of cable with a terminator at each end. All nodes (file server, workstations, and peripherals) are connected to the linear cable
- Popular on LANs because they are inexpensive and easy to install

# Network topology

Ring topology

- In a ring topology, every device has exactly two neighbors for communication purposes.
- All messages travel through a ring in the same direction.
- A failure in any cable or node breaks the loop and can take down the entire network
- To implement a ring network we use the Token Ring technology
- A token, or small data packet, is continuously passed around the network. When a device needs to transmit, it reserves the token for the next trip around, then attaches its data packet to it

# Network topology

Hybrid topology

- A combination of any two or more network topologies
- A hybrid topology always accrues when two different basic network topologies are connected
- It is a mixture of above mentioned topologies. Usually, a central computer is attached with sub-controllers which in turn participate in a variety of topologies

# Network Technologies

It can be classified under two category

- Based on transmission technology
- Based on scale

# Network Technologies

Based on transmission technology

- Broadcast
  - Broadcast network have a single communication channel that is shared by all the nodes on the network
- Point to point
  - There may exist multiple paths between a source-destination pair and the nodes in between provide a route to move the data from one to other until it reach to the destination

# Network Technologies

Based on scale

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)

# Network Technologies

Based on scale

- LAN
  - usually privately owned
  - used to links the devices in a single office, building or campus of up to few distance
  - restricted in size
  - run at speeds of 10 to 100 Mbps (but now much higher speeds can be achieved)
  - most common topologies are bus, ring and star

# Network Technologies

Based on scale

- MAN
  - designed to extend over the entire city
  - may be a single network or a connection of number of LANs

# Network Technologies

Based on scale

- WAN
  - provides long-distance transmission of data over large geographical areas that may comprise a country, continent or even the globe
  - not restricted in size

# What is a network?

Every network includes:

- At least two nodes
- A cable or wireless pathway, called Transmission Media
- Rules, called Protocols, so that computers can use the unified principle of data communication
- Networking Interface Cards (NIC)

# Why Layered Architecture?

- To make the design process easy by breaking unmanageable tasks into several smaller and manageable tasks (by divide-and-conquer approach)
- Modularity and clear interfaces, so as to provide comparability between the different providers' components
- Ensure independence of layers, so that implementation of each layer can be changed or modified without affecting other layers
- Each layer can be analyzed and tested independently of all other layers

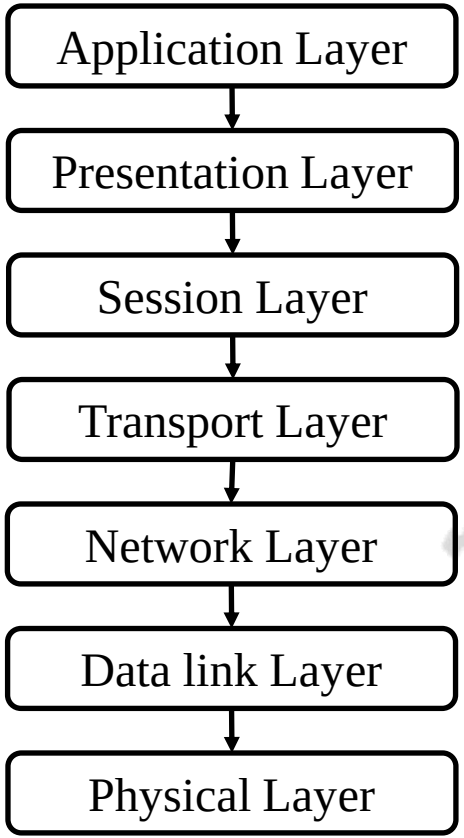
# OSI reference model

- OSI stands for Open Systems Interconnection
- It has been developed by ISO – “International Organization of Standardization”
- It is a 7 layer architecture
- Each layer is responsible for specific functionality
- All these 7 layers work collaboratively to transmit the data from one end (top to bottom) and receive the data at other end (bottom to top)

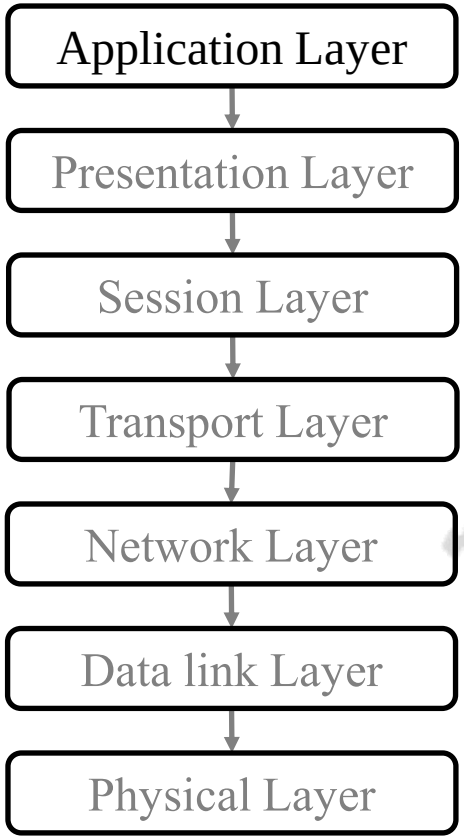
# OSI reference model (terminology)

- Protocol
  - is a formal set of rules and conventions that governs how computers exchange information over a network medium.

# OSI reference model

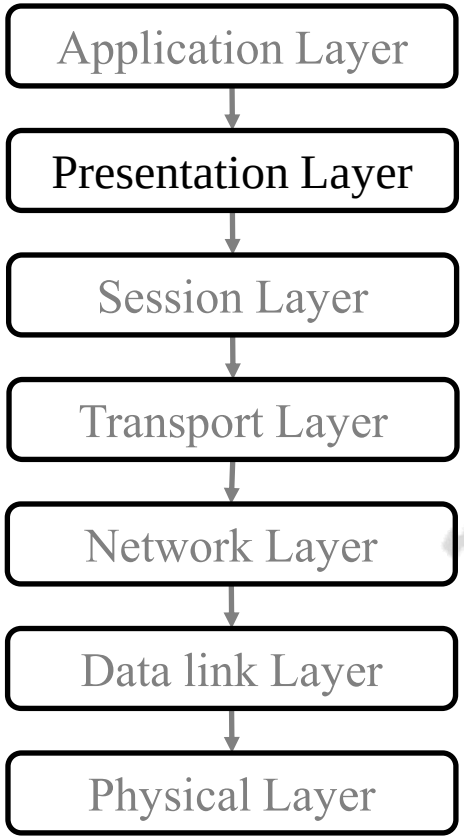


# OSI reference model and its services



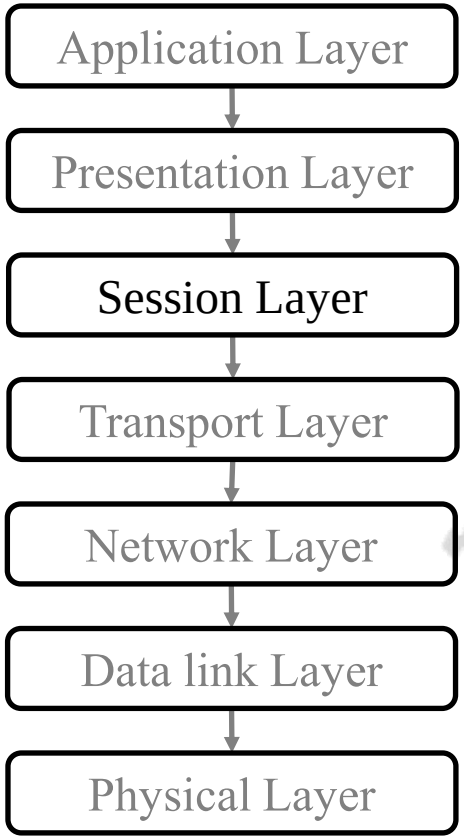

- This layer is responsible to generate the data, which has to be transferred over the network
- Eg: browser

# OSI reference model and its services



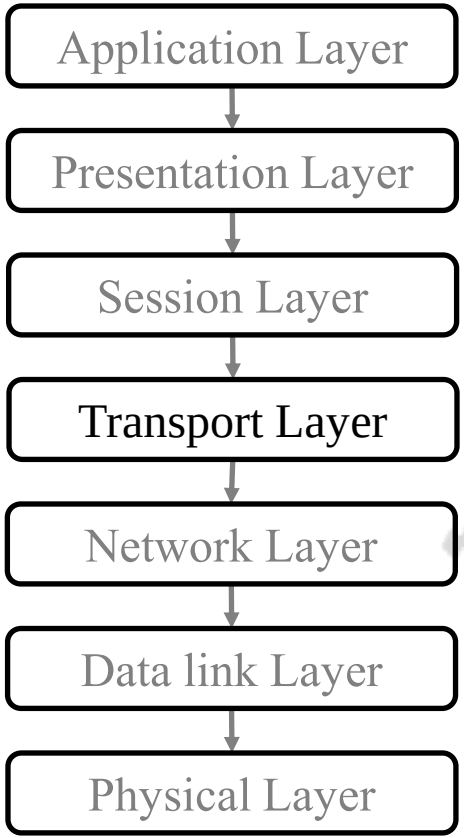

- The data from the application layer is extracted here and converted as per the required format to transmit over the network
- The functions of the presentation layer are :
  - Translation
  - Encryption/ Decryption
  - Compression

