BASICS OF NETWORKING

WSEPiNM KIELCE

IPBeja Instituto Politécnico de Beja

Co-funded by the Erasmus+ Programme of the European Union

Publication financed by the European Commission under the Erasmus + programme.
The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and neither the Commission nor the National Agency cannot be held responsible for any use which may be made of the information contained therein.

Content

1. Introduction

Cyber security, what is it? What is it and why is it so important? In an age where technology is everywhere, we cannot forget about our cyber security in this digitally comfortable world. Online, we are not invisible and our activities leave various traces or information behind us. Practically every day we use the facilities of the Internet, whether on social networks, forums or all kinds of sales platforms. Where we share our personal and financial data, send account numbers, pay with cards, phones and various digital currencies. What are the risks on the Internet? Identity theft, cloning of payment cards, loss of private files/data, phishing from bank accounts, fraud. In life, we take care of our safety, we watch ourselves, we buy medicines, we anticipate. Why don't we do this online? How many of you have an anti-virus installed on your computer? All of them? And on your phone? Anyone? Here we should ask ourselves whether we really spend most of our time on the web in front of a computer screen or perhaps on our phone? According to various statistics, over 70% of all web traffic already comes from mobile devices, especially our smartphones. Have you ever bought something on your phone or used it to enter your billing information for various transactions? Properly prepared devices for the web are only half the battle; the other factor that guarantees relative security is the awareness of the Internet user. You can be the best prepared and have the best equipment, but nevertheless without the right know-how you can make yourself a lot of unnecessary and unpleasant problems.

1.1. Network Communication

Today, few can imagine the world around us without computers, telephones
and many other consumer electronics devices. These devices offer us a multitude of functions and
and capabilities that make our daily activities easier, as well as helping us to work and study. Many of these functions would be useless without an important aspect, the ability to communicate and exchange data quickly.

Thanks to this possibility, we are able to reach friends who are currently on the other side of the world in seconds, pay the electricity bill in seconds or buy new trainers without leaving the house. Of course, I am not going to discuss all the advantages of internet access here, as this is not the main topic of the course, but I hope you realise that everything you can do with your computer or smartphone has one thing in common. That common denominator is, or rather is, the computer network, which was created decades ago and is the foundation of today's Internet.

What is the Internet today? It is nothing more than a computer network, a very elaborate one,
with many connected devices, but it is still a network.

2. Basic concepts

Let's define the basic concepts related to computer networks:

Computer network - A collection of devices, such as computers, printers, telephones and televisions, that are interconnected to exchange data. A transmission medium is used to connect the devices and a communication protocol is used to transmit data.

IPv4 address - This is a 32-bit number, entered in decimal form for ease of use (e.g. 192.168.31.190), to identify devices and address data on the network.

HOST - This is a device with an IP address that is the source or recipient of data transmitted over the network, i.e. it receives data from other devices or sends such data. The term host is sometimes used interchangeably with the term terminal device, as it usually refers to a computer, tablet or smartphone, i.e. a device with which the network user has direct contact.

Client - The device, or more precisely its software, uses the services provided by the server. The most common client today is the web browser, which allows the content of web pages hosted by a web server to be viewed. Examples of a client would also include FileZilla, which allows files to be exchanged over the Internet, and all sorts of email software to facilitate the use of mail. Game consoles or smartphones will also be clients, as long as they are connected to the Internet, of course.

Server - This is a computer with dedicated specialised software installed to serve other computers. The service that a server can provide is, for example, a website, email or file resource. A server can be any computer on which such software is installed and configured, such as APACHE, which is used to maintain and share websites, or MySQL, which is a database management system. A server is usually a dedicated computer with high computing power that is capable of handling multiple connections and queries simultaneously.

Transmission medium - In other words, the medium that is the network element through which devices communicate with each other and exchange data. This medium can be copper cable, fibre optic cable and radio waves (WiFi).

Communication protocol - This is the method or language of communication and data exchange between devices that defines the rules and principles of that communication.

Internet - It is a set of interconnected wide area networks that form a global computer network. The origins of the Internet can be traced back to the creation of the ARPANET network in the late 1960s, and the first Internet connection in Poland was launched in September 1990. The Internet is seen by many as a collection of sites to browse, but this is not the case, as the Internet is a collection of many wide networks spread across the globe, and websites are specific network services.

Intranet - This is a private internal network that uses exactly the same communication standards (protocols) as the Internet, but only has access to authorised users, such as employees of a particular company. In most cases, access to an intranet, or this internal company network, is via a website, so communication is said to use the same standards as the Internet.

Extranet - is an extensive variety of intranets that allow access to its resources not only to the employees of a given company, but also to other users.

DNS (Domain Name System) - A network service whose task is to change a human-readable name, the so-called mnemonic name, to the IP address of a device on the network. It is a basic service of the Internet, changing the addresses of websites to the corresponding IP addresses of the servers where these websites are stored, e.g. changing the internet address onet.pl to IP address 214.180.141.140.

DHCP (Dynamic Host Configuration Protocol) is an automatic configuration protocol that assigns an IP address, subnet mask or default gateway address to a host. It is the most common method of assigning IP addresses to computers on a network, as it does not require manual IP address configuration on each computer.

3. Data units in Networks

The basic unit used in computing to store data is 1 bit [b].
In computer networks, on the other hand, the unit of bits per second is used to define the throughput (speed) of the network, expressed in b/s or bps (bits per second).

Of course, 1 bit/s is small, so to use multiples of this unit to determine the size of a file, disk capacity or RAM, regardless of bits rather than bytes, these multiples are:

1. Kilobit [Kb],

2. Megabit [Mb],

3. Gigabit [Gb],

4. terabit [Tb].

Since in a computer network the unit is in bits, unlike file size or disk capacity, where bytes[B] are used instead of bits[B], the problem of conversion, or unit conversion, arises here.

1 byte[B] equals 8 bits[b] So if we want the size of a file in bytes, we need to multiply the number of bytes by 8. For example, if we want to calculate how many megabytes a file of 3 MegaBytes contains, we multiply its size by 8. The result is 24 MB.

3 MB - 8 = 24 MB

For inverse conversion, i.e. from bits to bytes, we need to do the inverse of multiplication, i.e. division. For example: a 40 Mb file will be converted to 5 MB.

40 MB ÷ 8 = 5 Mb

The ability to convert units is best suited to performing calculations on specific examples. Two solutions are described below.

Example 1

Assuming that our bandwidth is fixed at 300 Mbps, let's calculate how much data we download from the internet in two hours.

data:

Time: 2 hours

Bandwidth: 300 Mbps

Calculate:

1. seconds minutes are multiplied by minutes:

120 minutes - 60 seconds = 7200 seconds

2. convert the unit of data transfer from megabits to megabytes per second:

300MB/s ÷ 8 = 37.5MB/s

3. multiply throughput by time:

37.5 MB/s - 7200 seconds = 270000 MB ~ 270 GB

Answer to example 1: We will download 270 GB in two hours.

Example 2

Let's calculate the time it takes to download a 5 GB file, assuming that the bandwidth of our connection is fixed at 300 Mbps.

data:

File size: 5 GB

Bandwidth: 300 Mbps

Calculate:

1. convert the unit of data transmission from megabits to megabytes per second:

300 Mb/s ÷ 8 = 37.5 MB/s

2. convert file storage units from gigabytes to megabytes:

5 GB => 5120 MB

3. divide the file size by the bandwidth:

5120 MB ÷ 37.5 MB / s = 136.5 seconds ~ 2 minutes 16 seconds

Answer to example 2: We download a 5 GB file over a 300 Mbps connection in approximately 2 minutes 16 seconds.

TASKS TO BE COMPLETED ON YOUR OWN

Calculate when the contents of a DVD (4.7 GB) can be transferred over a 50 Mbps connection.

Calculate how much data can be transferred over a 500 Mbps connection in 15 minutes.

3.1. Transmission media

Transmission media is an extremely important issue related to computer networks. There are many reasons for this, the most important of which is that the choice of the right medium is the basis and guarantee of normal and efficient operation of computer networks.

3.2. Medium

In other words, the medium that is the network element through which devices communicate with each other and exchange data. This medium can be copper cable, fibre-optic cable and radio waves (Wi-Fi).

BREAKDOWN OF TRANSMISSION MEDIA

TYPE	COPPER CABLE		FIBRE OPTIC CABLE	
TYPE	COAXIAL CABLE	TWISTED PAIR CABLE	SINGLE-MODE OPTICAL FIBRE	MULTIMODE OPTICAL FIBRE

3.3. Coaxial cable

1 Construction:

- copper core,
- plastic insulation,
- copper screen,
- Outer shirt.

It ends with a connector called a BNC. Sometimes at the end of a coaxial cable we also find a so-called BNC terminator, whose function is to remove reflections from the signal transmitted over the cable.

2 Types:

There are two types of coaxial cable: thin coaxial cable and thick coaxial cable. The differences between the two varieties are as follows:

TYPE	**THICKNESS**	**LENGTH MAX**	**NETWORK STANDARD**	**MAXIMUM THROUGHPUT**
THIN	5 mm	185 M	10base-2	10 Mbps
THICK	10 mm	500 M	10base-5	10 Mbps

It is worth noting that coaxial cable is no longer used in the construction of new networks. It has been replaced by more efficient solutions such as twisted-pair
and optical fibres.

3.4. Twisted pair cable

1 Construction:

- 8 copper wires braided into 4 pairs,
- Outer shirt.

It is terminated with an RJ45 connector, also known as 8P8C.

Depending on the type of twisted pair cable, there are also protective foils and screens to protect the cable from unwanted elements that can affect data transmission, such as electromagnetic waves.

2. types of twisted pair cable:

- UTP - unshielded twisted pair,
- FTP - foil shielded twisted pair,
- STP - twisted pair shielded cable.

In practice, we may encounter different variants of the above types, the most important of which are:

- **U/UTP - unshielded twisted pair**
- **F/UTP - Foiled twisted pair**
- **U/FTP - twisted pair cable with each pair in a separate foil screen,**
- **F/FTP - twisted pair with each pair in a separate foil screen and additionally the whole bundle also in a foil screen**
- **S/FTP - twisted pair with each pair in a separate foil screen and additionally the whole bundle in a mesh screen**

The most common material used in twisted-pair shielding is polyester film coated with a layer of aluminium and copper.

