The Computer Networking Journey

Version 1.0
August-2024

By Dr. Shlomi Boutnaru

Created using Craiyon, AI Image Generato

Introduction

Our goal in this series is to interconnect between computer systems, or basically talk about how the Internet works. From the hardware perspective we have the end devices/hosts, cables, switchers, modems, routers and other (More details can be found here - https://blog.netwrix.com/2019/01/08/network-devices-explained/).

Basically a network architecture is a set of layers and protocols. A protocol is a set of rules which are agreed among peers on how communication should be conducted. Overall computer networking is made up of multiple protocols at different layers (their number can differ between networks). Regarding the layers, there is a protocol hierarchy sometimes called “protocol stack”.

On the sending side, every layer sends information (data and control) to the layer below until we get to the lowest layer. On the receiving side the information flows from the lower layer to the most upper one. Probably the most well known conceptual model for describing networking is the “OSI Model”. This model has 7 layers each handling different aspects of networking (as described next). Now we are going to go over each one of the layers.

Layer 1, aka “Physical Layer”, which is responsible for transferring bits over some medium (such as radio frequency or optical cables). The smallest atom in this layer is a “bit”.

Layer 2, aka “Data Link Layer”, which is responsible for splitting the “flow of bits” into frames and ensuring there are no transmission errors (they are protocols in this layer which can also fix some transmission errors and thus avoid the retransmissions by upper layers). The smallest atom in this layer is a “frame”.

Layer 3, aka “Network Layer”, which is responsible for routing the data between a sender and a receiver. There are two families of protocols in this layer: routed protocols (holding source and destination information needed for routing) and routing protocols (managing the routing tables among the routers across the network) - more on them in future write-ups. The smallest atom in this layer is a “packet”.

Layer 4, aka “Transport Layer”, which has two major protocol families: connectionless (not starting a connection before sending data and best effort) and connection oriented (creating a connection before sending data and adding acknowledgement mechanism to ensure data was received). Lastly, this layer also allows multiplexing a couple of applications for communication on the same hosts (like TCP/UDP ports). The smallest atom in this layer is “datagram”(connectionless) or ”segment” (connection-oriented).

Layer 5, aka “Session Layer”, which is responsible for initiating and creating a session between both ends of the communication.

Layer 6, aka “Presentation Layer”, which is responsible for ensuring the data passed between the sender and the receiver is understandable between both parties.

Layer 7, aka “Application Layer”, which is responsible for the protocol used by the application (web browsing, email, messaging, etc.) itself.

They are two sentences that help remember the layers by using the first letter of each layer (the first from upper to lower and the second form lower to upper). The sentences are: “**A**ll **P**eople **S**eems to **N**eed **D**ata **P**rocessing” and “**P**lease **D**on’t **T**hrow **S**uper **P**izza **A**way” (maye you know the second one with “Sausage” and not “Super” but it does not work for those not eating milk and meat together).

Also, it is important to remember that the “OSI Model” is a reference only, and not all the protocol stacks implement the entire 7 layers such as ISDN and TCP/IP (which we will talk about in the future). In the table below we can see for each layer a small list of protocols as an example[1].

OSI model

Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

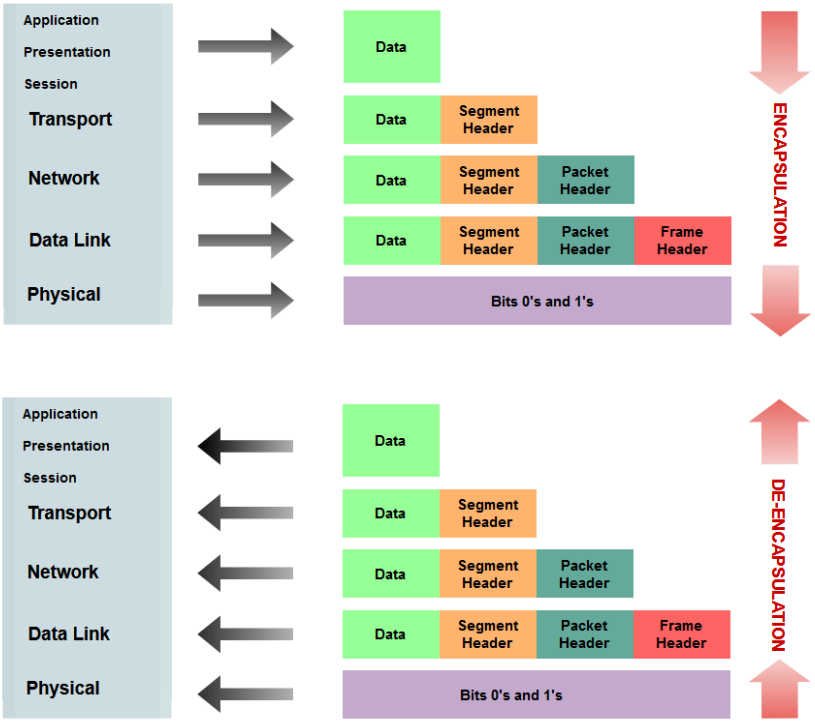
[1] https://infosys.beckhoff.com/content/1033/tf6310_tc3_tcpip/84246923.html

Data Encapsulation and De-Encapsulation

While sending data across networks different protocols are added as an overhead. In our case we focus on protocols which reference the OSI model. This model leveraged encapsulation and de-encapsulation for transmitting data - as shown in the diagram below[2].

Overall, in the case of the OSI model the data is encapsulated in the side of the sender. Starting from the application layer to the physical layer. Each layer takes the data from the previous layer and adds the current layer's header - as shown in the diagram below. Those headers are used for different tasks such (but not limited): error detection, error correction, flow control, congestion control, routing information and more[3].

Moreover, de-encapsulation is the reverse process of encapsulation. On the receiving side while the information flows (from the physical layer to the application layer) each layer reads the header from the corresponding layer in the sender side. After processing the header and performing the relevant tasks the header is removed and the data is passed to the next upper layer - as shown in the diagram below. Lastly, we can say the encapsulation works from upper to lower layers while de-encapsulation works for lower to upper layers.