# OSI reference model and its services



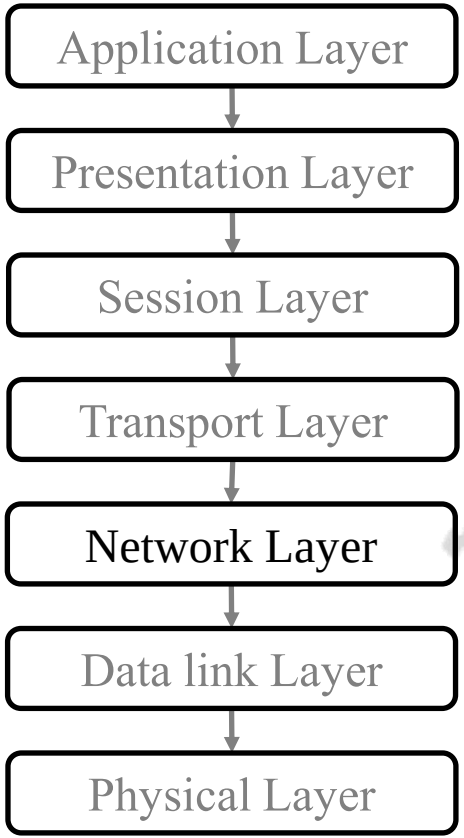

- This layer is responsible for establishment of connection, maintenance of sessions, authentication and security

# OSI reference model and its services



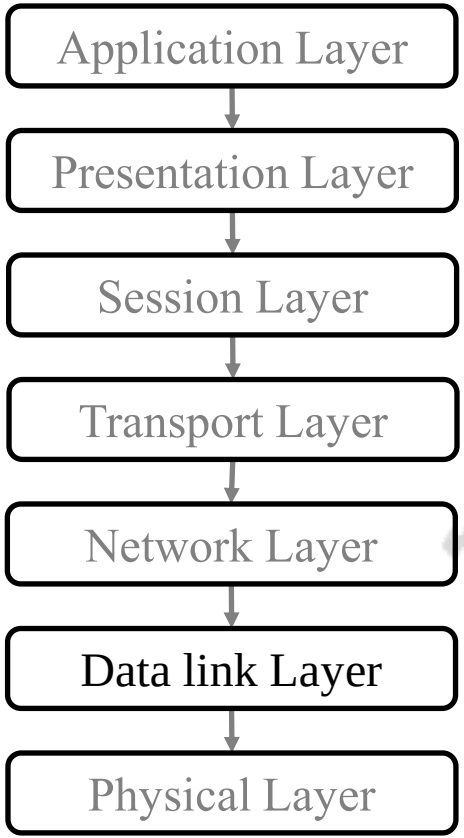

- The data in the transport layer is referred to as segments
- It is responsible for the End to End delivery of the complete message
- The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found
- Two type of services are provided:
  - Connection oriented
  - Connection less

# OSI reference model and its services



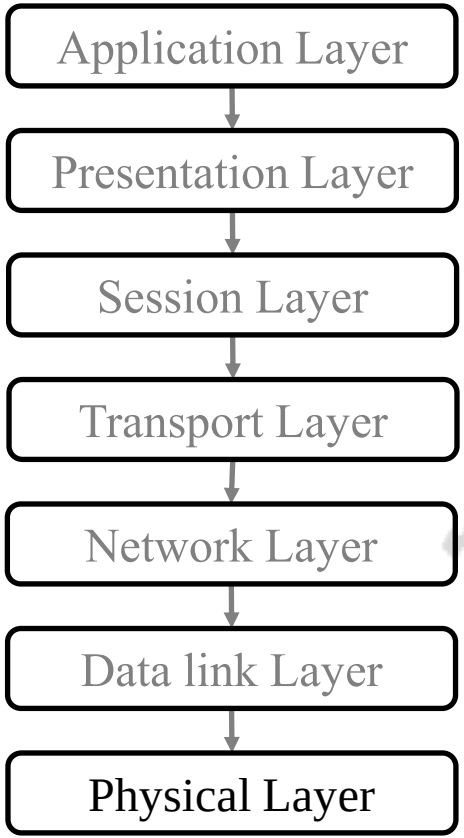

- Network layer works for the transmission of data
- It also takes care of packet routing i.e. selection of the shortest path
- The sender & receiver's IP address are placed in the header by the network layer.

# OSI reference model and its services



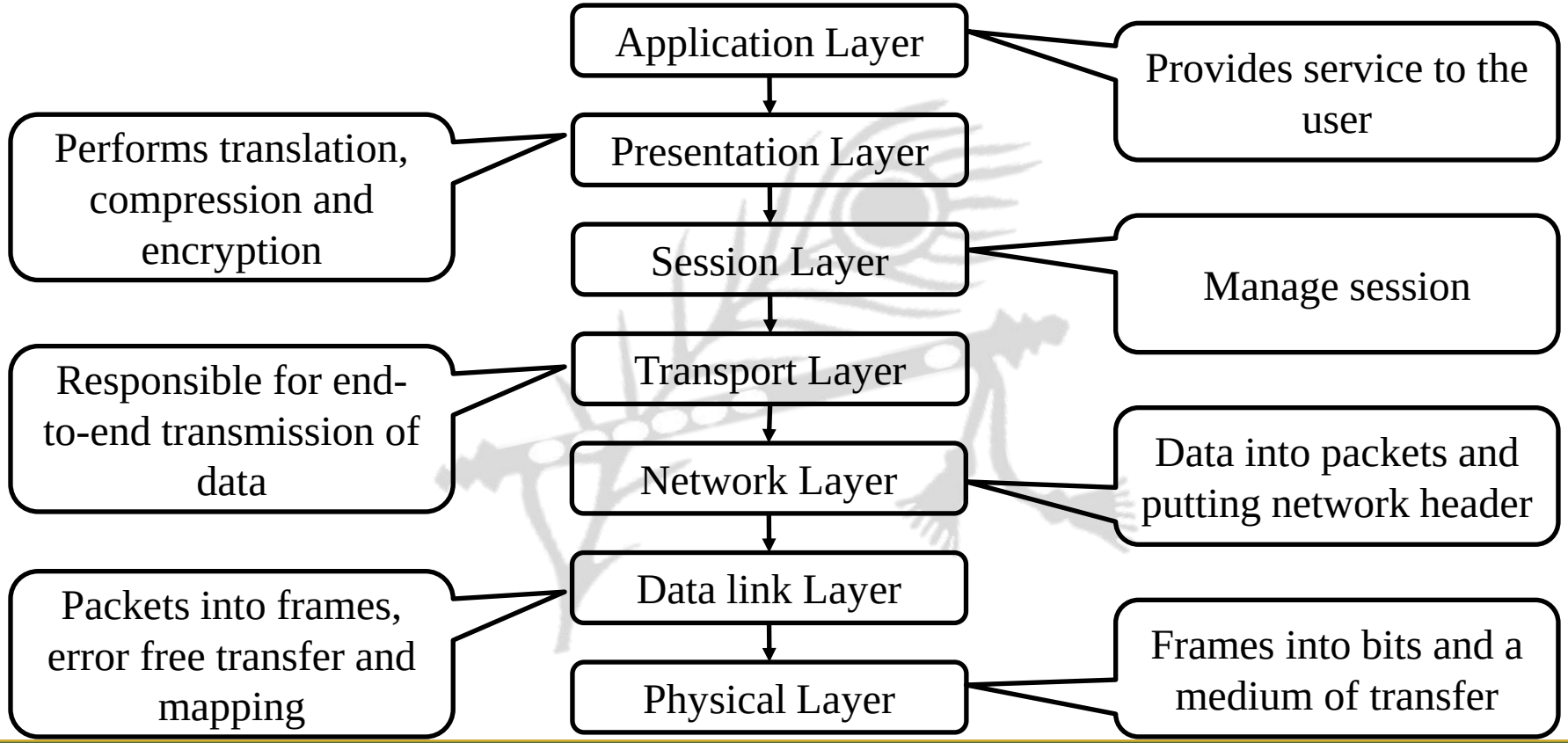

- The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer
- When a packet arrives, it is the responsibility of DLL to transmit it to the Host using its MAC address.
- Data Link Layer is divided into two sub layers :
  - Logical Link Control (LLC)
  - Media Access Control (MAC)

