01/10/2023

# Computer Networks

→ Computer Network is a collection of interconnected, autonomous computing devices.

→ Internet: Network of networks

→ Client - server model is widely used; where a single server generates web pages based on its database in response to 1000's of client requests; that may update the database.

* Types of Computer Networks:
  - → Broadband Access Networks
  - → Mobile and Wireless Access Networks.

* Types of Computer Network Topologies:

→ Personal Area Networks:

Ex: Wireless network that connects a computer with its peripherals.

→ Local Area Networks:

* Private network that operates within a single building such as home, office or factory.
* LANs are widely used to connect personal computers and other devices to let them share the resources and exchange information
* Wireless LANs → WiFi
* Wired LANs → point to point wired links (Switch connection) → Ethernet.
* Switch has multiple ports.
* Larger LANs are built using switches plugged in together using ports.

→ Metropolitan Networks:

* Covers a range ~~of~~ over a city.
* Ex: Television Networks.
  * Both television signals and internet being fed into centralized cable-head-end

→ Wide Area Networks:

* Spans a large geographical area
* Wired WAN → companies with branch offices in different cities.
* Offices contain computers intended for running user programs and these computers/machines are called HOSTS. and the network that connects these hosts is called SUBNET.

* SUBNET consists of 2 distinct components:
  → Transmission Lines: move bits b/w machines.
    → can be made up of copper wire, coaxial cable, optical fibre (or) radio links.
    → Companies use the lines from a telecommunications company.
  → Switching Elements:
    → Devices that connect 2 (or) more transmission lines.
    → When data arrive on an incoming line, switching element must choose an outgoing line to forward them.
    → also called router.
    → Routing algorithm helps in deciding the path.

→ Virtual Private Networks: (VPN)

- advantage of virtualization
- provides flexible reuse of resource (Internet Connectivity)
- operated by a commercial internet service provider

* Network Protocols:

→ Design Goals:

- Reliability ⇒ Handle errors, faults and failures
- Resource Allocation ⇒ sharing access to common
- Evolvability ⇒ improvements of protocol over time
- Security ⇒ defending the system from attacks

* Connection - Oriented Service:

- Acts like a tube where sender pushes bits from one end and receiver takes them from other end
- modeled after telephone system

* Connectionless Service:

- modeled after postal system
- Each message carries the full destination address
- Message is called packet at the network layer

* ISO-OSI Model:

→ International Standards Organization - Open Systems Interconnection:

* has seven layers
* Each layer should perform well-defined function

* Three concepts are central to the OSI model:
  - Services
  - Interfaces
  - Protocols.


→ Each layer performs some services for the layer about it ...

* TCP/IP MODEL:

→ LINK Layer:
- Describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer.
- Interface between hosts and transmission links

→ INTERNET Layer:
- job is to permit hosts to inject packets into any network.
- Defines an official packet format & protocol called Internet protocol and ICMP (Internet Control Message Protocol.
- Routing problem has largely been solved; but congestion can only be handled with help of higher layers.

→ TRANSPORT Layer:
- Communication b/w source and destination using end-to-end protocols.
- Protocols:
  - TCP: Transmission Control Protocol
  - UDP: User Datagram Protocol.

* TCP:
  - reliable connection-oriented protocol that allows a byte stream to be delivered from one device to other device without any errors.
  - divides the byte stream into discrete messages and passes each one on to the internet layer.
  - At the receiver, TCP reassembles the messages into O/P stream.
  - Also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

* UDP:
  - unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control.
  - used widely for one shot client server request queries where prompt delivery is more important than accurate delivery (transmitting speech or video).

* APPLICATION Layer:
  - contains higher-level protocols.
  - Protocols:
    - virtual terminal
    - File Transfer Protocol (FTP)
    - Simple Mail Transfer protocol (SMTP)
  - Domain Name System (DNS):
    - mapping host names onto their network addresses.
  - HTTP: Fetching pages on the WWW
  - RTP: delivering real-time media such as voice or movies.

* Physical Layer:

→ Guided Transmission Media: { Physical layer is used to transport bits from one machine to another.

*→ Transmission media that rely on a physical cable or wire are often called guided transmission media.

*→ Most commonly used guided transmission media are copper cable and fibre optics.

*→ Bandwidth is a measure of the carrying capacity of a medium.

1) Persistent Storage:

*→ We can transport data from one device to another is to write them into persistent storage such as magnetic (or) solid-state storage.

2) Twisted Pairs:

*→ Consists of 2 insulated copper wires.

*→ wires are twisted together in a helical form

*→ Common application is telephone system. All telephones are connected to telephone company using twisted pair cable.

*→ These cables can run several kilometers without amplification; but for further longer distances. the signal becomes too attenuated & repeaters are needed.

