

The Networking Journey

Version 2.0

May-2025

By Dr. Shlomi Boutnaru



created using [Craiyon AI Image Generator](#)

Table of Contents

Table of Contents.....	2
Introduction.....	4
Data Encapsulation and De-Encapsulation.....	6
Network Topology.....	7
Bus Topology.....	8
Ring Topology.....	9
Mesh Topology.....	10
Star Topology.....	11
LAN (Local Area Network).....	12
PAN (Personal Area Network).....	13
WAN (Wide Area Network).....	14
Circuit Switching.....	15
Packet Switching.....	16
Network Protocol.....	17
Network Delays.....	18
CSMA/CD (Carrier Sense Multiple Access with Collision Detection).....	19
MAC Address (Medium Access Control Address).....	21
ITU (International Telecommunication Union).....	22
FCC (Federal Communications Commission).....	23
IETF (Internet Engineering Task Force).....	24
RFC (Request For Comment).....	25
IEEE (Institute of Electrical and Electronics Engineers).....	26
IEEE 802 Standards.....	27
RF (Radio Frequency) Communication.....	28
Simplex Transmission Mode.....	29
Half Duplex Transmission Mode.....	30
Full Duplex Transmission Mode.....	31
TDM (Time Division Multiplexing).....	32
FDM (Frequency Division Multiplexing).....	33
CDM (Code Division Multiplexing).....	34
WDM (Wavelength Division Multiplexing).....	35
Ethernet (IEEE 802.3).....	36
Unicast.....	37
Broadcast.....	38
Multicast.....	39
Anycast.....	40
Broadcast Domain.....	41
Ethernet Switch (Layer 2 Switch).....	42
VLAN (Virtual LAN).....	43

Dot1Q (IEEE 802.1Q).....	44
Access Port.....	45
MPLS (Multi-Protocol Label Switching).....	46
Wake-on-Lan (WoL).....	47
PSTN (Public Switched Telephone Network).....	48

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 other¹.

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).

¹ <https://blog.netwrix.com/2019/01/08/network-devices-explained/>

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 from lower to upper). The sentences are: “**All People Seems to Need Data Processing**” and “**Please Don’t Throw Super Pizza Away**” (maybe 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 example².

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

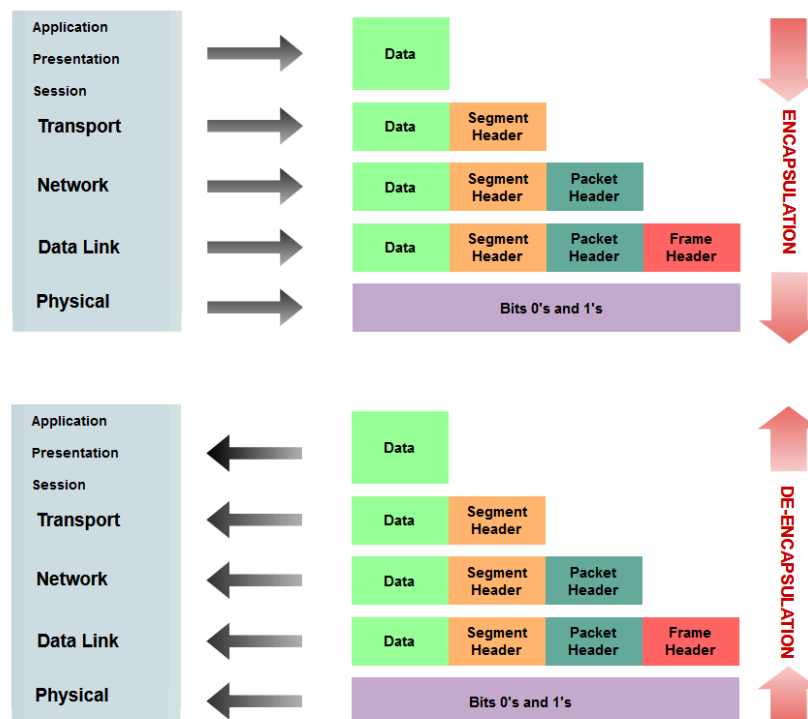
² https://infosvs.beckhoff.com/content/1033/tf6310_tc3_tcpip/84246923.html

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 below³.

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 more⁴.

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.



³ <https://www.educative.io/answers/what-are-encapsulation-and-de-encapsulation-in-networking>

⁴ <https://afteracademy.com/blog/what-is-data-encapsulation-and-de-encapsulation-in-networking/>

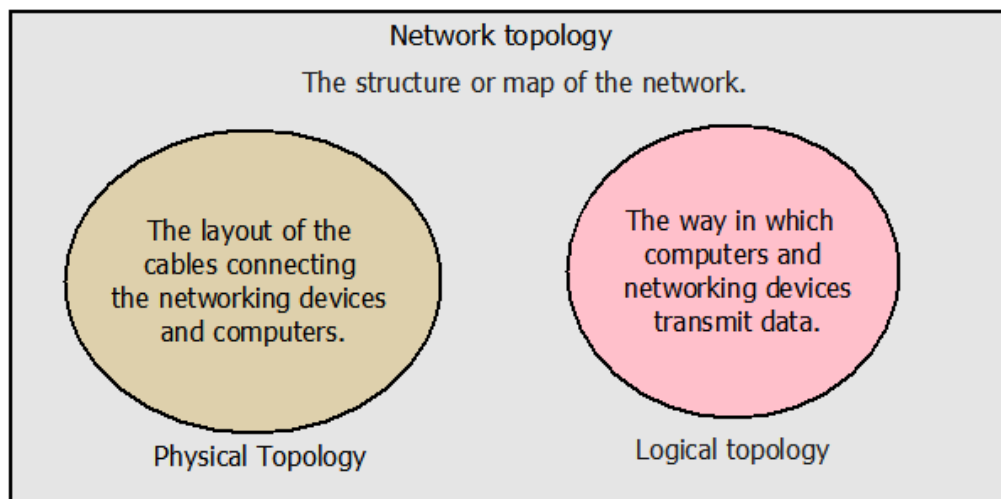
Network Topology

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 topologies⁵ - as shown in the diagram below⁶.

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 mesh⁷ - 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 ring⁸ - 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 them⁹.



⁵ https://en.wikipedia.org/wiki/Network_topology

⁶ <https://www.computernetworkingnotes.org/images/networking-tutorials/nt26-01-physical-lavout-vs-logical-lavout.png>

⁷ <https://www.computernetworkingnotes.com/networking-tutorials/differences-between-physical-and-logical-topology.html>

⁸ https://www.omniseu.com/basic-networking/difference-between-physical-topology-and-logical-topology.php?expand_article=1

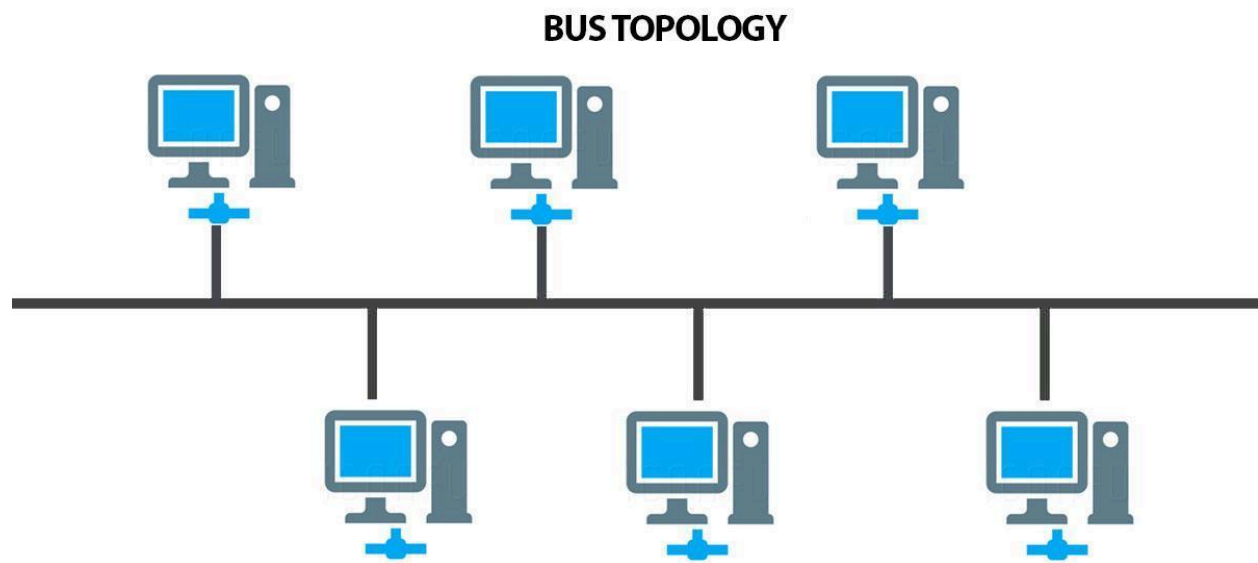
⁹ <https://blogs.arubanetworks.com/solutions/network-topologies-logical-vs-physical/>

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 cable¹⁰.

Overall, in a bus topology every network element (like computer/network device) is connected using a single cable - as shown in the diagram below¹¹. There are different network protocols which are targeting bus topology such as TDMA, Pure Aloha, CDMA, Slotted Aloha and more¹².

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 time¹³. We will cover in future writeups different technologies which can help deal with the disadvantages covered here.



¹⁰ <https://www.computerhope.com/jargon/b/bustopol.htm>

¹¹ <https://www.cablify.ca/an-introduction-to-network-topology/>

¹² <https://www.geeksforgeeks.org/types-of-network-topology/>

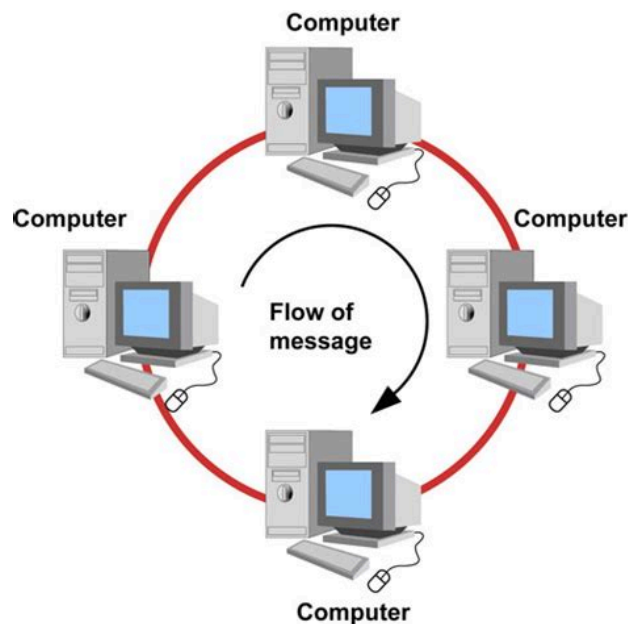
¹³ <https://www.cbttuggets.com/blog/technology/networking/what-is-bus-topology>

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 below¹⁴. 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 collisions¹⁵.

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 failure¹⁶.

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 transmission¹⁷ - more on that in future writeups.



¹⁴ <http://www.techiwarehouse.com/engine/e96bb2f2/Understanding-Ring-Topology>

¹⁵ <https://unstop.com/blog/ring-topology-in-computer-network>

¹⁶ <https://www.cbttuggets.com/blog/technology/networking/why-still-use-a-ring-network-topology>

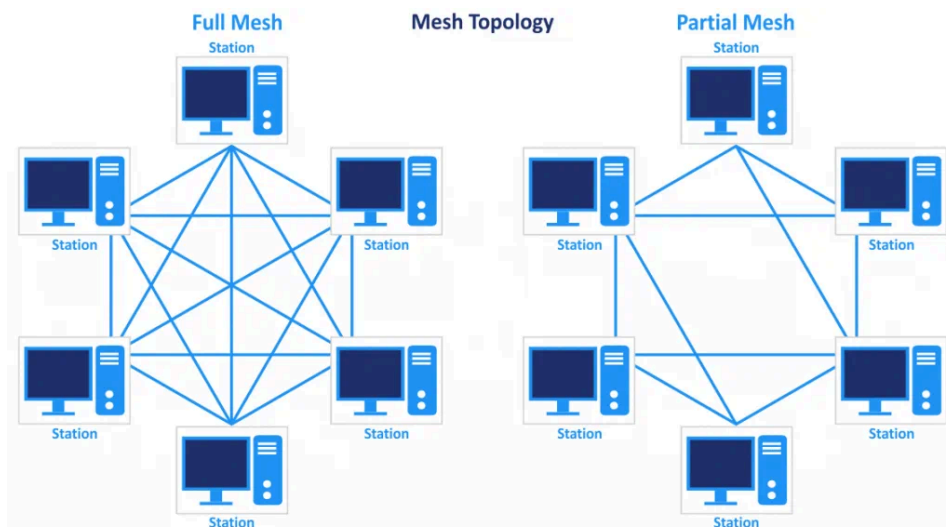
¹⁷ <https://www.lenovo.com/us/en/glossary/what-is-ring-topology/>

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 nodes¹⁸ - as shown in the diagram below¹⁹.