The type of twisted-pair cable that should be chosen to build a network depends on where the network is operating and the level of electromagnetic interference present in the location. In small local area networks, whether in a school or at home, the basic UTP type is most commonly used because it is sufficient for such a small network and is also the cheapest type of twisted pair cable.

3. twisted pair cable categories

In addition to twisted pair types, there are classes that define, among other things, the network standards in which they can be used.

CATEGORY	**NETWORK STANDARD**
3	Ethernet 10Base-T
5/5e	FastEthernet 100Base-TX GigabitEthernet 1000Base-T
6	GigabitEthernet 1000Base-T
6a	10-GigabitEthernet 10GBase-T
7	10-GigabitEthernet 10GBase-T

4 Technical parameters

- Signal attenuation - is the ratio of output voltage to input voltage, expressed in in decibels [dB]
- Signal propagation - This is the speed of the electrical impulse relative to the speed of light, expressed as a percentage [%].
- Resistance - is the resistance of a cable to current expressed in ohms [Ω].
- Near Crosstalk (NEXT) - this is interference in a given set caused by data transmission in a neighbouring set

Also from an installation point of view, an important parameter is the bending radius of the cable, which, for most solutions, is 4 times its outer diameter.

3.5. Fibre optic cable

Completely different from the transmission medium discussed earlier is fibre optic cable, due to the different materials used for the core. In the case of coaxial and twisted pair cable, the core or wire is copper, while in the case of fibre optic cables we are dealing with glass fibre. The use of glass fibre as the core building material also requires different types of transmission signals. In the case of copper media, this is electric current,
in the case of optical fibre, light, the most commonly used type being infrared light.

1 Construction:

- Core - has a higher refractive index,
- Coating - has a lower refractive index,
- paint protection coating,
- Reinforcement coating to protect the core during installation,
- outer shell.

We can also find the following types of connectors:

- LC
- MT - RJ
- MU
- DIN

2 Types of fibre optics:

As with copper and optical fibre, we can discuss the different types of this medium. The most common divisions are single-mode and multimode optical fibres.

In the case of single-mode optical fibres, only one beam of light passes through the glass core, resulting in the so-called signal blurring phenomenon, i.e. signal attenuation.

Using this type of optical fibre, signals can be transmitted over long distances without signal amplification equipment.

In multimode fibre, a larger portion of the beam is sent through the core, resulting in a higher degree of signal blur compared to single-mode fibre. This is because each beam sent through the core must travel a different path from the sender to the receiver.

That is why multimode optical fibre is used over short distances, up to a few kilometres.

Another difference between single-mode and multimode optical fibre is the core diameter used. For single-mode fibre optics, this is between 8 and 10 micrometres [µm], while for multimode fibre optics it is 50 or 62.5 micrometres.

3.6. Summary

Copper utilities

BENEFITS	FAILURES
Cheap to buy	**Short distances between network nodes**
Simple fault diagnosis and repair	**Susceptible to electromagnetic interference**
Hassle-free assembly and installation	**Slower than fibre optics**

Fibre optic media

BENEFITS	FAILURES
Definitely faster	**Complicated assembly and installation**
Virtually immune to electromagnetic interference	**Definitely more expensive to buy because of the equipment needed**
Transfers data over long distances	**Signal blur**

Wireless media

Several solutions are used for wireless media, but only one of them, radio waves, is actually used. The well-known Wi-Fi technology uses this medium for data transmission.

Radio waves are electromagnetic radiation in the frequency range from 3 Hz to approximately 3 THz. Radio wave sources can be natural or man-made, such as those emitted by mobile radio stations. Their main purpose is to transmit information and, in the case of telecommunications, data. There are several types of radio waves, with long, medium, short and ultra-short waves being used for data transmission.

When discussing radio waves, it is worth mentioning the standards used in wireless networks. They are important in terms of choosing the right Wi-Fi router.

STANDARD	FREQUENCY	MAXIMUM THROUGHPUT
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 GHz | 5 GHz	150 Mbps | 600 Mbps
802.11ac	5 GHz	Several Gbps

4. Types of Computer Networks

Computer networks can be divided in various ways, taking into account different criteria. The basic standard for subdividing a network is by the area in which the network operates, so subdivision by network area (coverage) is as follows:

Local Area Network (**LAN**) - a network covering the smallest area, such as a studio, school or several school buildings. A LAN also appears in your home if you use more or one computer.

Metropolitan Area Network (**MAN**) - a network covering an area larger than a room or building. A MAN network is spread over a city or metropolitan area.

Wide Area **Network** (**WAN**) - a wide area network combining LAN and MAN networks.

In addition to regional standards, networks can also be divided according to their architecture. We distinguish between networks with a client-server and peer-to-peer architecture.

In a client-server architecture, there is at least one computer serving the users of the network (these are the servers) and many computers using the services of the server (these are the clients). We use client-server architecture when browsing the web, sending emails or working with databases.

The situation is different with peer-to-peer architecture, also known as Peer2Peer (P2P).
In this case, the service is not provided by one or more computers, but by multiple computers with the same rights. Each computer on the network can simultaneously use and share resources. When using file-sharing services such as BitTorrent, we are using a peer-to-peer architecture.

4.1. Network topologies

We divide the network topology into physical, which defines how devices are connected to each other,
and logical, which describes how data is transferred between devices. Every computer network, even the smallest, has a physical and logical topology, which defines how devices are connected to each other and how data is transferred.

Computer network topology

It defines the relationships between devices on the network, the connections between them and how data flows.

4.2. Physical topologies

Physical network topologies include:

- Bus,
- Ring,
- Stars (Star).

These are the basic topologies that are the basis for building extended star and mesh topologies in large networks.

Physical bus topology

The bus topology is characterised by the fact that all devices are connected to a common transmission medium. The common transmission medium in this topology is coaxial cable. One disadvantage of this topology is the low throughput (up to 10 Mbps).

This topology is used to build a local area network. I deliberately use the word 'was' here because it is no longer commonly used. In addition to its low throughput, it is also very susceptible to network failures. When the coaxial cable breaks, the whole network stops working. The undoubted advantage of using this topology is the low cost of implementation, as there is no need for hundreds of metres of cable or any intermediate equipment.

Physical topology of the ring

In a ring topology, each device is connected to its two neighbours, forming a closed circle. As with the bus topology, this design does not use a large number of cables and additional equipment.

In addition, various transmission media can be used, from coaxial cable to copper twisted pair to fibre optic cable. The disadvantage of this topology is that the interruption of the medium or the failure of one of the computers can disrupt the entire network. To prevent this, so-called double rings are used, i.e. doubling the number of connections between devices. Such a topology is then called double ring topology.

Physical topology of stars

In a star topology, devices are connected to a central point, the access point to the network. In the past, this point was used as a hub, but now a switch is used. It is the most common topology in local area networks because it is easy to design, build and scale, fault-tolerant and easy to manage.

Another advantage is that it can be built using a variety of transmission media, such as twisted-pair copper, fibre-optic cable or radio waves (WLAN). However, a significant disadvantage can be the cost of construction, as additional equipment (switches) and many metres of cable are required.

4.3. Logical topologies

The logical network topology includes:

- peer to peer,
- pass the token,
- Multiple access.

Point-to-point logical topology

In a point-to-point topology, data is only transmitted from one device to another. These devices can be connected to each other directly, e.g. a computer to a switch,
or indirectly, over long distances, using an intermediate device, e.g. connecting two routers several kilometres apart.

In both cases, we can talk about logical point-to-point connections. This is a logical topology, often used in LANs that use a physical star topology.

Logical topology for token transfer

In a topology with token passing, data is passed sequentially to network devices. The device that receives a batch of data analyses it to see if it points to it. If the data is not intended for it, it will forward it to a neighbouring device. In this way, all devices transfer data between source and destination devices.

Multiple access logical topology

Multi-access topology (sometimes also called broadcast or logical bus topology) allows devices on a network to communicate over a single physical transmission medium. It was mostly used with physical bus and star topologies in the early stages of its development, when hubs were still used as network access points.

Every device in this topology can see the data sent over the network, as it is sent to all devices, but only the specific device to which the data is addressed can interpret it. As the devices in the network share a common medium, it is necessary to implement mechanisms to control access to this medium, these are: CSMA/CD, CSMA/CA and token pass.

Link (network) access method

The CSMA/CD method, a collision detection method, involves monitoring the state of the link. If the device that is to start a transmission detects that the link is idle, it starts such a transmission. If, during the transfer, it detects that another device on the network is also sending its data, the transfer will be interrupted. After a while, retry the transfer. Older versions of Ethernet use this mechanism.

The CSMA/CA method, a collision avoidance method, also involves monitoring the state of the link, but detecting that the carrier, i.e. the device where the transmission medium is idle, starts by sending information about its intent before transmission begins. This mechanism exists in wireless networks.

The token transfer method involves sending a special piece of data called a token or token from device to device, possession of which initiates the transfer.

5. ISO/OSI and TCP/IP layered models

The intercommunication of devices in a computer network consists of several stages, with several components. Each of them is equally important, as each performs the tasks required for proper communication. These steps are defined by the so-called hierarchical model. Anyone familiar with the layered model knows that an understanding of this is the basis for further knowledge and skills in the field of computer networks.

There are two layered models, the TCP/IP protocol model and the ISO/OSI reference model.
On the one hand, they are similar to each other, and on the other hand, each model communicates slightly differently. However, before we discuss these two models and explain the differences between them, we will tell you
you why and why you should use them, what they are used for and what the benefits of using them are.

Dividing the network communication process into layers brings many benefits, the most important of which are:

- easier definition of communication rules and principles (these are communication protocols),
- the ability to work with network equipment and software from different manufacturers,
- it is easier to understand the possibility of the whole communication process,
- Ability to manage the communication process.

Before the data from the source device reaches the end device, it has to travel a long way, during which it is first appropriately labelled, tagged, described with specific information allowing it to be identified, and then transferred between a number of intermediary devices until it reaches the recipient, who must then translate it.

Without such a model, which divides communication into smaller, more comprehensible and manageable
manageable stages and defines the tasks that need to be carried out in each layer, it will be difficult to manage network communication properly, because the numerous solutions and technologies create a huge chaos, uncontrolled. Imagine a situation where there is no such build-up, no rules describing communication,
and each hardware and software manufacturer creates its own independent system.

Of course, in one company's solution, communication will be very efficient and fast, but the solutions of two separate companies may be incompatible with each other. In practice, we use network hardware and software from different companies, thanks to the division into separate layers with rules and tasks describing their operation. These rules and tasks are the same for everyone, but each company, each manufacturer, be it hardware or software, can implement them in its own way.