*→ Twisted pairs can be used for transmitting either analog or digital information.

*→ Bandwidth depends on thickness of the wire & distance travelled.

3) Co-axial Cable:

* Has better shielding and greater bandwidth than unshielded twisted pairs; so it can span longer distances at higher speeds.
* 2 kinds of co-axial cables:
  - 50 ohm cable: intended for digital transmission from the start.
  - 75 ohm cable: used for analog transmission & cable TV.
* Co-axial cable consists of a stiff copper wire as core surrounded by an insulating material.
* Insulator is encased by a cylindrical conductor; often as a closely woven braided mesh.
* Outer conductor is covered in a protective plastic sheath.
* Construction & shielding of co-axial cable give it a good combination of high bandwidth & excellent noise immunity.
* These were widely used within the telephone system for long distance lines but these are replaced by fibre optic cables.
* Also used for delivering high speed internet connectivity to homes in many parts of the world.

4) Power Lines:

* deliver electrical power to houses & electrical wiring within the house distributes it electrical outlets.

5) Fibre Optics:

* Used for long-distance communication in network backbones
* high speed LANs & high speed internet access
* Optical transmission system has:
  - → Light source
  - → Transmission medium
  - → Detector.

  pulse of light
  1 → presence
  0 → absence.
* Transmission medium is an ultra-thin fiber of glass.
* Detector generates an electrical pulse when light falls on it.
* Modes:
  - → Multimode → different angles
  - → Single Mode → only st. line propagation.

→ 2 kinds of light sources → LEDs, Lasers.

→ The receiving end of an optical fibre consists of a photodiode; which gives off an electrical pulse when struck by light.

→ By making pulses more powerful; the error rate can be made small.

* Wireless Transmission:

1) Electromagnetic Spectrum:

→ when e's move; they create EM waves that can propagate through space.

$\lambda f = c$

→ no. of oscillations per second of a wave: frequency (f) (Hz)

→ distance b/w 2 consecutive maxima & minima: wavelength ($\lambda$)

→ EM waves travel with a speed same as speed of light.

2) Frequency Hopping Spread Spectrum:

→ Transmitter hops from frequency to frequency hundreds of times per second.
→ Popular for military communications because its hard to detect.
→ Good resistance to fading due signals taking different paths.

3) Direct Sequence Spread Spectrum:

→ Uses a code sequence to spread the data signal over a wider frequency band.
→ widely used commercially as a spectrally efficient way to let multiple signals.

4) Ultra-Wideband Communication:

→ Sends a series of low energy rapid pulses, varying their carrier frequencies to communicate information.
→ Rapid transitions lead to a signal that is spread thinly over a very wide frequency band.
→ UWB transmits in ways that do not interfere with carrier signals in the same frequency band.

* OSI Reference Model:

→ Purpose of the OSI model is to facilitate communication between different systems without requiring changes to the logic of the underlying hardware & software.

→ Layers:

Sender: top to bottom

Receiver: bottom to top.

* Intermediary nodes will process the data containing only down 3 layers. (physical layer, data link, network)
* Each layer can interact with the adjacent layers.
* Application Layer:
  → Enables the user to access the network resources.
  → Mail services, file transfer etc.
* Presentation Layer:
  → concerned with the syntax and semantics of the information exchanged b/w 2 systems.
  → Translation, Encryption and compression.

* Session Layer:
  → Establishes, maintains & synchronizes the interaction among communicating devices.
  → Process communication & Synchronization.
* Transport Layer:
  → responsible for process to process delivery of entire message.
  → End to end flow control. → Port addressing
  → Segmentation & reassembly
  → Error Control.
* Network layer:
  → responsible for delivery of data from the original source to the destination.
  → Logical addressing (source & destination IP address)
  → Routing (path)

* **Data link layer:**
responsible for moving data from one node to other node
→ framing (grouping); physical addressing (MAC)
→ flow control, error control and access control.

* **Physical layer:** transmitting bits over a medium.
→ It also provides electrical & mechanical signals
→ physical characteristics of the media.
→ representation of bits.
→ Synchronization of bits
→ Physical Topology:
  - Bus
  - Star
  - Ring
  - Mesh
  - Hybrid

* 3 types of transmission
  - Simplex
  - Half-Duplex
  - Full-Duplex.

* **Addressing in Networking:**
→ IP: 32 bits → MAC: 48 bits.

* → **Data link layer:**

→ **Design Issues:**
1) Providing a well-defined service interface to the network layer.
2) Framing sequences of bytes as self-contained segment
3) Detecting & correcting transmission errors.
4) Regulating the flow of data.

→ **Methods:**
  - Byte count
  - Flag bytes with byte stuffing.
  - Flag bits with bit stuffing
  - Physical layer coding violations.

