Networking

**Network** - connecting computers and other devices with communication lines so that computers (or their users) can exchange resources with each other. Resources in this case can be processor time, memory, information data, etc.

Several types of networks:

**LAN(Local Area Network)** - by combining a certain number of computers in a relatively small area. Compared to a wide area network (WAN), a local area network usually has a higher speed of data exchange, and the absence of the need to use a telecommunications communication line. For example network between computers in class in your school/college.

**WAN(World Area Network)** - a computer network covering vast territories. that is, any network whose communications connect whole megacities, regions or even states and contain tens, hundreds or even millions of computers.

**What is the difference between them?**

Of course, you could have guessed that in terms of size, it is true, there is a much larger number of devices in the global network, then there can be refrigerators, and computers, microwaves, phones, cars, servers and many other devices known to you. Also, WAN combines a much larger number of connection methods, addressing methods, protocols, and restrictions.

**The Internet** - is a global international network in which most modern devices are connected. also has the alternative name WWW World Wide Web. This is a network in which there are many servers for naming, addressing clients, services that you use every day, even now reading this text you are using this network. This is a very large and complex system, which consists of a hybrid topology, contains a lot of people who are responsible for Internet support, and people who give you the opportunity to use the Internet - they are called providers. Many connection and connection models are used, you have probably heard of fibre optic connection, twisted pair, Wi-Fi, optical connection. It does not have centralised management, because all devices are interconnected by a network and address each other without a central server. However, now the old IPv4 model is often used, which is not always enough for full use, that is why IPv6 was born, each device has its own unique address, and it can use it to communicate with other devices. In the 4th version, you need to use various devices such as routers, switches, hubs, switches, DNS servers to contact the client on the other side of the world, because the number of addresses in the 4th version is very limited, and we need to use devices to expand this range. Very soon there will be a transition to the 6th version only, without mentioning the 4th, but it is still quite difficult, since the technology is quite new, and requires detailed study by specialists, but it is much better.

**Global network -** for example, the Internet is a global network of interconnected computers that use dedicated routers and servers, allowing end users to access data scattered around the world. So a global network is a network that contains a very large number of devices and connects countries, continents, etc.

**Points of presence(PoP) -** artificial demarcation point or network interface point between entities.

**Internet exchange point(IXP) -** is a physical location through which Internet infrastructure companies such as Internet Service Providers (ISPs) and CDNs connect with each other. These locations exist on the edge of different networks, and allow network providers to share transit outside their own network.

**Client-server model -** This is a model in which there are clients and a server (or many servers if it is something big). That is, it means that if the client wants to get the information he needs, he must request it from the server through any network. If this is a Wikipedia page, you will ask the Wikipedia server over the Internet. If it is a private network, you can contact the server directly by making HTTP requests, as in the case of a global network, or by the usual method. This model is mostly used on the Internet. Also, you could see public APIs for working with some platforms, this is also a device of this model.

**Advantages of client-server model:**

* an easily scalable system that can be updated at any time and clients will receive up-to-date information
* enable third-party developers to use your platform through an API
* backups and security depends entirely on the server and interaction settings
* All files are stored in a central location

**Disadvantages:**

* there must be a connection to the server to receive data, if there is no connection - you will not be able to interact
* all interaction goes through the server, including if clients want to interact with each other, which gives a heavy load, hybrid models should be used.
* Specialist in a network management is needed
* Servers are not cheap
* If any part of the network fails a lot of disruption can occur

**P2P(peer-to-peer) model -** In this model, clients interact with each other directly, without a central server responsible for their communication. A great example is Torrent. That is, it can be a network in which each member has the opportunity to contact any other member of the network without a server between them. Such a topology is called Full-Mesh

**Advantages of P2P model:**

* no server is needed, clients interact with each other directly
* everyone knows each other in the network
* the transmission of information can be safer with reliable protection
* Easy data sharing
* no network management specialist required
* If one computer goes down, it doesn't affect any other part of the network.
* Much easier to set up than a client-server network

**Disadvantages:**

* It is the responsibility of each individual user to ensure that viruses do not enter the network
* Centralised backup copies of files and folders cannot be created
* Aside from permissions, there is little or no security. Users often do not need to log into their workstations.