# OSI reference model and its services



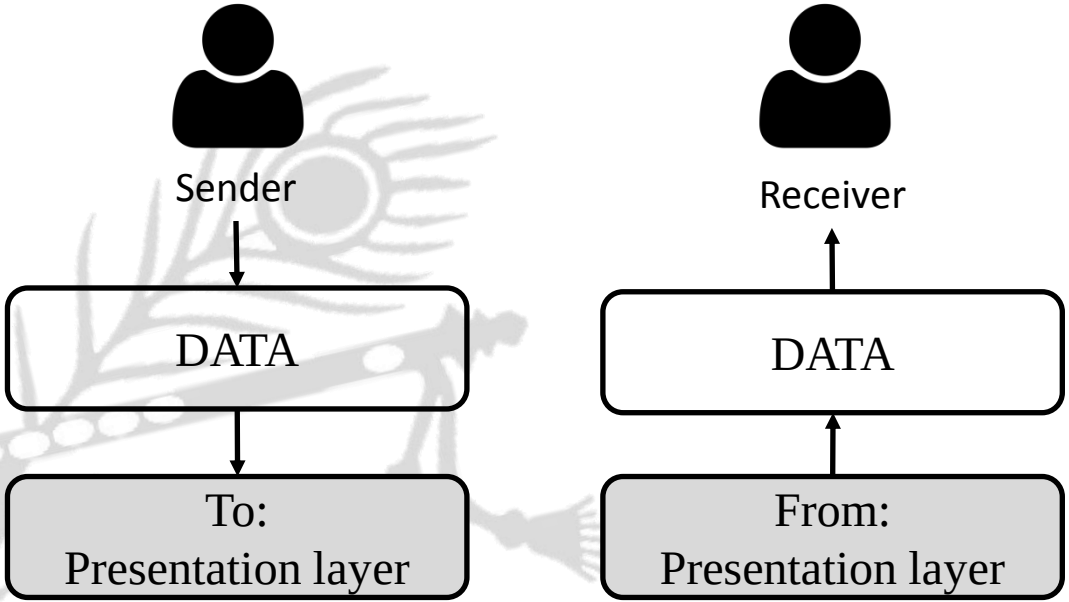

- It is responsible for the actual physical connection between the devices
- The physical layer contains information in the form of bits
- It is responsible for transmitting individual bits
- When receiving data, this layer will get the signal and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

# OSI reference model and its services (in brief)



# OSI reference model and its services (review)

Application Layer

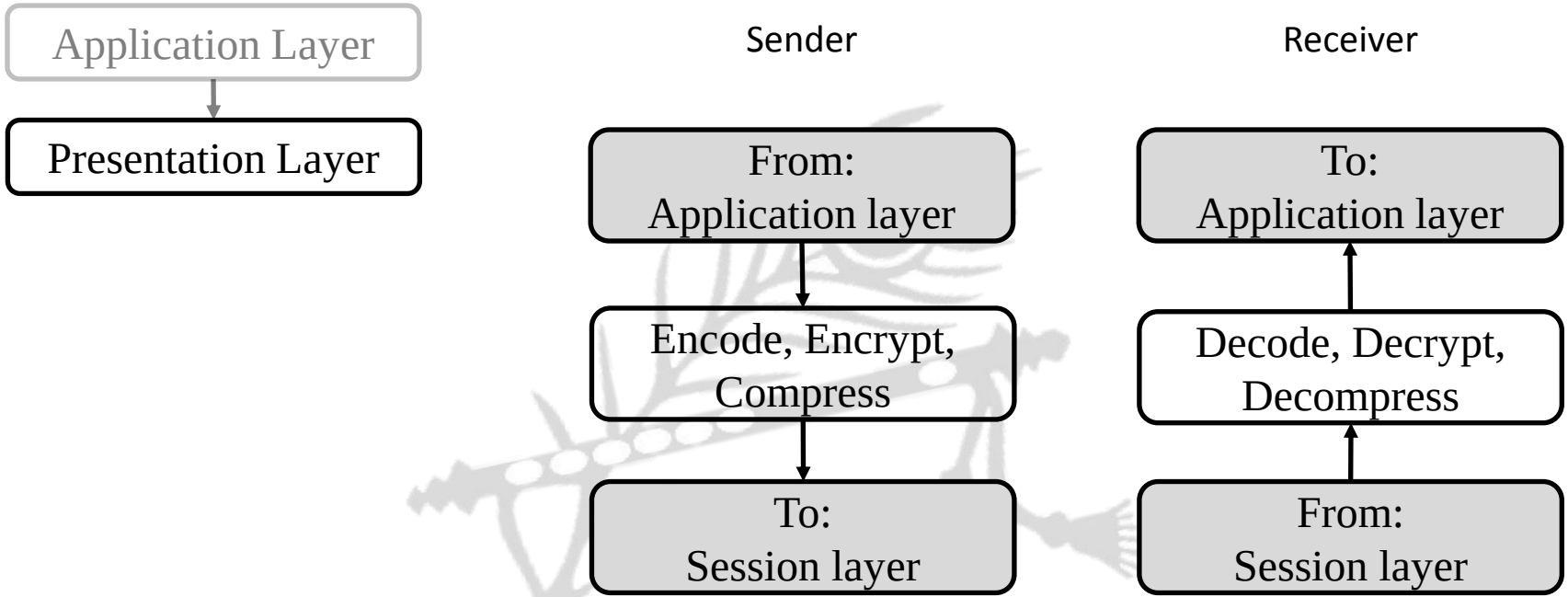


# OSI reference model and its services (review)

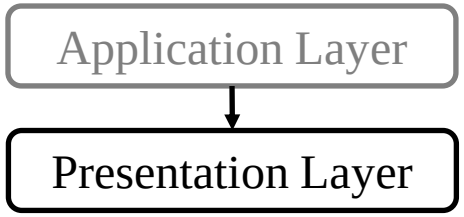
Application Layer

- responsible for generating the data
- contains a variety of protocols that are commonly needed by users
  - HTTP
  - FTP
  - SMTP

# OSI reference model and its services (review)

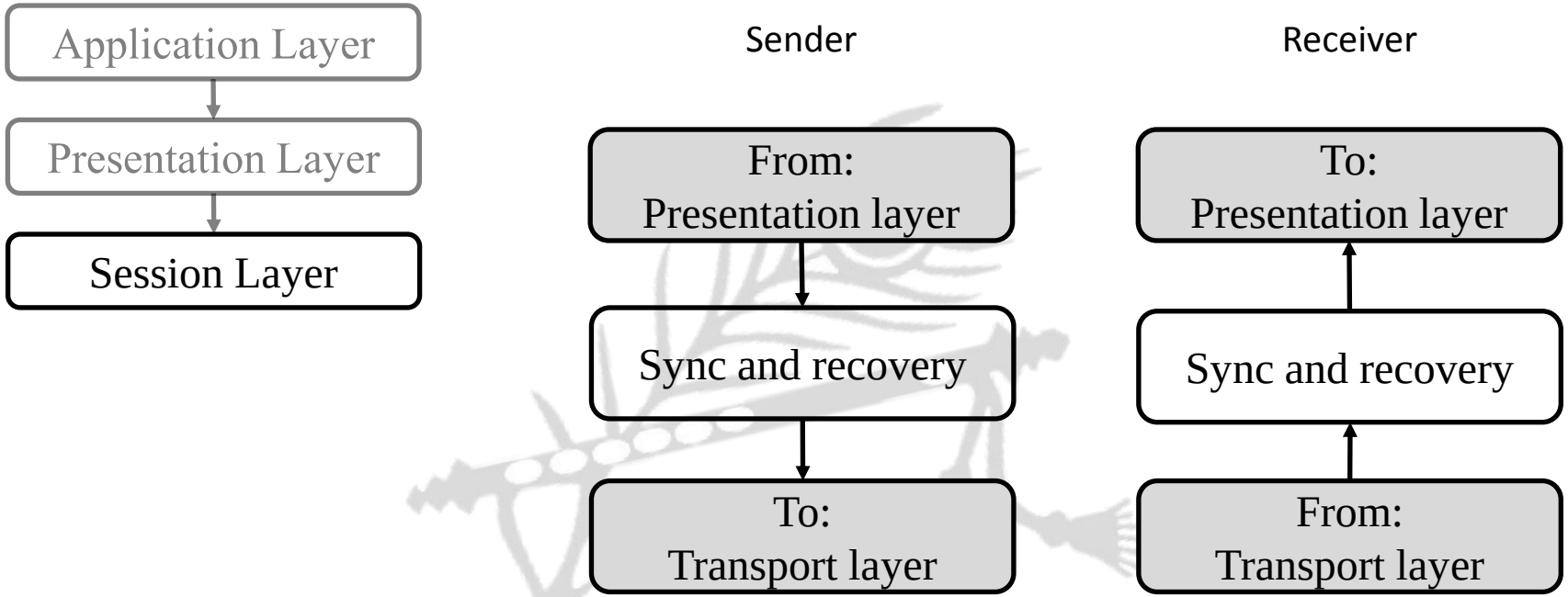


# OSI reference model and its services (review)

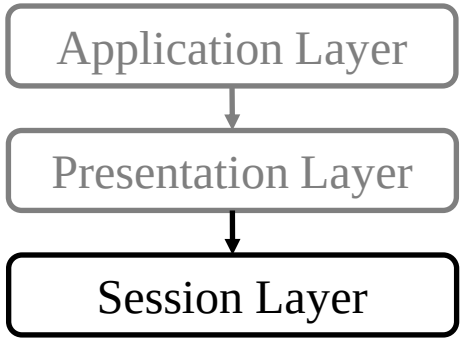



- Purpose
  - Make it possible for computers with different data representations to communicate
- Concerns
  - Syntax and semantics of information transmitted
  - Understands the nature of the data being transmitted
  - Converts ASCII, EBCDIC, etc

