CN101.3 - Data Communication and Network

Department of Network and Security

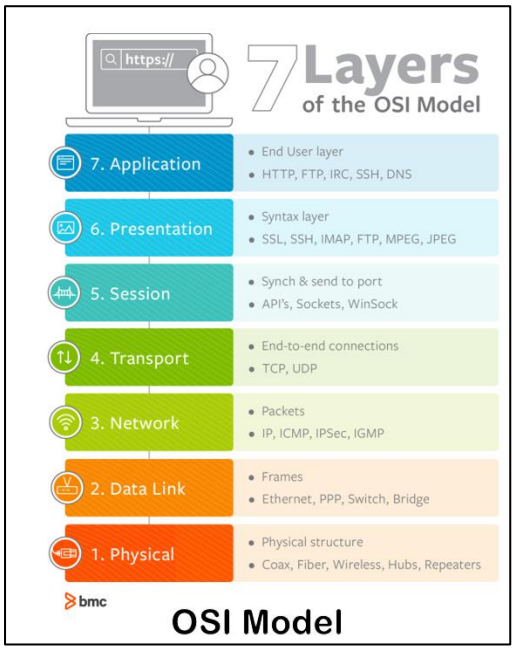
Layered Architecture

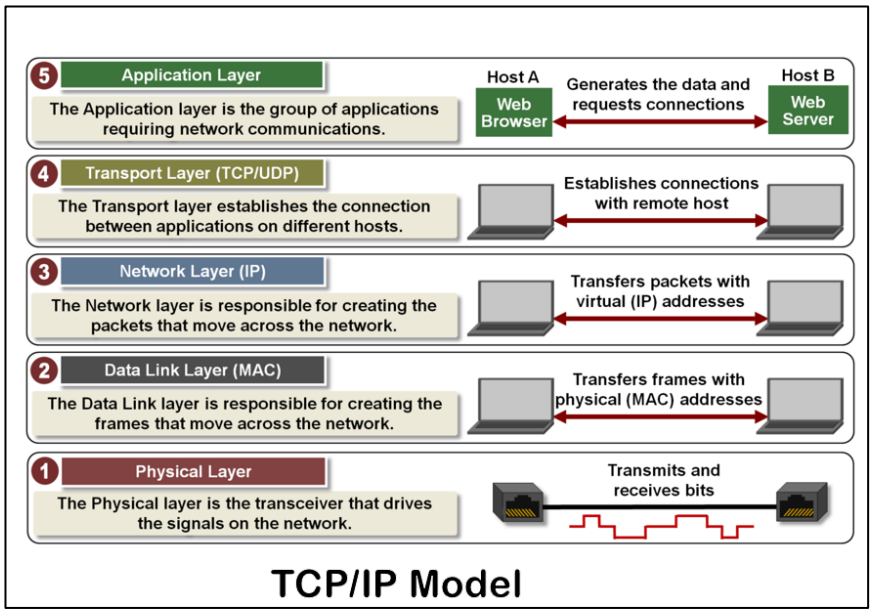
What is Layered Architecture?

Layered Architectures

There are two layered architectures

1. OSI 7 Layer architecture
2. TCP/IP protocol architecture





Why Layering?

- Networks are complex
- We need a way to organize the structure of network functionalities and to reduce the design complexities

Why do we require Layered Architecture?

- Reduce the complexity of the design (Divide and conquer approach) – this approach makes a design process in such a way that the unmanageable task are divided into small manageable tasks.
- Provides the independence of the layers, which is easier to understand and implement.
- Easy to modify without affecting other layers.
- Easy to test where each layer of the layered architecture can be analyzed and tested individually.

The OSI Model

- Stands for "**Open Systems Interconnection**"
- OSI model is a tool used by IT professionals to actually model or trace the actual flow of how data transfers in networks.
- So, basically, the OSI model is a logical model/representation of how the network systems are supposed to send data (or, communicate) to each other.

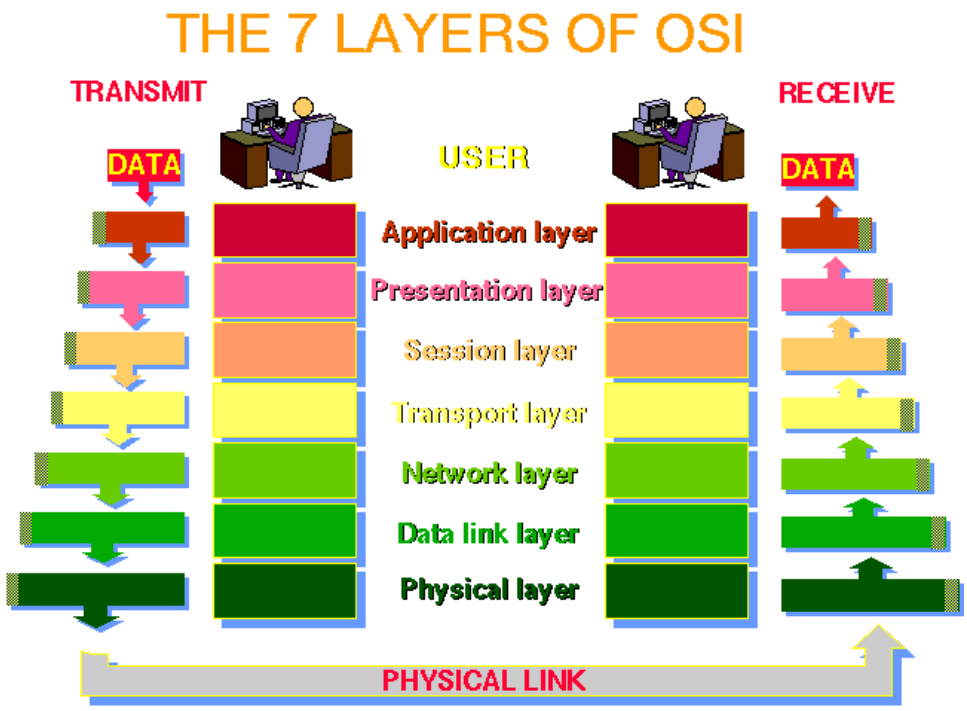
Why OSI Model?