→ Error Control:

* Protocol calls for the receiver to send back special control frames bearing +ve or -ve acknowledgements.
* Managing the timers and sequence numbers so as to ensure that each frame is ultimately passed to the network layer at the destination exactly once.

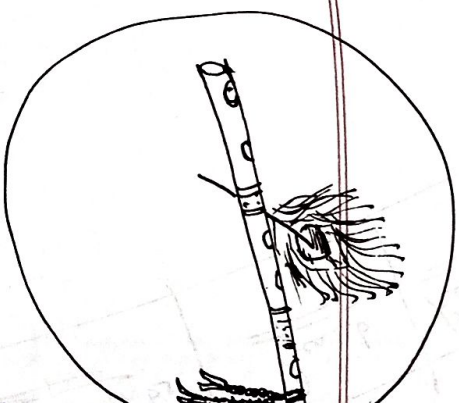
→ Flow control:

- Feedback-based flow control.
- Rate-based flow control.

→ Error Detection and Correction:

* Error correcting codes : Forward Error Correction
  - Hamming Codes
  - Binary convolutional codes.
  - Reed-Solomon Codes
  - Low density parity check codes.

* Error detecting codes:
  - Parity
  - CheckSums
  - CRCs.



A-Z : 65-90
a-z : 97-

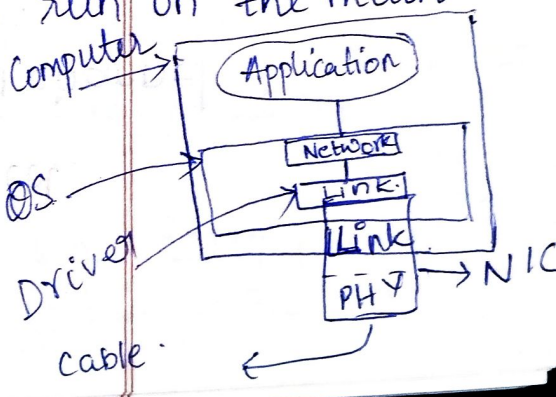
→ The packet passed accross the interface to data link layer ~~is pure data~~ from the network layer is pure data; whose every bit is to be delivered to the destination's network layer.

* Elementary Data Link Protocols:

→ Physical layer, data link layer and network layer are independent processes that communicate by passing messages back and forth.

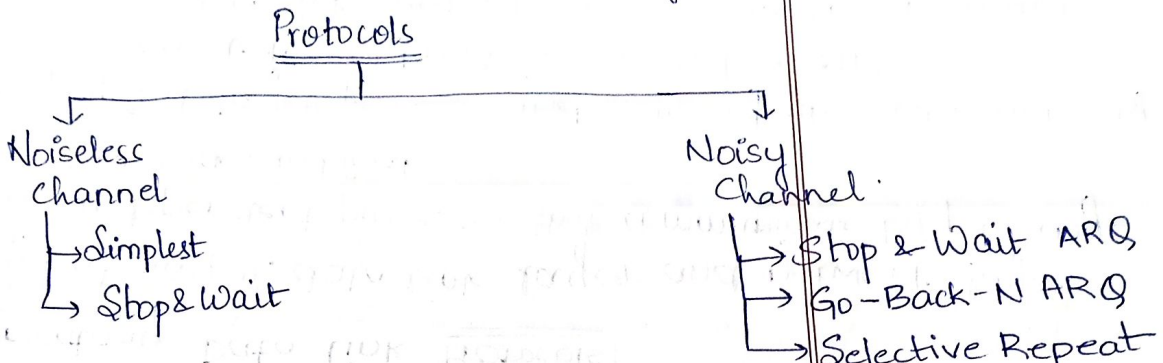
→ The physical layer process and some of the data link layer process on dedicate hardware called a NIC.

→ Remaining data link layer processes run on the main CPU as a part of the OS.



Protocols:

- Unrestricted Simplex Protocol
- Simplex Stop and Wait Protocol
- Simplex Protocol for a noisy channel




→ An unrestricted simplex protocol:

* Data is transmitted in one direction only.
  - → transmitting ($T_x$) and receiving ($R_x$) hosts are always ready.
  - → Processing time can be ignored.
  - → Infinite buffer space is available.
  - → No errors occur.

→ Simplex Stop and wait protocol:

* We assume that data is transmitted in one direction only.
* No errors occur.
* Receiver can only process the received information at a finite rate.

⇒ These assumptions show that; the transmitter cannot transmit the frames at a rate faster than the

receiver can process them.

⇒ To avoid this problem; the receiver sends an acknowledgement frame back to the sender telling the sender that the last received frame has been processed & passed to the host; permission to send next frame is granted; and the sender after sending the frame must wait for acknowledgement.