A typical example is operating systems. Some users use Windows, some come from a Linux distribution and some come from macOS. Each of these systems is different and each performs web tasks in a different way, but ultimately
on each of these systems, a web page or email will look the same or at least similar. Therefore, some of the most important benefits of
of using the hierarchical model include:

- management of the network communication process,
- define its rules and tasks,
- interoperability at the hardware and software level between network products from different manufacturers,
- and control the correctness of the communication.

Now that we know the purpose of the hierarchical models, let us move on to discuss their most important features. Both models originated a long time ago in the 1970s, but are still current and in use today. The first is the TCP/IP model, known as the protocol model. Each of its layers performs specific tasks using specific protocols. On the other hand, the ISO/OSI models, known as reference models, are more commonly used for analysis in order to better understand the communication processes taking place in a network and are models for the design of network solutions, both hardware and software.

In the case of the TCP/IP model, we can distinguish 4 layers, these are Application, Transport, Internet and Network Access.

The application layer allows users to use web services such as the web, email, file sharing, terminal connections and instant messaging. I always tell my students that this is the layer closest to the user because it allows us to take full advantage of the benefits of modern web services. For example, when we sit in front of a computer and launch a web browser, we are using the
the web at the application layer level.

Below this is the **transport layer**, whose main task is to handle communication between devices efficiently. At this layer, the data is split into smaller parts,
and then supplemented with additional information, allowing them to be distributed to the appropriate application on the target device and mounted on the target device in the
in the correct order.

Then there is the **internet layer**, whose main task is to find the shortest
and fastest route to the target device over the WAN, much like a car GPS, but also uses logical addresses (IP addresses) to address the data.

Finally, we have the **network access layer,** which encodes the data as pure bits (zeros
and ones) and passes them to the transmission medium and addresses them, this time via a physical address (MAC address).

The ISO/OSI model consists of 7 layers (application, presentation, session, transport, network, data link, physical).

At the top end of this model, we can distinguish the application layer, which works here very similarly to the TCP/IP model in that it enables network applications to be used by network end users.

Then there is the presentation layer, which transmits information to the application layer about the data format used, e.g. informs which file types will be transmitted, and is responsible for the correct encoding of the data on the source device and decoding on the Target device.

Below this is the session layer, which manages user sessions via website or video communication, for example.

Going one step further, we have the transport layer, which again is exactly the same as the in the TCP/IP model and in both cases the function of this layer is exactly the same.

Then there is the network layer, which is the equivalent of the Internet layer of the TCP/IP model, i.e. very similar functions such as addressing and determining the best path to transmit data.

Next we have the data link layer, whose main task is to control access to the transmission medium and address the data, but this time to transport it between hosts on the LAN.

Finally, the physical layer encodes the data into pure bits (1s and 0s) and transmits them over the transmission medium to the appropriate device.

The two models are very similar. The resulting difference can be seen in the upper layers; in the case of the ISO/OSI model, it is divided into 3 layers, whereas in the case of the TCP/IP model, the same function is performed by only one layer. The layers can be seen with a similar difference, in the ISO/OSI model we have two separate data link layers and physical layers, whereas in the case of the TCP/IP model there is only one network access layer.

6. Communication Process

Let's now look at the communication process using the TCP/IP model. As I mentioned earlier, this model describes a set of operational protocols that form what is called a protocol, sometimes referred to as a protocol stack. Where did the name come from? I explained that when we want to display a web page, first the application layer uses the HTTP protocol, then at the transport layer we use a
a protocol from this layer, such as TCP or UDP, and then at the Internet layer an IP protocol, in the network access layer, such as the Ethernet standard. Communication is based on a set of protocols, one on top of the other. Correctness can only be guaranteed if the entire protocol stack is used for communication.

First, the network user creates data at the application layer, this may be a query to a web server or they may be writing messages in a messenger. The data is then sent down the stack, first to the transport layer, where it is split into smaller pieces,
and then to the Internet layer, where they are given an address that allows the data to be sent over the WAN. They then go to the network access layer and are again assigned addresses, this time to the addresses of devices on the local network. Finally, the data is inserted into the transmission medium and sent via an intermediary to the end device, where it passes through the stack, reassembles and is passed to the application layer.

Remember

The process of transferring data from source to destination carries the data flowing through the layers on the source device, which is then encoded and transmitted over the transmission medium to the destination device, where the data goes onto the stack instead.

Before we delve into the communication process, we need to ask one more very important question. In order to ensure that the data reaches the right hosts and applications and remains as unchanged as possible by communicating the right information to them, we call this control information.

This information is added in three layers. The transport layer adds the application port numbers (the application port on the source host and the application port on the destination host), the internet or network layer, the IP address (including source and destination host), the network or data link layer, the MAC address (source host) and the local network router). The whole process of going through the layers in the stack, dividing them into smaller parts and adding control information (i.e. additional data) is called encapsulation. Of course, there is a reverse process of removing this additional information from the target device, called decapsulation.

Remember

Data flows through layers on the source device, surrounding it with information to identify the application and the target device, while the reverse process, where data flows up layers and removes this additional information on the target host, is decapsulation.

Adding this control information to each layer individually would slightly change the structure of the layers, which is logical because we are adding some information to the data that was not there before. Therefore, the naming of the data sets also changes. Normally, the data sent over the network is called protocol data units (PDUs), but as we move between layers their names change, so: At the application layer, we simply refer to PDUs as data. Later at the transport layer, we will refer to PDUs as segments or datagrams depending on the protocol used at that layer. A PDU at the Internet layer is already a packet, and at the network access layer we will have a frame. We will use the same nomenclature when analysing communication using the ISO/OSI model.

7. Discussion of the use of layers

It is now time to understand the process of layer-based communication in more detail. We will discuss this using the example of sending an e-mail. Originally, internet users created emails using email programs or web browsers. The application layer correctly encodes this data and passes it to the transport layer.

This layer divides the data into smaller parts, segments that are easier to transmit over the network. It's like when we want to move a huge corner from one place to another, it's hard to move the whole thing because it doesn't even fit through the door, so we take it apart instead of trying to combine it with moving it completely. it also adds control information that allows us to later assemble the segments on the end device in the correct order (although this is not always added, depending on the protocol used in this layer), but most importantly, it also adds the application port number (the application port on the server and the port on the client), information that allows us to later determine that this is an email and not a web page. We will talk more about application ports when we discuss the functions
and protocols of the application layer and the transport layer.

These segments are then transported to the Internet layer, where IP addresses are assigned - the sending device and the receiving device. This process is used so that the router (i.e. the intermediary device between the sender and receiver of the message) knows where to send the message. From this point, our segment is addressed by the packet.

The packet then goes to the network access layer, where a frame is created and provides the physical address of the sending device and the physical address of the router to which the computer to which the message is being sent is connected. With this address, the frames can then reach this router, which then sends them to the WAN.

However, before the transmission itself, the frame is encoded into bits and passed through the router to the destination device.

When these bits are received by the destination host, a reverse process of encapsulation
and decapsulation, in which frames are converted into packets, packets are converted into segments and the transport layer reassembles them in the correct order. Once this process is complete, the data is sent to the application layer, where the message is displayed. When we want to display a web page or send a file over the Internet, the communication process will be similar, except that different application layer protocols will be used to handle the sending of web pages or files instead of sending and receiving emails.

Finally, an important note - the communication process between the devices discussed here is simplified and we call it a contract. Why? Well, because we have omitted the process of data transfer between intermediary devices (i.e. routers). The routing process, i.e. the transfer of data between routers in a wide area network and the possibility of using different transmission media in the process from sender to receiver, is a vast and complex issue that we will not discuss now. Of course, it is an extremely important phase of communication and we will certainly pay attention to it, but only if our knowledge and skills in computer networking allow us to do so.

Well, now each of you knows what the communication process looks like when presented
and presented on the layered TCP/IP protocol model, which looks very similar on the ISO/OSI reference model. So if you are asked (e.g. by a teacher
to take a test) to describe the communication process based on the ISO/OSI model, you should have no problem.

8. Network addressing

Let us now clarify a very important question, namely addressing in the network. You may have noticed that this question comes up 3 times when discussing the communication process, because information related to addresses or numbers is added to as many as three layers.

But this time, let's start at the bottom of the stack and see that the TCP/IP model network access layer and the ISO/OSI model data link layer have come up with the concept of physical addresses. You ask what this physical address is. No. A physical address, also known as a MAC address, is a 48-bit hexadecimal encoded number on the network card of the end device, or computer. This address can be of the form: 28-80-23-D6-BE-14, given at the card creation stage. It consists of two equal parts, the first being the manufacturer's identifier and the second being the card's identifier.

All of these hexadecimal codes are used to find a host on the local network, the LAN, is this address, the physical address of the source host and the router on the local network, the gateway connecting our local network and the WAN, in TCP/ The encapsulation process of the IP model access layer network and the ISO/OSI model data link layer.

Moving upwards, we have the Internet layer of the TCP/IP model and the Network layer of the ISO/OSI model. In these layers, IP addresses, also called logical addresses, are added during the encapsulation process. These addresses are the IP address of the sender computer and the IP address of the receiver computer. I won't go into the details of the construction, use and calculation of IP addresses here, as there is already an episode in our channel (click to enter) that is entirely dedicated to IP addresses, and I'll just say that these addresses are located on different networks to transmit data Hosts are usually hundreds of kilometres apart geographically.

Finally, we have the transport layer, which does not use addressing to detect hosts like the previously discussed layers, but instead uses port numbers to assign data to specific applications in the operating system. Remember,
that today's computers allow multiple applications to run simultaneously. At the same time, we can use the browser to surf the Internet, listen to Internet radio, send and receive e-mail and even play online games. If applications are not partitioned, if port numbers are not assigned at the transport layer to allow specific network services to be identified, we may experience that incoming e-mails will appear on the screen at lower degrees during gameplay, in text editors There will be messages from the instant messenger. See how it's all thought out, logically laid out, no chance, which is why I love computer networks so much.

8.1. Summary

In computer networks, in order to facilitate the description and control of the various stages of communication and for standardisation, a layered model is used so that hardware and software from different manufacturers are compatible with each other. Communication on a network is carried out using rules and rules known as the adoption of communication protocols. The process of network communication involves passing data down the stack on a source device, encoding it into bits and sending it to a destination device, where the data is passed on and interpreted at the destination device. At each layer, the data comes with control information, port numbers and logical and physical addresses, which are then encoded and sent to the recipient. The process of flowing data down the stack and transferring control information and addresses is called encapsulation, while at the end devices, as data travels up the stack, this process is called decapsulation.