- OSI (Open Systems Interconnection) is a reference model for how applications communicate over a network.
- A reference model is a conceptual framework for understanding relationships.
- OSI model was introduced by International Organization for Standardization (ISO) in 1984

Overview of OSI Model

- The OSI Model is composed of seven layers with **the application layer,** which is **closest to the end user**, at the top, going all the way down to **physical layer**, in which the actual data transfer happens with the use of **a transmission medium**.

How it's work



01. Physical Layer

- This is the layer on which the real transmission of data bits takes place through a medium.
- This layer is, as the name suggests, all the physical stuff that connects the computers together.
    1. Responsible for electrical signals, light signal, radio signals etc.
    2. Hardware layer of the OSI layer
    3. Devices like repeater, hub, cables, Ethernet work on this layer
    4. Protocols like RS232, ATM, FDDI work on this layer

02. Data Link Layer

- This layer is responsible for organizing bits into frames and ensuring hop to hop delivery. Also assign the mac address of sender and receiver.
- This is the layer on which the Switches operate on. Since routers operate at the network level, hence we can say that the MAC address resides at the data link layer.
- All the computers in a specific network get plugged into a switch so that they can communicate with each other.
- Responsible for encoding and decoding of the electrical signals into bits.
- Manages data errors from the physical layer
- Convers electrical signals into frames
- Devices like Switch work at this layer

03. Network Layer

- The main job of this layer is to move packets from source to destination and provide inter-networking.
- This is the layer that the routers operate on. Since routers operate at the network level, hence we can say that the IP address is at the network level.
- Logical addressing (IP Addressing) happens inside the Network layer.
    - Logical Addressing
    - Routing
    - Path determination
- Different network protocols like TCP/ IP, IPX, AppleTalk work at this layer

04. Transport Layer

- This layer has a very important job. It segments data and It decides how much information should be sent at a time. Segment contains Port No, Sequence no and data
- So, when you are communicating with a website, this layer will decide how much data you can transfer and receive at a given point of time.
- Also, this layer provides reliable process to process message delivery and error recovery.
- Responsible for the transparent transfer of data between end systems
- Responsible for end-to-end error recovery and flow control
- Responsible for complete data transfer.
- Protocols like TCP, UDP work here
- UDP – Video Games, Movies, Online Streaming (UDP faster than TCP)
- TCP – WWW, Email, File transfer

05. Session Layer

- This layer has the job of maintaining proper communication by establishing, managing and terminating sessions between two computers. For example, whenever we visit any website, our computer has to create a session with the web server of that website.
- Responsible for establishment, management and termination of connections between applications.
- The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end.
- It deals with session and connection coordination.
- Works with APIs and NETBIOS

06. Presentation Layer

- This is the layer in which **the operating system operates with the data**. Main functions of this layers **includes translation, encryption and compression of data**. Basically User interacts with Application layer, which sends the data down to Presentation layer.
- Responsible for data representation on your screen
- Encryption and decryption of the data
- Responsible for Translation, Compression and Encryption data.

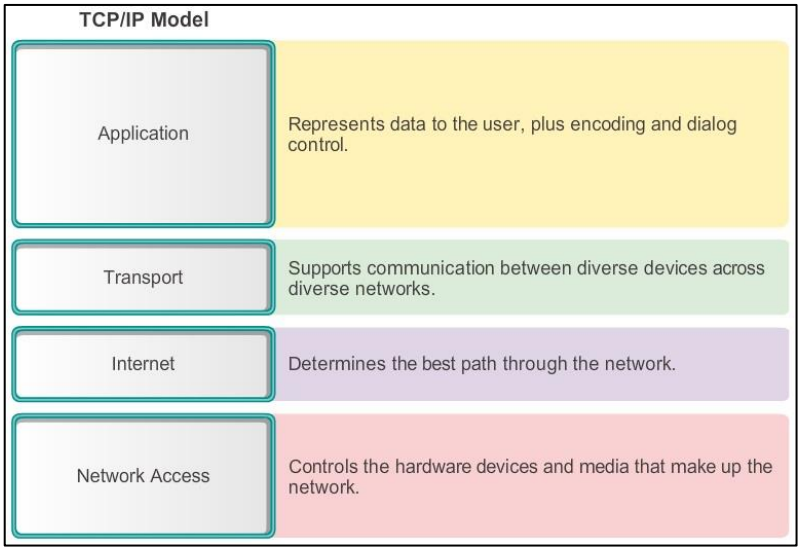
07. Application Layer

- This is the topmost layer in the seven OSI Layers. This is the layer that the end-user (can be a computer programmer, or a regular PC user) is actually interacting with. This layer allows access to network resources.
- Application layer supports application, apps, and end-user processes.
- This layer is responsible for application services for file transfers, e-mail, and other network software services
- Protocols like Telnet, FTP, HTTP work on this layer.