[2] https://www.educative.io/answers/what-are-encapsulation-and-de-encapsulation-in-networking
[3] https://afteracademy.com/blog/what-is-data-encapsulation-and-de-encapsulation-in-networking/

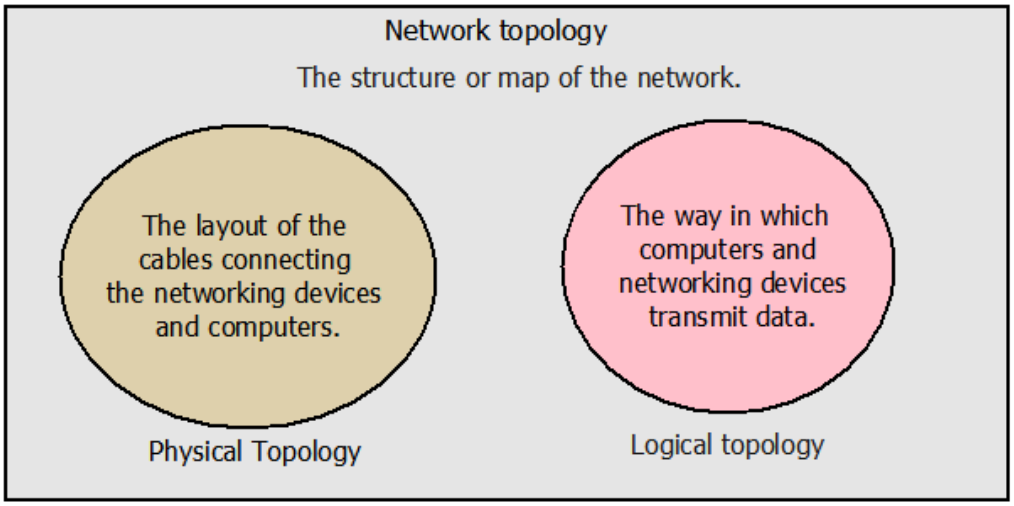
Network Topology

A network topology defines the way in which the network entities (devices/node/etc) are arranged and connected between each other. We can cluster the different network topologies to two main categories: physical topologies and logical topologies[4] - as shown in the diagram below[5].

Overall, a physical topology is focused on the placement/layout of the different network components and the connectors between them. In this case we can think about network cables and network equipment (switch/routers/bridges/access points/repeaters/etc). There are several types of physical topologies like: bus, star hybrid and mesh[6] - more on them in future writeups.

Moreover, a logical topology is focused on the way in which the data flows inside the network between the entities/nodes/elements/devices. There are several types of logical topologies like: bus, hub, star and ring[7] - more on them in future writeups.

Lastly, we can say that a network topology is an application of graph theory. In this case network devices can be modeled as nodes/vertices and their connections can be modeled as lines/edges between them[8].



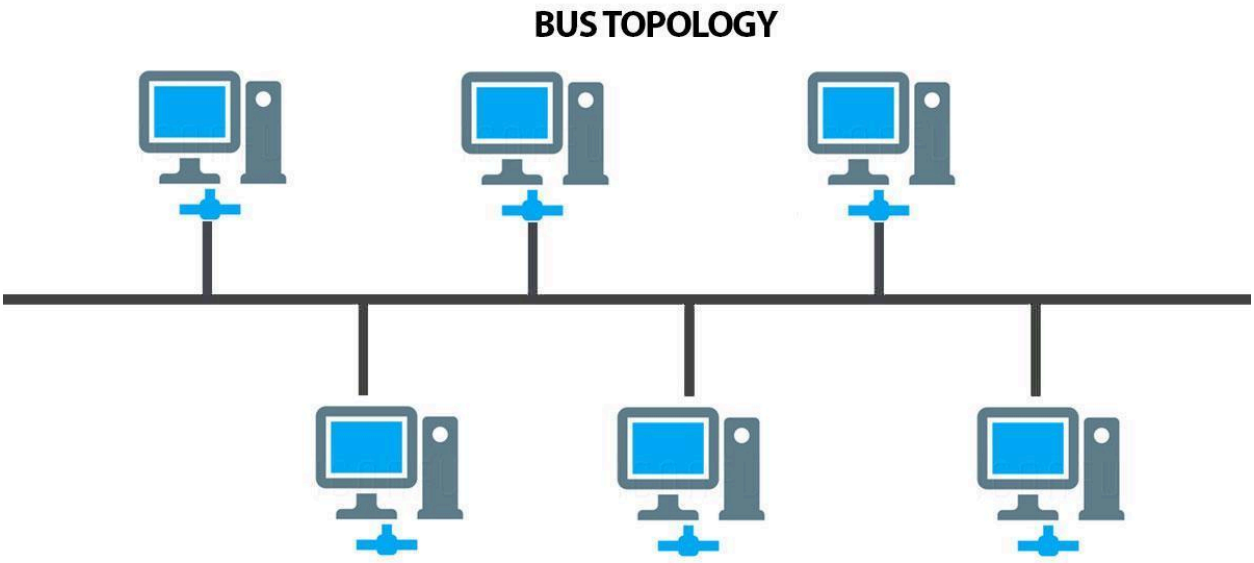
[4] https://en.wikipedia.org/wiki/Network_topology
[5] https://www.computernetworkingnotes.org/images/networking-tutorials/nt26-01-physical-layout-vs-logical-layout.png
[6] https://www.computernetworkingnotes.com/networking-tutorials/differences-between-physical-and-logical-topology.html
[7] https://www.omnisecu.com/basic-networking/difference-between-physical-topology-and-logical-topology.php?expand_article=1
[8] https://blogs.arubanetworks.com/solutions/network-topologies-logical-vs-physical/

Bus Topology

A bus topology (sometimes called “Line Topology”) . As with other topologies it has different advantages and disadvantages. In case of advantages we can think about examples like: the topology being uncomplicated and inexpensive, requires less cable length than other topologies (such as star topology) and it's the most straightforward method for connecting computers or peripherals in a linear fashion. However, bus topology does not scale well and a terminator is needed in both ends of the main cable[9].