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 networks²⁰.

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”²¹ and OLSR routing protocol which stands for “Optimized Link State Routing Protocol”²².



¹⁸ <https://www.computerhope.com/jargon/m/mesh.htm>

¹⁹ <https://www.nakivo.com/blog/types-of-network-topology-explained/>

²⁰ <https://www.lenovo.com/us/en/glossary/mesh-topology/>

²¹ https://www.digi.com/resources/documentation/Digidocs/90002002/Concepts/c_zb_AODV_mesh_routing.htm

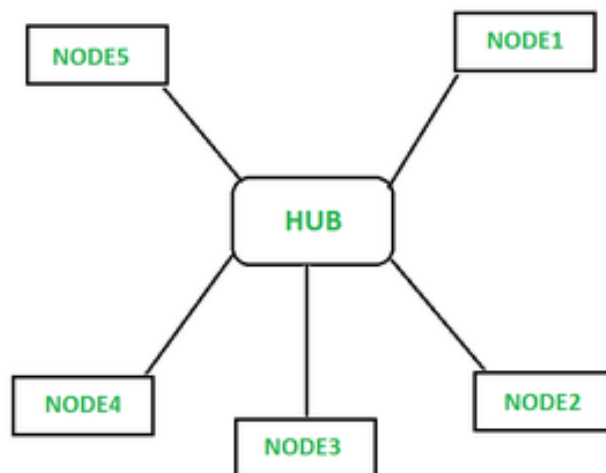
²² <https://openwrt.org/docs/guide-user/network/wifi/mesh/olsr>

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 device²³. This type of topology is most used in the case of LANs²⁴.

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 network²⁵- 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 more²⁶.



²³ <https://medium.com/@boutnaru/the-computer-networking-journey-mesh-topology-2fe1a5550e06>

²⁴ <https://medium.com/@boutnaru/the-nlan-local-area-network-18b3bf4b51d8>

²⁵ <https://www.geeksforgeeks.org/advantages-and-disadvantages-of-star-topology/>

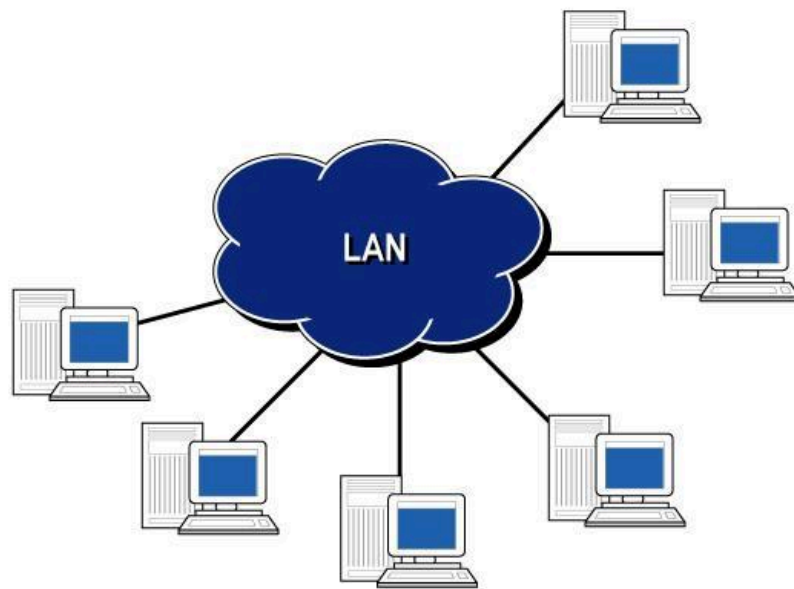
²⁶ <https://www.javatpoint.com/star-topology-advantages-and-disadvantages>

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 below²⁷. 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 more) entities/devices/nodes in an office²⁸.

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 servers²⁹.

Moreover, until the 1980s, LAN was limited to research/education/public sector/defense applications. Also, LANs help connect devices in up to 1km radius³⁰. 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.



²⁷ <http://chrezsoft.blogspot.com/2010/07/pengertian-lan-wan-man.html>

²⁸ <https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html>

²⁹ <https://www.cloudflare.com/learning/network-layer/what-is-a-lan/>

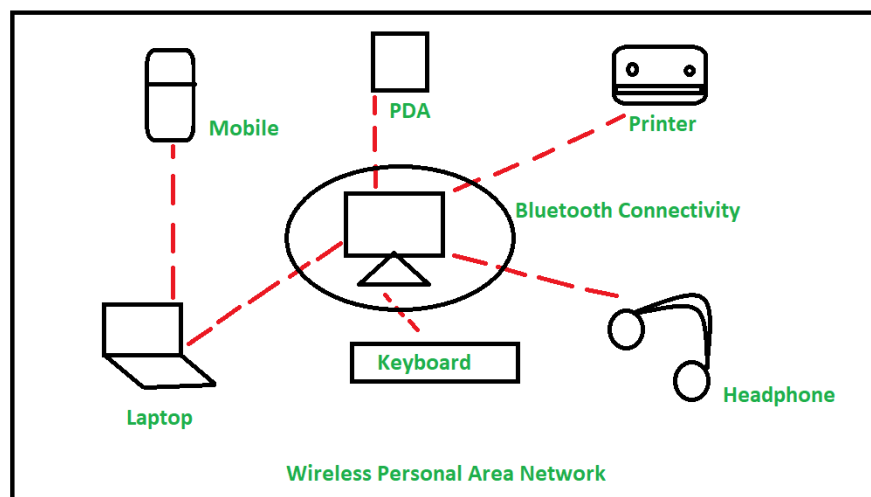
³⁰ <https://www.spiceworks.com/tech/networking/articles/what-is-local-area-network/>

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 LAN³¹ which is connected to the Internet³².

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”³³.

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 more³⁴.



³¹ <https://medium.com/@bournaru/the-computer-networking-journey-mesh-topology-2fe1a5550e06>

³² <https://www.cloudflare.com/learning/network-layer/what-is-a-personal-area-network/>

³³ <https://www.geeksforgeeks.org/overview-of-personal-area-network-pan/>

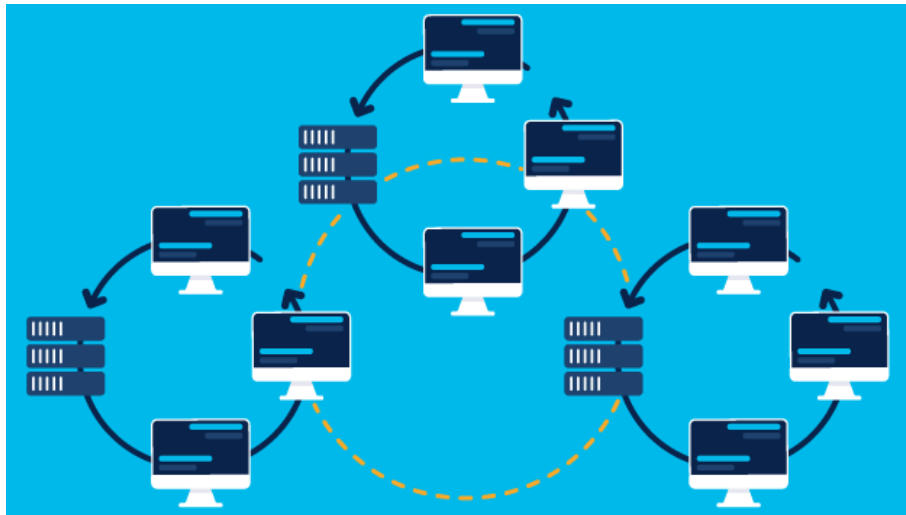
³⁴ <https://blog.greencloudvps.com/personal-area-network-pan-an-overview.php>

WAN (Wide Area Network)

WAN (aka Wide Area Network) is a collection of LANs³⁵ 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”³⁶.

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 limiting³⁷.

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 more³⁸.



³⁵ <https://medium.com/@boutnaru/the-nlan-local-area-network-18b3bf4b51d8>

³⁶ <https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html>

³⁷ <https://aws.amazon.com/what-is/wan/>

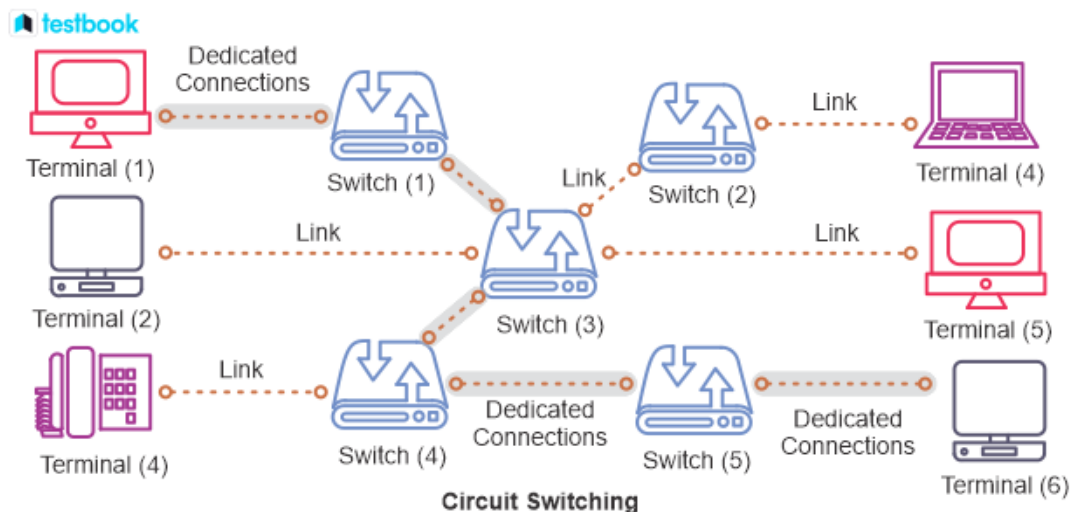
³⁸ <https://www.javatpoint.com/advantages-and-disadvantages-of-wan>

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”³⁹.

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 closed⁴⁰.

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 more⁴¹.



³⁹ <https://www.geeksforgeeks.org/circuit-switching-in-computer-network/>

⁴⁰ <https://testbook.com/physics/circuit-switching>

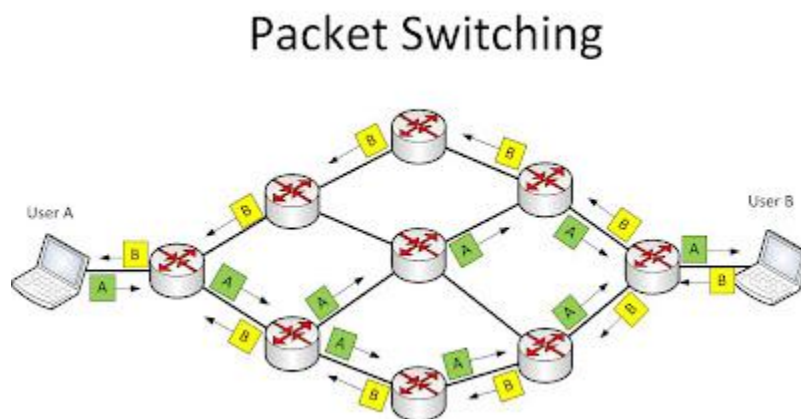
⁴¹ <https://www.educba.com/circuit-switching-advantages-and-disadvantages/>

Packet Switching

As opposed to “Circuit Switching”⁴² “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 route⁴³ - as shown in the diagram below⁴⁴.

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 provided⁴⁵ - those of course are not all the differences between the 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 more⁴⁶.



⁴² <https://medium.com/@boutnaru/the-networking-journey-circuit-switching-bc628e8cf034>

⁴³ <https://avinetworks.com/glossary/packet-switching/>

⁴⁴ <https://packet-network.blogspot.com/2011/>

⁴⁵ <https://www.geeksforgeeks.org/difference-between-circuit-switching-and-packet-switching/>

⁴⁶ <https://www.rfwireless-world.com/Terminology/Advantages-and-disadvantages-of-packet-switching.html>

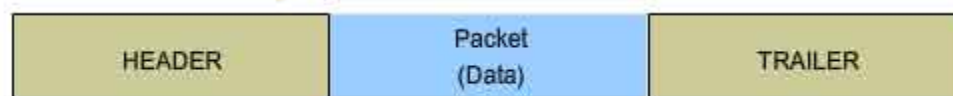
Network Protocol

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 devices⁴⁷.