9. Application layer protocols

9.1. HTTP protocol

When we launch a web browser, instant messaging or file-sharing programme, these applications create a communication interface between the computer network
and the user. Of course, the application software itself, the computer program itself, is not sufficient for efficient communication, as the above communication protocols are required for this, but they are implemented in these programs. An example of an application layer protocol, probably one of the most popular, HTTP, is implemented in web browsers and, like all instant messaging and other programmes that communicate over a network, also implement a corresponding protocol.

When we enter the address of a web page in the browser, the so-called URL (Uniform Resource Locator), and after pressing the Enter key, our browser connects to the server where the page is stored and requests a specific resource - most of which are usually files containing pages of content. If the server has the requested resource, it sends its contents to the browser, which interprets the HTML code of which the page consists,
and displays its content to the user. In reality, the process is somewhat complicated. Let's take a web address as an example:

http://www. cybersecurity.co.uk/fundamentals.html

Once entered and confirmed, the browser first checks the protocol type, then the Internet domain name and finally considers the name of a specific file. Later, our browser calls the DNS server to change the mnemonic name
(i.e. cybersecurity.pl) to the IP address of the server on which the page is stored.

The browser, knowing this address, sends a request to the server to access the file tomijerry.html located in the domain alamakota.pl. If the server has the resource in response, it sends an appropriate message with the contents of the requested file. The content of this file, HTML code, is interpreted by the browser and displayed as a web page.

The HTTP protocol defaults to port 80 and defines several basic message types, i.e. a request for communication between a client and a web server, the most important of which are: GET and POST.

9.2. GET method

GET is used to request a particular web page from a server. Its syntax looks like this:

GET /fundamentals.html HTTP/1.1

In addition to the name of the requested resource, it also contains the protocol version used. When the server receives such a message, such a request, it responds to the client with the appropriate message
(with the headers shown below) and the requested resource:

HTTP/1.1 200 OK/fundamentals.html

The GET request also contains the following information: the host name (e.g. wp.pl), the name of the browser that sent the request, the file types accepted by the browser and the preferred language or character encoding of the page. The server response contains the following information: the server time, the name of the server application (e.g. APACHE) or the expiry time of the document.

If, for some reason, the web server cannot send back the resource, it sends back an
error message, such as 404 notifying that the requested resource was not found or 403 notifying that access to the resource is prohibited. Selected messages and error codes are shown in the table below.

[table from paste below].

Customer error code:

Code Description Meaning

400 Bad Request The server could not process the request due to a client error

401 Unauthorised requests Requests for resources that require authentication

403 Forbidden The server understands the request, but the security configuration prevents it from
it returns the requested resource

404 Not Found The server could not find a resource at the specified URL

405 Method not allowed The method contained in the request is not allowed for the indicated resource

406 Not Acceptable The requested resource cannot return a response that the client can handle

407 Proxy authentication required Proxy authentication required

408 Request timeout Request timeout elapsed - client did not send request to server within specified time period

409 Conflict The request could not be fulfilled due to a conflict with the current state of the resource

411 Length requested - server refused to complete request due to missing Content-Length header in request

415 Unsupported Media Type Unknown request way - the server refused to accept the request because its syntax was not understood by the server

[end of table]

Server error code:

Code Description Meaning

500 Internal Server Error Internal server error - the server has encountered a problem that prevents it from completing the request

501 Not Implemented The server does not have the capabilities required for the query

502 Invalid gateway error The server - acting as a gateway or intermediary - received a bad response from the host server and could not fulfill the client's request

503 Service unavailable Service unavailable - the server is currently unable to complete the client's request due to overloading

504 Gateway Timeout Exceeded - the server acting as a gateway or intermediary did not receive a response from the specified HTTP, FTP, LDAP, etc. server within the specified time or a DNS server is required to handle the request

505 HTTP Version Not Supported - the server does not support or refuses to support the HTTP version specified by the client

9.3. POST method

Another type of message is a POST message, which is used to send data to a server. For example, when there is a form on a page that sends data to the server, such as a registration form, the data we put in it is sent with a POST message.

Although the HTTP protocol is very popular and probably the most widely used of all application layer protocols, it is not secure. The POST method sends data to the server in plain text. If the transmission between client and server is intercepted, it is possible to read the information you want to send to the server.

This is very dangerous, which is why nowadays most websites can send some information to the server, e.g. those sites that require a login already use HTTPS, which encrypts the communication between the client and the server, running on port 443.

Other types of messages that clients can send to the web server are:

Data for my table:

Remove the request to remove the resource from the server

Head requests resources from the server in the form of headers

Link Request establishes relationships between existing resources

OPTIONS Requesting the server to identify supported methods

Put requests the server to receive the file from the client

Trace requests the server to return the headers of the message sent by the client

9.4. Electronic mail

Email uses two application layer protocols that work together. One is used to send mail, which is the SMTP protocol, and the other to receive messages, which is POP3. Today, IMAP can also be used to receive messages
e-mail. These protocols are closely related to the applications, the processes running on client computers and servers that create and receive messages. These processes are MUA (Mail User Agent), MTA (Mail Transfer Agent) and MDA (Mail Delivery Agent).The MUA process runs on the client machine and the other two processes run on the mail server.

A simplified process for sending emails using a proxy is as follows:

1 The user creates an e-mail message and uses the MUA process to forward it to the mail server and the MTA process running on that server.

2. this process analyses the message headers, including. To define the recipient of the message and check that the user to whom the message points is in its user list.

(3) If so, it passes the message to the MDA process, which is responsible for delivering it to the appropriate recipient.

(4) If the recipient of the message does not have an account on this server, the MTA process forwards the message to the MTA process on another server where the user account is located.

5 The server passes the message to the MDA process, which delivers the message to the intended recipient.

The following table shows the ports on which the email protocol operates.

Protocol	**Port number**
IMAP	143
POP3	110
SMTP	25
Encrypted IMAP	993
Encrypted POP3	995
Encrypted SMTP	465 or 587

9.5. FTP protocol

A third, equally popular web service is the ability to send and receive files via FTP (File Transfer Protocol). The service is also a communication protocol when we want to upload website files to a web server or simply want to upload some files to a server and share them with other users. To perform the operation of uploading files to the server or downloading resources from the server, we need to use an FTP client and, of course, such a service must also be running on the server. FTP clients are available on every operating system, for example via the command line, which is inconvenient but works.

If you only use FTP for downloading files, you can do so safely using a web browser. Most, if not all, popular browsers have built-in FTP clients.

However, if you want to upload files to a server, it is advisable to use dedicated software such as FileZilla or WinSCP - these are free and can be easily downloaded from the web.

WinSCP FTP client

With this protocol, two connections must be established between the client and the server in order to communicate properly. The first connection is only used to send commands and messages and is called a control connection (it runs on port 21), while the second connection runs on port 20 and is used to transfer files to and from the server. To protect access to the FTP server, user authentication is used, which is exactly the same as for logging in to profiles or emails on social networks, but sometimes, when the resource is available to a larger audience, anonymous access is granted to so-called users, therefore no authorisation is required.
This solution should only be used if the user is allowed to download data
from the server. Uploading files, i.e. placing them on the server, is always only accessible to users with a login and password.

9.6. SSH protocol

Another commonly used application layer protocol is the remote host management protocol known as SSH (Secure Shell). For non-IT professionals, the name has little meaning, as it is not a protocol, website or
email used by 'ordinary bread eaters'. Administrators use it to manage servers, which are often located in different geographical locations, not necessarily at their workplace. For example, it is also used by people who have bought VPS servers and therefore manage them. This protocol is derived from another remote access protocol, the TELNET protocol, and is probably a better version. Why? Because TELNET, by the way, is probably the oldest protocol at the application layer, it does not encrypt the communication between client and server, messages are sent in plain text, so it is possible to intercept the communication and wonder what session the information is being sent in. In his view, this is an unacceptable situation, so the host is managed remotely using the encrypted SSH protocol.

The default algorithm for encrypting communications is RSA, but the slightly weaker DSA algorithm can also be used to encrypt data. When the SSH server is installed, a pair of keys is created - the server's public and private keys - which are used to encrypt and decrypt communications. When a client connects to the server for the first time, it saves the server's public key in a known_hosts file on disk.

It then creates a so-called session key, which is used to encrypt all communication. The session key is encrypted with a public key previously received from and sent back to the server. From this point on, all communication is encrypted with the session key.

By default, SSH runs on port 22. PUTTY is one of the most popular client programs for using SSH, it is free, can be downloaded from the web and requires no installation. To connect remotely to a host, simply launch it, enter the hostname or its IP address, select SSH if it is not selected by default, and click Open. If you are connecting to a remote host for the first time, confirm that you want to connect
and we can manage it remotely.

9.7. DNS protocol

DNS is a protocol, a service that translates human-readable domain names into IP addresses for devices on the Internet. Imagine a situation where DNS does not exist, but we want to display our favourite websites in the browser. We need to enter the IP address rather than the domain name, i.e. the address in word form, for example: 212.56.93.112. For most of us this is no problem, some numbers can be memorised. On the other hand, there are many websites on the Internet and it is difficult to remember many numerical addresses. What's more, it's easy to make a mistake in such digital records, and in the world of the Internet, such a small mistake can lead to a different page than we expected.

This is one side of the coin, and the other side is that the IP address of the server may not change very often. When our website changes IP address and the DNS service doesn't work, we have to re-learn that address and remember it. DNS solves this problem for us because it changes this address in its record database and assigns it to the domain name. Then, for us users, it doesn't matter what the IP address of the site is, the important thing is, that we know its address and domain name and they do not change.

DNS is a service that runs in a client-server architecture, but here we are not treating the clients as computer programmes such as browsers or file-sharing programmes. This computer only runs a system service called DNS Resolver, which handles all applications on client computers whose names need to be changed. Whenever we configure a network device, or just a computer, we should specify two DNS server addresses so that if one does not communicate, the other acts as a name substitution.