Overall, in a bus topology every network element (like computer/network device) is connected using a single cable - as shown in the diagram below[10]. There are different network protocols which are targeting bus topology such as TDMA, Pure Aloha, CDMA, Slotted Aloha and more[11].

Lastly, in case of a shared medium (i.e. the bus) when a device sends data it is broadcasted along the bus and every connected device can read the information. Thus, to avoid network problems only one node can send data at a time[12]. We will cover in future writeups different technologies which can help deal with the disadvantages covered here.



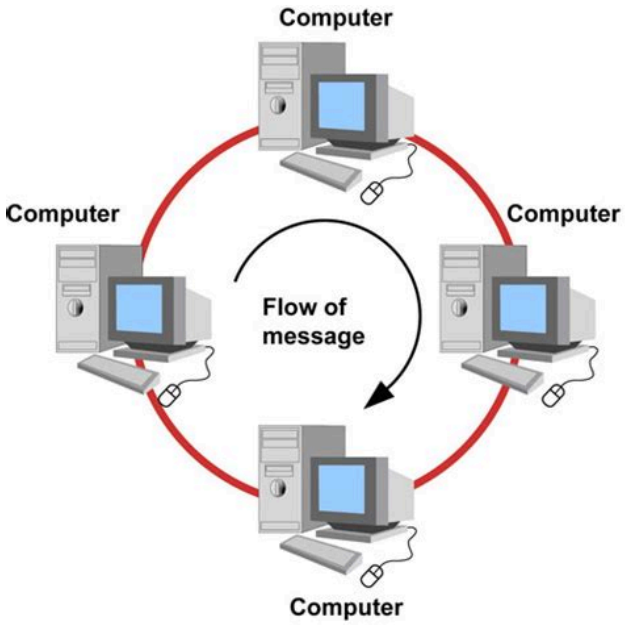
[9] https://www.computerhope.com/jargon/b/bustopol.htm
[10] https://www.cablify.ca/an-introduction-to-network-topology/
[11] https://www.geeksforgeeks.org/types-of-network-topology/
[12] https://www.cbtnuggets.com/blog/technology/networking/what-is-bus-topology

Ring Topology

A ring topology is built in a way that causes the data to flow in a loop at a specific direction. Thus, each node is connected only to two other nodes in the network - as shown in the diagram below[13]. One of the biggest benefits of a ring topology is the fact there is no central node, due to that there is no single point of failure. Also, because only one one can transmit data at a time we avoid the issue of collisions[14].

Moreover, a well architected ring can provide predictable and constant data rate. Also, each node gets an equal time share for sending data. However, it is difficult to debug/troubleshoot issues in such topology when even a single failed NIC (network interface card) can cause a network failure[15].

Lastly, there are different examples of devices/protocols using the ring topology such as: “Token Ring” and “FDDI” (Fiber Distributed Data Interface). Also, in some implementations based on a ring topology (like “Token Ring”) there is a use of a token passing mechanism for controlling data transmission[16] - more on that in future writeups.



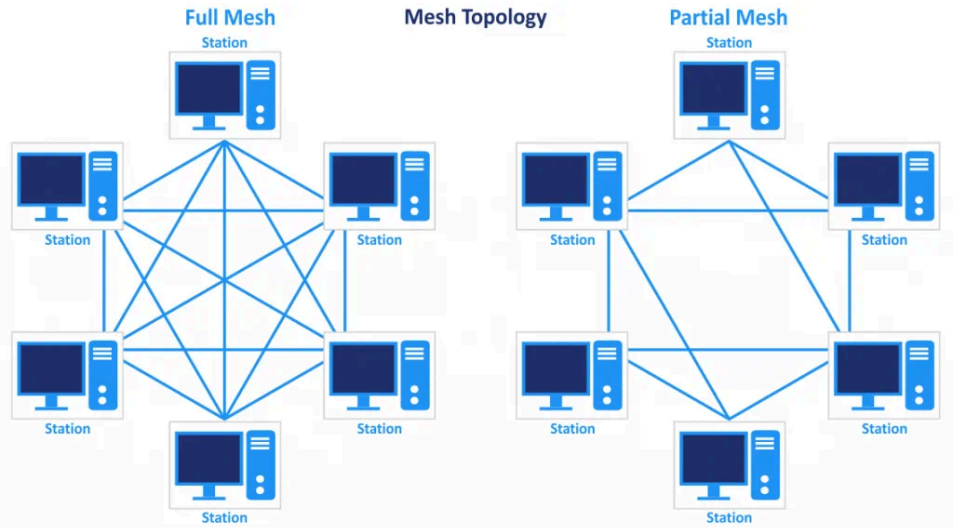
[13] http://www.techiwarehouse.com/engine/e96bb2f2/Understanding-Ring-Topology
[14] https://unstop.com/blog/ring-topology-in-computer-network
[15] https://www.cbtnuggets.com/blog/technology/networking/why-still-use-a-ring-network-topology
[16] https://www.lenovo.com/us/en/glossary/what-is-ring-topology/

Mesh Topology

In a mesh topology every device on the network is interconnected to every other device which is on the network. Thus, there is a dedicated link between every two nodes. So in case we have N nodes on the network there will be N(N-1)/2 links, that is the case of a "Full Mesh Topology". In the case of a "Partially-Connected Mesh Topology" at least two nodes on the network have connections to multiple other nodes[17] - as shown in the diagram below[18].

Overall, among the advantages of mesh technology are: providing robustness and fault tolerance, supporting high scalability, ensuring efficient data transmission and better privacy and security (due to the direct connections). Also, mesh topology is common in different wireless networks[19].

Lastly, it is important to know that there are specific routing protocols for mesh networks such as: AODV routing protocol which stands for "Ad-hoc On-demand Distance Vector"[20] and OLSR routing protocol which stands for "Optimized Link State Routing Protocol"[21].