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 IEEE⁴⁸, “The Internet Engineering Task Force” aka IETF⁴⁹, “The International Telecommunications Union” aka ITU⁵⁰, “The International Organization for Standardization” aka ISO⁵¹ and “The World Wide Web Consortium” aka W3C⁵².

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 below⁵³. The goal of the header is to hold information relevant for the protocol and to pass it to the corresponding layer⁵⁴ 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.



⁴⁷ <https://www.comptia.org/content/guides/what-is-a-network-protocol>

⁴⁸ <https://www.ieee.org/>

⁴⁹ <https://www.ietf.org/>

⁵⁰ <https://www.itu.int/en/Pages/default.aspx>

⁵¹ <https://www.iso.org/home.html>

⁵² <https://www.w3.org/>

⁵³ http://www.highteck.net/EN/DataLink/Data_Link_Layer.html

⁵⁴ <https://medium.com/@boutnaru/computer-networking-part-1-introduction-b3f15e28ec85>

Network Delays

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

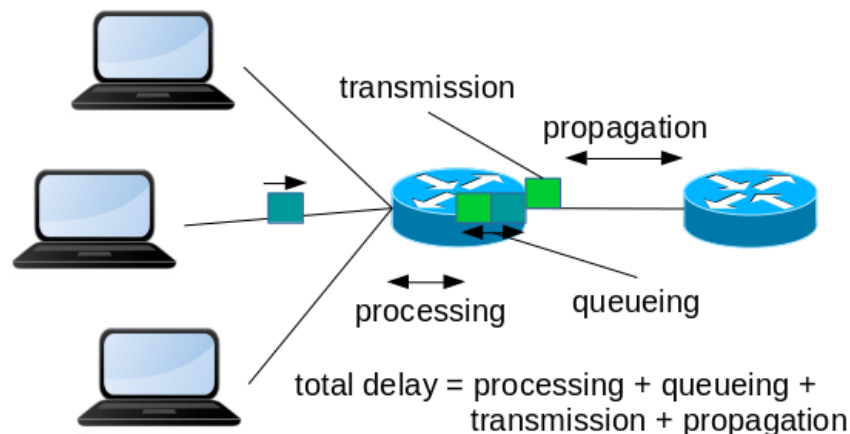
“Bandwidth Delay”, is the total time it takes to transmit data over a specific network link. It is also known as “Transmission Delay”. Let's think about sending 64Kb at 640kb/s - it will take 0.1 seconds.

“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 “Store and Forward Delay”. In case the network devices also perform encryption/decryption (or other data manipulations) this time is also included in the “Processing 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 diagram⁵⁵



⁵⁵ <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 model⁵⁶. 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 delay⁵⁷) 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 part⁵⁸). Lastly, each one of the hosts will pick a random number and wait until sending the data again (called backoff⁵⁹). You can see the entire flow in the diagram below⁶⁰.

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).

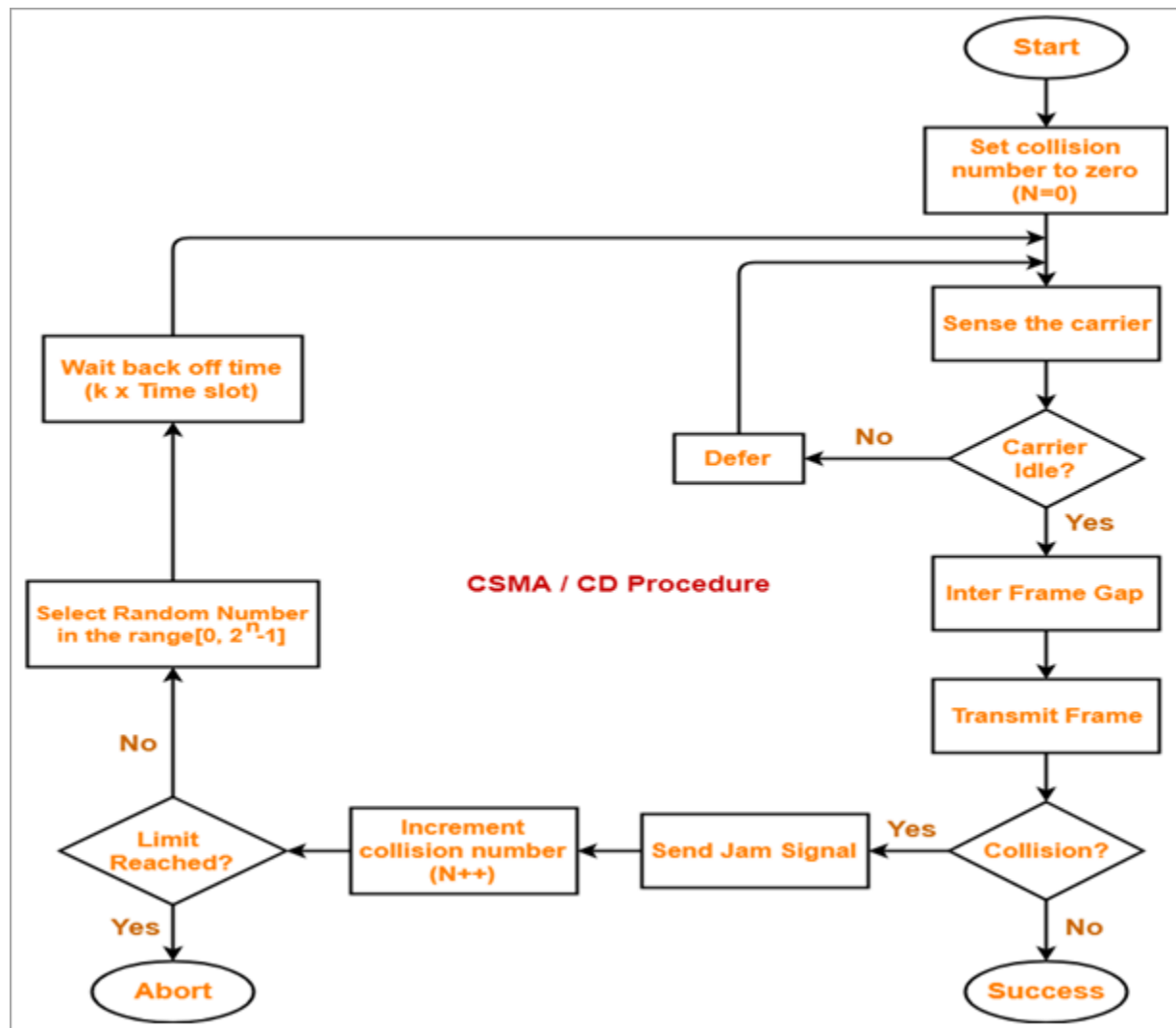
⁵⁶ <https://medium.com/@boutnaru/computer-networking-part-1-introduction-b3f15c28ec85>

⁵⁷ <https://medium.com/@boutnaru/computer-networking-part-2-network-delays-89514ed05154>

⁵⁸ <https://www.geeksforgeeks.org/collision-detection-csmacd/>

⁵⁹ <https://www.geeksforgeeks.org/back-off-algorithm-csmacd/>

⁶⁰ <https://www.softwaretestinghelp.com/what-is-csma-cd/>

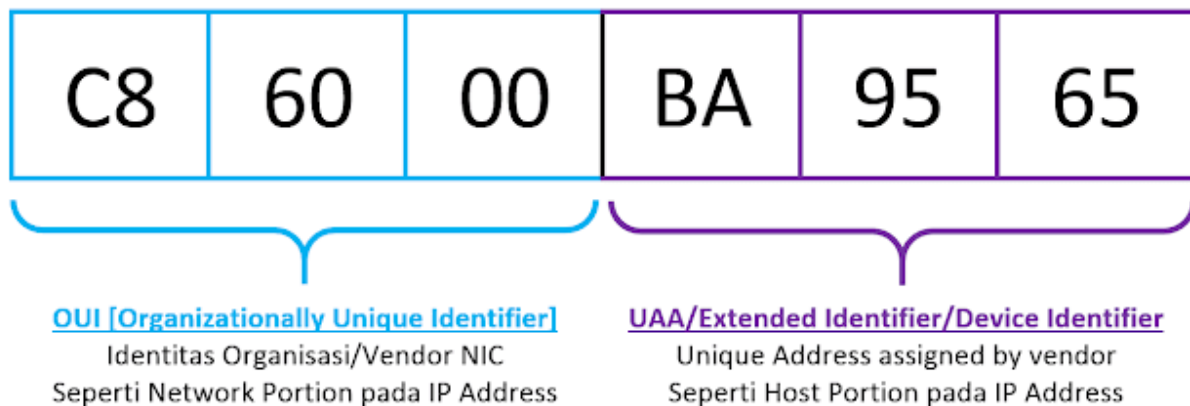


MAC Address (Medium Access Control Address)

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 configuration⁶¹.

Moreover, a MAC address is a 48-bit number that is given during the manufacturing of the network device - as shown in the diagram below⁶². 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 device⁶³.

Lastly, we can check our MAC address using different OS commands. On Windows we can use “ipconfig /all”⁶⁴ or “getmac”⁶⁵. On Linux/macOS we can use “ifconfig”⁶⁶.



⁶¹ <https://medium.com/@boutnaru/computer-networking-part-1-introduction-b3f15c28ec85>

⁶² <https://leerhacking.blogspot.com/2017/01/what-is-mac-address-why-it-is-used.html>

⁶³ <https://www.geeksforgeeks.org/mac-address-in-computer-network/>

⁶⁴ <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig>

⁶⁵ <https://medium.com/@boutnaru/the-windows-process-journev-getmac-exe-displays-nic-mac-information-f1762755c1df>

⁶⁶ <https://ss64.com/osx/ifconfig.html>

ITU (International Telecommunication Union)

ITU (International Telecommunication Union) is a “United Nations” agency which specializes in digital technologies (ICTs). ITU is made up of: 1000+ companies, 194 Member States, universities and more. The headquarters of the ITU is located in Geneva (Switzerland) - as shown in the image below⁶⁷. There are also regional offices on every continent. By the way, ITU is the oldest agency in the UN family⁶⁸.

Overall, ITU is composed of three main sectors: ITU-R (radio communication), ITU-T (standardization) and ITU-D (development). Each of those managing a different aspect of the covered by the ITU⁶⁹. Thus, ITU is involved in: broadband networks, wireless technologies, aeronautical\maritime navigation, radio astronomy, oceanographic\satellite-based earth monitoring ,fixed-mobile phone, Internet and broadcasting technologies⁷⁰.

Lastly, examples of standards that were published by ITU (and related to communication) are: ISDN (Integrated Services Digital Network), OTN (Optical Transport Network), WDM (Wavelength-division multiplexing), DSL (Digital Subscriber Line), Fax standards (like T.2/T.4/T.30/T.37/T.38), SS7 (Signalling System 7) and more⁷¹.



⁶⁷ <https://www.britannica.com/topic/International-Telecommunication-Union>

⁶⁸ <https://www.itu.int/en/about/Pages/default.aspx>

⁶⁹ https://en.wikipedia.org/wiki/International_Telecommunication_Union

⁷⁰ <https://www.ungeneva.org/en/about/organizations/itu>

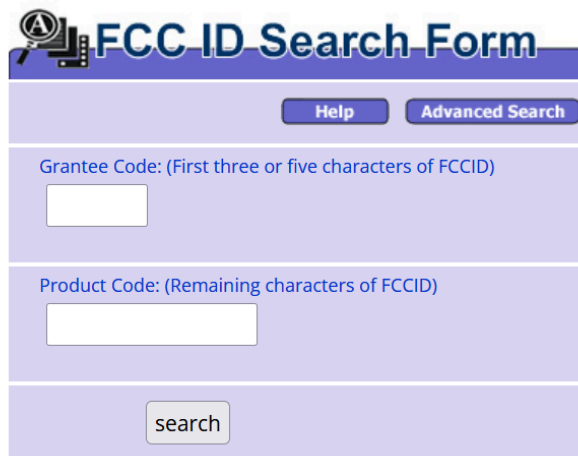
⁷¹ <https://en.wikipedia.org/wiki/ITU-T>

FCC (Federal Communications Commission)

FCC (Federal Communications Commission) regulates interstate and international communications by radio, television, wire, satellite and cable. It is an independent U.S. government agency overseen by Congress. Basically, the FCC is the federal agency responsible for implementing and enforcing America's communications law and regulations⁷².