# OSI reference model and its services (review)

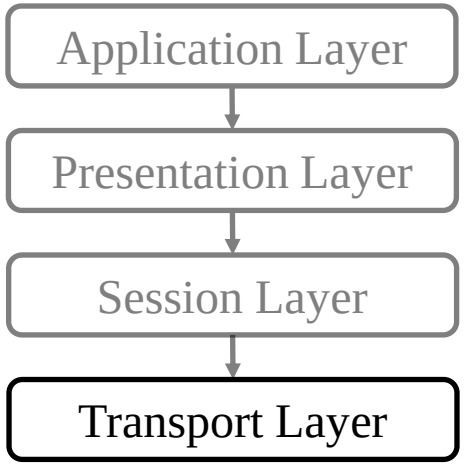


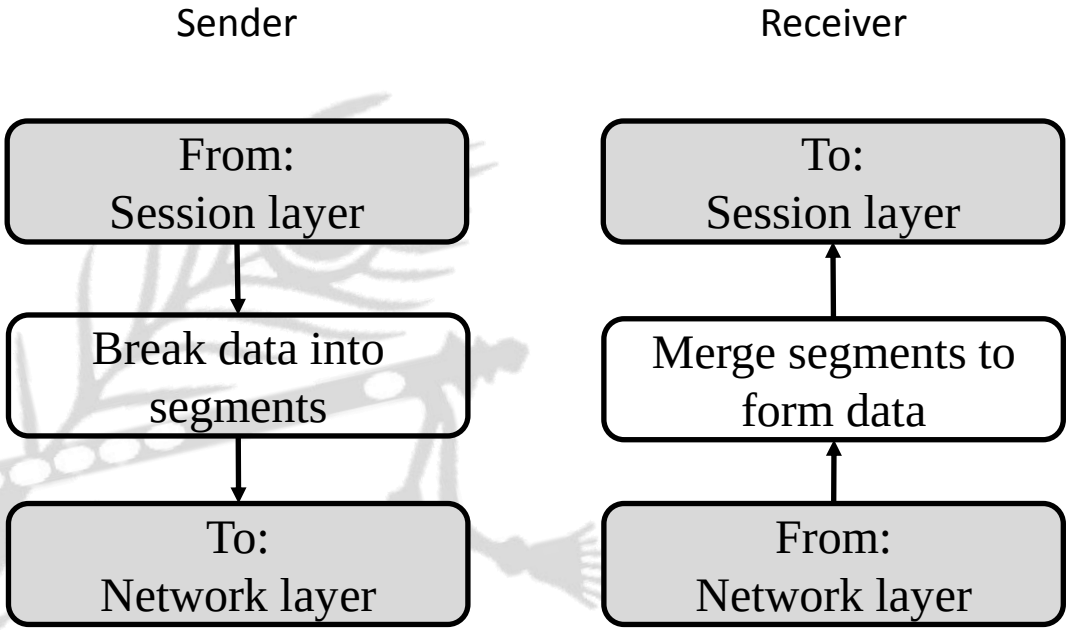
# OSI reference model and its services (review)



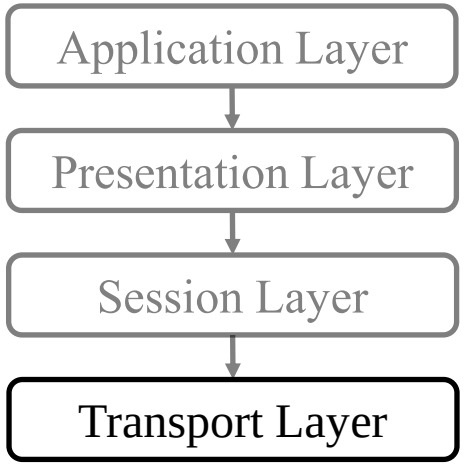

- Purpose
  - Allow users on different machines to establish sessions between them
- Concerns
  - Authentication and authorization
  - Check Pointing
  - Dialog control
  - Logical grouping of operation
  - Synchronization

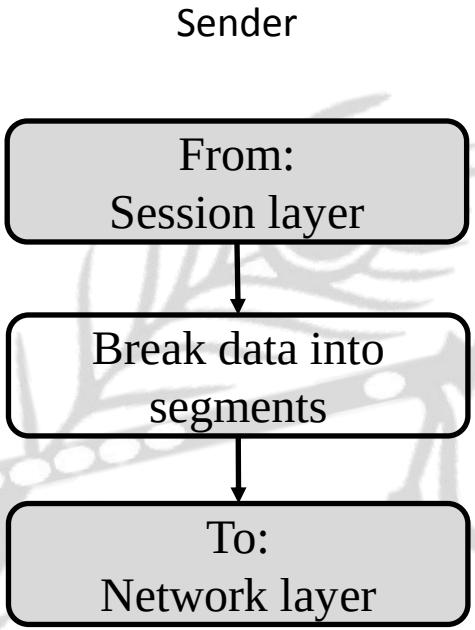
# OSI reference model and its services (review)

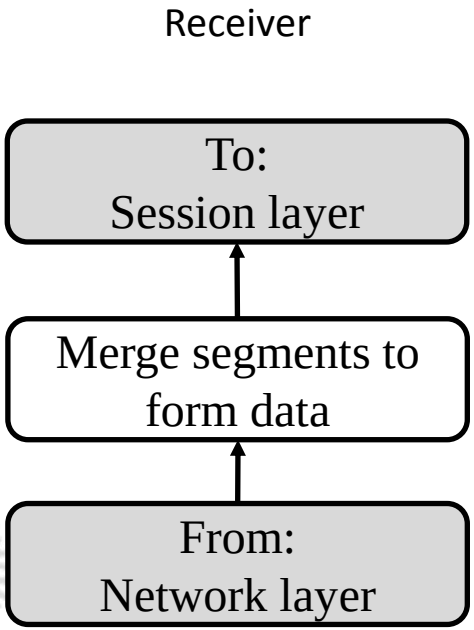



# OSI reference model and its services (review)



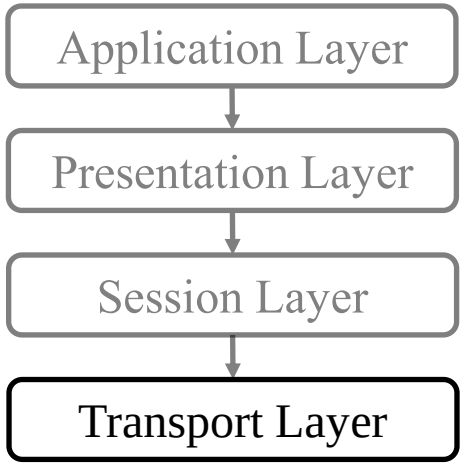



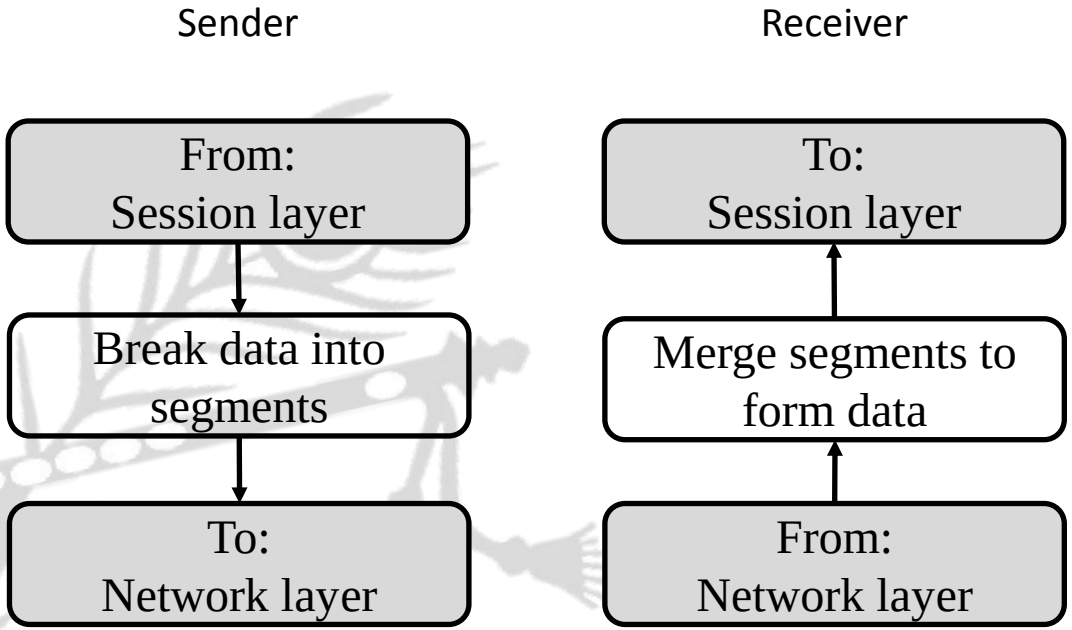




Two protocols used in this layer:

