IDATA2304

# Topologies

Mesh topology refers to network where every node is connected to all other nodes in the network. There is also another type called partial mesh topology, where each node does not need to connect to every node, but is still connected to a collection of other nodes.  
  
A bus topology is a network where nodes tap into a line/cable. This topology is prone to collisions due to all nodes being connected to a single line. Therefore, each node will listen for any activity, and send its data when the coast is clear. If a collision were to occur, the node will wait a random amount of time, before trying to send the data again.  
  
A star topology is a network where all nodes on a network are connected to a single point. This type of network can be a lot faster as the data does not need to travel far. A disadvantage is that a lot of responsibility is laid on the central point, causing complete network outage if that point were to fail.

A ring topology is a network where each node in a network is connected to each other like a ring. Compared to a bus topology, collisions are not a problem here. However, id one of the nodes were to fail, the communication will be severely affected as nodes can no longer communicate with nodes past failed node.

# Network types

Lan, or local area network is a computer network limited within a specific area such as homes, offices, schools, etc.  
  
Wan, or wide area network is a telecommunications network that extends over a large geographical area.  
  
When two or more networks are connected, they make an internetwork, or internet. Note, an internet is not the Internet. The internet is composed of millions of interconnected networks.  
  
A circuit switching network is a configuration in which a physical path is obtained and dedicated to a single connection between two endpoints in the network for the duration of a dedicated connection.

A packet switching network is a method of grouping data into packets that are transmitted over a digital network. Packets are made of a header and a payload.

# Internet history

The first version of the Internet was created by ARPANET in 1969 at the university of Los Angeles. It was the first wide-area packet switching network.   
In 1974 the protocol for end to end delivery of data was achieved.

## Physical layer

## Data signals

Periodic analog signals are signals which repeats themselves after a specific interval of time. They can be divided into simple or composite. A simple signal is a sine wave, while a composite signals are a combination of multiple sine waves.   
A digital signal is a composite of analog signal with frequencies between zero and infinity, They can have more than two levels. Each level needs Log2L bits for a L levels signal.  
  
Signals can have impairments such as Attenuation (Loss of energy), distortion () and noise (External noise or crosstalk).

# Data link layer

Communication at the data link layer is node-to-node, meaning the movement of data from one node of a network to the next,  
Terms:

* Frames: Data blocks in the data link layer are called frames. The size of a frame can vary. In a fixed-size frame the frame is always fixed. In variable sized frame the frame needs to be outlined.
* Framing: Provides a way for a sender to transmit a set of bits that are meaningful to the receiver. It does this by packing the bits into frames, and giving the frames a header containing source and destination address.
* Flow Control: Restricts and coordinates number of frames or amount of data sender can send just before it waits for an acknowledgement from receiver.
* Error control: Detects errors in transmitted frames and retransmits all the erroneous frames. It detects errors by checking for lost or damaged frames.
* Point-to-point: Communication between two nodes without any host or any other networking in between. This means that a point-to-point connection does not need to use MAC addresses.
* Unicast: Send data over a single hop between source and destination.
* Multicast: Not a concern in layer 2
* Broadcast: Frames addressed to reach every computer on a given LAN segment. The source MAC address will be set to all “F”s (ff:ff:ff:ff:ff:ff)  
  Addressing: Encapsulates the source and destination’s MAC address in the header of each frame to ensure node-to-node delivery.

ARP (Address resolution protocol)  
ARP is responsible for mapping IP addresses to MAC addresses within a local network. ARP uses broadcast messages to discover addresses associated with a specific IP address on the same network. When a device wants to communicate with another device on the local network, but only knows the IP address and not the corresponding MAC address, it sends an ARP request which is a broadcast message sent to all devices connected to the local network asking which of the devices has given IP address. The device which has this address, will respond with its own MAC address in an ARP reply. The first device will save this mapping in its cache and is now able to send data directly to the correct device.  
  
Redundancy means adding extra bits for detecting errors at destination. There are three main techniques for detecting errors in frames:

Parity check: Adds an extra bit to data to ensure the total number of 1s in the data. Including the extra bit, the system will check if the number of 1s are either odd or even.

Checksum: Adds a sum or hash of data blocks to the transmission. The receiving end performs the same calculation and check if the calculated sum is equal to the transmissions sum. If they differ, an error is detected.

Cyclic Redundancy check: Uses division and remainder operations to generate a fixed-size check value appended to the data. If the received CRC doesn’t match the calculated one, an error is detected.

DLC (Data link control) is the service provided by the data link layer. It deals with procedures for communication between two adjacent nodes no matter whether the link is dedicated or broadcast.

COF (Character oriented framing) is a link layer function where the packets from the network layer are encapsulated into frames based on specific characters. The data frames can be of fixed length or variable length.  
  
Bit-oriented framing works at the bit level, delimiting frames based on patterns of bits. This method is more efficient, but also more complex.  
  
Connectionless protocols operates without establishing a dedicated connection between sender and receiver. Here data frames are handled independently, without relying on sequence numbers. This approach is mostly found in LAN data-link layer protocols.  
Connection-Oriented protocols establish a logical link between nodes before data transmission begins. After a connection has been established, related frames are transmitted. After all frames are transmitted, the connection will be terminated.  
  