Internet protocols

**Internet protocol -** a network layer protocol for transferring datagrams between networks.

There are basic protocols, and many secondary ones:

1. **IPv4 IPv6** - Internet Protocol - Version 4 is 4 numbers separated by a dot, received from the DHCP server of your switch, router, hub, etc. Example 192.168.1.1 can have a total of 4.3 billion combinations, 4 bytes per part. Version 6 is 128 bits per part, there can be 340 undecillion combinations (a lot), example 2001:db4::ff00:52:7498
2. **TCP** - Transmission Control Protocol - a communications standard that enables application programs and computing devices to exchange messages over a network
3. **UDP** - User Datagram Protocol - is a communications protocol that is primarily used to establish low-latency and loss-tolerating connections between applications on the internet
4. **TCP/IP OSI/RM** - main hybrid stack with IPv[4/6] and TCP protocols. a set of Internet protocols. The name comes from the name of the core protocols of the Internet.
5. **HTTP/HTTPS** - HyperText Transfer Protocol [Secure] - used to transfer html/htm pages, make accessible website, page or user. By default use 80 or 443 for ssl ports
6. **FTP/SFTP** - [SSH/ Secure] File transfer protocol - used for transferring files over network, sftp uses ssh for this. 21/22 ports
7. **SSH** - The Secure Shell Protocol is a cryptographic network protocol for operating network services securely over an unsecured network.
8. **Telnet** - is an application protocol used on the Internet or local area network to provide a bidirectional interactive text-oriented communication facility
9. **SMTP** - **Simple Mail Transfer Protocol**
10. etc…

Why are there so many protocols? because there is an OSI model that has 7 layers:

1. **Physical Layer** - The physical layer is responsible for the physical cable or wireless connection between network nodes. It has the ability to determine which technology and method is used and interacts with the raw data of other layers.
2. **Data Link Layer** - The link layer establishes and breaks connections between two physically connected nodes in the network. It breaks the packets into frames and sends them from the source to the destination. Uses LLC, MAC addresses.
3. **Network Layer** - The network layer performs two main functions. This is the division of segments into packets, and the assembly of packets, and the routing of packets using the detection of the optimal delivery path over the network. It is already using the IP address and delivering packets.
4. **Transport Layer** - The transport layer takes the data transmitted at the session layer and breaks it into pieces on the transmission side. It also reproduces them at the receiving end, turning them back into data that can be used in further delivery.
5. **Session Layer** - The session layer creates communication channels(sessions) between devices
6. **Presentation Layer** - The presentation layer prepares data for the application layer. It defines how the two devices should code, encrypt and compress the data so that it is received correctly at the other end.
7. **Application Layer** - The application layer is used by end-user software such as web browsers and email clients. FTP, SFTP, POP, HTTP[S], SMTP, DSS, SSH

**ISP role -** They allow users to connect to the Internet.

**Bandwidth -** refers to maximum data transmission capacity of a channel.

**Data Rate -** refers to the actual data transmission speed.

**Connection methods and advantages/disadvantages**

#### **MOBILE**

**A:** Portability, the ability to use the mobile network in most cities and villages;You don't need powerful antennas, you can put many antennas forming honeycombs that will cover the required area. If you use 5G, this is a very high speed connection to the Internet;

**D:** There are places where mobile communication does not catch, this is an open area far from civilization, not everywhere there are antennas that finish. The presence of obstacles, due to the peculiarities of wave propagation technologies in space - various factors affect the quality of the connection, it can be rain, snow, or even the fact that you are in a building with a metal roof.

#### **WIFI**

**A:** Mobility, ease of use, for example at home. Ideal for a home network with a small number of devices, a router/broadband with a Wi-Fi antenna is required. New versions of Wi-Fi are very fast.

**D:** After all, no matter what the speed is - it is much lower than when using a wired connection. If you live in an apartment where there are also many Wi-Fi points around - they can overlap each other, creating an interference phenomenon that can worsen the signal, for this you need to change the channel, but here you need to understand in a little more detail.