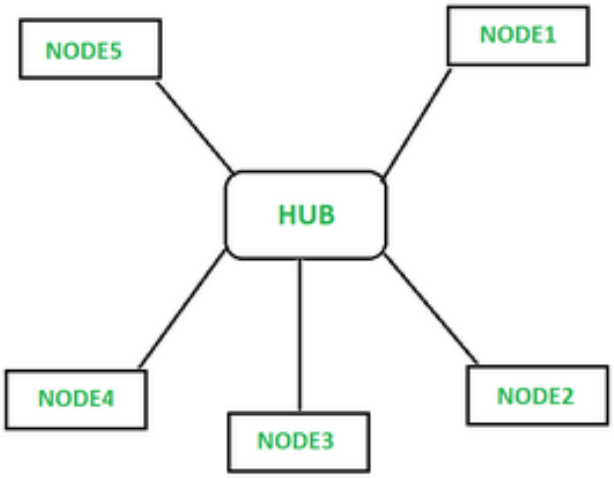
[17] https://www.computerhope.com/jargon/m/mesh.htm
[18] https://www.nakivo.com/blog/types-of-network-topology-explained/
[19] https://www.lenovo.com/us/en/glossary/mesh-topology/
[20] https://www.digi.com/resources/documentation/Digidocs/90002002/Concepts/c_zb_AODV_mesh_routing.htm
[21] https://openwrt.org/docs/guide-user/network/wifi/mesh/olsr

Star Topology

In a star topology every device on the network is connected to a central device. As opposed to a mesh topology in which every device on the network is interconnected to every other device[22]. This type of topology is most used in the case of LANs[23].

Overall, in case of a star topology we need more cables than a bus topology, however if a cable fails, just one node is going to be brought down. The central device to which all the nodes are connected is a hub/switch. Thus, when any network entity wants to transfer information it transfers the information to the central node that sends it to everyone (in case of a hub) or to the specific node (in case of a switch). The hub/switch controls all the functions of the network[24]- as shown in the diagram below.

Lastly, as with any other network topology also a star topology has pros and cons. Examples of advantages are: no distributions when connecting/disconnecting devices from the network, easily manageable, multiple stars can be connected for extending the network, reliability and more. Among the disadvantages are: dependent on a central device (which is a single point of failure), requires more cabling than a bus, performance is highly dependent on the central device and more[25].



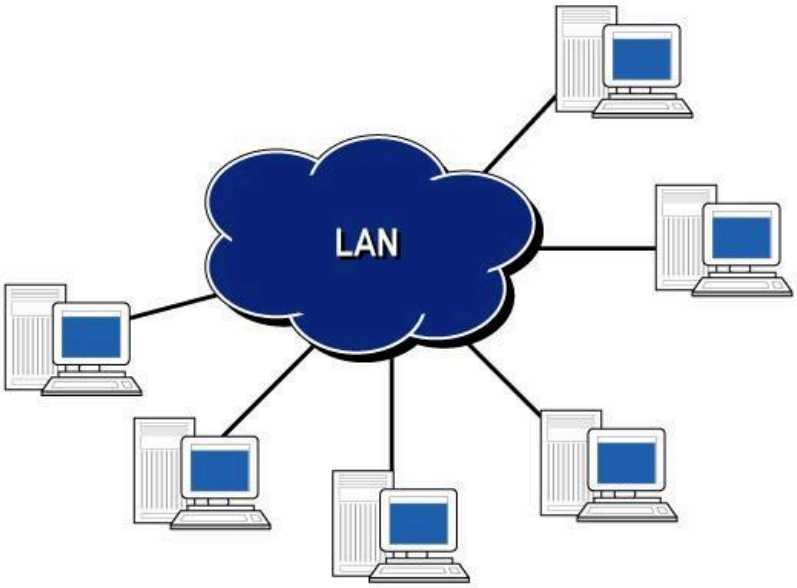
[22] https://medium.com/@boutnaru/the-computer-networking-journey-mesh-topology-2fe1a5550e06
[23] https://medium.com/@boutnaru/the-nlan-local-area-network-18b3bf4b51d8
[24] https://www.geeksforgeeks.org/advantages-and-disadvantages-of-star-topology/
[25] https://www.javatpoint.com/star-topology-advantages-and-disadvantages

LAN (Local Area Network)

LAN (aka Local Area Network) is a collection of entities/devices/nodes that are connected with each other in one physical location - as shown in the diagram below[26]. Examples of such physical locations are: office, building or home. It is important to understand that a LAN can be anything from a home network to an enterprise network with thousands (or mode) entities/devices/nodes in an office[27].

Overall, a LAN does not have to connect to the Internet, the only requirement is that we have devices which are able to exchange data. There are a variety of devices that connect to a LAN such as: laptops, IOT devices, game consoles, printers, personal computers and servers[28].

Moreover, until the 1980s, LAN was limited to research/education/public sector/defense applications. Also, LANs help connect devices in up to 1km radius[29].Lastly, there are different LAN technologies which can be used such as: Ethernet, WLAN (Wireless LAN), VLAN (Virtual LAN) - more on them and others in future writeups.



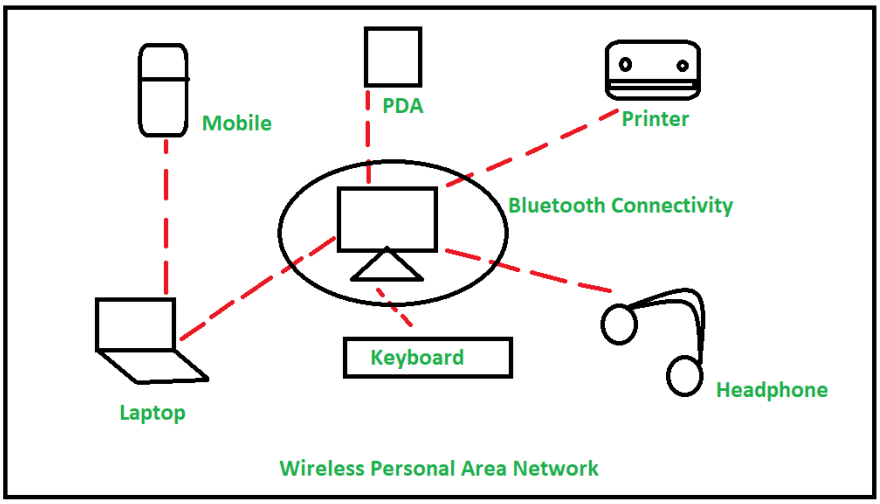
[26] http://chrezsoft.blogspot.com/2010/07/pengertian-lan-wan-man.html
[27] https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html
[28] https://www.cloudflare.com/learning/network-layer/what-is-a-lan/
[29] https://www.spiceworks.com/tech/networking/articles/what-is-local-area-network/