Overall, in 1934, the "Communications Act" was passed by the Congress. This led to the replacement of the FRC (Federal Radio Commission) with the FCC. The "Communications Act" also put the telephone communications under the FCC's control. The FCC was also created to help break up some of the communications monopolies that had developed by 1934⁷³.

Lastly, the FCC assigned a "FCC ID" to each electronic device in the U.S. This code is used to identify and certify that the device meets the necessary regulatory standards for wireless communication (like if it operates within the prescribed limits of radio frequency emissions). Thus, "FCC ID" helps to ensure that electronic devices comply with regulations set by the FCC⁷⁴. By the way, we can also search for relevant documentation using the "FCC ID"⁷⁵ - as shown in the screenshot below.

A screenshot of the FCC ID Search Form. The form has a purple header with the title "FCC ID Search Form" and a magnifying glass icon. Below the header, there are two buttons: "Help" and "Advanced Search". The form contains two input fields: "Grantee Code: (First three or five characters of FCCID)" and "Product Code: (Remaining characters of FCCID)". At the bottom of the form is a "search" button.

⁷² <https://www.fcc.gov/about/overview>

⁷³ <https://www.mitel.com/en-gb/articles/history-federal-communications-commission-fcc>

⁷⁴ <https://www.lenovo.com/us/en/glossary/fcc-id/>

⁷⁵ <https://www.fcc.gov/oet/ea/fccid>

IETF (Internet Engineering Task Force)

The IETF (Internet Engineering Task Force) is the major standard development organization for the Internet. It was founded in 1986, since then it makes voluntary standards that are often adopted by network operators\Internet users\equipment vendors. By doing so it helps shape the trajectory of the development of the Internet. It is important to understand that the IETF does not have any control over the Internet and what standards are going to be adopted or not⁷⁶.

Moreover, IETF works on many networking technologies in different areas such as: security and privacy, IOT (Internet of Things), automated network management and more⁷⁷. The technical documents which are published by the IETF are called RFCs (Request for Comment)⁷⁸.

Lastly, IETF has three week-long meetings every year. The average participants are about 1000-1500 on site and about 600+ remote participants - as shown in the image below⁷⁹. We can cluster the participants into the following groups: vendors, academia, network operators, civil society, consultants and more⁸⁰. After each meeting official records are published like the agenda\presentations\bluesheets\etc⁸¹. Also, there is a YouTube channel where recordings of all of the sessions are posted usually 24 hours after the session⁸².



⁷⁶ <https://www.ietf.org/about/introduction/>

⁷⁷ <https://www.ietf.org/technologies/>

⁷⁸ <https://www.rfc-editor.org>

⁷⁹ <https://www.ietf.org/how/meetings>

⁸⁰ <https://www.ietf.org/meeting/guide-ietf-meetings/>

⁸¹ <https://www.ietf.org/meeting/past/>

⁸² <https://www.youtube.com/user/ietf>

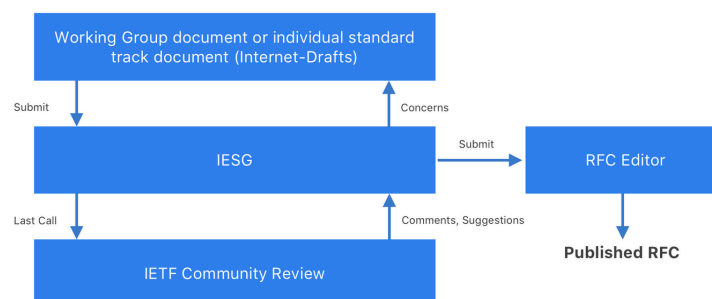
RFC (Request For Comment)

RFC (Request For Comment) is a technical document that is published by the IETF⁸³. RFCs describe the Internet's technical foundations (think about addressing, routing, and transport technologies). Also, RFCs can specify protocols (examples are TLS 1.3, QUIC, and WebRTC). Moreover, RFCs are sequentially numbered. The first one (Title: Host Software) was published in 1969 (the RFC series predates the IETF). Today, there are more than 9000 documents in the series⁸⁴.

Overall, if we were to create a list of the most fundamental RFCs the following would probably be included: UDP (RFC 768, IP (RFC 791) , TCP (RFC 793), “Address Allocation for Private Internets” (RFC 1918) and “Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content” (RFC 7231) . RFCs can be published in different formats: HTML, plain text, HTMLised, PDF and RFCXML. The authoritative website for RFC is the “RFC Editor”⁸⁵. For transparent information about the process of an RFC we can use the “IETF Datatracker”. It contains data about the documents, working groups, meetings, agendas, minutes, presentations, and more regarding the IETF⁸⁶. The submission flow is explained in the diagram below⁸⁷.

Lastly, in almost every “April Fools’ Day” (1st of April) since 1989 the “RFC Editor” is publishing one (or more) humorous RFC. Examples are: “A Historical Perspective On The Usage Of IP Version 9” (01-April-1994), “The Transmission of IP Datagrams over the Semaphore Flag Signaling System” (01-April-2007), “Complex Addressing in IPv6” (01-April-2017) , “The Addition of the Death (DTH) Flag to TCP” (01-April-2023) and “Faster Than Light Speed Protocol” (01-April-2024). Before 1989 the first humorous RFC that had been published was “TELNET RANDOMLY-LOSE Option” in 1978⁸⁸.

Simplified IETF Submission Flow



⁸³ <https://medium.com/@boutnaru/the-computer-networking-journey-ietf-internet-engineering-task-force-de104ba4fb8f>

⁸⁴ <https://www.ietf.org/process/rfc/>

⁸⁵ <https://www.rfc-editor.org/>

⁸⁶ <https://datatracker.ietf.org/>

⁸⁷ <https://basics.domains/presentations/18/domain-name-basics/request-for-comments-rfc>

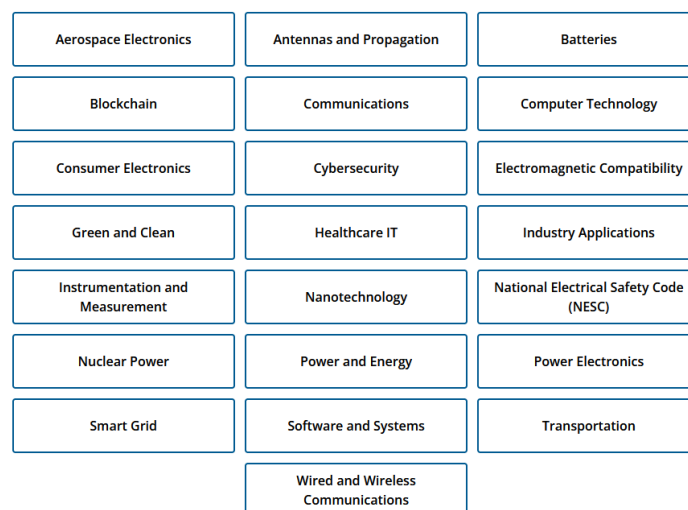
⁸⁸ https://en.wikipedia.org/wiki/April_Fools%27_Day_Request_for_Comments

IEEE (Institute of Electrical and Electronics Engineers)

IEEE (Institute of Electrical and Electronics Engineers) is professional association for electronics engineering, electrical engineering, and other related disciplines. IEEE is composed of technical societies. Each society is targeting a specific area of knowledge and provides publications/conferences/networking and other services in those areas. Examples of such are: “Aerospace and Electronic Systems Society”, “Broadcast Technology Society”, “Antennas & Propagation Society”, “Electronics Packaging Society”, “Computer Society”, “Microwave Theory and Technology Society”⁸⁹ and “Communications Society”⁸⁹.

Overall, IEEE is the world’s largest technical professional organization dedicated to advancing technology for the benefit of humanity. We can search for IEEE standards using the “IEEE SA” (Standards Association). The standards are clustered into 22 different categories such as: blockchain, nanotechnology, cybersecurity, power electronics, healthcare IT , smart grid, batteries and more⁹⁰ - as shown in the diagram below.

Lastly, as of 2024 there are over 460,000 members as part of IEEE. Those members are spreaded across 190 countries (>66% outside the US). Also, more than 170,000 are student members⁹¹. For searching among books, conferences, courses, journals, magazines and standards we can use “IEEE Xplore”. By the way, as of 2024 it contains more than 6.4M items⁹².



⁸⁹ https://en.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers

⁹⁰ <https://standards.ieee.org/standard/>

⁹¹ <https://www.ieee.org/about/at-a-glance.html>

⁹² <https://ieeexplore.ieee.org>

IEEE 802 Standards

“IEEE 802” is a family of standards for LAN (Local Area Networks)/PAN (Personal Area Network)/MAN (Metropolitan Area Network) protocols⁹³. Those standards are managed\maintained\developed by the IEEE organization⁹⁴.

Overall, as examples among the “IEEE 802” working\study groups we have the following⁹⁵: “802.1” (Higher Layer LAN Protocols Working Group), “802.3” (Ethernet Working Group), “802.11” (Wireless LAN Working Group), “802.15” (Wireless Specialty Network (WSN) Working Group), “802.18” (Radio Regulatory TAG), “802.19” (Wireless Coexistence Working Group) and “802.24” (Vertical Applications TAG). Also, there are also working\study groups focused on “Hibernating and Disbanded”⁹⁶ - a short list of the standards is show in the diagram below⁹⁷.

Lastly, the origin of the “802” in the name of the committee\standards is due to the fact the committee was established on February 1980⁹⁸. By the way, the network standards as part of “IEEE 802” are restricted to networks carrying variable-size packets (as opposed to cell relay). Also, services\protocols as part of “IEEE 802” are mapped to the lower two layers of the OSI model: “Physical Layer” and “Data Link Layer”. The “Data Link Layer” is splitted into LLC (Logical Link Layer) and MAC (Media Access Control)⁹⁹.

IEEE 802 Standards		
Standard	Name	Topic
802.1	Internetworking	Routing,Bridging,and network-to-network Communications
802.2	Logical Link Control	Error and flow control over data frames
802.3	Ethernet LAN	All forms of Ethernet media and interfaces
802.4	Token BUS LAN	All forms of Token Bus media and interfaces
802.5	Token Ring LAN	All forms of Token Ring media and interfaces
802.6	Metropolitan Area Network	MAN technologies,Addressing, and Services
802.7	Broadband technical Advisory Group	Broadband network media,interfaces, adn other Equipments
802.8	Fiber Optic Technical Advisory Group	Fiber Optic media used in token-passing Networks like FDDI
802.9	Integrated Voice/ Data Network	Integration of voice and data traffic Over a single network medium
802.10	Netwok Security	Network access controls,encryption,Certification, and other Security topics
802.11	Wireless Networks	Standards for wireless networking for many different broadcast frequencies and usage techniques
802.12	High-Speed Networking	A variety of 100 Mbps-plus technologies,including 100 BASE-VG
802.14	Cable Broadband LANs and MANs	Standards for designing network over coaxial cable-based broadband connections.
802.15	Wireless Personal Area Networks	The coexistence of wireless personal area networks with Others wireless devices in unlicensed frequency bands.
802.16	Broadband Wireless Access	The atmospheric interface and related functions associated with Wireless Local Loop(WLL)

⁹³ <https://www.nakivo.com/blog/types-of-network-topology-explained/>

⁹⁴ <https://medium.com/@boutnaru/the-networking-journey-ieee-institute-of-electrical-and-electronics-engineers-192149f7eca6>

⁹⁵ <https://www.ieee802.org/>

⁹⁶ <https://www.ieee802.org/NADots.shtml>

⁹⁷ <https://uk.pinterest.com/pin/760263980839464680/>

⁹⁸ <https://forums.anandtech.com/threads/what-does-802-mean-in-ieee-standards.1827153/>

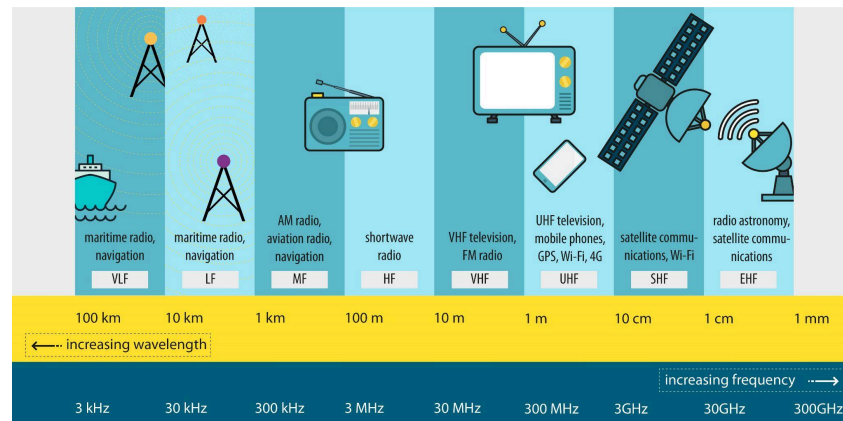
⁹⁹ <https://ldapwiki.com/wiki/Wiki.jsp?page=IEEE%20802>

RF (Radio Frequency) Communication

RF (radio frequency) is an electromagnetic signal which can be used for communication (without cables aka wireless). Radio waves have a frequency running from 3kHz to 300 GHz. By the way, RF propagation occurs at the speed of light. Also, it does not need any medium (like air) in order to travel. Examples of communication standards which are based on RF are: Bluetooth, BLE (Bluetooth Low Energy), ZigBee, GPS (Global Positioning System) and Wi-Fi¹⁰⁰.