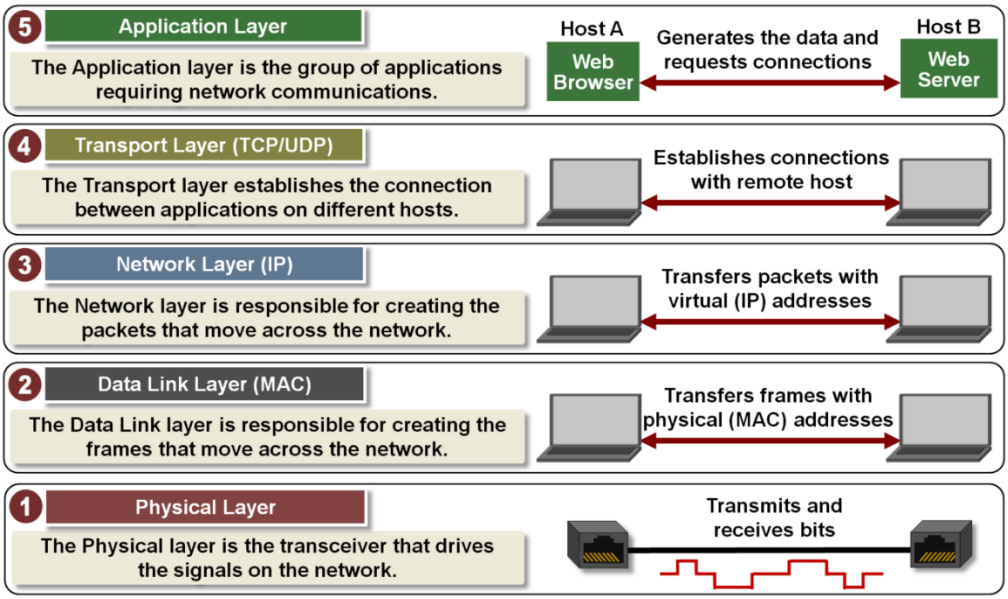
TCP/IP Model

- TCP/IP Model helps you to determine how a specific computer should be connected to the internet and how data should be transmitted between them.
- The purpose of TCP/IP model is to allow communication over large distances.
- TCP/IP stands for Transmission Control Protocol/ Internet Protocol. TCP/IP Protocol Stack is specifically designed as a model to offer highly reliable and end-to-end byte stream over an unreliable internetwork.