#### 

#### **DIAL-UP**

**A:** Low Cost, safety, availability.

**D:** Speed lags, old technology, unstable connection, demands a phone line

#### **BROADBAND**

**A:** Connectivity, speed, VoIP

**D:** Signal strength, security

#### 

#### **DSL**

**A:** No new wires needed for service. DSL runs over standard phone lines,

**D:** old, slow technology

#### 

#### **CABLE**

**A:** The fastest data transfer technology, it is often used together with Wi-Fi. Great speed, privacy, security.

**D:** lack of mobility, with a large number of servers, for example, there will be a large number of wires, and they are not always cheap

#### 

#### **SATELLITE**

**A:**Availability anywhere on the planet (soon this will be possible), in the field at home, easier to set up, all you need is an antenna for communication, which is already built into new models of iPhones, as well as starlink antennas. Thanks to Elon Musk.

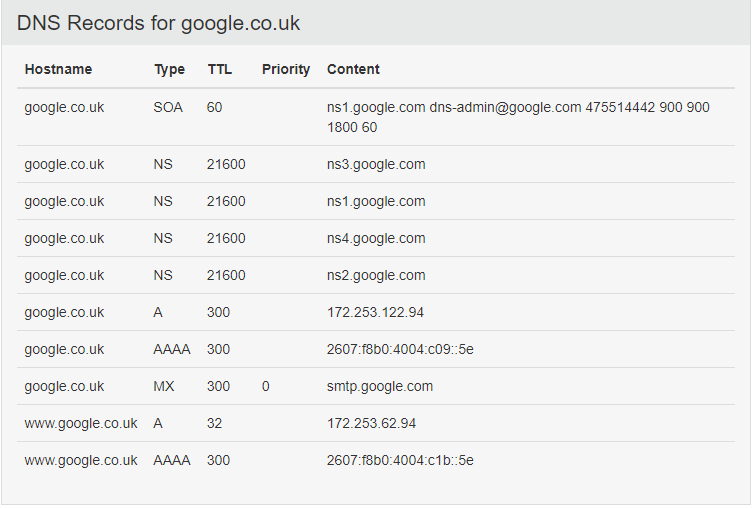
**D:** There is a possibility of a large, medium ping due to long distances, I think it will be fixed soon, the Internet speed is relatively not very high, not everyone can use it for what, because there is no necessary coverage by satellites (now a large number of satellites are being launched into orbit, so it will be fixed soon) . Price.

DNS

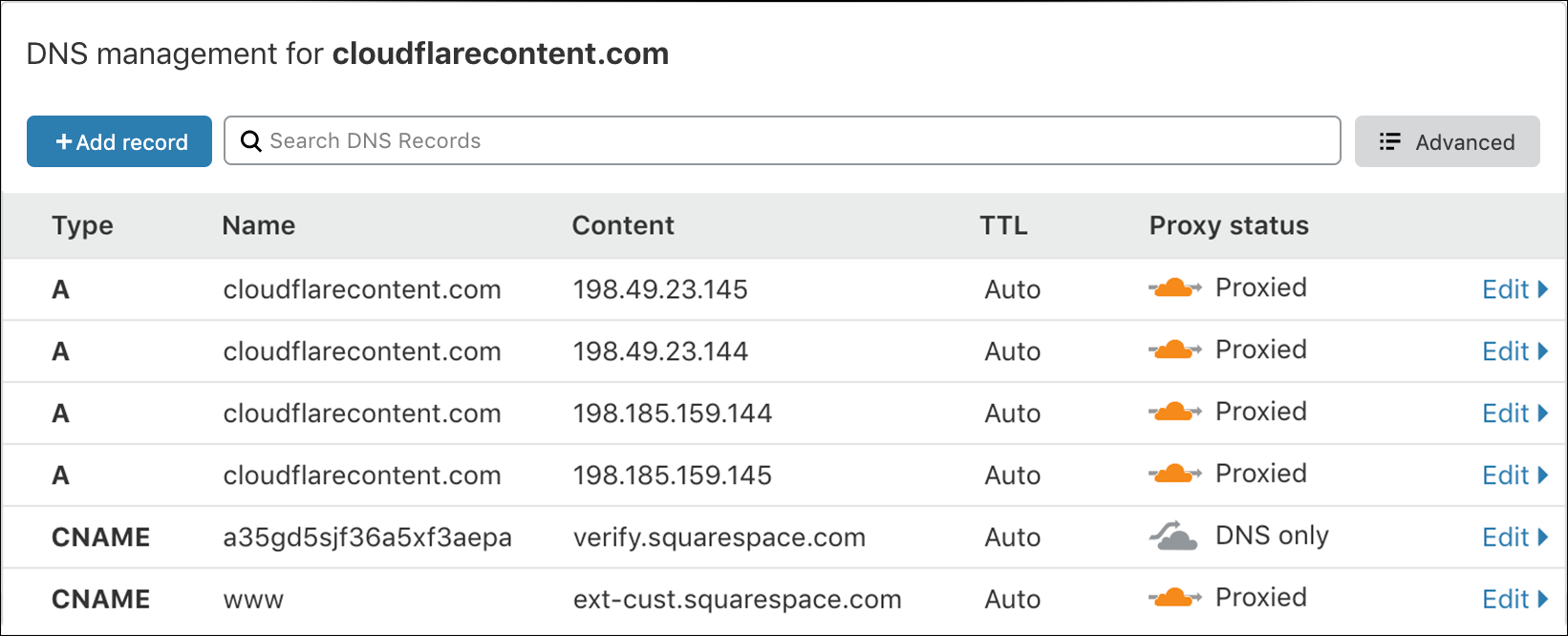
**DNS(Domain Name System)** - this system is designed so that computers working in the World Wide Web can determine the IP address of the server by the letter name - the domain - and contact it for content. In turn, the domain is the name of your website on the Internet. Domain names are of the first, second, third and many, many more levels