Overall, RF communications are categorized based on their frequency, each spectrum band has its own characteristics and thus suitable for different use-cases. VLF (Very Low Frequency) ranges between 3 kHz -30 kHz and is used as part of maritime operations, submarines and navigation. LF (Low Frequency) ranges between 30 kHz - 300 KHz (also called “ground waves”) which is suitable for long-distance communication due to its long wavelength and ability to withstand big terrains like mountains. MF (Medium Frequency) ranges 300 kHz -3 MHz that is used in AM radio transmission as well as emergency distress signals. HF (High Frequency) ranges from 3 MHz - 30MHz is mostly used by the aviation industry, NFC (near-field communication) and weather broadcasting stations¹⁰¹ - as shown in the diagram below.

Lastly, VHF (Very High Frequency) ranges from 30 MHz - 300 MHz which is used for example by TV broadcasting. UHF (Ultra High Frequency) ranges from 300 MHz - 3 GHz, it is leveraged by technologies such as: Wi-Fi, LTE and GPS¹⁰². SHF (Super High Frequency) ranges from 3 GHz - 30 GHz and are utilized for fixed line-of-sight communication like satellite communication¹⁰³. EHF (Extremely High Frequency) ranges from 30 GHz - 300 GHz and had been used for intersatellite communication and other user cases in which atmospheric attenuation is not a factor¹⁰⁴.



¹⁰⁰ <https://www.mouser.co.il/applications/rf-wireless-technology/>

¹⁰¹ <https://www.telecomreview.com/index.php/articles/reports-and-coverage/5091-deep-dive-on-spectrum-bands>

¹⁰² <https://firstsourcewireless.com/blogs/blog/all-you-need-to-know-about-the-difference-between-vhf-and-uhf>

¹⁰³ <https://resources.pcb.cadence.com/blog/2023-super-high-frequency-shf>

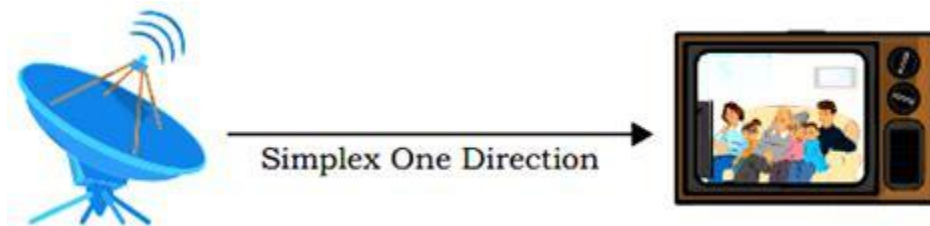
¹⁰⁴ <https://www.britannica.com/topic/telecommunications-media/Radio-transmission>

Simplex Transmission Mode

In case of a “Simplex” transmission mode a network entity can send or receive information (not both). Thus, simplex provides a unidirectional form of communication between devices. Examples for such communication flows are: television, radio broadcasting and aircraft VHF AM¹⁰⁵ - as shown in the diagram below¹⁰⁶.

Overall, simplex communication has different advantages such as: simplicity, cost-effectiveness, there are no collisions (so we don't need anti-collisions mechanisms). Also, it is best suited for applications where only one-way communication is needed¹⁰⁷.

Lastly, in case a send uses the simplex transmission mode it does not have any idea if the data sent was received or its quality at the other side of communication¹⁰⁸. It is important to understand that simplex can be logical only or hardware based.



¹⁰⁵ <https://www.swatcom.com/simplex-half-duplex-full-duplex-explained/>

¹⁰⁶ <https://www.sarthaks.com/3458407/what-is-a-simplex-communication>

¹⁰⁷ <https://www.geeksforgeeks.org/difference-between-simplex-half-duplex-and-full-duplex-transmission-modes/>

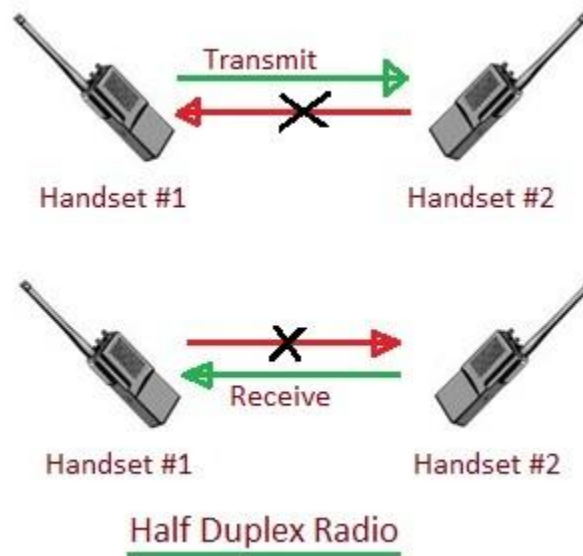
¹⁰⁸ <https://studv.com/academy/lesson/simplex-half-duplex-duplex-communication-channels.html>

Half Duplex Transmission Mode

In case of a “Half Duplex” transmission mode a network entity can send and receive information but not simultaneously (at the same time), as opposed to full duplex communication¹⁰⁹. Thus, devices can transmit in one direction only each time. A great example for that is the usage of walkie-talkies - as shown in the diagram below¹¹⁰. Due to that half duplex is used to conserve bandwidth when only single communication is needed¹¹¹.

Overall, there are a couple of disadvantages when using half duplex communication which we need to focus on (examples described next). First, there is a need for coordination between the transmitting and receiving devices (can complicate the communication flow). Second, there is a delay between transmission and reception, this can cause problems in some scenarios (such as VOIP). Third, this type of communication flow is less reliable because both sides can't transmit at the same time¹¹².

Lastly, there are also benefits (part of them are detailed next) with using half-duplex communication. Resource efficiency by using the same channel for both transmitting and receiving data. Reduce power consumption and simpler hardware design than full-duplex because we don't need extra components to handle simultaneous communication¹¹³.



¹⁰⁹ <https://medium.com/@boutnaru/the-networking-journey-full-duplex-communication-mode-a2d795218570>

¹¹⁰ <https://www.everythingrf.com/community/what-is-half-duplex>

¹¹¹ <https://www.comms-express.com/infozone/article/half-full-duplex/>

¹¹² <https://www.geeksforgeeks.org/transmission-modes-computer-networks/>

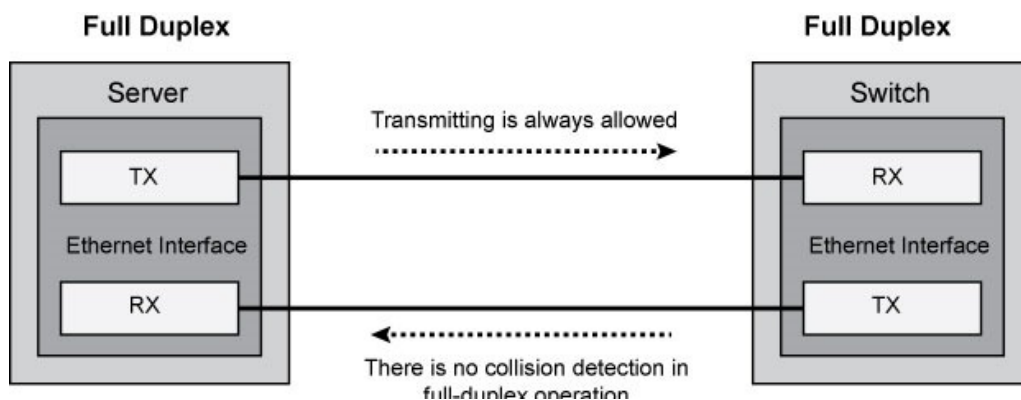
¹¹³ <https://nordvpn.com/cybersecurity/glossary/half-duplex/>

Full Duplex Transmission Mode

In case of a “Full Duplex” transmission mode a network entity can send and receive information simultaneously (at the same time). This is done by providing two separate communication channels\paths - as shown below¹¹⁴. One for each operation (transmitting and receiving). By doing so it enables devices to send and receive data independently¹¹⁵.

Overall, it is important to understand that in case we don't have physically different mediums (Ethernet can use two physical twisted pairs inside the same jacket) for each channel we can leverage multiplexing techniques for implementing full duplex communication. Such techniques are: “Time Division Multiplexing” (like WinMax, LTE-TDD in 4G and DECT wireless telephony) and “Frequency Division Multiplexing” (like ADSL, CDMA2000 and LTE)¹¹⁶.

Lastly, we can summarize the advantages of full-duplex communication to the following: high speed communication (we don't need any delay/clearing the channel before sending/receiving data), reduced latency due to the parallel communication and better utilization of bandwidth¹¹⁷. There are also half duplex and simplex communication modes.



¹¹⁴ <https://learningnetwork.cisco.com/s/question/0D53i00000Kt6geCAB/half-or-full-duplex-collisions>

¹¹⁵ <https://www.coursera.org/articles/full-duplex>

¹¹⁶ [https://en.wikipedia.org/wiki/Duplex_\(telecommunications\)](https://en.wikipedia.org/wiki/Duplex_(telecommunications))

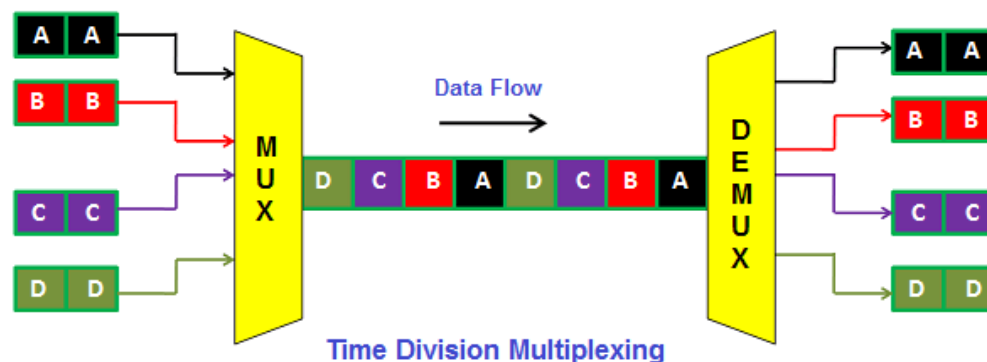
¹¹⁷ <https://www.geeksforgeeks.org/difference-between-simplex-half-duplex-and-full-duplex-transmission-modes/>

TDM (Time Division Multiplexing)

TDM (Time Division Multiplexing) is a technique for transferring multiple signals in parallel over a single communication line/medium/channel. TDM splits the communication channel into “time slots” on which each signal is transmitted - as shown in the diagram below. We can divide TDM to the following types: “Synchronous TDM“, “Statistical TDM” and “Asynchronous TDM”¹¹⁸.

Overall, there are different benefits for using TDM like: efficiency, flexibility, reliability, scalability (support multiple communication channels such as copper, optical fibers and wireless) and compatibility with other communication types¹¹⁹. We can summarize the operation of time division multiplexing to the following phases: channel division, time slot allocation, signal interleaving, transmission, demultiplexing and signal reconstruction¹²⁰.

Lastly, TDM is leveraged as part of different communication technologies such as: DSL (Digital Subscriber Line), T1/E1 lines and more¹²¹. By the way, TDM was created for telegraphy based communications systems in the late 1800s. However, it had become most common application in digital telephony in the second half of the 20th century¹²².