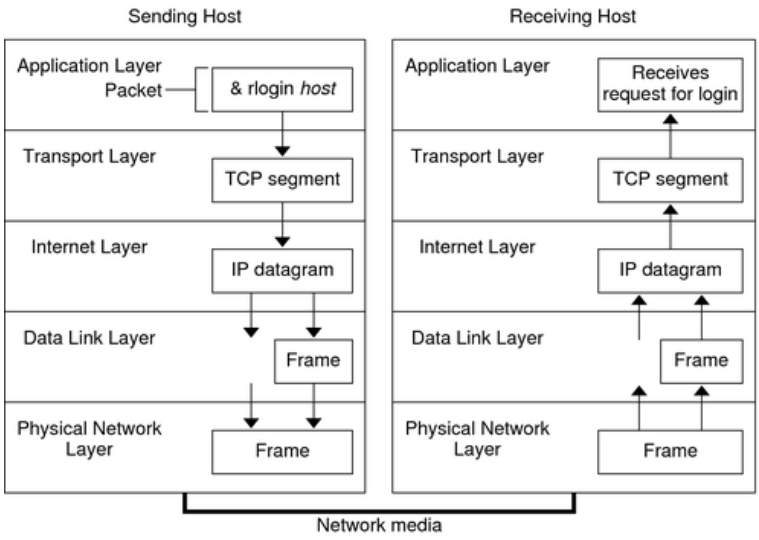
TCP/IP Model-Original



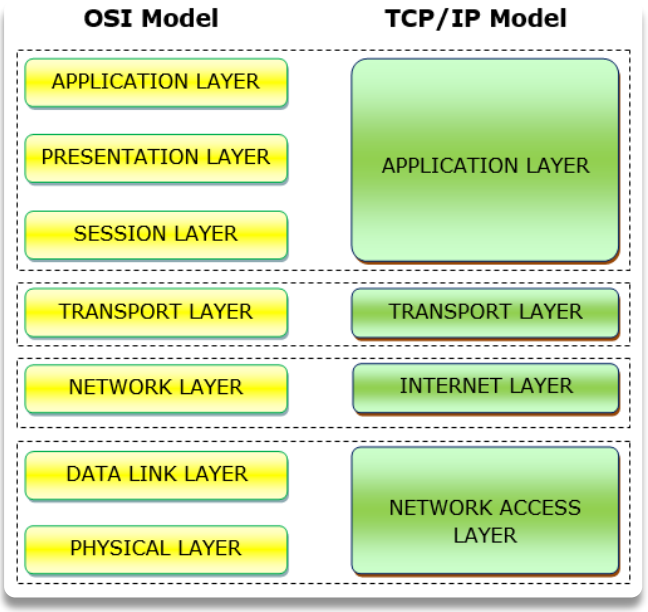
TCP/IP Model-New version



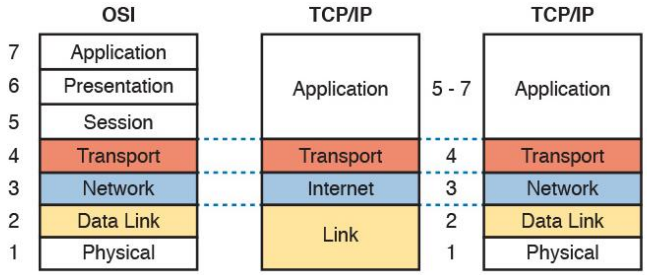
TCP/IP Model

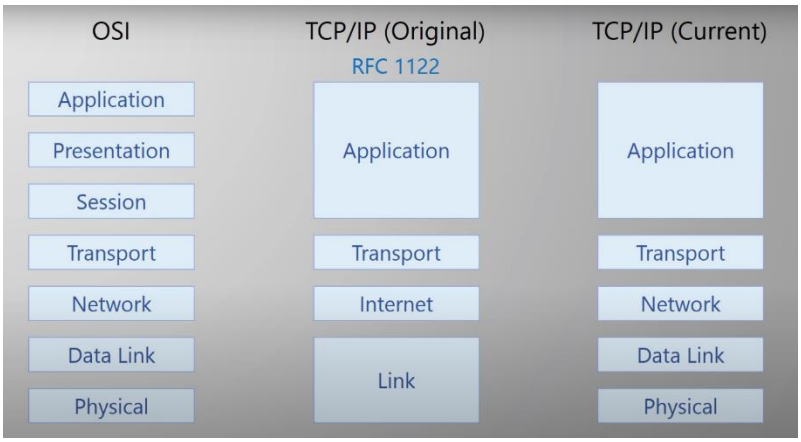


OSI VS TCP/IP



Overall Architecture- Overview





Data link Layer

What is a Protocol?

A set of **rules or procedures** for transmitting data between electronic devices.
Example Computers, smart phones
Any Examples?

- HTTP
- HTTPS
- FTP
- SSH

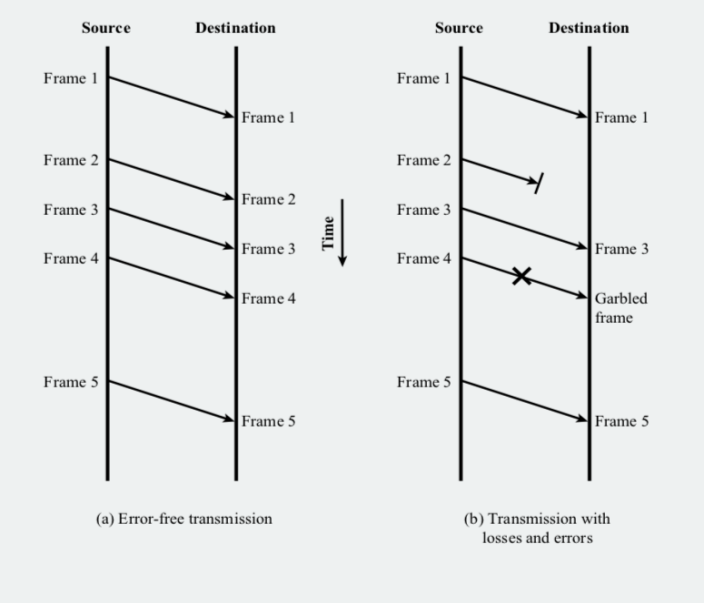
Data Link Layer Responsible for?

- Data Link layer is responsible for **implementation of point-to-point** flow and **error control** mechanism
- Some requirements and objectives for effective data communication between two directly connected transmitting – receiving stations are
    - Flow Control
    - Frame Synchronization
    - Error Control

Flow Control

- Technique for assuring that a transmitting entity does not over- whelm a receiving entity data
- The receiving entity typically allocates a data buffer of some maximum length for a transfer
- When data are received the receiver must do a certain amount of processing before passing the data to the higher-level software
- In the absence of flow control, the receiver's buffer may fill up and overflow while it is processing old data

