Networking

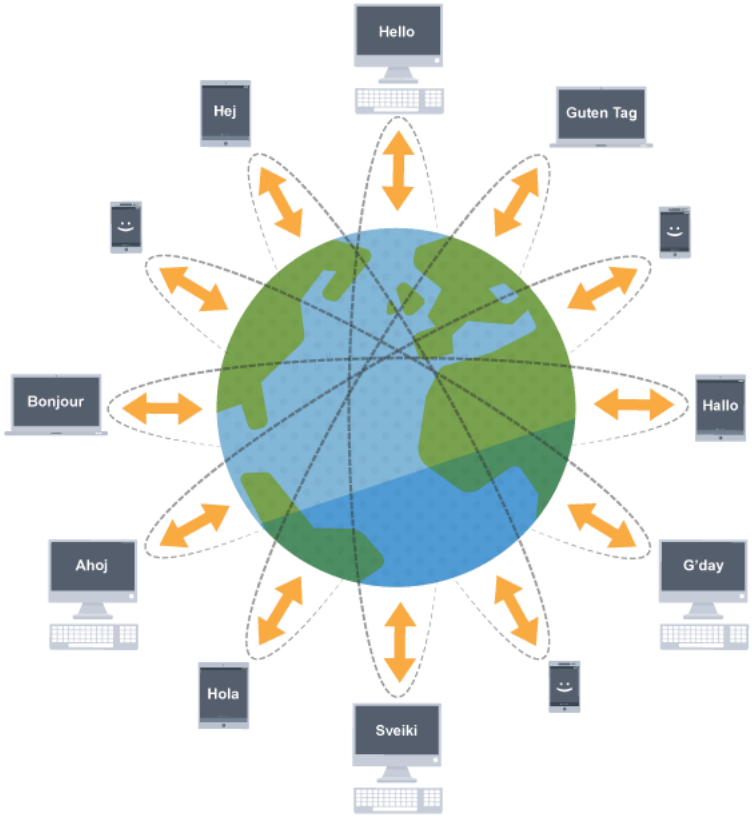
Contents

1 What it is

A network is two or more *computers* (or other electronic devices) that are **connected** together, usually by cables(guided) or Wi-Fi(unguided).

2 benefits of a network

1. sharing hardware, such as printers, computers, phones, tablets, scanners, etc...[1]
2. sharing software, allowing:
    - multiple users to run the same programs on different computers
    - data to be shared, so that other people can access shared work
    - you to access your data from any computer on the network



[1] All these pieces of hardware are usually addressed as **endpoints** as long as they have the ability to communicate effectively within a network

Networking is crucial if you want to use your computer to communicate. Without it you couldn't send an email, a text or an instant message and that would be so bad.

We use a huge network on a daily basis and this is called the internet. Around three billion people use the internet to share data, news and resources, amongst many other things.

2.1 guided wiring

Is quicker than unguided, it consists in physical wires. Optic Fiber is on the top of this list but can't be twisted. You can install a optic cable for a much longer distance and you won't get the same troubles you would get with copper cables for example

2.2 unguided wiring

This is Wi-Fi essentially. You can have a 2.4Ghz signal to reach longer distance but won't be nicely matched with a 5Ghz device

3 LAN vs WAN

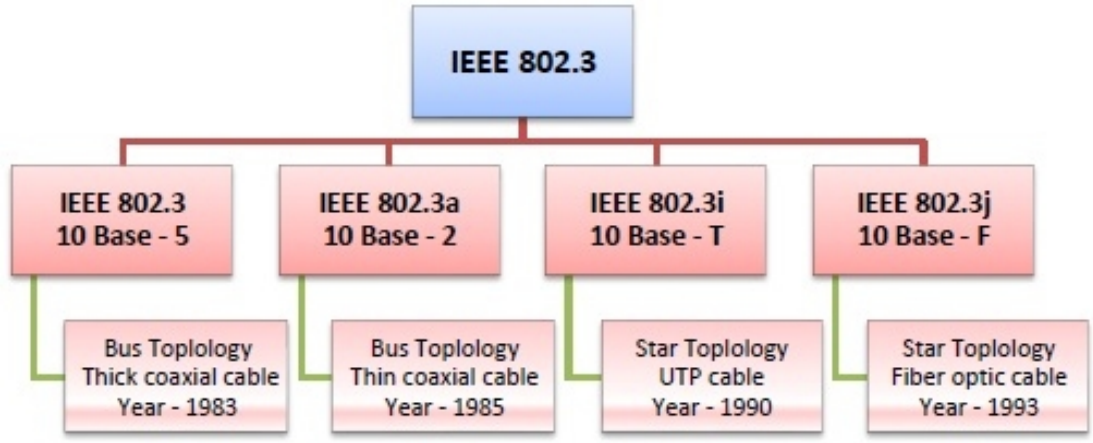
LAN, which stands for local area network, and WAN, which stands for wide area network, are two types of networks that allow connection between computers. As the naming conventions suggest, LANs are for smaller, more localized networking — in a home, business, school, etc. — while WANs cover larger areas, such as cities, and even allow computers in different nations to connect. LANs are typically faster and more secure than WANs, but WANs enable more widespread connectivity

4 IEEE 802.3

IEEE 802.3 is a set of standards and protocols that define Ethernet-based networks. Ethernet technologies are primarily used in LANs, though they can also be used in WANs as well. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks.

IEEE 802.3 Popular Versions There are a number of versions of IEEE 802.3 protocol. The most popular ones are.