¹¹⁸ <https://www.spiceworks.com/tech/networking/articles/what-is-tdm/>

¹¹⁹ <https://community.fs.com/encyclopedia/tdm.html>

¹²⁰ <https://phoenixnap.com/glossary/time-division-multiplexing>

¹²¹ <https://www.baudcom.com.cn/blog/time-division-multiplexing>

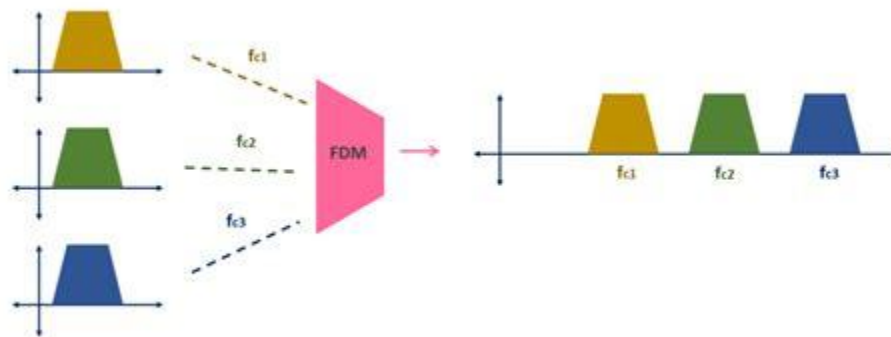
¹²² <https://www.mitel.com/features-benefits/time-division-multiplexing-tdm>

FDM (Frequency Division Multiplexing)

FDM (Frequency Division Multiplexing) is a technique for transferring multiple signals simultaneously over a single communication line/medium. FDM does that by dividing the frequency spectrum into channels¹²³. Using a multiplexor we can combine different signals over the same medium that supports all frequencies¹²⁴ - as shown in the diagram below¹²⁵.

Overall, the demultiplexing phase separates the different signals from the common channel (based on the frequencies). Thus, it is the inverse of the multiplexing phase¹²⁶. By the way, in order to prevent signal interference and overlap, adjacent logical sub-channels are separated by a vacant bandwidth¹²⁷.

Lastly, as with every technology also FDM has its advantages and disadvantages. Among the advantages we can find: simultaneous transmission, simple implementation, frequency selectivity and robustness to noise. Among the disadvantages we have: limited bandwidth, expensive equipment, difficulty of channel assignment and the need for guard bands¹²⁸.



¹²³ <https://www.symestic.com/en-us/what-is/fdma>

¹²⁴ <https://www.sciencedirect.com/topics/social-sciences/frequency-division-multiplexing>

¹²⁵ <https://www.allaboutelectronics.org/frequency-division-multiplexing-fdm-explained/>

¹²⁶ <https://study.com/academy/lesson/frequency-division-multiplexing-advantages-examples.html>

¹²⁷ <https://www.fs.com/blog/unraveling-the-mysteries-of-fdm-tdm-and-wdm-4210.html>

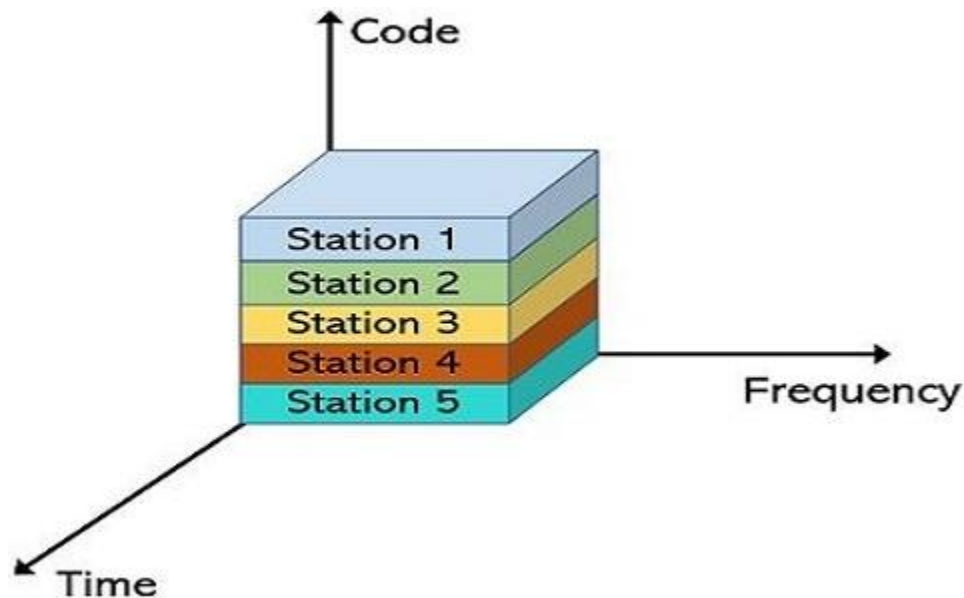
¹²⁸ <https://globaldatabase.ecpat.org/files/sign-pdf-form/wp-content/F4E6/download/frequency-division-multiplexing-advantages-and-disadvantages.pdf>

CDM (Code Division Multiplexing)

CDM (Code Division Multiplexing) is a technique for transferring multiple signals simultaneously over a single communication line/medium. CDM does that by allocating a unique code for each channel. Thus, every channel can leverage the same spectrum at the same time¹²⁹ -as shown in the diagram below.

Overall, CDM can help with resistance to interference. Also, it allows secure communication by using unique codes that maintain separation between different signals transmitted through the same channel. Although the coded signals are transmitted simultaneously over the shared medium the receiving end can separate the individual signals by correlating the signal with the original codes¹³⁰.

Lastly, it is important to know that there are two main types of CDM. First, DSSS (Direct Sequence Spread Spectrum) in which the signal is spread over a wider frequency range by directly modulating it with a spreading code. Second, FHSS (Frequency Hopping Spread Spectrum) in which the signal is spread over a wider frequency range by rapidly switching between a set of predetermined carrier frequencies¹³¹.



¹²⁹ <https://www.elprocus.com/code-division-multiplexing/>

¹³⁰ <https://www.devx.com/terms/code-division-multiplexing/>

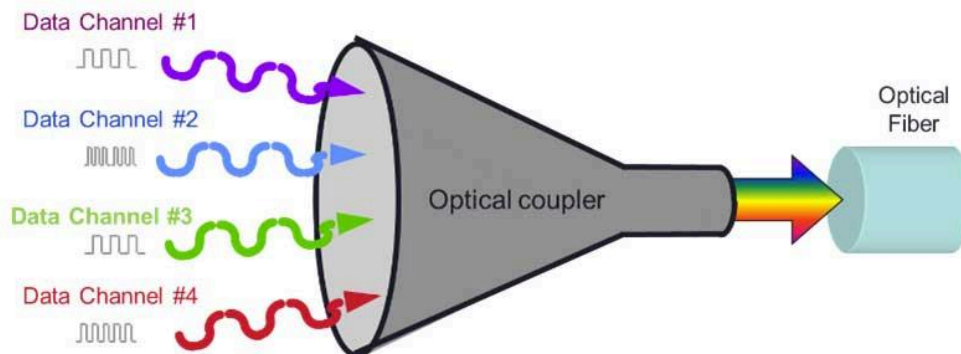
¹³¹ <https://www.telecomtrainer.com/cdm-code-division-multiplexing/>

WDM (Wavelength Division Multiplexing)

WDM (Wavelength Division Multiplexing) is a transmission technique used with fiber-optics. It provides the ability to use multiple light wavelengths (colors) for transmitting data over the same medium. Thus, because we can have two (or more) colors traveling on the same fiber multiple signals can be sent. Today we have two major types of WDM in use: CWDM (Coarse WDM) and DWDM (Dense WDM)- a diagram describing the concept is shown below¹³².

Overall, the transceivers (SFP which stands for “small form pluggable”) convert electric signals to optical signals. The receiving transceivers convert the optical signals to electric signals. By the way, the transceivers are always wavelength-specific in any fiber optic network. In case of WDM multiplexing they are named “colored” transceivers¹³³.

Lastly, WDM provides different benefits such as (but not limited to): ultra large capacity transmissions (like 40\100 Gbps), long range transmissions, transparent transmission, simplified operations and flexible\resilient expansion¹³⁴.



¹³² <https://www.ciena.com/insights/what-is/What-Is-WDM.html>

¹³³ <https://blog.velco.tech/wdm-multiplexing>

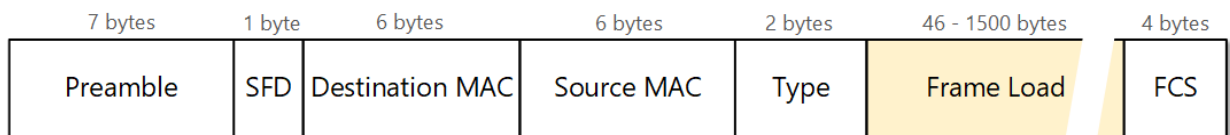
¹³⁴ <https://www.fs.com/blog/wdm-basics-understanding-wavelength-division-multiplexing-technology-8361.html>

Ethernet (IEEE 802.3)

After taking in general about CSMA/CD¹³⁵ it is time to go deep into the Ethernet protocol and explain the headers of the Ethernet protocol. Our goal is to explain the general layout of an Ethernet frame.

Overall, an Ethernet frame is preceded by a preamble (7 bytes) and a start of frame delimiter (1 byte - “10101011”). After that we have the beginning of the Ethernet header. The header starts with destination and source addresses, both addresses are 6 bytes long MAC address¹³⁶.

Moreover, after that we have a 2 byte which defines what is the protocol in the next layer (for example 0x0800 represents IPv4). Next there is the data itself and the last field is 4 byte long of a Cyclic Redundancy Check, aka CRC¹³⁷. Lastly, we can see the layout of an Ethernet frame in the diagram below¹³⁸.



¹³⁵ <https://medium.com/@boutnaru/computer-networking-part-3-ethernet-overview-d04a5f20c58b>

¹³⁶ <https://medium.com/@boutnaru/the-networking-journey-mac-address-medium-access-control-address-a7a6b34e0e8b>

¹³⁷ <https://www.geeksforgeeks.org/ethernet-frame-format/>

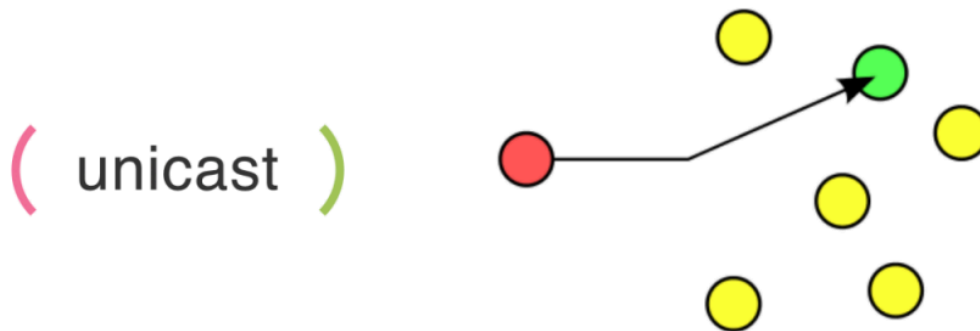
¹³⁸ <https://www.networkacademy.io/ccna/ethernet/switching-logic>

Unicast

Unicast communication describes a flow of information that is sent from one network entity/node/device/element to another. Thus, we have only one source and one destination¹³⁹ - as illustrated in the diagram below¹⁴⁰.

Moreover, the biggest advantage of using unicast communication is that we have an intimate link between the sender and the receiver. Due to that, they can establish a feedback channel in order to identify errors and enable error correction mechanisms like retransmissions¹⁴¹.

Lastly, probably the biggest issue with unicast communication is the inability for sending communication data to multiple devices simultaneously¹⁴².



¹³⁹ <https://erg.abdn.ac.uk/users/gorry/course/intro-pages/uni-b-mcast.html>

¹⁴⁰ <https://pall.as/ipv6/ipv6-addressing-and-subnetting/>

¹⁴¹ <https://www.sciencedirect.com/topics/computer-science/unicast>

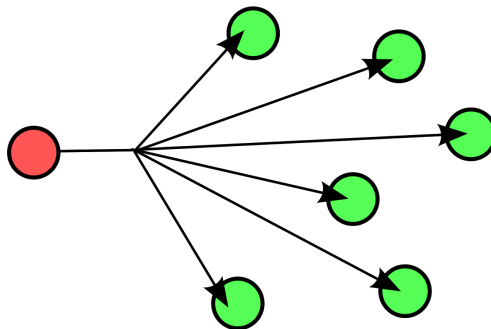
¹⁴² <https://castr.com/blog/unicast-vs-multicast-vs-broadcast/>

Broadcast

Broadcast communication describes a flow of information that is sent from one network entity/node/device/element to all other entity/node/device/element on a specific network. Thus, we have only one source and multiple destinations¹⁴³ - as illustrated in the diagram shown below¹⁴⁴.

Overall, the broadcasting mechanism in computer networks allows a message to be sent and received by all nodes in the network. Examples of such communication flows are: radio and television transmissions. By the way, usually there is a specific address which is used as a “broadcast address” in each network¹⁴⁵.

Lastly, although broadcast can create network storms they can also improve network efficiency. This is due to the fact that broadcast can eliminate the need of sending each entity/node/device/element on the network the message separately, as we would need in case of unicast¹⁴⁶.