It so happens that people are not robots and not some precise mechanisms, so it is difficult for most to work and memorise numbers. Especially now in the era of digital technologies, where almost everyone has the opportunity to access the Internet and use it for their own purposes. The main one is the collection of information, for this we usually use various websites, for example Google. One of its IP addresses is 172.253.122.94, but remembering that many digits can be difficult, and it will be much more difficult than remembering google.co.uk. Many people thought so, and in 1983 Paul Mockapetris expanded the possibilities of the Internet by inventing the domain name system.

For example, we can use the https://who.is/dns/ service to view DNS records for this site.



Example of dns editor in cloudflare:



Here we can see 10 dns records(who.is first screenshot), they have different types.

* **NS** - name server - indicate where the entire DNS zone of the domain is stored, there should be more than one such record for fault tolerance.
* **A** - is used to specify a domain name that will be redirected to the IP address you specified. This process is hidden by your browser, but when you specify a domain in the search bar, you are actually working with many IP addresses. That is, the A record defines the IP address of the domain name in the IPv4 network.
* **AAAA** is the same system as A records only for IPv6.
* **MX** - indicate the addresses of the mail servers of the domain, there may be several of them and they have priority; the lower the priority value, the higher it is.
* **CNAME** - Canonical Name - is a record that makes a copy of another domain, in some sense binds the subdomain for which the record was created to a valid (canonical) domain name. A CNAME completely copies all records of another domain, thereby creating a complete copy of another address. For example www CNAME record to A record.
* **The TTL (Time To Live)** parameter determines the storage time of DNS records in the DNS system cache. It is used to reduce the load on the DNS server by reducing the number of requests to them, however, with large values, it increases the time for changes to the domain settings to take effect (DNS servers can return old data from the cache until it is updated). Simply put, the longer the TTL, the less the load on the DNS server, but the longer it takes for changes to the domain settings to take effect. The default for most DNS servers is 15 minutes.

Since DNS works on a hierarchical basis, it resembles a tree. The tree has a vertex - the root zone - for which the null name is reserved, and the root servers are responsible for it. This zone is inconspicuously present in all domain names - it is the dot that is usually omitted when writing, for example, "facebook.com." Root servers, there are only 13 of them, contain information about first-level domains (uk, net, info, etc.).

**What the DNS server sees when it is accessed:**

1) The browser is checking its cache - maybe you recently visited Facebook and this information was saved. If not, the next step.

2) The browser asks for help from the operating system on your computer. It checks in its own DNS cache and in the hosts file. If nothing is found, the request is sent to the server that is registered as a DNS server in the computer settings.

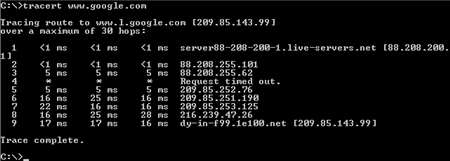
3) Your provider's DNS server first checks its cache (perhaps one of your neighbours just logged into Facebook). And checks his local database (maybe he keeps the facebook.com zone). If nothing is found, this server makes several queries and compiles a response for you.