- TCP – follow same route
- UDP – may follow same route

# OSI reference model and its services (review)

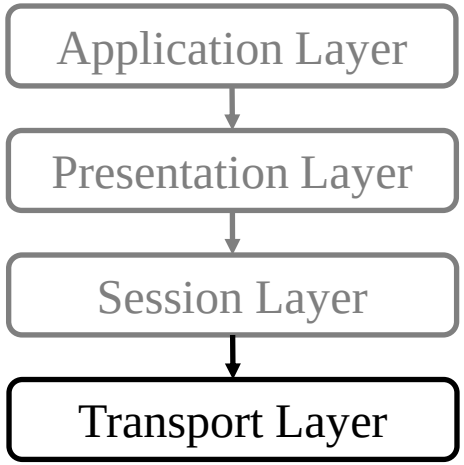



Function of this layer:

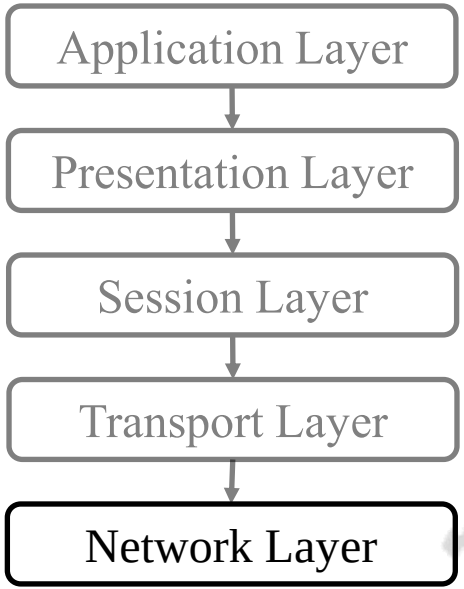
- Service point addressing
- Segmentation and reassembling
- Connection control
- Flow control
- Error control

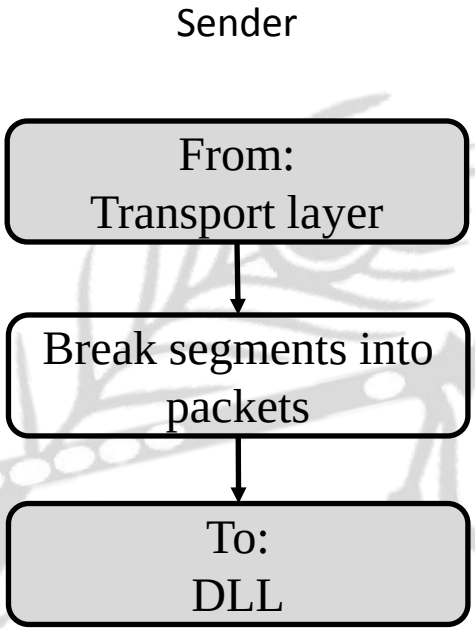
# OSI reference model and its services (review)

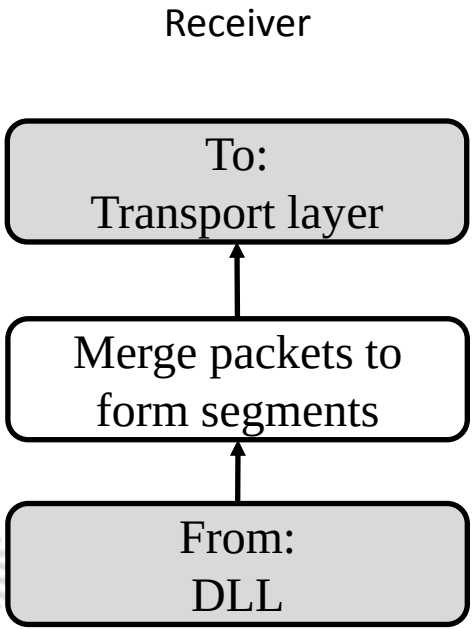



- Purpose
  - Accept data from above it, split it up into smaller units, pass them to network layer, and ensure that the pieces all arrive correctly at the other end
- Concerns
  - Service Decisions: What type of service to provide; error-free point to point, datagram, etc
  - End-to-end: it carries data all the way from the source to the destination
  - Reliability: Ensures that packets arrive at their destination
  - Hides network: Allows details of the network to be hidden from higher level layers
  - Mapping: Determines which messages belong to which connection
  - Flow control: keeps a fast transmitter from flooding a slow receiver

# OSI reference model and its services (review)



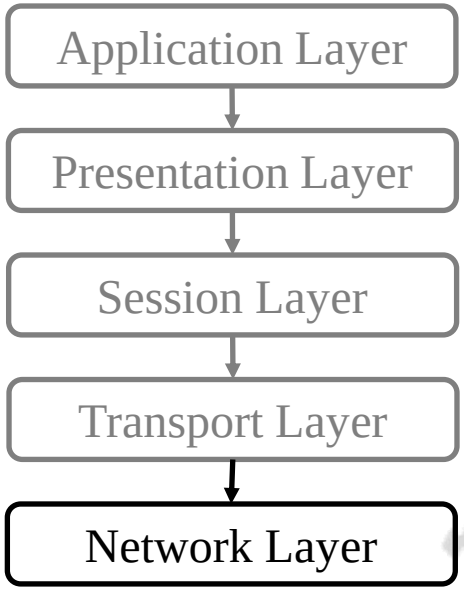




Protocol used:

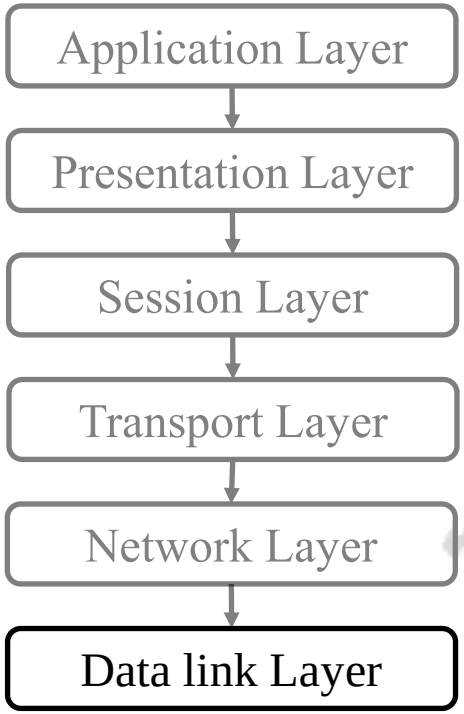
- IP

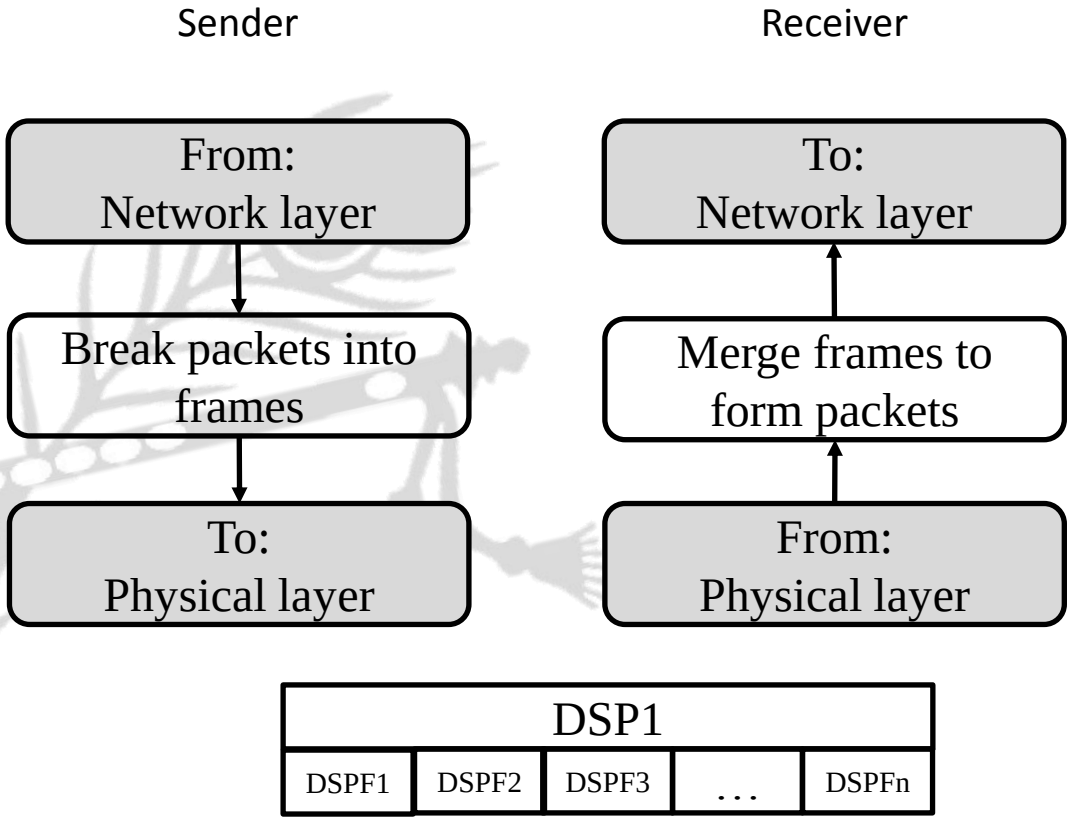
# OSI reference model and its services (review)