Model of Frame Transmission

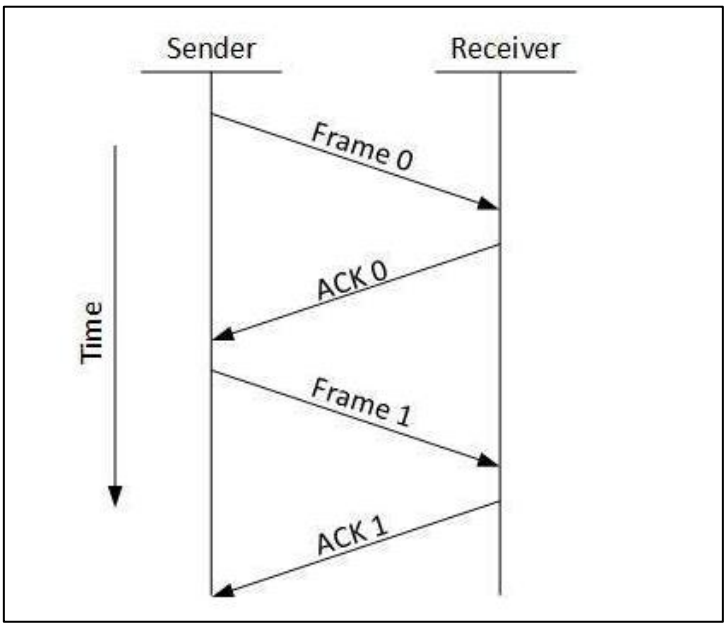


Methods to control the flow

- Stop and Wait Flow Control
- Sliding Window Flow Control

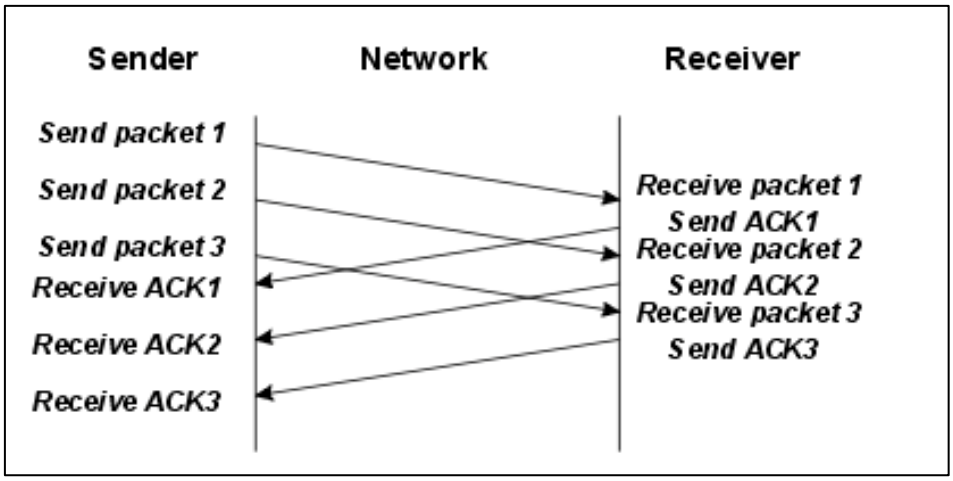
Stop and Wait Flow Control

- This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.
- Simplest form of flow control
    - Source transmits frame
    - Destination receive frame and replies with acknowledgement (ACK)
    - Source waits for ACK before sending next frame
    - Destination can stop flow by not sending ACK



Sliding Window Flow Control

- In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent.
- Receiver has buffer n long
- Transmitter sends up to n frames without ACK
- ACK includes number of next frame expected
- Receiver can ACK frames without permitting further
- transmission. (Receive not Ready)



Error Control Techniques

When data frame is transmitted, there is a possibility that data frame may be lost in the transit, or it is received corrupted.

Requirements for error control mechanism

- Error Detection – The sender and receiver, either both or any, must ascertain that there is some error in the transit
- Retransmission after timeout – If an ACK of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame
- Positive ACK - When the receiver receives a correct frame, it should acknowledge it.
- Negative ACK – When the receiver receives a damaged frame or a duplicate frame, it sends a NACK
- Error Detection – The sender and receiver, either both or any, must ascertain that there is some error in the transit
- Retransmission after timeout – If an ACK of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame
- Positive ACK - When the receiver receives a correct frame, it should acknowledge it.
- Negative ACK – When the receiver receives a damaged frame or a duplicate frame, it sends a NACK

Automatic Repeat Request ARQ

Collective Name for error control mechanism

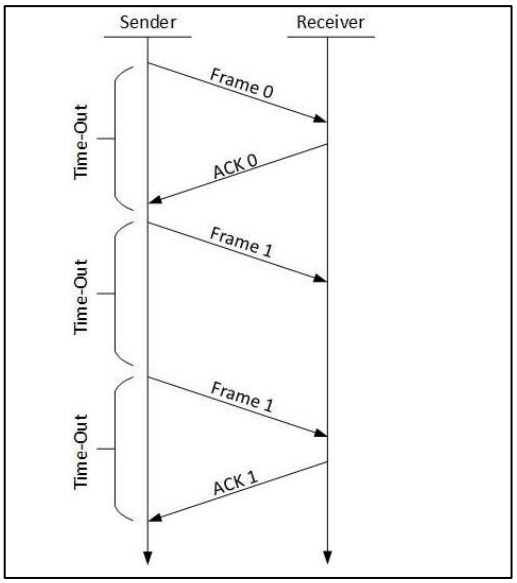
Versions of ARQ,

- Stop and wait ARQ
- Go-Back-N ARQ
- Selective Reject ARQ

Stop-and-wait ARQ

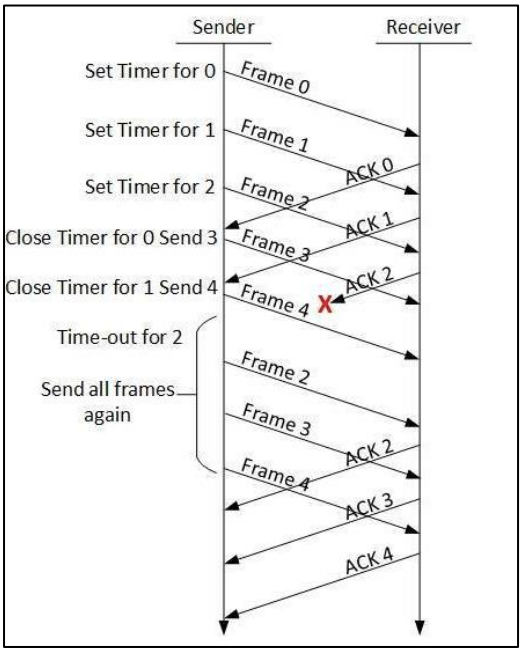
The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.