DNS servers store all sorts of records, including A and AAAA records containing end device addresses and MX records supporting mail exchanges, as it is important to remember that DNS not only translates domain addresses into IP addresses for websites, but also applies to the email server. The name swap looks like this for me:

1 The client sends a query to the DNS server, which checks whether the record exists in its database.

2. if so, translates the name into an IP address and sends it back to the client:

(3) If not, it contacts other servers to have the record in question included in their database:

Sending requests to other servers for a DNS server that does not find a record in its database can cause a lot of network traffic, which is a confusing situation. To prevent excessive and unnecessary network traffic, when another server finds a record and sends it to the server assigned to your device, the latter saves the record in a cache, so that in future you do not have to refer to another server for the same address. This will certainly speed up later name changes, as our DNS servers no longer search for records on other servers, but replace the names immediately. Similarly, DNS services on personal computers store previously translated names. This can be verified by entering ipconfig /displaydns on a Windows PC. We will then see which mappings are stored in our computer's DNS service cache.

9.8. DNS hierarchy

This hierarchy of DNS servers takes the form of an inverted tree, with the root, the top-level DNS server, at the top. The top-level server stores information
about how to reach the top-level server, which in turn stores information
about how to reach the second level server, etc. Top-level domains specify the country (. pl.de or . uk) or type of organisation (. org . com or . gov).

In an example address such as Pocztowy.wp.pl, we distinguish between a top-level domain (. pl), then a second-level domain (wp.pl) and finally a third-level domain (Pocztowy.wp.pl Of course, not all addresses have to contain as many levels of domains as possible, not just top-level and second-level domains, such as wp.pl, pasja-informatyki.pl, Szkola.pl.

9.9. DHCP protocol

Like DNS discussed earlier, DHCP is a protocol that operates as a service rather than as a program or application. DHCP allows computers connecting to a network to obtain IP addresses, subnet masks, gateway and DNS server addresses and other settings from a pre-configured address pool. A DHCP server can be configured on a separate computer and will be a separate device on the network that assigns IP addresses to client computers, or it can run on an existing server as a separate service, a separate process.

Currently, the router in our home also allows us to configure such a service. Assigning addresses to client computers via the DHCP service (so-called dynamic assignment) is a very convenient solution for administrators, especially in large networks where new computers and their users frequently appear. In a network with 100, 200 or 500 computers and a large number of mobile devices, simply configuring IP addresses would be a tedious and, most importantly, time-consuming task.

Of course, not all devices on the network can obtain addresses in this way, as some, such as application servers, databases, user authentication, network printers or routers, should and must have addresses statically assigned, i.e. distributed manually. Why? Because a DHCP service configured on a server does not always permanently assign a given IP address to a computer. It only leases such an address for a period of time specified when configuring DHCP, maybe hours, days, but not permanently, although there are exceptions to this, I will tell you when configuring a specific DHCP server.

The deactivated machine returns the leased address, which is returned to the pool. Another machine can then lease this address. When a server, router or network printer leases these addresses, they may have to return them to the pool after a period of time and there is no guarantee that they will receive the same address again. Client computers that communicate with any server or other important device running on the network refer to it by its IP address, if the IP address changes frequently, some services for users on the local network may not be available for some time, especially in the company All the more Unacceptable.

In order for a Windows computer to obtain an address from a DHCP server, the option "Obtain an IP address automatically" must be selected in the network configuration.

9.10. Summary

The application layer protocols described in this section are only a small part of the overall list of application layer protocols available. There are many other services on a computer network, each running on a different protocol. It is hard to list them here, so the most popular and commonly used ones are listed. For those interested in exploring the topic of application layer communication protocols in more depth, I refer you to the literature. The following table contains a set of popular application layer protocols and their port numbers. They are certainly useful for checking before examinations or professional tests.

Protocol	Description	Port
HTTP	Hypertext transfer protocol	80
HTTPS	Encrypted HTTP protocol using SSL or TLS protocols	443
POP3	Protocol for the receipt of mail	110 (encrypted 995)
IMAP	Mail receiving protocol to manage folders in the mailbox	143 (encrypted 993)
SMTP	Mail sending protocol	25 (encrypted 465 or 587)
FTP	File transfer protocol	21 (commands) and 20 (files)
FTPS	Encrypted FTP protocol	990
TELNET	Terminal connection protocol	23
SSH	Encrypted terminal connection protocol	22
DNS	Protocol for changing domain names to IP addresses	53
DHCP	Protocol for automatic configuration of hosts on the network	67 and 68 (IPv6 - 546 and 547)
LDAP	Directory services protocol (e.g. AD in WS)	389 (coded 639)
SNMP	Network equipment configuration protocol	161
MySQL	Database management system	3306
PostgreSQL	Database management system	5432

10. Task of the transport layer

The transport layer or transport layer (these names can be used interchangeably) is a very important part of the communication process. The most important tasks of this layer include:

- establish and maintain connections (sessions) between hosts,
- track connections between hosts,
- Divide the data into smaller pieces,
- Identify individual applications,
- data flow control,
- Retransmission in case of data loss.

Call tracking, which are conversations between hosts, allows multiple applications to send and receive data simultaneously. On one computer, we can check our mail, use electronic banking or communicate with friends. At the moment, it seems natural to us that it is actually difficult to imagine a situation without this possibility, but it is worth remembering that this is possible thanks to the transport layer.

The ability to use multiple services at the same time also includes splitting data, i.e. breaking it into smaller pieces. This allows for more efficient communication, as large amounts of data are not transmitted simultaneously. If it were not for segmentation, only one application could receive data at a time and the other applications we use would have to wait their turn. As you can see in the image below, segments are sent alternately, web page segments, email segments, instant messenger segments, etc. are sent alternately. The whole process of alternating the transmission of multiple application segments is called multiplexing.

Another important task or function of the transport layer is to pass data to the relevant application. Each application has its own identifier to uniquely define it. This identifier is the port number of the application.

It is assigned to a segment or datagram during encapsulation at the transport layer level and guarantees the delivery of data to a specific application.

As with IP addresses, port numbers are assigned by the IANA (Internet Assigned Numbers Authority), which divides port numbers into 3 groups:

Port group name	Numbering range	Application
Well known	0 - 1023	Server services and applications
Registered	1024 - 49151	User services and applications
Dynamic	49152 - 65535	Randomly selected for customer applications

Well-known ports, i.e. ports 0 to 1023, are registered for services and specific server applications, e.g. web servers default to port 80 and POP3 servers default to port 110. A set of applications with known ports, including transport layer protocols, as shown below.

Application layer protocol	Port number	Transport layer protocol
HTTP	80	TCP
HTTPS	443	TCP
POP3	110 (encrypted 995)	TCP
IMAP	143 (encrypted 993)	TCP
SMTP	25 (encrypted 465 or 587)	TCP
FTP	21 (commands) and 20 (files)	TCP
FTPS	990	TCP
TELNET	23	TCP
SSH	22	TCP

DNS	53	TCP or UDP
DHCP	67 and 68 (IPv6 - 546 and 547)	UDP
LDAP	389 (coded 639)	TCP or UDP
SNMP	161	UDP

The second group, registered ports, is used by applications installed on the user's computer. For example, if we install the MySQL database management system application on our computer, it will run on port 3306.The third and last group, the dynamic port number, is randomly assigned to the client application, e.g. when a client sends a request to the server to share a web page, the server by default accepts the request on port 80, but the client receives the request from the server. The incoming response will not be sent to port 80, as this is reserved for the web server process, but to a random number of ports allocated from the dynamic port pool.

Multiple applications cannot run on the same port number. Once an application is running on port 53 (DNS), it is impossible for another application to no longer be able to run on that port.

If we already know what an application port is, let's introduce another concept. This will be a socket.
You have already encountered the concept of sockets when discussing motherboards and processors in computer technology classes, and it also appears in computer networks. A socket is a combination of an IP address and a port number:

192.168.20.20:80

A socket uniquely identifies a particular process running on a device, so, for example, when our browser invokes a web server to serve a web page, server requests will be sent to its socket, the process (web server application).

10.1. TCP header

TCP is a complex, connection-oriented protocol that aims to guarantee reliable data transfer and flow control. Up to 20 bytes of control data are added to the TCP header during encapsulation, but this is required for TCP reliability. Applications using this protocol include web browsers, email clients and file transfer programs. You can see the TCP segment mode below. The numbers in brackets indicate the number of bits reserved for the field.

BIT (0)			**BIT (15) BIT (16)**	**BIT (31)**
Source port (16)			Destination port (16)	
Sequential number (32)				
Confirmation number (32)				
Heading length (4)	Reserved (6)	Code bits (flags) (6)	Window (16)	
Checksum (16)			Urgency index (16)	
Options (0 or 32)				
Application layer data (variable length)				

- Source port - the port of the application sending the data.
- Destination port - the application port to which data is sent.
- Sequence number - the number of the last byte in the segment.
- Acknowledgement number - the number of the next byte expected by the recipient.
- Length - the length of the entire TCP segment.
- Code bits (flags) - control segment information.
- Window - Amount of data that can be transmitted without confirmation.
- Checksum - used to verify the uploaded data.
- Emergency indicator - only used when the URG flag is set.

10.2. 3-part reconciliation

TCP is a connection protocol, which means that before a source host can send any data to a destination host, a connection must be established between them. This combination is called a three-way handshake. The source host, i.e. the client, sends a segment containing the SYN flag (SYN is a serial number synchronisation flag), and the segment also contains the client's random serial number (also called the ISN, SEQ=100), which is used for subsequent merged data fragments.

On receipt of this segment, the destination host, i.e. the server, is informed that the client wishes to establish a connection with it. In response, the server sends a segment with the SYN and ACK flags set (the ACK flag informs the client that the server has received the previous segment), the sequence number received from the client is incremented by 1 (ACK = 101) and its random sequence number (SEQ = 300).

Finally, the client sends the segment back to the server with the ACK flag set, acknowledging receipt of the previous message with the server sequence number incremented by 1 (SEQ=101, ACK=301). This completes the connection process and allows the data to be transmitted correctly. The three-step reconciliation process is shown below.

Only after a TCP connection has been established with the server can the client send the relevant data, such as a request for a web page or file.

Finally, when all data has been transmitted, the session must be closed. The client then sends a segment to the server with the FIN flag, which informs the server of its intention to close the session, which responds with an acknowledgement segment with the ACK flag that it has received such a segment. The server then also sends a segment with the FIN flag, and the client responds with an acknowledgement segment with the ACK flag. This causes the TCP session to be closed.