¹⁴³ <https://networklessons.com/tag/broadcast>

¹⁴⁴ <http://basicnetworkingknowledge.blogspot.com/2015/03/7communication-types-in-networking.html>

¹⁴⁵ <https://www.geeksforgeeks.org/what-is-broadcasting-in-computer-network/>

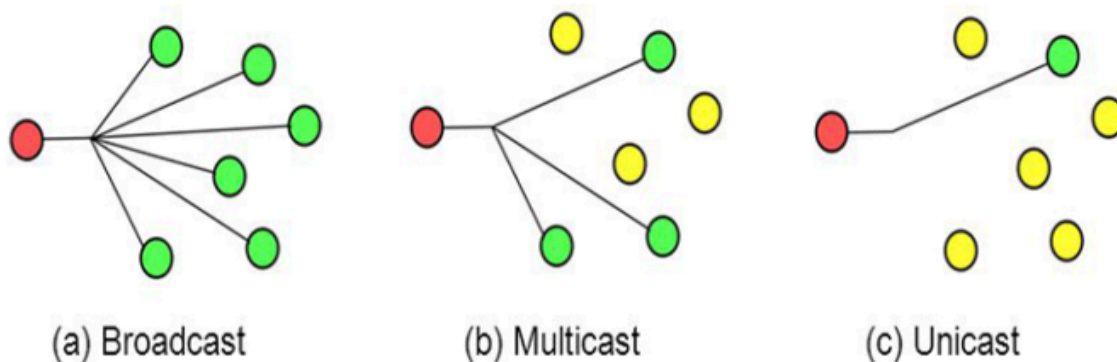
¹⁴⁶ <https://orhanergun.net/multicast-vs-broadcast>

Multicast

While unicast¹⁴⁷ is sending data to a specific node on the network and broadcast¹⁴⁸ is sending data to every node on the LAN¹⁴⁹ we also have multicast (which has the ability to send data to multiple hosts at a time).

Overall, multicast communication allows us to send data to multiple network entities/nodes/devices/elements - as shown in the diagram below¹⁵⁰. Basic terms in the realm of multicast are: “Multicast Group” (entities registered to receive specific multicast traffic), “Distribution Tree” (pathway formed by multicast-enabled routers to reach all entities in a specific multicast group) and “Multicast Address”¹⁵¹.

Lastly, examples of protocols which leverage multicast communication are: UPNP (Universal Plug and Play), OSPF (Open Shortest Path First), mDNS (Multicast DNS), SLP (Service Location, RIP (Routing Information Protocol). By the way, there is also IGMP (Internet Group Management Protocol) which is used on IPv4 networks to establish multicast group memberships¹⁵².



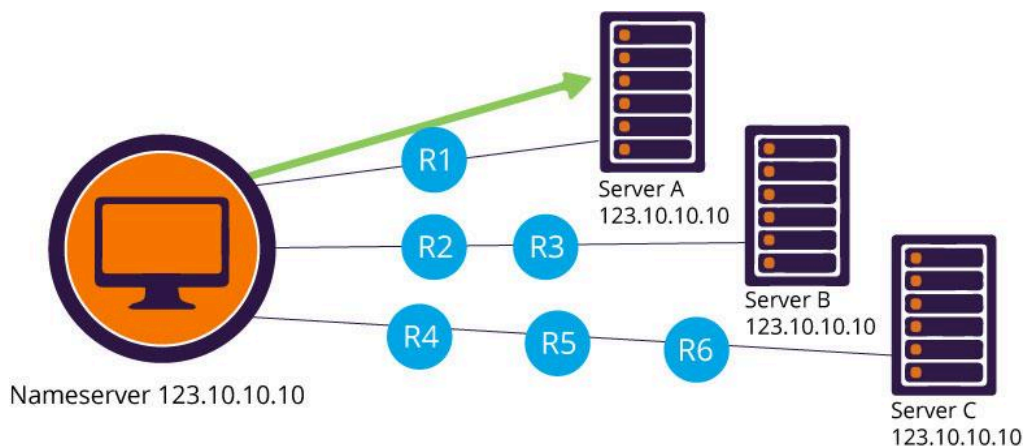
¹⁴⁷ <https://medium.com/@boutnaru/the-networking-journey-unicast-1e14b0acf5ec>
¹⁴⁸ <https://medium.com/@boutnaru/the-networking-journey-broadcast-1a8c7c521ecf>
¹⁴⁹ <https://medium.com/@boutnaru/the-nlan-local-area-network-18b3bf4b51d8>
¹⁵⁰ <https://radiocrafts.com/why-is-multicasting-becoming-essential-for-mesh-networks/>
¹⁵¹ <https://www.auvik.com/franklyit/blog/multicast-networking/>
¹⁵² https://en.wikipedia.org/wiki/Multicast_address

Anycast

Anycast is a network transmission mode. In which a specific networking address leverages routing for allowing incoming requests to be routed to a variety of locations/network entities. For example it is used by CDNs (Content delivery network) for routing traffic to the nearest data center and also can be used for facing high traffic volume, network congestion, and DDoS attacks¹⁵³.

Overall, anycast is an IP addressing schema which provides the ability of multiple network nodes to share the same IP address. By doing so multiple physical destination servers can be logically identified by a single IP address. Thus, using anycast routers can send the request to the most relevant destination based on different properties such as: number of hops, shortest distance, lowest transit cost, minimum latency and more¹⁵⁴ - as shown in the diagram below¹⁵⁵.

Lastly, we can summarize anycast as technology that provides multiple paths to a group of network entities that each have the same IP address. Using it we can scale stateless services: DNS (Domain Name System) and HTTP (HyperText Transfer Protocol) and more¹⁵⁶. Anycast is tightly coupled with the BGP (Border Gateway Protocol), which ensures that the anycast routes are advertised among ASes (autonomous systems) over the Internet¹⁵⁷.



¹⁵³ <https://www.cloudflare.com/learning/cdn/glossary/anycast-network/>

¹⁵⁴ <https://www.thousandeyes.com/learning/techtorials/anycast>

¹⁵⁵ <https://www.imperva.com/blog/how-anycast-works/>

¹⁵⁶ <https://learn.microsoft.com/en-us/windows-server/networking/dns/deploy/anycast>

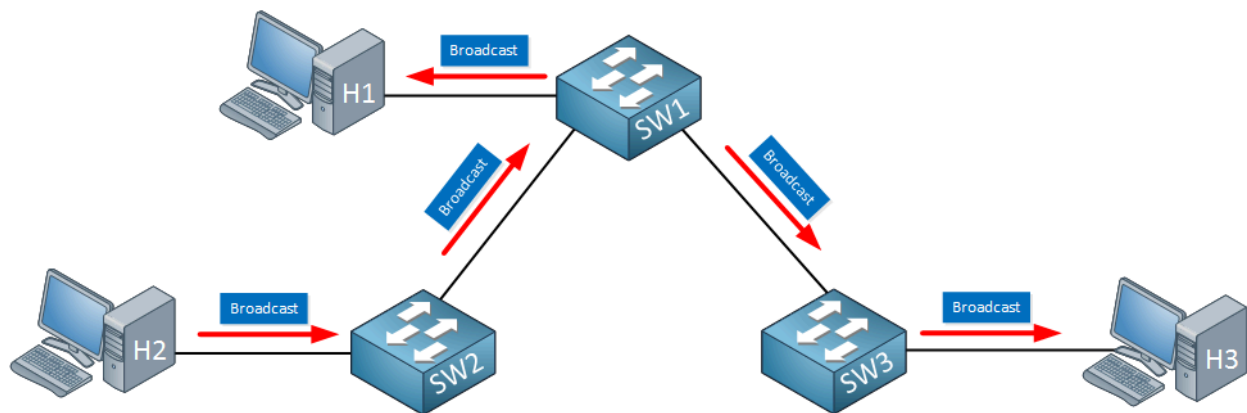
¹⁵⁷ <https://www.noction.com/blog/bgp-anycast>

Broadcast Domain

When talking about LANs (Local Area Networks) broadcasts are “one-to-all” communication. This means that if an entity in the network sends a broadcast frame everyone in the network receives a copy of that frame. In the case of the Ethernet protocol, a broadcast is denoted by a destination MAC of all “1”s or “FF-FF-FF-FF-FF-FF”, which is aka “Broadcast Address”¹⁵⁸.

Overall, when an Ethernet switch¹⁵⁹ gets a frame that has a destination MAC address of “FF-FF-FF-FF-FF-FF” it forwards the frame to all the computers/switches that are connected to it - as shown in the diagram below¹⁶⁰.

Thus, we can say that a broadcast domain is a collection of network entities that can receive or send broadcast traffic from each other. In the diagram shown below H1,H2,H3, SW1,SW2 and SW3 are part of the same broadcast domain. Lastly, there are specific network technologies that can split a network to different broadcast domains like routers and VLANs - more on them in future writeups.



¹⁵⁸ <https://www.networkacademy.io/ccna/ethernet/broadcast-domains>

¹⁵⁹ <https://medium.com/@boutnaru/the-networking-journey-ethernet-switch-layer-2-switch-e23a195146e3>

¹⁶⁰ <https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/broadcast-domain>

Ethernet Switch (Layer 2 Switch)

In general a “Layer 2 Switch” is a network device which operates on the link layer (OSI Layer 2). In our case we talk about “Ethernet Switches” which states that the switch uses MAC addresses¹⁶¹ to determine the path in which the frames should be forwarded¹⁶².

Overall, a switch has physical sockets also known as physical ports into which Ethernet cables are connected. By doing so we connect a network entity to the switch or a switch to another switch - as shown in the image below¹⁶³.

Moreover, each Ethernet switch has a CAM (Content Addressable Memory). It is a memory region which is used to store information like the MAC address available behind every physical port¹⁶⁴. Every time a frame gets into the input buffer of a physical port the switch checks the destination address in the CAM table and writes the frame to the output buffer of the relevant physical port.

Lastly, we can summarize the function of Ethernet switches into the following, forwarding/filtering frames based on MAC addresses and the information in the CAM table and learning building the CAM table based on network traffic. There is also loop elimination that I am going to detail in future posts¹⁶⁵.



¹⁶¹ <https://medium.com/@boutnaru/the-networking-journey-mac-address-medium-access-control-address-a7a6b34e0e8b>

¹⁶² <https://www.techopedia.com/definition/8011/layer-2-switch>

¹⁶³ <http://www.digitaltrends.com/computing/differences-between-ethernet-cables/>

¹⁶⁴ <https://www.greycampus.com/opencampus/ethical-hacking/arp-and-cam-cable>

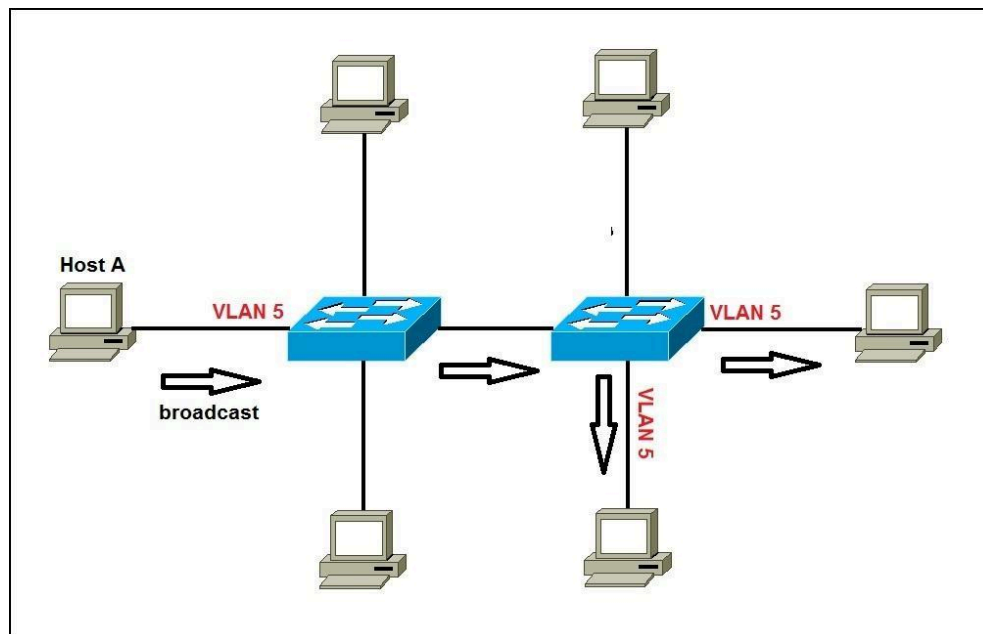
¹⁶⁵ <https://www.utepo.net/article/detail/Detailed-Explanation-for-Operating-Principles-of-Ethernet-Switches-in-Each-Layer.html>

VLAN (Virtual LAN)

VLAN (Virtual LAN) allows splitting an Ethernet switch¹⁶⁶ to multiple virtual/mini switches. Every virtual switch is basically a collection of physical ports (which are configured in the same VLAN) that are operated as a single entity independently from other ports. We can think about it as if we had N different physical switches (where N is the number of configured VLANs). From the perspective of the switch a VLAN is just a number assigned to a physical port, where the default VLAN (in most vendors) is VLAN 1¹⁶⁷.