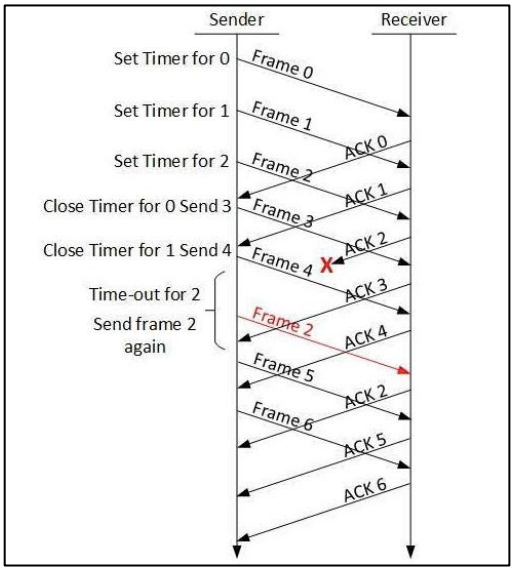
Go-Back-N ARQ

- Stop and wait ARQ mechanism does not utilize the resources at their best, When the acknowledgement is received, the sender sits idle and does nothing.
- In Go-Back-N ARQ method, both sender and receiver maintain a window.

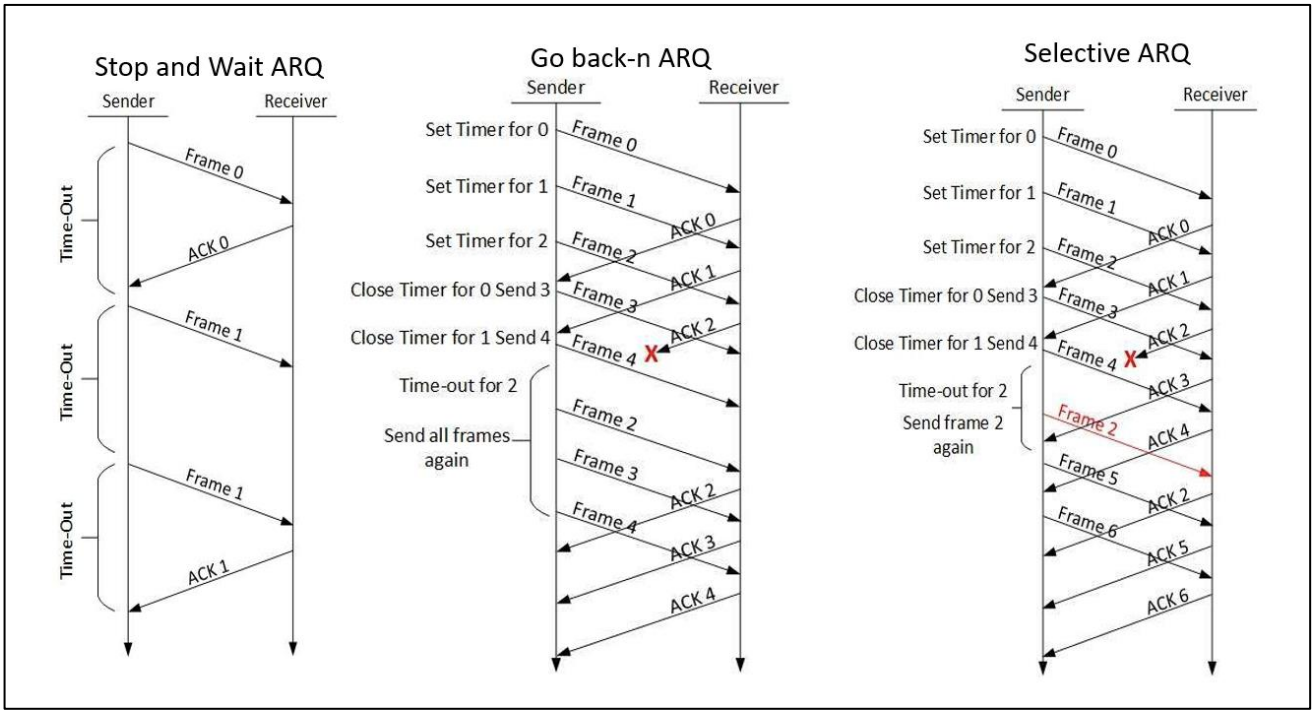


Selective-Reject ARQ

- Also Called selective retransmission
- Only rejected frames are retransmitted
- Subsequent frames are accepted by the receiver and buffered
- Minimize retransmission