Flag	Application
URG	Indicates the existence of an urgency indicator field in the header (urgent)
ACK	Indicates the existence of an acknowledgment number field in the header.
PSH	Forced packet transmission (push)
RST	Reconnecting (reset)
SON	Synchronisation of sequential numbers
FIN	End of data from sender

10.3. TCP window

The reliability of data delivery within a TCP session relies on the client sending an acknowledgement of receipt of previously sent data. Before the server can send another portion of data to the client, it must receive this acknowledgement of receipt. This sometimes causes delays in the delivery of segments as they are not sent continuously. However, these problems are acceptable when reliability of communication is required.

Assuming that 1000 bytes of data will be sent in a segment with sequence number 1, when the client receives 1 part of the data, it will send a segment with confirmation number 1001 to the server. The next byte, starting with byte 1001. When the server sends 1000 more bytes, the received acknowledgement number will be 2001, the next number will be 3001, the next 4001
and so on.

Of course, in reality, when the host has to acknowledge the receipt of such a small amount of data each time, this can cause a lot of bandwidth overload, e.g. the page load time can be long. Therefore, more data is sent and acknowledged by the feedback. The amount of data the server can send before receiving an acknowledgement from the client is called the window size, in this case 3000 bytes.

This size is specified in the TCP segment header and, in addition to determining how much data can be transmitted without acknowledgement, allows control of the flow of data between devices. If a client encounters a blocking while receiving data and a segment is lost, the device can send information to the server to reduce the size of this window, the amount of data that can be received without acknowledgement, slowing down the transfer, but preventing the loss of a segment. After some time, the window size returns to its original size. The change in window size during transfer is called a dynamic window or sliding window.

10.4. UDP protocol

Another protocol that implements some transport layer functions is the UDP protocol. However, in this case it is much simpler, as the protocol does not implement any mechanism to guarantee reliability of data delivery or flow control.

The UDP protocol is a simple connectionless protocol and its greatest advantage is the low overhead of control data added during the encapsulation process. UDP only adds 8 bytes of control data in the datagram. The header of a UDP datagram looks like this:

BIT (0)	**BIT (15) BIT (16)**	**BIT (31)**
Source port (16)	Destination port (16)	
Length (16)	Checksum (16)	
Length of application layer (variable length)		

- Source port - specifies the application port from which data is to be sent.
- Destination port - specifies the application port to which data is sent.
- Length - 16-bit field specifying the length of the entire UDP datagram
- Checksum - a 16-bit field used to validate the data being sent.

Connectionless UDP means that the source host does not send any information to establish a connection with the destination host before the communication process starts. The general rule of thumb is that if a source device wants to start a transfer, it wants to send the data it has just completed without prior agreement.

If we compare it to interpersonal communication, in the case of the TCP protocol it would be something like: Hey Tom, focus because I'm about to talk to you and only when I get this message will a normal conversation start, of course only if Tom replies: OK, I'll start listening. In the case of UDP, it didn't notify Tom that I was about to start communicating something important to him, I just started the conversation.

Applications or services that use this transport protocol include DNS, DHCP, VoIP telephony and video streaming.

Why these? Well, the answer is simple, these applications value speed over reliability of communication, or rather the need to receive all the data being transmitted. Imagine a situation where we are watching a video broadcast or playing a game with friends, like CS. It is difficult to compete in the game or watch anything when packets are late.

Someone might ask: but why the delay? Well, TCP segments, for example, are much larger than UDP datagrams, and TCP has to acknowledge the data delivered, so they are sent across the network in large volumes, more than in UDP.

For applications using this particular protocol, it can be tolerated,
that occasionally packets may be lost or corrupted. For DNS services, if a datagram is lost, the query is simply resent to the DNS server
and it would not be a tragedy if the datagram did not arrive during the session, as messages can always be repeated. For applications using the TCP protocol, loss or confusion is no longer acceptable. Datagrams are received in the order in which they are received, and if there are multiple datagrams, it is the responsibility of the specific application to ensure that they are correctly assembled.

10.5. NETSTAT command

How can I display the connected connections of our computer to various servers
in Windows? To do this, you can use Wireshark, through which we were able to check everything that passes through our network card, and also use the NETSTAT command in the Windows console. Once entered, we can keep track of what active connections we have. The output of this command shows the type of transport layer protocol used for the connection, the socket of my computer, i.e. the IP address
with the port number, the socket of the server to which we are connected, and the connection status.

The programmes can be called with various arguments, and a list and description of these will be displayed when the netstat /help command is entered.

As you can see from the image above, there are a lot of these connections, and that's because, first of all, I use Windows 10, which is known to send something to Microsoft's servers almost all the time, and besides that, I have set up synchronisation with cloud services
and there is an antivirus program that also connects to its servers. So how do we check which services our computer is connected to? Simply run the netstat -f command and copy the domain name (PPM -> Tag -> Select Domain Name -> CTRL + C or PPM -> Copy).

We can see the owner of the domain through whois.domaintools.com and its search engine. Just paste in the copied domain name. As you can see, the owner of this domain is Google.

11. Network layer tasks and protocols

The Network Layer (ISO/OSI model - Layer 3), also known as the Internet Layer, receives fragmented data from the Transport Layer and then performs operations to enable packets to be transmitted across the network. These operations include:

- Addressing data using IP addresses;
- Data encapsulation, i.e. the assignment of additional information required by the network layer protocol in use;
- Routing, i.e. selecting the best route for the parcel;
- Decapsulation, which removes this additional information when the packet reaches its destination.

We know that network communication is governed by certain rules, a communication protocol. We also know that each layer uses its own protocol, independent of the other. The network layer, where they also appear, is no different. The most common communication protocol for this layer is IPv4. The most important reason to use it is that it is an open protocol. This means that it does not belong to any one company or business, so it can communicate between devices from different manufacturers. It already follows IPv6, which is also an open protocol.

Currently, many device and software manufacturers are using these protocols in parallel. Maybe in the future IPv6 will completely replace IPv4, but I don't think it's too soon. Of course, there are also proprietary protocols, such as the IPX protocol owned by Novell, which specialises in developing network operating systems, or the AppleTalk protocol developed by Apple. However, it is safe to say that IPv4 is by far the most widely used network layer protocol.

11.1. IPv4 protocol

The IPv4 protocol is designed in such a way that there is no need to add much control data during the encapsulation process. It provides only the basic functionality required to transmit packets from source to destination. It is connectionless, meaning that it does not establish a connection before sending data and operates on a 'best effort' basis, meaning that it does not use flow control or any acknowledgements of data delivery as the TCP protocol does, but does everything it can to make the communication efficient. It is also a medium-independent protocol, meaning that data can be transferred between hosts regardless of the medium used.

After all, in one network we may be using twisted pair, in another fibre, and in a third radio waves. The IP protocol works exactly the same in every network. The problem that can arise when sending data over different media is the maximum packet size, which is the MTU (Maximum Transmission Unit) value, if the packet is too large, the routers connected to the network will split it into smaller pieces. This process is called fragmentation, which is another term from our internet dictionary.

To help understand how IPv4 works and how packets are transmitted over the Internet, I will use the example of a package sent by my aunt from the United States to explain how it works. The package consists of 3 cardboard boxes joined together. My aunt wrote an address for the gift and sent it to the courier company. When she sends the package, she gives up additional options such as confirmation of receipt or tracking. An employee of the company marks the carton with the destination and return address before releasing the parcel. It was transported by car to the port along with dozens of other parcels, where it was packed into a container and then crossed the ocean.

At the port of destination, the containers are unpacked, the parcels sorted and then transported by car to the various cities and local pick-up points. From the pick-up point by car, the parcel is supposed to be delivered to the specified address, but it turns out that the three combined cartons are too big to be transported on a trolley, so the courier separates them into individual cartons and delivers them to you as such. As your aunt has not chosen the additional options, the courier company has not provided her with a receipt. You can do this yourself, e.g. call your aunt to say thank you 🙂

Converting this to IP communication would look like this:

- The parcel is sent without prior notification to the recipient - we have a connectionless mode;
- During the encapsulation process, a source and a destination address are assigned
- in our case, the recipient's home address is the destination address and the aunt's home address is the return address;
- The consignment did not contain much control data, which could slow down communication - for which my aunt gave up an extra option, confirmation and tracking;
- Parcels arrive at their destination via fibre optics, twisted pairs and radio waves - as parcels are delivered by various means of transport: boats, large cars, small cars;
- The parcel is too large to be sent in its entirety through one of the networks, making it fragmented - i.e. the parcel is split at some point so that it can be transported in a small car;
- The IP did not send an acknowledgement of receipt of the package - just as the company did not assure the aunt that the package had arrived.

Like any communication protocol, IPv4 also has standardised headers to add control information. An example of a typical IPv4 header is shown below.

Version	**IHL**	**Type of service**	**Package length**	
Identification			Flag	Moving a fragment
TTL	Protocol		Header checksum	
Source address				
Destination address				
Options			Filling	

- destination IP address - the IP address of the device to which the data is directed;
- source IP address - the IP address of the device that is sending the data;
- Time to Live (TTL) - An 8-bit field indicating the remaining lifetime of the packet. The TTL value decreases by at least 1 each time the packet passes through the router (that is, after each hop). When the value reaches 0, the router discards the packet and removes it from the network data flow. This mechanism prevents the infinite transmission of packets that cannot reach their destination between so-called routers. routing loops. If routing loops are allowed, the network will be overloaded with packets that never reach their destination. Decreasing the TTL value at each hop ensures that it will eventually reach 0, and packets with a TTL field of 0 will be discarded.
- Protocol - this 8-bit value specifies the higher (transport) layer protocol used, such as UDP or TCP.
- Type of Service (ToS) - contains an 8-bit value that determines the priority of each packet.
- Fragment Offset - A field used when reconstructing packets split by routers. Indicates the order in which each packet should be arranged during reconstruction.

- More Fragments (MF) flag - A single bit used with the Fragment Offset field for packet partitioning and reconstruction. Setting the MF flag indicates that the fragment is not the last fragment in the packet. When the receiving host notices an incoming packet with MF = 1 set, it checks the Fragment Offset field to place the fragment during packet reconstruction. When the receiving host notices that an incoming packet has MF = 0 set and has a non-zero value in the fragment offset field, it will use the fragment as the last block of the reconstructed packet.

- DF (Don't Fragment) flag - A single bit which, if set, indicates,
that packet fragmentation is not allowed. Packet fragmentation is not allowed if the DF flag is set.

- Version - contains the version number of the IP protocol (in this case IPv4).

- Header length (IHL) - determines the size of the packet header.