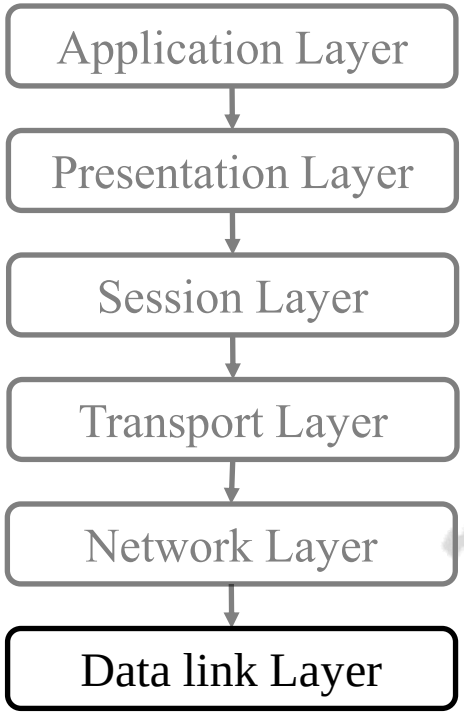

- Purpose
  - Route packets from source to destination
- Concerns
  - Routing: What path is followed by packets from source to destination. Can be based on a static table, can be determined when the connection is created, or can be highly dynamic, being determined a new for each packet, to reflect the current network load
  - Congestion: Controls the number packets in the subnet
  - QoS: Quality of Service provided
  - Fragmentation
  - Heterogeneity: Interfacing so that one type of network can talk to another
  - Addressing, packet size, protocols

# OSI reference model and its services (review)



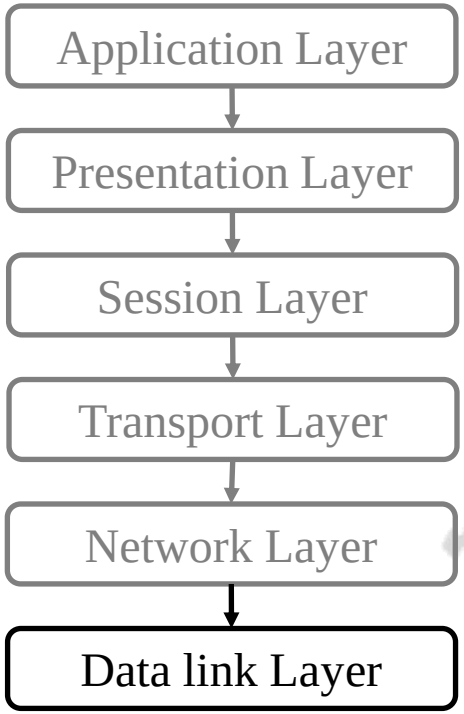
# OSI reference model and its services (review)




It contains two sub-layers:

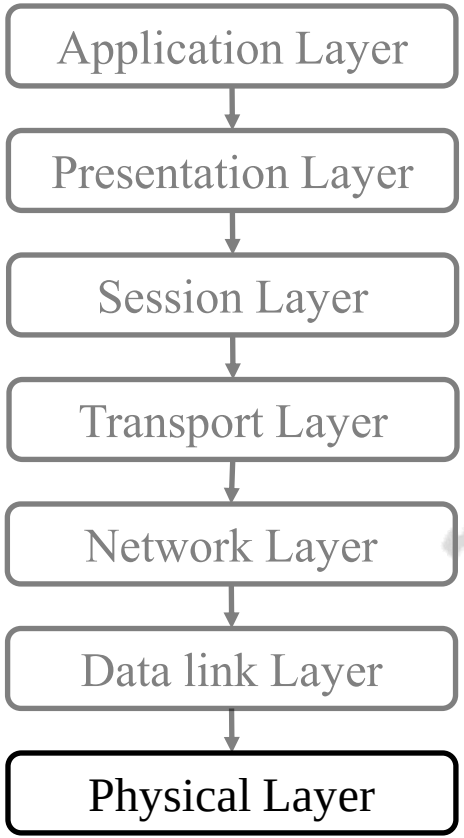
- Logical Link Control Layer
  - It identifies the address of the network layer protocol from the header
  - It also provides flow control
- Media Access Control Layer
  - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer

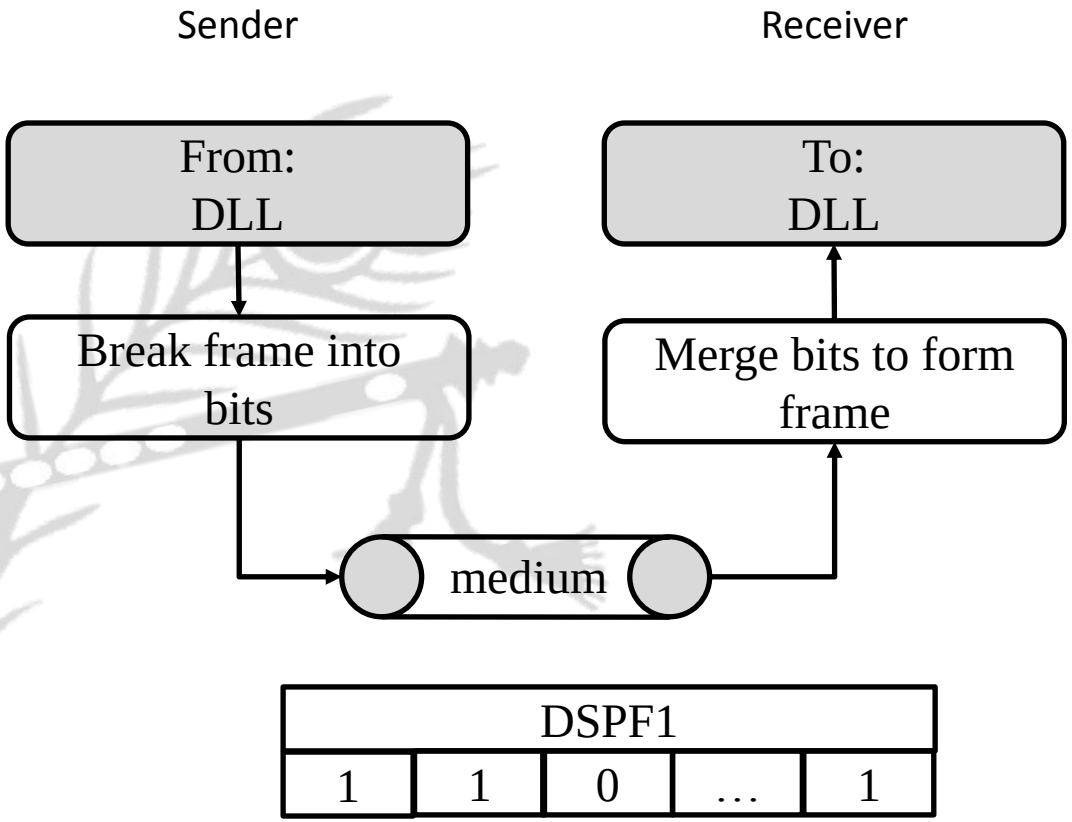
# OSI reference model and its services (review)