PAN (Personal Area Network)

PAN (aka Personal Area Network) is a network that connects electronic devices which are close to the user. We can take as an example a wireless mouse/keyboard and a computer. The connections in PAN can be wired (USB/Firewire/etc) or wireless (Bluetooth/WiFi/irDA/Zigbee/etc). Although devices within a PAN exchange data they don't connect directly to the Internet, however they can connect to a LAN[30] which is connected to the Internet[31].

Thus, we can categorize personal area networks in two main clusters: "Wireless PAN" (as shown in the diagram below) and "Wired PAN". When talking about ranges it is common to say that a PAN's range is about 10 meters or 33 feet. Due to that, it is relevant for "Body Area Networks", "Offline Networks" and "Home Networks"[32].

Lastly, as with any other network topology also a star topology has pros and cons. Examples of advantages are: portable, easily configurable, low energy consumption and more. Among the disadvantages are: short range, low data transfer rates, line of sight propagation and more[33].



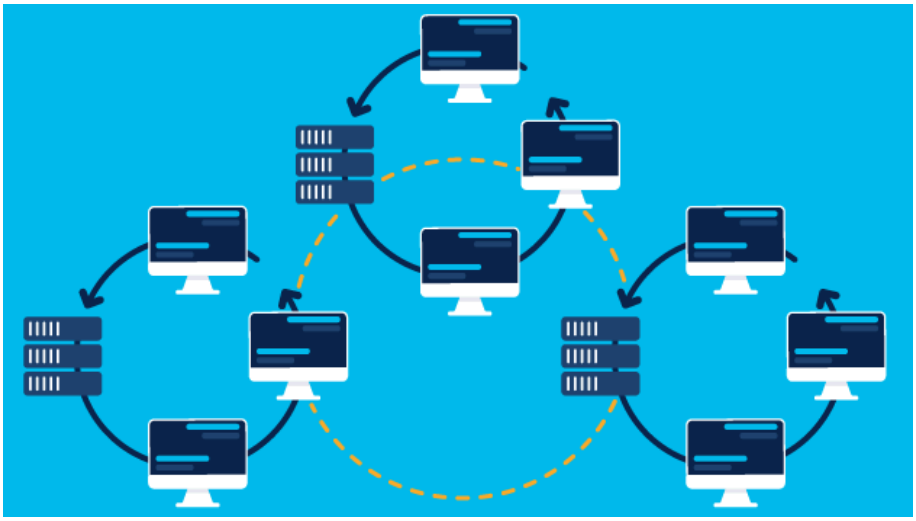
[30] https://medium.com/@boutnaru/the-computer-networking-journey-mesh-topology-2fe1a5550e06
[31] https://www.cloudflare.com/learning/network-layer/what-is-a-personal-area-network/
[32] https://www.geeksforgeeks.org/overview-of-personal-area-network-pan/
[33] https://blog.greencloudvps.com/personal-area-network-pan-an-overview.php

WAN (Wide Area Network)

WAN (aka Wide Area Network) is a collection of LANs[34] or other networks which are connected with each other. Thus, we can think about it as a network of networks - as shown in the diagram below. There are different types of WAN technologies like: “ATM”, “SDH”, “SD-WAN”, “SONET”, “Frame Relay”[35].

Overall, there are different techniques for performing WAN optimizations. Among those techniques we can find: network segmentation which leverages traffic shaping, traffic flow management (caching, compressing data and eliminating redundant data copies) and rate/connecting limiting[36].

Lastly, we have two main WAN connections: point-point WANs and switched WANs - more on those in future writeups. As with any other network types, WANs also have their pros and cons. Examples of advantages are: broad network coverage, simple communication for long distance and more. Among the disadvantages are: WANs confront more security challenges than LANs, connectivity issues, high maintenance, installation/setup fees and more[37].



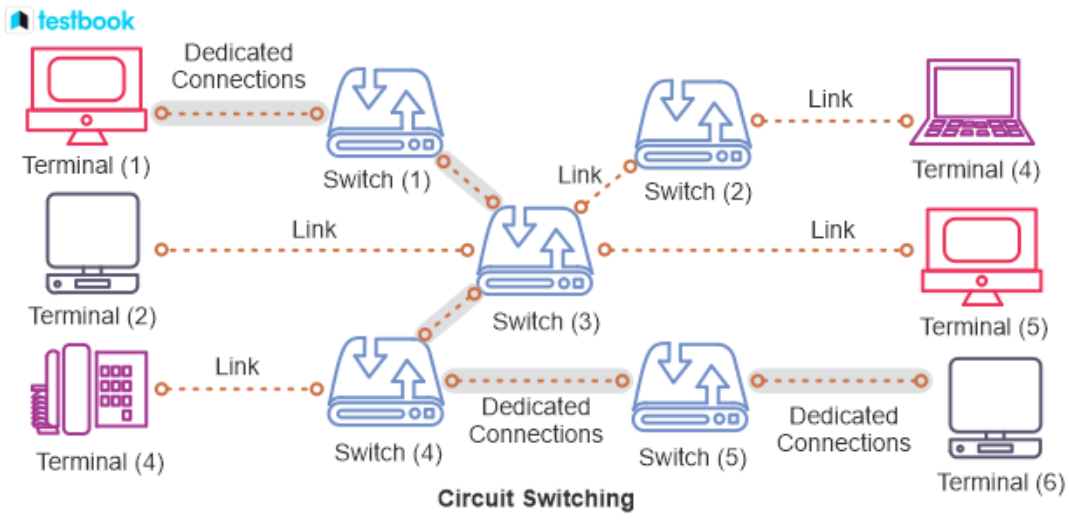
[34] https://medium.com/@boutnaru/the-nlan-local-area-network-18b3bf4b51d8
[35] https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html
[36] https://aws.amazon.com/what-is/wan/
[37] https://www.javatpoint.com/advantages-and-disadvantages-of-wan