- Packet length - this field gives the total size of the packet in bytes, including the
including header and data.

- Identification - this field is used to uniquely identify the fragment of a split IP packet.

- Header checksum - this field is used to check for packet header errors.

- OPTIONS - this is the space in the IPv4 header for additional fields to support other services. However, it is rarely used.

11.2. IPv4 addressing

One of the key tasks of the network layer is addressing. Addressing in IP networks is very similar to the addressing we humans use. Of course, only at the logical level is the addressing mechanism different. Hosts in the network are grouped together for easy management and addressing.

Like people, we live on specific city streets. As a result, my American aunt's shipment above will reach the recipient without a problem. First by ferry to Poland, then by truck to your town, and then by smaller car to the street
and house number. This is very similar to host addressing. Packets sent between networks first arrive at the network to which the host belongs, and are then sent to a specific host. This type of addressing is called hierarchical addressing because the general information, which is, in the case of data transfer, the network address, is read first, followed by the specific information, which is the IP address of the specific host.

[For an extended tutorial on IP addressing, including a discussion of how to perform calculations on IPv4 addresses, see our channel:

]

In a computer network, hosts can communicate with each other in three ways:

- use single transmission;
- via multi-mission;
- via transmission.

Unicast broadcast is the most common and is used for a typical connection between two hosts. For example, when a client sends a request to a server, it uses a single broadcast transport to do so.

Using multicast transmission can significantly reduce the bandwidth consumption of a network, as a single packet is not sent to multiple hosts like a unicast transmission, but a single packet is sent that can reach multiple recipients simultaneously.

Routers can use multicast to exchange routing information and distribute software. Multicast uses a special pool of addresses, called group addresses, and in the IPv4 protocol this is the range shown below:

from **224.0.0.0** to **239.255.255.255**

Broadcast, on the other hand, sends a packet to all hosts on a given network. This uses a special address, the broadcast address, so that the addresses of all hosts on the network are not stored in the IP packets. It is technically impossible, then, to use one and two broadcasts, for example, when the address of a particular device is unknown. This type of transport is most often used in local networks, and broadcasting is rarely used to communicate with hosts outside a given local network.

Throughout the IPv4 address pool, there are various groups of addresses known as special purpose addresses. These are addresses that are not used for WAN communication. Among these special addresses are the so-called loopback addresses. A loopback address is nothing more than an address of its own.In addition to the valid IP address used for communication, each computer on the network is also assigned its own address, most commonly 127.0.0.1. In addition, each address in the pool is used to verify the IPv4 configuration on the host.

Another special type of address is the local link address. These address types are used when a host should get an IP address from a DHCP server, but for some reason the address is not available. The host will then receive an address from the local link address pool. Data transfers using such addresses can only take place on the local network where the host data is running. There is also a final set of special addresses, TEST-NET addresses. As with locally-connected addresses, these are only used for communication on the local network, for educational purposes. They can be used in documentation or examples, such as online courses. However, they should not be used permanently. The special address ranges are shown in the table below:

Address range	**Name**
127.0.0.1 - 127.255.255.254	Loopback
169.254.0.1 - 169.254.255.254	Local-Link
192.0.2.0 - 192.0.2.254	Educational (Test-Net)

11.3. Network layer testing

Every operating system implements programs that allow us to test the network layer. One of these is the PING programme, which is used to test connectivity between hosts. This name is available on Windows and various Linux distributions. The other is the TRACERT programme, which is used to test routing between a source host and a destination host. On Linux kernel-based systems, the same programme is called TRACEROUTE.

PING uses another network layer protocol, ICMP, to send an echo request datagram and wait for a response. When the response is received, it shows us the elapsed time between sending the request and receiving the feedback. PING can be used for testing:

- The so-called local stack, i.e. to verify the correct installation of the IP protocol on the computer, it is sufficient to enter the PING command in the Windows console, using one of the feedback addresses, i.e. in the range 127.0.0.1 to 127.255.255.254:

- A connection is established to a host on the local network, then instead of the loopback address, the address of the host on the local network is entered (e.g. 192.168.0.1):

- Connect to the host on the remote network. Here, if you want to check communication with the server where the page is stored, you can enter the domain name, i.e. facebook.com, instead of the IP address:

Sometimes we may not receive a response to an echo request sent by the PING programme, even if the remote network is working and communicating correctly. This is because some network administrators restrict or completely prevent the insertion of ICMP datagrams into their networks for security reasons.

Another part of network layer testing is to examine the routing of packets from the source host to the destination host. Thousands of routers operate in the wide area network, creating what is known as the Internet, connections between local networks spread across the globe.

To check which routers a packet is being sent through, e.g. from a computer to a web server, we will use TRACERT for Windows or TRACEROUTE for Linux. They work in exactly the same way and, similarly to PING, use the ICMP protocol
protocol and echo messages. To perform the test, simply type TRACERT in the console along with the address of the target host. This can be an IP address, or a domain address if you want to test routing to a specific host, such as wp.pl.

Below you can see the routing test to the server where the Wirtualna Polska website is hosted.

12. Data link layer tasks

The main and essential role of the data link layer is to provide higher layers with access to the transmission medium. Data moving down the stack as it passes through the layers must at some point be delivered to the medium through which it reaches its destination, the receiving host. This is the primary function of the data link layer: it stores data from higher layers on the medium.

The network layer discussed in the previous section of this course included segments with IP addresses received from the transport layer during the encapsulation process to form packets. These packets arrive at the data link layer before being sent to the destination host, and then pass through the data link layer to the transmission medium. Before this, however, the packets received further control information, this time the physical address of the device, the 48-bit MAC address.

The packets then become frames and it is these frames that go into the carrier for onward transmission to the destination host. The MAC address is assigned during the manufacture of the card and stored in the ROM. The ROM is read-only, so it is not possible to change the assigned addresses at card or hardware level. However, such addresses can be changed at the device system level, for example in the operating system. Sometimes administrators make such changes at the system level, e.g. when they do not want to reconfigure the network hardware, such as when a new computer comes on the network.

The data link layer itself is the intermediary between the transmission medium and the network software. In the case of terminal devices, i.e. computers, servers or telephones, it is the only layer implemented not only in the software domain, but also in the hardware domain. The physical representation of the data link layer is the network card that we install in our computer. These cards are the interface between the network software and the transmission medium. Since the data link layer operates on two levels, on the hardware and software level, its functions and tasks are also divided into two smaller sub-layers:

- LLC (Logical Link Control),
- MAC (media access control).

The LLC sublayer frames information about the network layer protocol in use, so that different network layer protocols, such as IPv4, IPv6 or IPX, can use the same transmission medium and network card, and its functions in the computer are performed by the network card driver. On the other hand, the MAC sublayer defines the access rules to the medium and performs the addressing functions. The MAC method was discussed in the first episode of this series.

In summary - the data link layer:

- receive data from the network layer,
- create frames that can be transmitted through the medium,
- gives the physical address of the frame,
- Responsible for controlling access to the medium.

This layer is implemented on end devices such as computers, but also on routers and switches.

Data link layer frame and communication

There are many solutions and many network standards to implement Layer 2 functionality. We have Ethernet standards, we have wireless networks, and finally we have many network protocols running over WANs such as Frame Relay. So there is no such thing as a universal frame. Each network standard has its own structure, specific to a particular solution. To summarise the topic, we can assume that a typical second level framework consists of 3 main parts:

Headline	Data	Footer
source and destination MAC addresses **frame start signal**	network/Internet layer packets	end-of-frame signal **checksum**

Let us now follow the process of inter-device communication, focusing on the functions of the data link layer. Suppose our computer sends a request to a web server on a remote network.

The data to send such a request is already encapsulated in a single packet with the application's port number and logical address, i.e. the IP address of the computer and server.

Before a packet enters the transmission medium, the data link layer must construct a frame with the corresponding MAC addresses of the frame's sender and receiver. In the case of the MAC address of the sender, the thing is obvious, it is just the MAC address of the computer, but what about the address of the destination host? If the computer and the web server are not on the same network and the MAC address of its network card cannot be determined, this is technically impossible. Why? Because MAC addresses are only used for communication within a network and never outside the network. Therefore, the MAC address of the router interface to which our computer is connected will be stored in the frame field containing the destination MAC address.

The frame is sent through the transmission medium to the first router. The latter, upon receiving the frame, decapsulates it so that it can read the IP address of the device to which the packet is going. IP addresses cannot be read directly from Layer 2 frames, so decapsulation is required. Once the IP address is read from the packet (once the frame is decapsulated, the data becomes a packet again), compare it with the entry in the routing table and find the entry that indicates that the server network is routed through other routers.

It will then create a new frame in which the source address will be the MAC address of the interface that connects to the other router, and the destination MAC address of that router.

The frame then passes through the medium to the second router, which encapsulates the frame again to read the IP address from the packet. It finds that the recipient of the data is a device operating on the network, directly connected to it, so the encapsulation process performed by the second router happens again, this time it enters the MAC address of its second router in the MAC address field. The interface is used as the source address and the MAC address of the address server is used as the destination address.

The frames prepared in this way go to the server, which also decapsulates them. This time, however, it is the device to which the data points, so it decapsulates them completely, that is, it additionally reads the application port number in order to send the data to the corresponding specific application, in this case a web service.

The network service then prepares the response data. The data goes first to the transport layer, where the application port number is assigned, then to the network layer, forming a packet with the corresponding IP address, and finally to the data link layer, where a frame is prepared from the packet, marked with the MAC addresses of the server and router for the connected server.

The response is then passed to the media, which is then sent to the client. During this process, it passes through two routers, which perform a decapsulation and recapsulation process, and because they have to read the IP address, they can pass on the response. Finally, the response belongs to the client. This unpacks the data, allowing the browser to display the web page.

12.1. ARP protocol

As network users, when we transfer data from one device to another, we know the IP address or domain name of the device, so we can perform such transfers. Even worse are MAC addresses, on the basis of which we network users do not determine the recipient of the data, this happens outside of us. In IPv4-based computer networks, a protocol called ARP (Address Resolution Protocol) is used to obtain information about the MAC address of a particular device.

ARP is a mechanism that allows logical (i.e. IP) addresses to be mapped to physical (i.e. MAC) addresses. Suppose a computer that wants to send data to another device knows its IP address, but does not know its MAC address. To know this address, the computer sending the data will create an ARP broadcast frame and broadcast it to all devices on the same network before sending the specified data. The source address field of the frame stores the address of the computer that prepared the frame and the destination address field stores the broadcast MAC address: FF-FF-FF-FF-FF-FF.