Stop-and-wait protocol is a basic ARQ (Automatic Repeat request) method where the sender transmits one frame and then waits for an acknowledgement from the receiver before sending the next frame.  
  
Piggybacking is an optimisation technique used in data communication protocols to improve efficiency by allowing a device to combine its data with acknowledgment or other control information within a single transmission. This method reduces the number of messages sent.

HDLC (High-Level Data Link Control) is a link layer protocol widely used in telecommunications. It employs bit-oriented communication over both point-to-point and multipoint links, implementing the stop-and-wait protocol for reliable data transfer. It serves as the foundation for various practical protocols like PPP and Ethernet.  
  
PPP (Point-to-Point Protocol) is derived from HDLC and operates with character-oriented or byte-oriented framing. Primarily designed for point-to-point links, PPP does not provide inherent flow control. However, it effectively controls and manages data transfer between devices, offering a standardized method for establishing and maintaining communication over point-to-point connections in networks.  
  
RAP (Random Access Protocols) int data link layer enable devices to share a common channel for transmission without a predefined schedule. They allow devices to access the channel randomly, minimizing collisions and contention for network access.

Pure ALOHA is a basic random-access protocol where devices transmit data whenever they have information to send. It does not check for channel availability before transmitting, leading to a higher collision probability.  
Slotted ALOHA divides time into slots, ensuring transmissions occur at specific intervals. This reduces collisions, but still requires devices to commend for slots, improving efficiency compred to Pure   
  
CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is a network protocol used in ethernet LANs. Devices listen to the network before transmitting to detect ongoing transmissions and initiates a backoff algorithm, and retransmits data, aiming to manage collisions and maintain efficient data transmission within ethernet networks.  
  
Reservation based methods involve reserving the right to transmit data. Stations send reservation signals to request permission for transmission.   
Polling works by a central controller, often called a master or a hub, interrogating devices one by one to determine which station has data ready for transmission.   
Token Passing involves stations sharing a special token that grants the right to transmit data.  
  
Channelization is a set of methods by which the available bandwidth is divided among the different nodes for simultaneous data transfer. The three channelization methods are:

FDMA (Frequency Division Multiple Access) involves dividing the available frequency spectrum into distinct channels and allocating each user or communication stream to a specific frequency band. This enables multiple users to share to simultaneously access the network by utilizing different frequency ranges without interfering with each other.  
  
TDMA (Time Division Multiple Access) divides signals into time slots, allowing multiple users to share the same frequency channel by allocating unique time intervals to each user.  
  
CDMA (Code Division Multiple Access) enables multiple users to share the same frequency spectrum at the same time by assigning a unique code to each user. These codes are used to encode and differentiate each user’s signal, allowing multiple signals to coexist on the same frequency without causing interference.

# Network layer

The network layer refers to data blocks as packets. The network layer is doing the service of a carrier delivery of packages from a sender to a receiver without changing or using the contents.  
Packetizing: Encapsulating the payload in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination.

Routing is the process of determining the best path for data packets to travel from one network to another. It involves making decisions based on network conditions, such as traffic, shortest paths and available resources.  
  
Forwarding is the actual transmission of data packets along the chosen path determined by the routing process. It involves passing packets from one network to another based on the information in the packet headers.

Services:

* Error control: Only for header, not whole datagram.
* Checksum is added
* Packet in the network layer may be fragmented at each router.
* No flow or congestion control in the network layer.

IPSec is a set of protocols used to secure internet connection at the “IP layer”. IPSec can be employed to create VPN’s or secure communication channels between devices and networks. Because of this we can also conclude that VPNs is a part of the network layer.

Packet switching is a network layer process that involves routing and forwarding data divided into packets from one network to another. Routers, acting as switches, establish connections between input and output ports. Two primary packet-switched approaches exist: The datagram approach, offering a connectionless service where packets are individually routed, and the virtual-circuit approach, providing a connection-oriented method where a predetermined path is established for packets to follow.

IPv4 addresses are 32-bit numerical labels assigned to devices participating in a computer network. They are expressed in a format like xxx.xxx.xxx.xxx, where each “xxx” is a number between 0 and 255. This allows for approximately 4,3 billion addresses. Because of the limited amount of addresses in IPv4, there has been an increasing adoption of IPv6, which uses 128-bit address space. They look something like this: 2001:0db8:85a3:0000:0000:8a2e:0370:7334 .   
  
Classful addressing was an early method of allocating IP addresses in the IPv4 system, dividing the address space into 5 classes: A, B, C, D, E.

DHCP (Dynamic Host Configuration Protocol). It’s a network management protocol used to automatically assign on IP addresses and other network configuration settings to devices on a network. It allows devices to obtain IP addresses, Subnet masks, default gateways, DNS servers and other parameters automatically.  
  
NAT (Network Address Translation). It operates at the network layer and is used to modify network address information in IP packet headers when they are transmitted from one network to another. NAT primarily enables multiple devices within a LAN to share a single public IP address to access the internet.

ICMP (Internet Control Message Protocol) is used to send error messages and operational information, allowing devices to communicate status or error information regarding IP packet processing. ICMP messages are used by network devices such as routers or hosts to convey information about network connectivity, errors, congestion, or troubleshooting issues, including ping requests snd responses for network testing and diagnostics.