Overall, the goal of the switch is to block traffic across the VLAN boundary even if both network entities are connected to the same physical switch (but are assigned to different VLANs). Thus, we can say that every VLAN is by itself a broadcast domain¹⁶⁸, even if the VLAN is configured across different physical switches - as shown in the screenshot below.¹⁶⁹

Moreover, every physical port can be in one of the following states: access port, trunk port and some also have auto-negotiation (in which using a dedicated protocol the port can request to be in one of the previous modes). An access port can be a member of one VLAN only, while a trunk port can carry traffic of multiple VLANs. Lastly, because of the separation between VLANs at Layer 2 we need routers in order to cross between them.



¹⁶⁶ <https://medium.com/@boutnaru/the-networking-journey-ethernet-switch-layer-2-switch-e23a195146e3>

¹⁶⁷ <https://www.practicalnetworking.net/stand-alone/vlans/>

¹⁶⁸ <https://medium.com/@boutnaru/the-networking-journey-broadcast-domain-b1621400b160>

¹⁶⁹ <https://geek-university.com/vlans-explained/>

Dot1Q (IEEE 802.1Q)

In order to support VLANs¹⁷⁰ we need to add some information on top of the Ethernet () frame. One of the protocols that can be used for that is Dot1Q (aka IEEE 802.1Q), which is the industry standard for VLAN tagging. Dot1Q adds a 4-byte tag to the layer 2 header (Ethernet), which supports up to 4096 VLANs (because the field of the VLAN number is 12 bits long). Due to the header modification the CRC value of the frame is recalculated¹⁷¹.

Overall, the Dot1Q header is composed of 4 different fields: TPID (Tag Protocol Identifier), PRI (Priority), CFI (Canonical Format Indicator) and VID (VLAN ID). TPID defines the frame type, the value “0x8100” indicates an IEEE 802.1Q frame. PRI ranges from 0-7, a larger value indicates a higher priority frame (in case of congestion). CFI is used to ensure compatibility between Ethernet and Token Ring networks, if its value is “0” it states the MAC address is encapsulated in canonical format which is the default for Ethernet (and “1” if not). VID ranges from 0-4095 and marks to which VLAN the frame belongs, because “0” and “4095” are reserved; we can use 1-4094¹⁷².

Lastly, the VLAN tag is added in the Ethernet frame after the source address and before the type field - as shown in the diagram below¹⁷³. The overall size of the VLAN tag is 4 bytes: TPID (2 bytes), PRI (3 bits), CFI (1 bit), VID (12 bits).

¹⁷⁰ <https://medium.com/@boutnaru/the-networking-journey-vlan-virtual-lan-074046b374c4>

¹⁷¹ <https://ipccisco.com/lesson/dtp-and-vlan-frame-tagging-protocols-isl-dot1-q/>

¹⁷² <https://support.huawei.com/enterprise/en/doc/EDOC1100088104>

¹⁷³ <https://networklessons.com/switching/802-1q-encapsulation-explained>

Access Port

An access port is a mode that we can configure on a physical port of a layer 2 switch. Ports configured in that mode can have only one VLAN¹⁷⁴ associated with them¹⁷⁵ - as shown in the diagram below¹⁷⁶.

Overall, frames sent/received from access ports are not tagged¹⁷⁷. This means that if we sniff the network communication on a device we won't see any tagging (Dot1Q/ISL) information and just the plain Ethernet¹⁷⁸ protocol.

Thus, access ports are usually used to connect devices like PCs/printers to a network. Based on that we can understand that the traffic sent/received is part of the same broadcast domain¹⁷⁹. Because we don't have any VLAN tagging the connected device should not be aware of that¹⁸⁰.



¹⁷⁴ <https://medium.com/@boutnaru/the-networking-journey-vlan-virtual-lan-074046b374c4>

¹⁷⁵ <https://www.grandmetric.com/knowledge-base/design-and-configure/access-port-configuration-example/>

¹⁷⁶ <http://www.slideshare.net/sanss40/vlan-10706040>

¹⁷⁷ <https://www.n-able.com/blog/vlan-trunking>

¹⁷⁸ <https://medium.com/@boutnaru/the-networking-journey-ethernet-ieee-802-3-4562e66204a8>

¹⁷⁹ <https://medium.com/@boutnaru/the-networking-journey-broadcast-domain-b1621400b160>

¹⁸⁰ <https://www.networkingsignal.com/access-port-vs-trunk-port/>

MPLS (Multi-Protocol Label Switching)

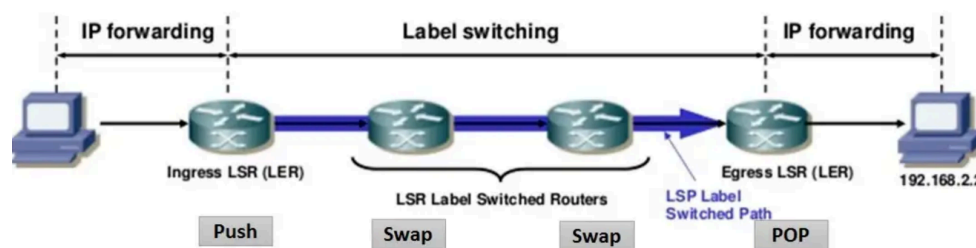
MPLS is a protocol for high-performance communication protocol. It directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. It is basically switching packets. Thus, we can think about it as a protocol that is between the data link layer (layer 2) and the network layer (layer 3), because of that it is commonly thought as a layer 2.5 protocol.

The name of the protocol is composed of “Multi Protocol” because it can encapsulate packets from various protocols. Also, “Label Switching” due to the fact labels are used for switching. The paths (LSP==Label Switch Path) are not established hop-by-hop they are targeted at a particular source-destination pairs¹⁸¹.

We can use MPLS to forward all kinds of network traffic, including IPv4 and IPv6, as well as native ATM, SONET and Ethernet frames. MPLS is used in different use cases such as: enterprise WANs (Wide Area Networks), Metro Ethernet networks, MPLS VPNs (Virtual Private Networks), QoS (Quality of Service), traffic engineering and more¹⁸².

The core component of an MPLS network is a LSR (Label Switching Router). An ingress LSR is labeling an incoming packet and the egress LSR strips the label and forwards the packet. An example of an MPLS network is shown in the diagram below¹⁸³. By the way, there are also intermediate LSRs (which are between the ingress and egress) that swap the label of the packet and forwards them to the next one.

If we want we can go over the relevant MPLS code in the Linux kernel¹⁸⁴. The major one is the kernel mode responsible for the MPLS (Address Family in the socket lingo) support under Linux¹⁸⁵, which enables the configuration and management of MPLS networks (like VPNs and QoS as stated earlier).



¹⁸¹ <https://medium.com/@krisha.india/https-medium-com-vaishali-bhatt-what-is-mpls-6a98ce43fbe2>

¹⁸² https://medium.com/@laurayu_653/mpls-network-how-does-it-work-e38d1d684201

¹⁸³ https://miro.medium.com/max/4800/1*kAlj_oGYBxHZRvTuWdtWBw.webp

¹⁸⁴ <https://elixir.bootlin.com/linux/v6.1/source/net/mpls>

¹⁸⁵ https://elixir.bootlin.com/linux/v6.1/source/net/mpls/af_mpls.c

Wake-on-Lan (WoL)

Wake-on-Lan (aka WoL) is a network protocol which enables devices (such as computers) to be awakened remotely while they are on a very low power mode/sleep mode. This is done by a “magic packet” which is sent over the network¹⁸⁶.

Overall, the typical “magic packet” is based on UDP which has a destination port of 7 or 9. The packet is targeted to the broadcast address of the LAN - as shown in the image below¹⁸⁷. There are also cases that WoL can be operated by using unicast/multicast¹⁸⁸.

In order for WoL to work it should be enabled both in the system motherboard and the NIC (network interface card). Thus, for the motherboard case we should use the BIOS/UEFI menu¹⁸⁹. Under Linux for some NICs we can use “ethtool” in order to query/modify WoL support¹⁹⁰. Lastly, WoL is also supported under Windows¹⁹¹.

```
-----Wake-On-LAN Magic Packet-----

Time received:
      01/28/08      03:01:11
UDP Header:
  |-Source IP      : 192.168.1.4
  |-Destination IP : 192.168.1.255
  |-Source Port    : 49464
  |-Destination Port : 7
  |-UDP Length     : 116
  |-UDP Checksum   : 34009
MAC Address:
      00 E0 4C 31 03 AC
Password:
      00 00 00 00 00 00
Raw Data (108 bytes):
      FF FF FF FF FF FF 00 E0 4C 31 03 AC 00 E0 4C 31
      03 AC 00 E0 4C 31 03 AC 00 E0 4C 31 03 AC 00 E0
      4C 31 03 AC 00 E0 4C 31 03 AC 00 E0 4C 31 03 AC
      00 E0 4C 31 03 AC 00 E0 4C 31 03 AC 00 E0 4C 31
      03 AC 00 E0 4C 31 03 AC 00 E0 4C 31 03 AC 00 E0
      4C 31 03 AC 00 E0 4C 31 03 AC 00 E0 4C 31 03 AC
      00 E0 4C 31 03 AC 00 00 00 00 00 00
```

¹⁸⁶ <https://www.manageengine.com/products/oputils/tech-topics/what-is-wake-on-lan.html>

¹⁸⁷ <https://www.howtogeek.com/70374/how-to-geek-explains-what-is-wake-on-lan-and-how-do-i-enable-it/>

¹⁸⁸ <https://wiki.archlinux.org/title/Wake-on-LAN>

¹⁸⁹ <https://wiki.archlinux.org/title/Wake-on-LAN>

¹⁹⁰ <https://linuxconfig.org/introduction-to-wake-on-lan>

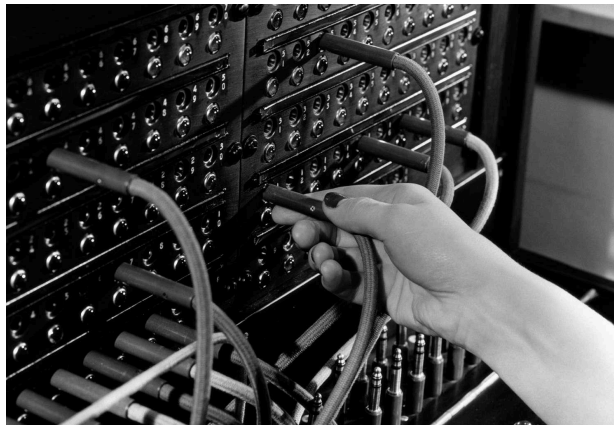
¹⁹¹ <https://learn.microsoft.com/en-us/troubleshoot/windows-client/deployment/wake-on-lan-feature>

PSTN (Public Switched Telephone Network)

PSTN (Public Switched Telephone Network) is a network based on circuit switching¹⁹². It is a traditional telephone network pr, which provides voice communication across the globe. PSTN is also known as landlines\fixed lines\POTS (Plain Old Telephone Service). It uses copper wires and analog voice signals to connect telephones using standard phone numbers¹⁹³.

Overall, the technology of PSTN is outdated and is being replaced in businesses with VOIP (Voice over IP), which can be managed by them or based on cloud solutions¹⁹⁴. We can think about the PSTN as the worldwide network which is composed of: telephone lines, underground wires, switching centers, cellular networks including cell towers and satellites¹⁹⁵.

Lastly, the basic technology behind PSTN is switching (which is used to connect between subscribers). In the beginning the switching was performed manually by operators¹⁹⁶ - as shown below¹⁹⁷.



¹⁹² <https://medium.com/@boutnaru/the-networking-journey-circuit-switching-bc628e8cf034>

¹⁹³ <https://www.nextiva.com/blog/what-is-pstn.html>

¹⁹⁴ <https://gomomentum.com/pstn/>

¹⁹⁵ <https://www.twilio.com/en-us/blog/what-is-pstn>

¹⁹⁶ https://en.wikipedia.org/wiki/Public_switched_telephone_network

¹⁹⁷ <https://www.lifewire.com/what-is-pstn-3426739>