- IEEE 802.3: This was the original standard given for 10BASE-5. It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500m
- IEEE 802.3a: This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise)
- IEEE 802.3i: This gave the standard for twisted pair (10BASE-T) that uses unshielded twisted pair (UTP) copper wires as physical layer medium. The further variations were given by IEEE 802.3u for 100BASE-TX, 100BASE-T4 and 100BASE-FX
- IEEE 802.3j: This gave the standard for Ethernet over Fiber (10BASE-F) that uses fiber optic cables as medium of transmission

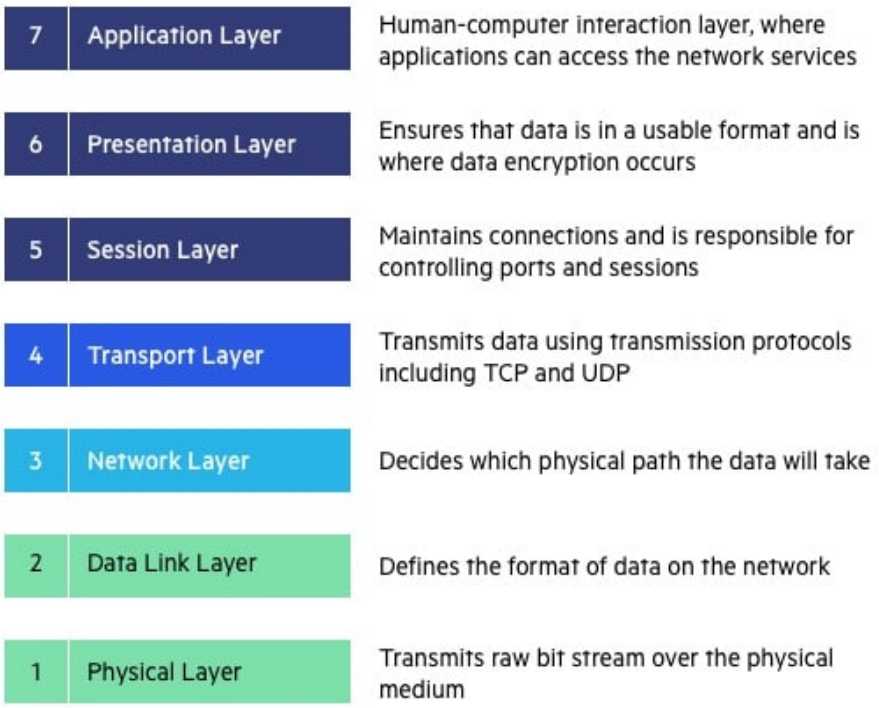


5 Protocols

Protocols are kind of rules defined in advance to make sure two or more devices know in advance what to expect if they send a particular message and what to expect in return

5.1 OSI standard

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s



The modern Internet is not based on OSI, but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.

OSI was introduced in 1983 by representatives of the major computer and telecom companies, and was adopted by ISO as an international standard in 1984.

5.2 good mnemonic for OSI

Every layer of the OSI model can be remembered with the mnemonic : Please Do Not Throw Sausage and Pizza Away

5.3 theory vs practice

Even if The Transmission Control Protocol/Internet Protocol (TCP/IP) model came before the Open Systems Interconnection (OSI) model it is what is used in practice today, and it has only five layers:

- Application layer
- Transport layer
- Network access layer
- Network interface layer
- Hardware layer

This may look drastically different from the OSI model, primarily because some functions are encompassed in a single layer: the application layer. In TCP/IP, this provides users with the physical standards, transport functions, network interface, and internetworking functions that correspond with the first three layers of the OSI model. In other words, in the TCP/IP model, these services are all done in the application layer.

TCP/IP is connection and connectionless

5.4 horizontal vs vertical approach

There's a debate on which one is vertical and which is horizontal so that point won't be discussed in this documents

6 ARP/RARP/DHCP

Address Resolution Protocol translates MAC addresses into IPs so that from the network layer we can communicate over the internet with IPs while RARP demands another computer (usually a server) to assign the demanding one with an IP which is essentially what DHCP is doing that's why RARP got obsolete

6.1 ARP Tables

These are used from every component in a network to know which MAC address the packet needs to point at

6.2 Three-way-handshake

This is when the client sends the ARP request to the server. The server does an aknowledgment and answers with an ARP reply saying both its MAC and its IP. It all happens like this :

When Computer 1 wants to talk to Computer 2 in a local area network by Ethernet cables and network switches, with no intervening gateways or routers. Computer 1 has a packet to send to Computer 2. Through DNS, it determines that Computer 2 has the IP address 192.168.0.55.

To send the message, it also requires Computer 2's MAC address. First, Computer 1 uses a cached ARP table to look up 192.168.0.55 for any existing records of Computer 2's MAC address (00:EB:24:B2:05:AC). If the MAC address is found, it sends an Ethernet frame containing the IP packet onto the link with the destination address 00:EB:24:B2:05:AC. If the cache did not produce a result for 192.168.0.55, Computer 1 has to send a broadcast ARP request message (destination FF:FF:FF:FF:FF:FF MAC address), which is accepted by all computers on the local network, requesting an answer for 192.168.0.55.

Computer 2 responds with an ARP response message containing its MAC and IP addresses. As part of fielding the request, Computer 2 may insert an entry for Computer 1 into its ARP table for future use.

Computer 1 receives and caches the response information in its ARP table and can now send the packet