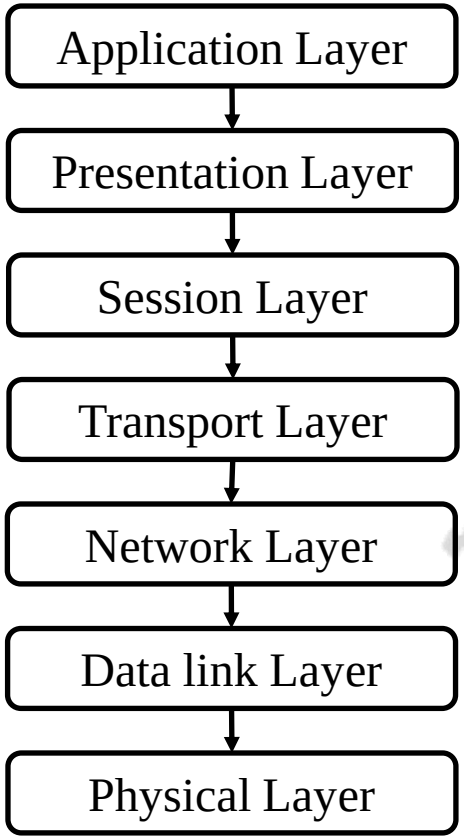

- Purpose
  - Transform a raw transmission line into a line that appears free of undetected transmission errors to the networks layer
- Concerns
  - Framing: Breaks apart input data into frames and transmit the frames sequentially
  - Error handling: if the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame
  - Flow control: keeps a fast transmitter from drowning a slow receiver in data
  - Physical Addressing
  - Access Control (CSMA/CD, Token passing)

# OSI reference model and its services (review)



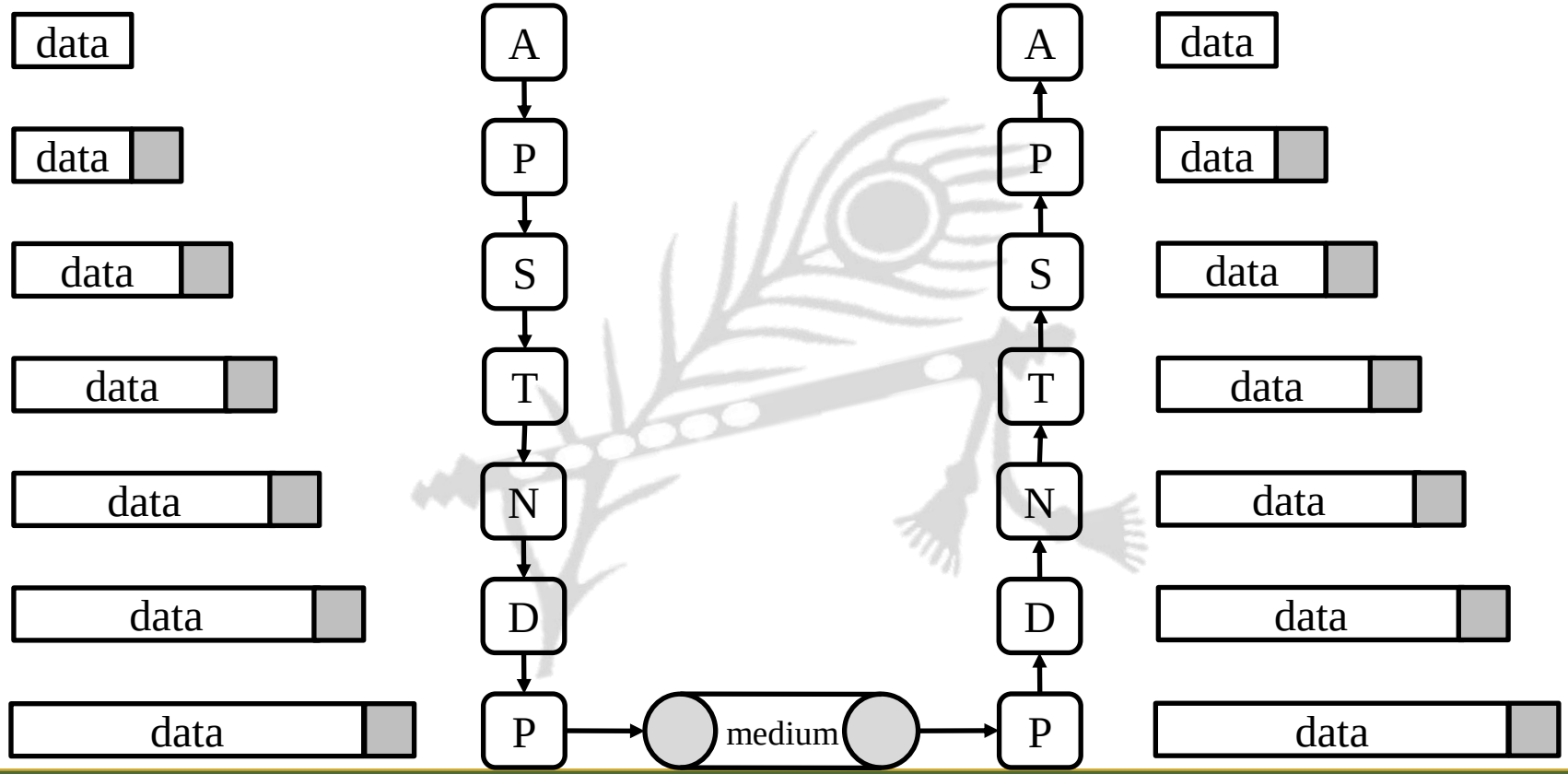



# OSI reference model and its services (review)

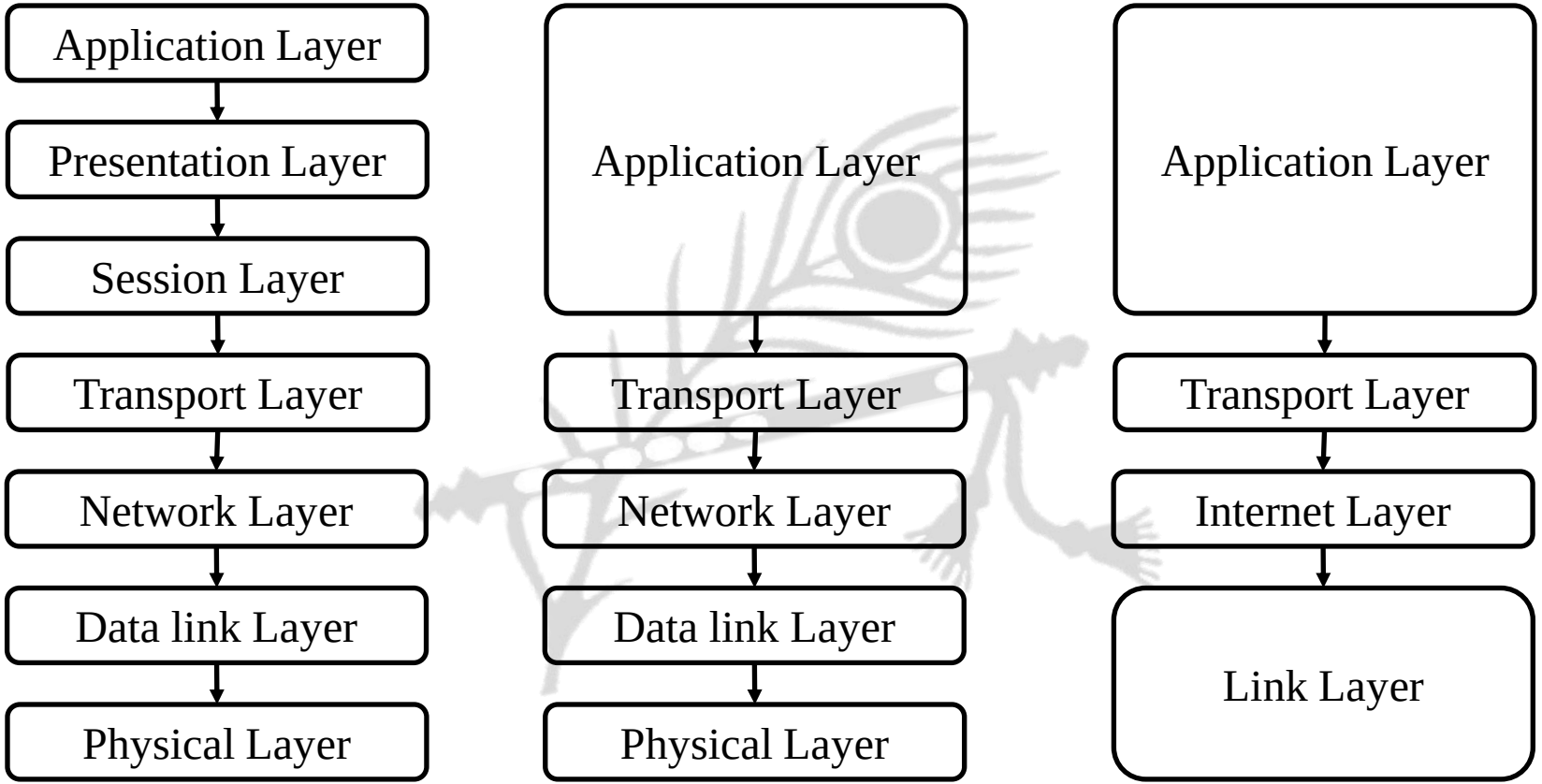



- Purpose
  - Transmits raw bits across a medium
- Functional
  - Flow of data (simplex, half duplex, full duplex)
  - Topology
  - Encoding