→ A simplex protocol for a noisy channel:

* Frames may be either damaged or lost completely.
* Transmission errors in the frame are detected by the hardware checksum.
* Sender would send a frame and the receiver would send ACK frame if frame is received correctly.
* If frame is in error; the receiver simply ignores it; transmitter would time out and would retransmit it.
* The flaw for the above is if ACK frame is lost or damaged; duplicate frames are accepted at receiver without receiver knowing it.
* To overcome this problem; the receiver be able to distinguish a frame that it is seeing for the first time from a retransmission.
  - One way to achieve this is to put a sequence number in the header of each frame it sends.
  - Any wrong sequence numbered frame arriving at the receiver is rejected as a duplicate.

→ Piggybacking:

* Temporarily delaying transmission of outgoing acknowledgement so that they can be hooked onto the next outgoing frame.
* Higher channel bandwidth utilization : Advantage.
* If the wait time to piggyback is longer than sender timeout period then sender retransmits.

→ Sliding Window Protocols:

* These are bidirectional protocols (max sending window size, receiving window size).
  - → One-bit sliding window protocol (1, 1)
  - → Go back N (>1, 1)
  - → Selective Repeat (>1, >1)

** These 3 differ in terms of efficiency, complexity & buffer requirements.

** Sending and receiving windows:

→ Sender maintains a set of sequence numbers of frames permitted to send which fall within sending window.

→ Receiver maintains a set of sequence numbers of frames permitted to accept which fall within receiving window.

→ Sender and receiver window size may be fixed or variable size.

→ Senders window contains frames which are to be sent & not yet acknowledged also called outstanding frames.

→ When a packet arrives from network layer
  - → Next highest sequence no. is assigned
  - → Upper edge of the window advanced by 1.

→ When an acknowledgement arrives:
  ↳ Lower edge of window advanced by 1.

→ If the maximum window size is 'n'; the sender needs n buffers to hold the unacknowledged frames.

If the window grows to its maximum size; the sending data link layer must forcibly shut off the network layer until another buffer becomes free.

→ The receiving data link layer's window corresponds to the frames it may accept. Any frame outside the window is discarded without comment.

→ When a frame whose sequence number is equal to the lower edge of the window is received; it is passed to the network layer; an acknowledgement is generated; and the window is rotated by one.

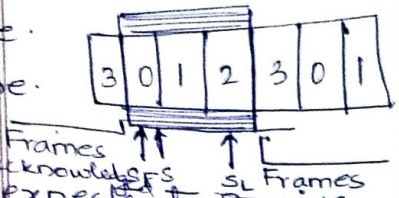
→ Receiver's window always remains at its initial size.

* Sender Sliding Window:
  ↳ size of the window is atmost: $2^m - 1$
    where m: no. of bits for the sequence number.
  ↳ size of the window can be variable (eg: TCP)
  ↳ Window slides to include new unsent frames when the correct ACKs are received.

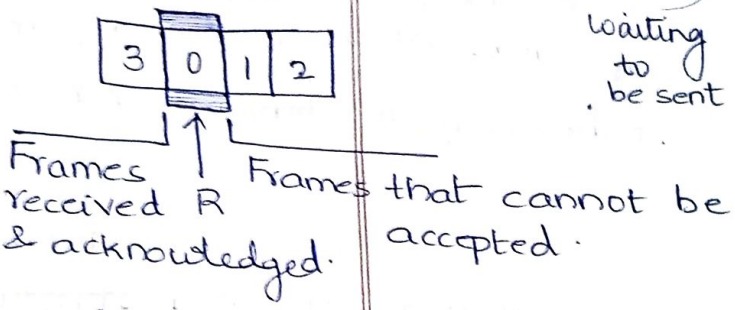
* Receiver Sliding window:
  ↳ Size of the window at the receiving site is always 1.
  ↳ Receiver is always looking for a specific frame to arrive in a order and any frame out of order is discarded.

→ Sender has 3 variables:
  ↳ S: Sequence of recently sent frame

→ $S_F$: sequence no. of the first frame.
→ $S_L$: Sequence no. of the last frame.




Receiver only has one variable.
→ R: sequence no. of the frame it expects




* Performance of STOP and WAIT Protocol:

Long transit time + high bandwidth + Short frame length ⇒ disaster.

→ In stop & wait, there is only one frame that is sent and waiting for acknowledgement.

→ To improve efficiency, multiple frames must be in transition ⇒ PIPELINING:

→ Solutions
- → Go back n protocol
- → Selective repeat protocol.

* Go-back 'n' protocol:

→ Improves efficiency of stop and wait
→ Allow a window of upto $w_s$ outstanding frames.
→ Use m-bit sequence numbering.
→ Receiver discards all subsequent frames following an error.
→ Receiving window size = 1
→ Wasting a lot of bandwidth if error rate is high.