Circuit Switching

In “Circuit Switching” a connection is established between the source and the destination before data is transferred. Thus, dedicated resources are saved for every specific connection. By using that we get a guaranteed data rate. This means data can be transmitted without any delays once the circuit is established (besides those of the network medium of course). We can summarize the phases of “Circuit Switching” as: “Circuit Establishment”, “Data Transfer” and “Circuit Disconnection”[38].

Overall, the name of “Circuit Switching” is based on the fact that a dedicated circuit is created during the lifetime of a connection - as shown in the diagram below. We can find circuit switching used in long distance communications like landline telephone. It is important to understand that a circuit is created only when needed and destroyed when the connection is closed[39].

Lastly, “Circuit Switching” has its pros and cons (as we have with other technologies). Examples of advantages are: ease of management, reliability, bandwidth assurance and more. Among the disadvantages are: waste of resources, low efficiency, limited scalability and more[40].



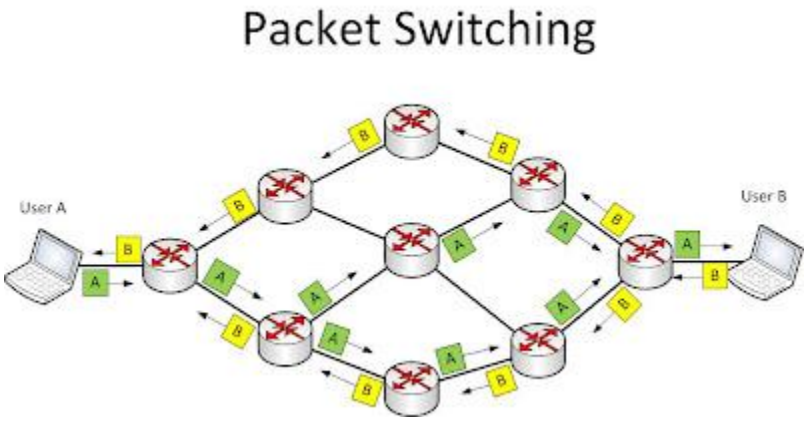
[38] https://www.geeksforgeeks.org/circuit-switching-in-computer-network/
[39] https://testbook.com/physics/circuit-switching
[40] https://www.educba.com/circuit-switching-advantages-and-disadvantages/

Packet Switching

As opposed to "Circuit Switching"[41] "Packet Switching" splits the data to be transferred to blocks/packets. This is done for a more efficient transfer due to the fact each packet can be sent in a different route[42] - as shown in the diagram below[43].

Thus, in contrast to "Circuit Switching" which has three phases ("Connection Establishment", "Data Transfer" and "Connection Released") in "Packet Switching" we just start sending the data. Also, in "Packet Switching" every packet knows the final destination but the intermediate path is decided by the routers, while in "Circuit Switching" entire path address is provided[44] - those of course are not all the differences between the two technologies and just examples.

Lastly, "Packet Switching" has its pros and cons (as we have with other technologies). Examples of advantages are: efficiency (think about many users sharing the same channel simultaneously), improved fault tolerance, reliability and more. Among the disadvantages are: protocols used complex and require high initial implementation costs, in case the network becomes overloaded packets are delayed\discarded\dropped and more[45].



[41] https://medium.com/@boutnaru/the-networking-journey-circuit-switching-bc628e8cf034
[42] https://avinetworks.com/glossary/packet-switching/
[43] https://packet-network.blogspot.com/2011/
[44] https://www.geeksforgeeks.org/difference-between-circuit-switching-and-packet-switching/
[45] https://www.rfwireless-world.com/Terminology/Advantages-and-disadvantages-of-packet-switching.html

Network Delays

In order to explain it we need to go over the following concepts: “Bandwidth Delay”, “Propagation Delay”, “Processing Delay” and “Queuing Delay”.

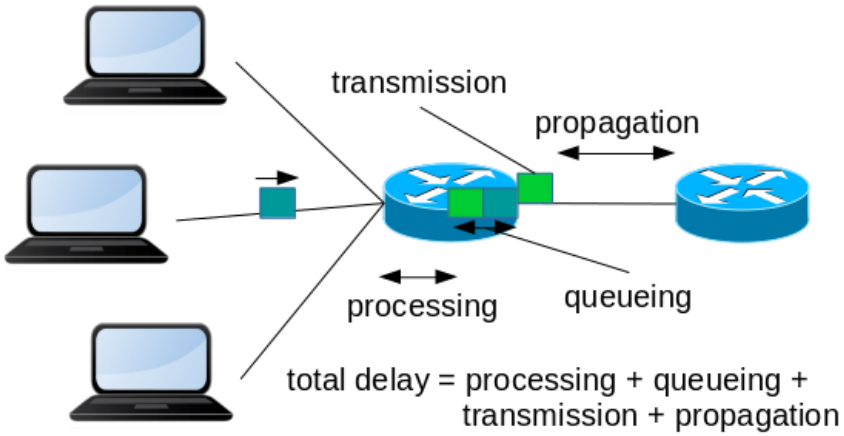
“Bandwidth Delay”, is the total time it takes to transmit data over a specific network link. It is also known as “Transmission Delay". Let's think about sending 64Kb at 640kb/s - it will take 0.1 seconds.

“Propagation Delay”, is the time it takes for the packet/frame to cross over the transmission medium. In case we are sending data over 200km cable in which the signal travels at 100km/ms it will take 2ms.