ARQ

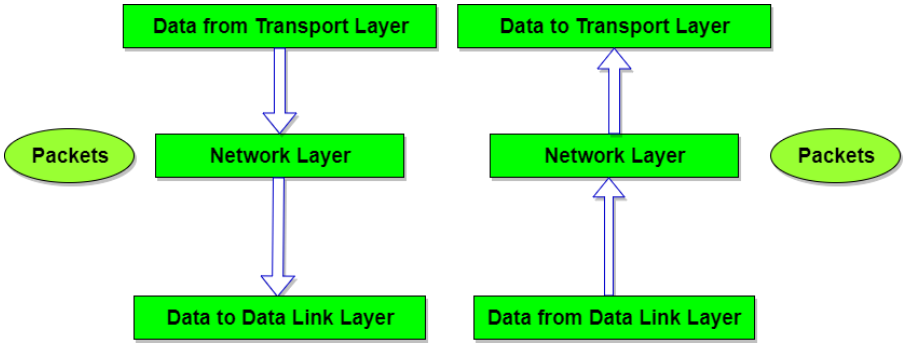


Network Layer

Network Layer Responsible for?

Network layer is Third layer of OSI model and it's responsible for routing packets from one node (networked device) to another between networks

How it's Working?



Protocols that work on this layer

- IP
- ICMP
- IPSEC

Role of the layer

- Logical Addressing
- Routing and Forwarding
- Fragmentation

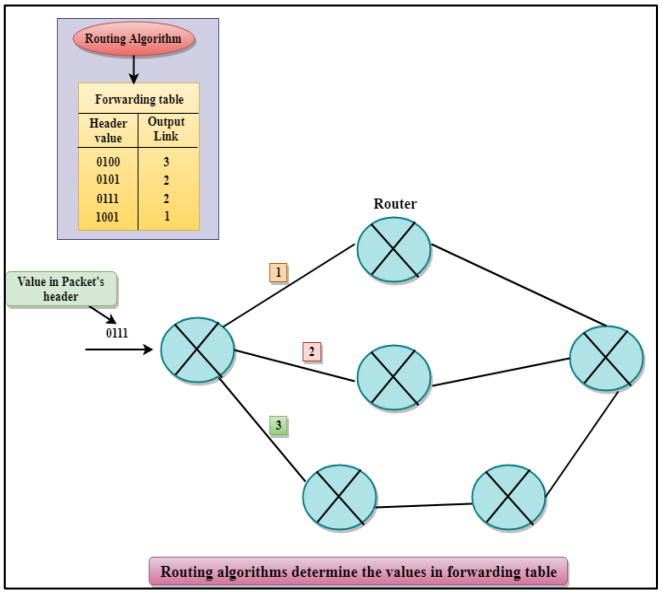
01. Logical Addressing

- Layer 3 uses Logical IP Addressing
- IP address assigned in this layer
    - Ipv4: 192.168.1.1
    - Ipv6: 2001:0db8:85a3:0:0:8a2e:0370:7334
- Ip address are assigned statically or Dynamically

02. Routing and Forwarding

Routing

- The route or path taken by packets as they flow from a sender to a receiver.
- These paths are defined by routing algorithms



Forwarding

- Forwarding action of transferring packet from an input link interface to the appropriate output link interface.

03. Fragmentation

- Fragmenting is breaking up large packets into smaller chunks(Smaller data blocks)
- Fragmentation is necessary for data transmission, as every network has a unique limit for the size of datagrams that it can process

WAN Technology

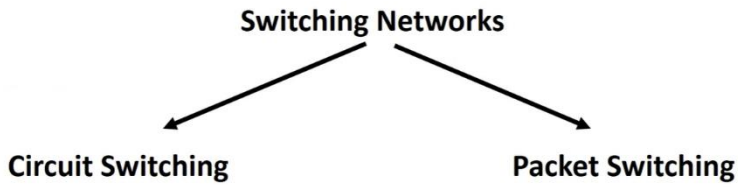
Switched Communications Networks Terminologies

Nodes – Switching devices that provide communication

Stations – Devices attached to the network

Communications Network – Collection of nodes

Switching Networks



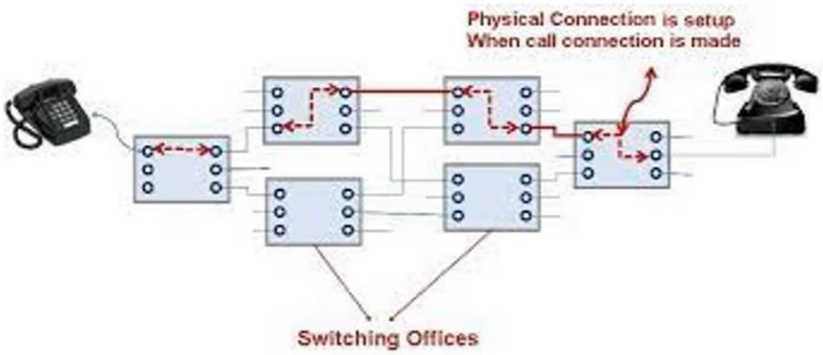
Circuit switching

- Method use for establishing **a physical dedicated communication path** between the sender and the receiver.
- Circuit switching is **connection-oriented.**

Circuit Switching has three phases
- Establish
- Transfer
- Disconnect

Establish ------→ Transfer ------→Disconnect

- **Need to have physical path & Dedicated path, in order to establish the connection**
- **Ordinary voice phone service is circuit switched.**

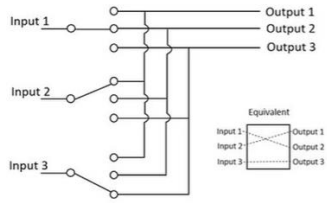


Circuit Switching

Space Division Switching

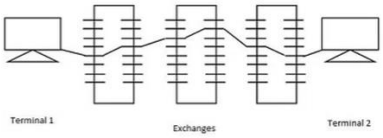
Signal paths are physically separated from one another

Originally designed for analog networks, but it is being used for both analog and digital switching



Time Division Switching

Use digital time division techniques to set up and maintain virtual circuits
It comes under Digital switching technique.