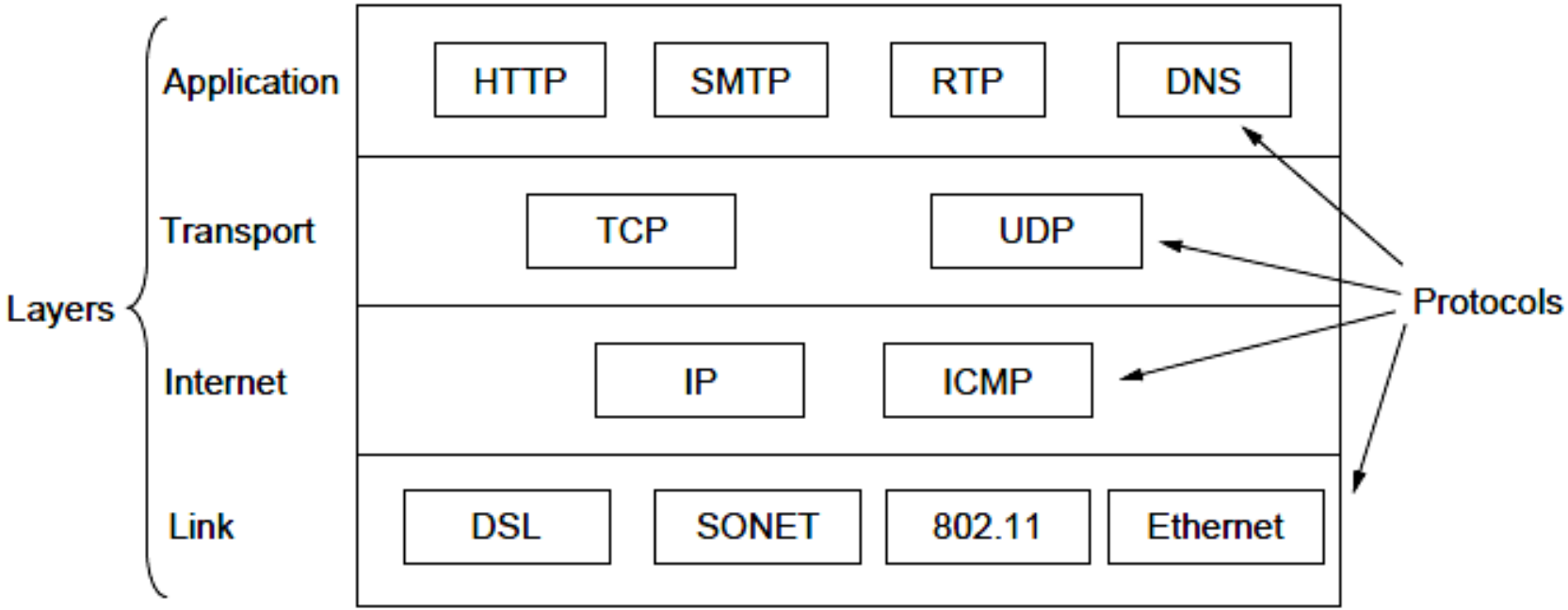
# An exchange using OSI reference model



# TCP/IP reference model



# TCP/IP reference model



# TCP/IP reference model

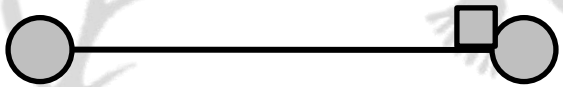
- Concepts central to the OSI model
  - Services
  - Interfaces
  - Protocols
- OSI has good definition of service, interface, and protocol. Fits well with object oriented programming concepts.
- Protocols are better hidden
- TCP/IP model did not distinguish between service, interface, and protocol
- With TCP/IP, the protocols came first; model was just a description of the protocols

# Transmission Mode

- Three types of data flow mode can be used
  - Simplex
  - Half duplex
  - Full duplex

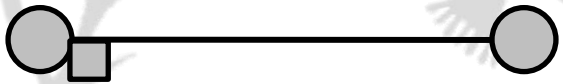
# Transmission Mode

- Simplex
  - there is only unidirectional flow of data
  - only one of the node on a link can transmit, the other can only receive
  - this mode use the entire capacity of the channel to send data in one direction
  - Eg: one way road



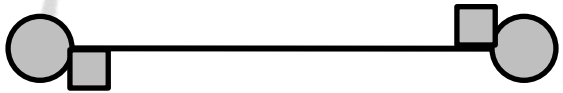
# Transmission Mode

- Half duplex
  - there is bidirectional flow of data but at a time only one node can send
  - each node can both transmit and receive, but not at the same time
  - when one node is sending, the other can only receive, and vice versa
  - the entire capacity of the channel can be utilized for each direction
  - Eg: walkie-talkies



# Transmission Mode

- Full duplex
  - there is bidirectional flow of data
  - each node can both transmit as well as receive simultaneously which can be achieved by two ways
    - either the link must contain two physically separate transmission paths, one for sending and other for receiving OR
    - the capacity is divided between signals travelling in both directions
  - the entire capacity of the channel can be utilized for both direction
  - Eg: mobile communication



# Networking Hardware

- Networking hardware includes all computers, peripherals, interface cards and other equipment needed to perform data-processing and communications within the network like
  - Network Interface Card
  - Switch
  - Router
  - Bridge etc

# Networking Hardware

- Network Interface Card
  - Network interface cards, commonly referred to as NICs, are used to connect a PC to a network
  - The NIC provides a physical connection between the networking cable and the computer's internal bus
  - NICs come in three basic varieties: 8-bit, 16-bit, and 32-bit. The larger the number of bits that can be transferred to the NIC, the faster the NIC can transfer data to the network cable

# Networking Hardware

- Network Interface Card

# Networking Hardware

- Hub
  - A hub joins multiple computers (or other network devices) together to form a single network
  - On this network, all computers can communicate directly with each other
  - The networking hub is a junction box with several ports in the back for receiving the Ethernet cables that are plugged into each computer on the LAN

# Networking Hardware

- Hub (Types)
  - Passive: This type of hub does not amplify or boost the signal. It does not manipulate or view the traffic that crosses it. The passive hub does not require electrical power to work.
  - Active: It amplifies the incoming signal before passing it to the other ports. It requires AC power to do the task.
  - Intelligent: They are also called as smart hubs. It function as an active hub and also include diagnostic capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

# Networking Hardware

- Repeater
  - Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater
  - A repeater is an electronic device that receives a signal, cleans the unnecessary noise, regenerates it, and retransmits it at a higher power level so that the signal can cover longer distances without degradation

# Networking Hardware

- Switch
  - A network switch is a small hardware device that joins multiple computers together within one network
  - Network switches appear nearly identical to network hubs, but a switch generally contains more intelligence than a hub
  - Unlike hubs, network switches are capable of inspecting data packets as they are received, determining the source and destination device of each packet, and forwarding them appropriately
  - Allow several users to send information over a network at the same time without slowing each other down

# Networking Hardware

- Router
  - A device to interconnect SIMILAR networks, e.g. similar protocols and workstations and servers
  - A router is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them
  - Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another

# Networking Hardware

- Bridge
  - A bridge is a device that connects a local network to another local network
  - The function of a bridge is to connect separate networks together
  - Bridges map the Ethernet addresses of the nodes residing on each network segment and allow only necessary traffic to pass through the bridge. When a packet is received by the bridge, the bridge determines the destination and source segments

# Networking Hardware

- Bridge (types)
  - Local bridges: Directly connect local area networks (LANs)
  - Remote bridges: Can be used to create a wide area network (WAN) link between LANs
  - Wireless bridges: Can be used to join LANs or connect remote stations to LANs (wirelessly)

# Networking Hardware

- Gateway
  - Gateways are used to interconnect two different networks having different protocols
  - Networks using different protocols use different addressing formats
  - A gateway is a network point acts as an entrance to another network
  - Gateways are also called protocol converters

# Difference

- Bridge:
  - device to interconnect two LANs that use the SAME logical link control protocol but may use different medium access control protocols
- Router:
  - device to interconnect SIMILAR networks, e.g. similar protocols and workstations and servers
- Gateway:
  - device to interconnect DISSIMILAR protocols and servers

# Difference

**Hub**

- Physical layer
- signal or bits
- Non-intelligent device
- LAN
- Half duplex
- MAC address

**Switch**

- Data link layer
- frames
- Intelligent device
- LAN
- Half/Full duplex
- MAC address

**Router**

- Network layer
- packets
- Intelligent device
- LAN, MAN, WAN
- Full duplex
- IP address