4) First, the request is sent to the closest root server. The addresses of the root servers are usually recorded in the settings of all DNS servers, since they change very rarely. The root server responds that it does not know the address of “facebook.com” and returns a list of servers that host all .com domain records.

5) Thus, the provider's server records the received information in the cache, and when searching for all domains ending in .com, it will refer to this small number of servers. Therefore, he asks the first server from the list: what is the address of facebook.com? The received address is sent to your computer and the browser shows you the Facebook feed.

This is the case for any website.

You can use the traceroute Windows terminal utility to trace the entire path to your website.



Usually, many large companies allocate many servers to offload the load on those servers, and several types of servers are used. Everything is also built according to the principle of a tree, where immediately upon request you get to the DNS server, and depending on the URL address you choose, it will redirect your request to the main or secondary server, which will process it and return an answer.

To configure servers on Linux, you can use any server, for example nginx or apache. There are also companies that allow you to configure DNS along with a free SSL certificate to increase your security, such as CloudFlare.

To set up a domain name on your server, you need - to have a server and a white ip address, to have a domain and its settings, if you do not have an SSL certificate, you can use cloudflare.

So we now have all the components, in the settings panel of your domain (dns editor) we redirect all traffic to the cloudflare server by adding NC records. In Cloudflare's dns editor, we already do redirection with the help of AAAA or A or CNAME records. So, if the Cloudflare servers notice a familiar URL, the DNS servers check their cache, otherwise they find the desired IP address in the database and redirect you to your website, where the web server is on port 80 or 443. You should also know that you need to separately configure the web server and add ssl on your web server. Usually, changing DNS records can be buffered for several hours, but if you are lucky, everything will change immediately.

Network topology

A network topology(layout, configuration, structure) of a computer network usually refers to the physical location of network computers relative to each other and the way they are connected by communication lines.

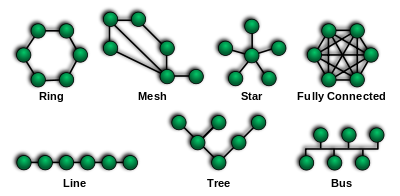
There are several basic network topologies: star, bus, and mesh and several secondary ones that are built in combination.

Bus topology: In this case, the computers are connected to each other by a coaxial cable.

Information transmitted from one network computer to another is distributed, as a rule, in both directions. The main advantages of such a scheme are the cheapness and simplicity of cable routing in rooms, and the possibility of almost instant broadcasting to all stations of the network. The main disadvantage of the common bus is its low reliability: any defect in the cable or any of the numerous connectors completely paralyses the entire network. Another disadvantage of the common bus is its low performance, since with this connection method, only one computer can transmit data to the network at any time.

Star topology: In a star topology, each peripheral node (a computer workstation or any other peripheral device) is connected to a central node called a hub or switch. This topology is mostly used, because you can connect to the node you like, while the candles and hubs or routers have a large and convenient functionality for configuring the network

Mesh topology: This type of topology is obtained from the fully connected topology by removing some possible connections. This is a network topology in which there are at least two computers with two or more paths between them.



The advantages and disadvantages of a network

Advantages: The ability to easily exchange information, even over intercontinental distances, will be much cheaper than ordinary correspondence or delivery of an information product. A large number of software, sites for communication, data exchange, working with files. The ability to create your own networks, even private ones, to organise communication between devices.

Disadvantages: But if you are engaged in the installation of servers, network connection technologies, then it can be a bit expensive. Because usually good internet equipment and cables are not cheap. Network management is quite complex and requires experience and knowledge in networks, for this there is a profession of system administrator, network installation specialist, providers, etc. Your network can be compromised and infected with viruses that can steal or destroy your data from servers and other devices, or a hacker can do it directly.

Sources of information:

<https://en.wikipedia.org/wiki/Network_topology>

https://who.is/dns/google.co.uk

<https://www.cloudflare.com/en-gb/learning/cdn/glossary/internet-exchange-point-ixp/>

https://www.imperva.com/learn/application-security/osi-model/