Advantages	Disadvantages
The bandwidth used is fixed.	Since dedicated channels are used, the bandwidth required is more.
The quality of communication is increased as a dedicated communication channel is used.	The utilization of resources is not full.
The rate at which the data is transmitted is fixed.	Since a dedicated channel has been used, the transmission of other data becomes impossible.
While switching, no time is wasted in waiting.	Circuit switching is expensive because every connection uses a dedicated path establishment.
It is preferred when the communication is long and continuous.	Great for only voice communication

Packet Switching

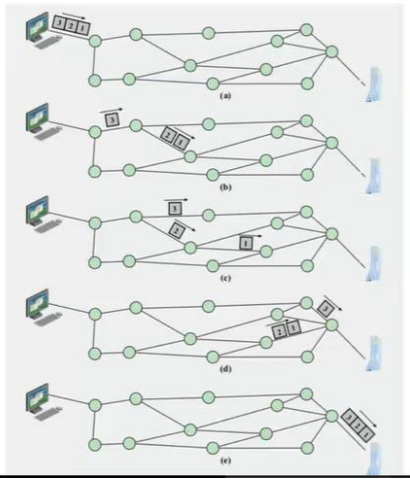
- packet switching **does not require the use of a dedicated channel**.
- Packet-based networks **break down a message into smaller data** packets which then look for the **most efficient route available.**
- Packet switching is defined as the **connectionless**

- Packet contain user data and control information
  - User data may be part of a larger message
  - Control information includes routing (Addressing)

Packet Switching

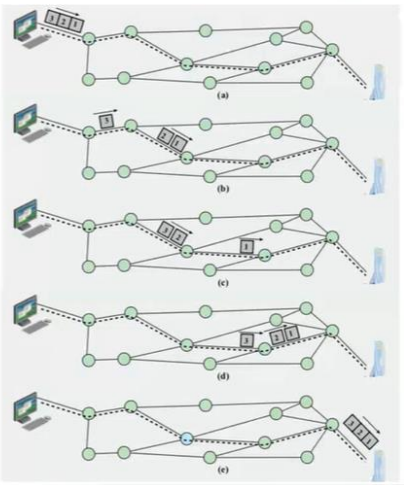
Datagram

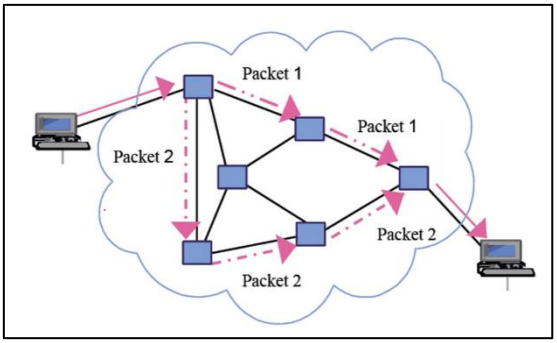
Each packet is treated independently with no reference to the previous packet

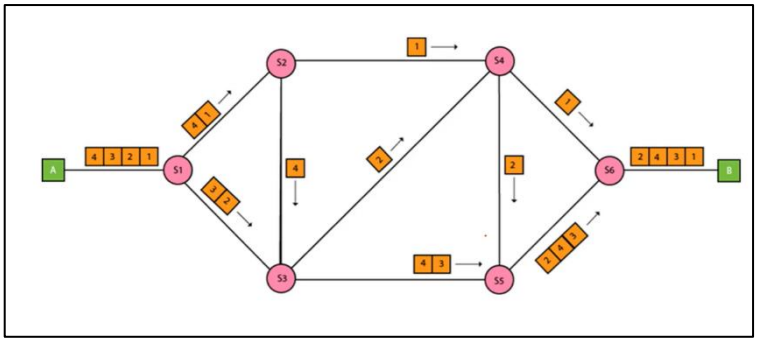


Virtual Circuit

A preplanned route is established before any packets are sent.







Advantages	Disadvantages
More efficient than circuit switching	Not ideal for applications that are in constant use, such as high volume voice calls
Data packets are able to find the destination without the use of a dedicated channel	There is a lack of security protocols for data packets during transmission
Reduces lost data packets because packet switching allows for resending of packets	High-volume networks can lose data packets during high-traffic times; those data packets cannot be recovered or resent during transmission
More cost-effective since there is no need for a dedicated channel for voice or data traffic	

Circuit Switching vs Packet Switching

Circuit Switching	Packet Switching
Physical path between source and destination	No physical path
All packets use same path	Packets travel independently
Reserve the entire bandwidth in advance	Does not reserve
Bandwidth Wastage	No Bandwidth wastage
No store and forward transmission	Supports store and forward transmission