“Processing Delay”, is the time it takes to read the header of the packet (in case of a router)/frame (in case of a switch) and decide where to send it (what port/interface). It is also known as “Sore and Forward Delay”. In case the network devices also perform encryption/decryption (or other data manipulations) this time is also included in the “Procession Delay”.

“Queuing Delay”, is the time a packet is waiting in the queue of the router for other packets to be processed.

The total network delay is the sum of all of those (Total=“Bandwidth Delay”+“Propagation Delay”+“Processing Delay”+“Queuing Delay”). In the image below we can see an illustration of the different delays on top of a network diagram[46]



[46] https://developers.redhat.com/blog/2017/08/31/on-link-modeling-network-emulation-and-its-impacts-on-applications

CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

From this part we are going to talk about common protocols used in the different layers of the OSI model[47]. We are going to start with layer 2 aka “Data Link Layer”. Probably one of the most used layer 2 protocols is Ethernet. It is a family of protocols used mostly for LAN (Local Area Network) communication.

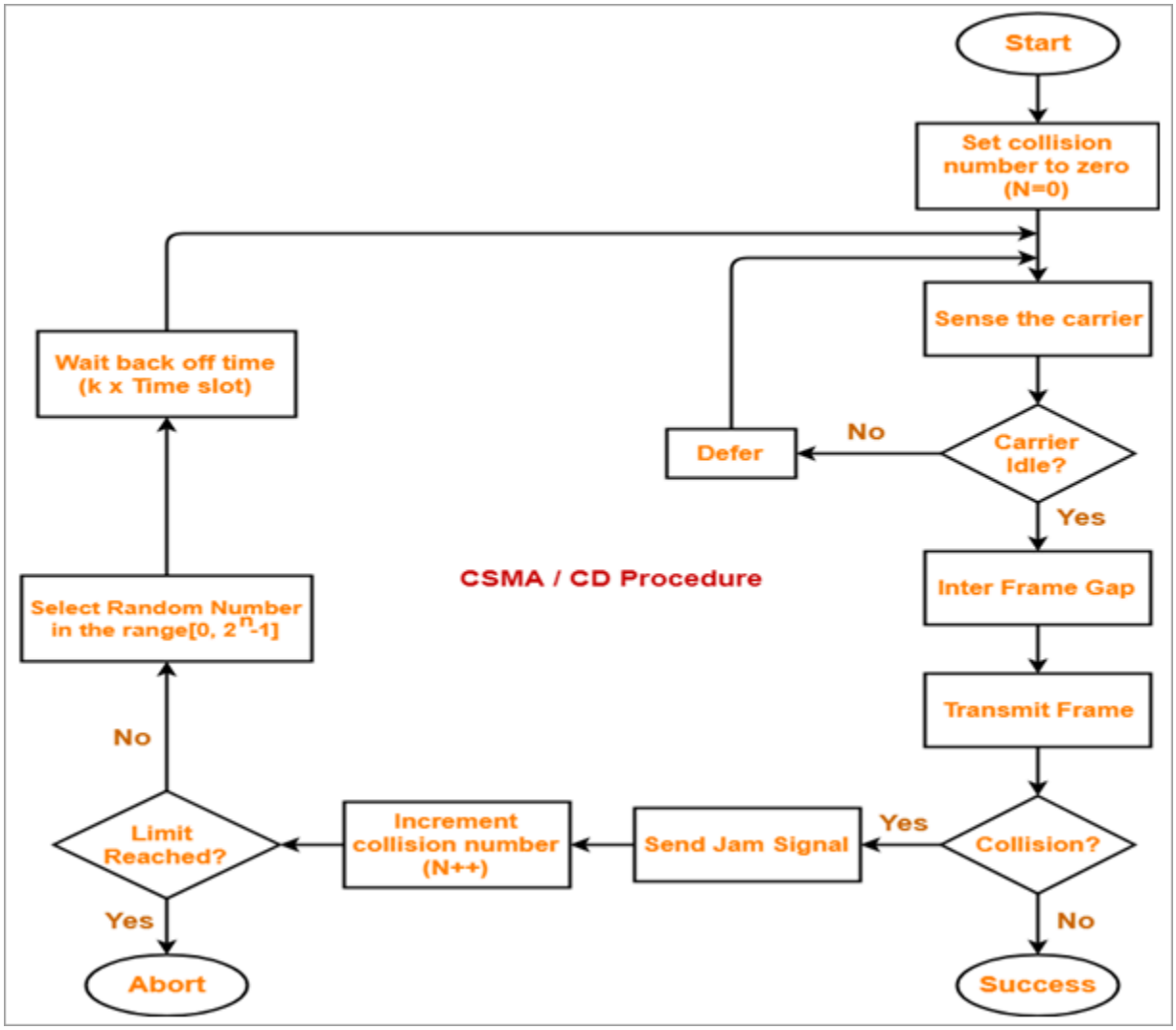
Ethernet is based on the concept of CSMA\CD (Carrier Sense Multiple Access with Collision Detection) - let’s explain that. First a host on the LAN sends frames over the network and in parallel it listens for incoming data (Carrier Sense). Also, each other host on the LAN listens on the network (Multiple Access). A host starts a transmission only when it does not “sense” any other transmission on the network (“carrier”).

However, we can still have a race condition. Think about a case when some host has started a transmission but a different host on the network does not hear that (due to delays such as propagation delay[48]) and it starts a transmission too.

Due to the parallel transmission if we are using a shared bus (like when the hosts are connected using a hub) a collision will occur. Because both of the senders are listening while transmitting they will identify the collision because of the wave interference (this is the Collision Detection part[49]). Lastly, each one of the hosts will pick a random number and wait until sending the data again (called backoff[50]). You can see the entire flow in the diagram below[51].

It is crucial to understand that it is a shared bus. Those collisions are the reason for reduction in efficiency and in case of high collision rate not being able to use the entire speed rate of our network equipment. Having said that, in case of smart layer 2 switches, there is a PVC (Private Virtual Circuit) which limits or even eliminates those problems (depending on the network devices).

[47] https://medium.com/@boutnaru/computer-networking-part-1-introduction-b3f15c28ec85
[48] https://medium.com/@boutnaru/computer-networking-part-2-network-delays-89514ed05154
[49] https://www.geeksforgeeks.org/collision-detection-csmacd/
[50] https://www.geeksforgeeks.org/back-off-algorithm-csmacd/
[51] https://www.softwaretestinghelp.com/what-is-csma-cd/

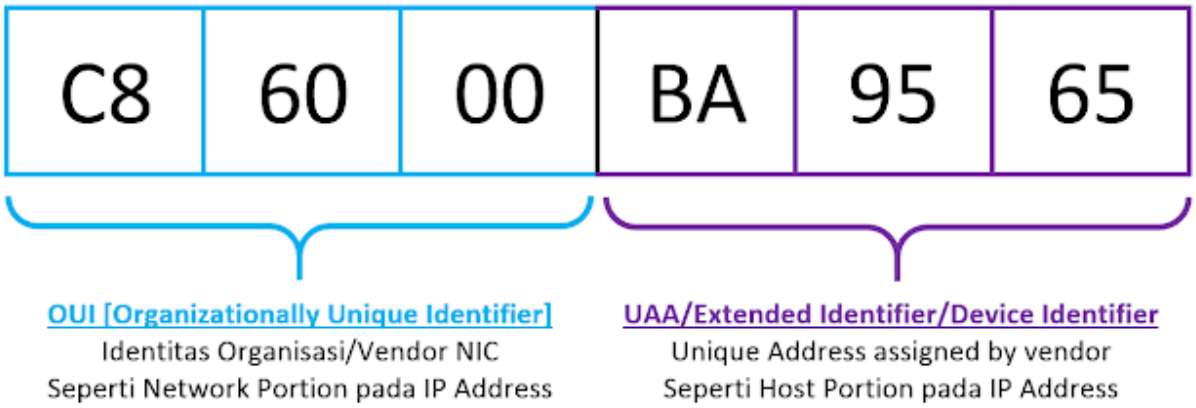

Start
Set collision number to zero (N=0)
Sense the carrier
Carrier Idle?
No
Defer
Yes
Inter Frame Gap
Transmit Frame
Collision?
Yes
Send Jam Signal
Increment collision number (N++)
Limit Reached?
No
Select Random Number in the range[0, 2^n-1]
Wait back off time (k x Time slot)
Yes
Abort
No
Success
CSMA / CD Procedure

MAC Address (Medium Access Control Address)

In general, in order to communicate and transfer data from one network device to the other, we need some kind of an address. A MAC (Medium Access Control) addressing schema at the "Data Link" layer. It is also known as the "Physical Address" of the network device (NIC) - although it is something that can be changed by OS configuration[52].

Moreover, a MAC address is a 48-bit number that is given during the manufacturing of the network device - as shown in the diagram below[53]. Usually it is displayed as a 12-digit hexadecimal number. The first 6 digits identify the manufacturer, which is aka OUI (Organizational Unique Identifier). Examples are: "3C:D9:2B" (HP), "CC:46:D6" (Cisco) and "3C:5A:B4" (Google). Those prefixes are assigned to vendors by "IEEE Registration Authority Committee". The other 6 digits are assigned by the manufacturer and represent the network device[54].

Lastly, we can check our MAC address using different OS commands. On Windows we can use "ipconfig /all"[55] or "getmac"[56]. On Linux/macOS we can use "ifconfig"[57].



[52] https://medium.com/@boutnaru/computer-networking-part-1-introduction-b3f15c28ec85
[53] https://leerhacking.blogspot.com/2017/01/what-is-mac-address-why-it-is-used.html
[54] https://www.geeksforgeeks.org/mac-address-in-computer-network/
[55] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig
[56] https://medium.com/@boutnaru/the-windows-process-journey-getmac-exe-displays-nic-mac-information-f1762755c1df
[57] https://ss64.com/osx/ifconfig.html

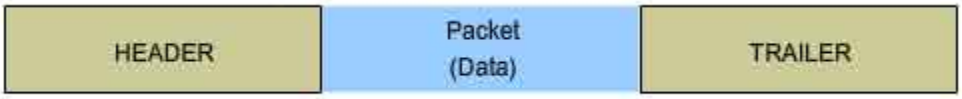
Network Protocol

A network protocol can be defined as a well established set of rules that determine the way to transfer data between network entities/elements/nodes/devices. By using network protocols connected devices can communicate even if they are based on different design/hardware/software. We can think about network protocols as “speaking languages” for network devices[58].

Moreover, most of the time (but not limited to) network protocols are created by different technology organizations based on industry standards. Examples of such organizations are: “The Institute of Electrical and Electronics Engineers” aka IEEE[59], “The Internet Engineering Task Force” aka IETF[60], “The International Telecommunications Union” aka ITU[61], “The International Organization for Standardization” aka ISO[62] and “The World Wide Web Consortium” aka W3C[63].

Overall, a generic protocol is composed of a header and a payload after it, sometimes we can also have a trailer - as shown in the diagram below[64]. The goal of the header is to hold information relevant for the protocol and to pass it to the corresponding layer[65] on the other side of the communication. The header/trailer can be textual or binary (based on the network protocol definition).

Lastly, there are numerous well known protocols such as Ethernet, Dot1Q, ISL, IP, TCP, UDP, HTTP/S, SMTP, SNMP, BGP, OSPF, ICMP, IGMP, DNS, NTP, Kerberos and more.



[58] https://www.comptia.org/content/guides/what-is-a-network-protocol
[59] https://www.ieee.org/
[60] https://www.ietf.org/
[61] https://www.itu.int/en/Pages/default.aspx
[62] https://www.iso.org/home.html
[63] https://www.w3.org/
[64] http://www.highteck.net/EN/DataLink/Data_Link_Layer.html
[65] https://medium.com/@boutnaru/computer-networking-part-1-introduction-b3f15c28ec85