Each device that receives a frame decapsulates it into a packet and checks that the IP address of the destination field is its address. If the destination IP address is not its own, it will ignore the packet; if it is its IP address, it will create a new frame storing its MAC address and send it for transmission.

The computer sending the broadcast frame now knows the physical address of the device it wants to communicate with and can start that communication. IP to MAC mapping information is stored in each device's ARP table for later use. By default on Windows systems, such entries last up to 10 minutes and are then deleted. To view the ARP table, run arp -a from the console. As you can see, there are several entries here, which means that there has been communication between my computer and another device in the last 10 minutes.

12.2. Ethernet

Work on this standard dates back to the 1970s, when Xerox, one of the largest technology companies, decided to design an open network communication standard that would serve people for years to come. In the late 1970s, it developed a standard for local area networks and became the prototype for Ethernet. Today, Ethernet is the standard that can be found in most local computer networks around the world and, due to its many advantages, it has also become the standard for city networks and, in some cases, even wide area networks.

Ethernet is a complete set of networking solutions implemented at both the data link layer and the physical layer. The development of this technology is currently being overseen by the IEEE (Institute of Electrical and Electronics Engineers), which published its standard in 1985 and describes it under the numbers 802.2 and 802.3. The 802.2 standard includes functions related to the LLC sublayer, which is related to the MAC sublayer and the physical layer of the OSI model.

Many factors contribute to the success of Ethernet-based solutions, including:

- easy to implement,
- reliability,
- ability to adapt new technologies,
- Implementation costs are relatively low.

12.3. Evolution of Ethernet

Let us now discuss the evolution of Ethernet. The initial versions of the standard, called thick networks (so-called thick Ethernet) and thin networks (so-called thin Ethernet), had few capabilities compared to what we have today. The older versions operate on a copper transmission medium (coaxial cable). They use a physical bus topology, which is characterised by all devices being connected to a common medium. The solution requires media access control, which is implemented using the CSMA/CD approach

After many years of using solutions based on bus topology as a transmission medium, it turns out that this solution is no longer efficient enough. The rapid growth of the network has led to ever higher user demands for bandwidth and reliability. Instead of coaxial cables, twisted-pair cables, UTP cables and new topologies are widely used. Star topologies appeared, the same ones used today, but using hubs instead of switches as the central point of the network. No one had heard of switches then.

The use of hubs improved the performance of computer networks to some extent, but it soon became apparent that this solution was not ideal either. The basic feature of a hub is that it transmits data to all the devices connected to it. It works like this,
that a computer that wants to send data to another device performs this communication through the hub. The latter, on the other hand, is not so clever as to transfer data to the appropriate device, it simply sends data to all those connected to it.

Only the devices to which the data is sent analyse the addressing to determine whether they are recipients. If they are not recipients, they ignore the data, and if they are, they interpret it.

This type of solution means that although the physical topology is a star topology, it is logically similar to that used in the previous generation of Ethernet. Here, too, a link access method based on CSMA/CD is used, which has become inefficient due to the rapid growth of the network. In addition, each hub creates a so-called collision domain.

The more devices connected to the hub, the larger the collision domain,
and the larger the collision domain, the greater the likelihood of collisions, limiting throughput and creating requirements for frequent data retransmissions. More collisions are not the only problem associated with using hubs. Other disadvantages of such devices include limited scalability and increased delays in data transmission, among other things due to the aforementioned shocks.

Efforts to address the weaknesses of hub-based Ethernet continued over the years until the invention of a smart networking device called a switch, which solved the problems that plagued earlier versions of Ethernet.

Switches in computer networks are still around today and there is no indication that this will change any time soon. Why are these devices so popular and why are they so smart? Well, unlike a hub, a switch does not send data to all the devices connected to it, but only to the specific device for which the data is destined, obviously bypassing broadcasting, such as the ARP transmission discussed earlier. A logical point-to-point topology exists between the switch port to which the device is connected and the device itself. Data sent to a particular device is sent to it and only to it.

The use of a switch almost completely eliminates the risk of collisions, as devices do not have to compete with each other for access to the medium. At the same time, the size of the collision domain is limited, as such a domain consists only of the switch ports and the devices connected to it. There are many more advantages of switches. Each device connected to a switch port has a dedicated bandwidth available.
For example, if a switch offers a transfer rate of 100 Mbps, this bandwidth will be available to each device connected to it.

With a hub, this bandwidth is shared between all devices. By using a switch, data can also be transmitted in full-duplex mode,
which means that the devices connected to it can receive and send data simultaneously.

There are several versions of the Ethernet standard in use today. The most popular of these is the standard offering nominal throughputs of up to 100 Mbps, known as the FastEthernet standard. Transmission in this standard is over only 2 copper pairs rather than 4 twisted pairs. It is a common solution used in many computer networks.
In most cases it meets the requirements of computer networks.

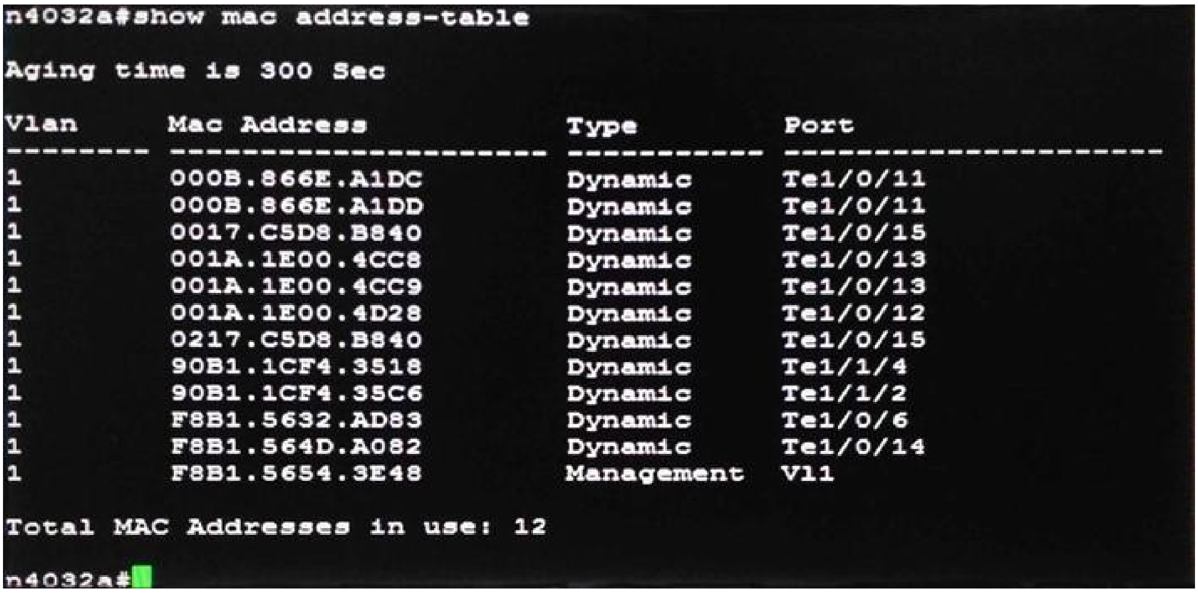
The Gigabit Ethernet standard can be used when the demand for network bandwidth increases with the amount of data being transmitted. Nominally, it provides a throughput of
1 Gbps. If the 1000BASE-T standard is used, all copper twisted pair cables are used for transmission. This version of Ethernet is used by large local networks that use
VoIP telephony and transmit large amounts of various types of media.

Using the Ethernet standard, data can also be transmitted over fibre optic links, in which case the Gigabit Ethernet standard is called 1000BASE-SX or LX. There are also Ethernet standards that provide communication at 10 or even 100 Gbps. They are mainly used in metropolitan and wide area networks because they are very, very expensive to implement and few people can afford to use this type of solution in a local area network. The table below shows the most popular versions of the Ethernet standards and the transmission medium they use:

Ethernet standard	Maximum throughput	Transmission medium used	Maximum distance
100BASE-TX (fastEthernet)	100 Mbps	UTP (cat. 5/5e)	100 metres
100BASE-FX (fastEthernet)	100 Mbps	Optical fibre (single/multi-mode)	400/2000 metres
100BASE-T (gigabitEthernet)	1 Gbps	UTP (cat. 5e)	100 metres

100BASE-TX (gigabitEthernet)	1 Gbps	UTP (cat. 6)	100 metres
100BASE-SX (gigabitEthernet)	1 Gbps	Multimode optical fibre	550 metres
100BASE-LX (gigabitEthernet)	1 Gbps	Single-mode optical fibre	2000 metres
10GBASE-T (10gigabitEthernet)	10 Gbps	UTP (cat. 6/7)	100 metres
10GBASE-LX4 (10gigabitEthernet)	10 Gbps	Single-mode/multi-mode optical fibre	300/10000 metres

The switches described above use MAC addresses to transfer data between devices connected to the switch ports. Every switch has something called a MAC address table. This is nothing more than a collection of information that determines which device, actually what MAC address of a device is connected to a particular port.



```
n4032a#show mac address-table

Aging time is 300 Sec

Vlan     Mac Address             Type        Port
-------- ----------------------- ----------- ---------------------
1        000B.866E.A1DC          Dynamic     Te1/0/11
1        000B.866E.A1DD          Dynamic     Te1/0/11
1        0017.C5D8.B840          Dynamic     Te1/0/15
1        001A.1E00.4CC8          Dynamic     Te1/0/13
1        001A.1E00.4CC9          Dynamic     Te1/0/13
1        001A.1E00.4D28          Dynamic     Te1/0/12
1        0217.C5D8.B840          Dynamic     Te1/0/15
1        90B1.1CF4.3518          Dynamic     Te1/1/4
1        90B1.1CF4.35C6          Dynamic     Te1/1/2
1        F8B1.5632.AD83          Dynamic     Te1/0/6
1        F8B1.564D.A082          Dynamic     Te1/0/14
1        F8B1.5654.3E48          Management  Vl1

Total MAC Addresses in use: 12

n4032a#
```

Entries in such a table are added dynamically and not by the administrator. The switch retrieves the information stored in the table during the learning process. From a received frame, the switch reads the source MAC address and adds it to its table, assigning the port number on which it received the frame. In turn, if it does not know to whom to send such a frame because there is no entry for the recipient's MAC address in the table, a process called flooding occurs.

This can be compared to broadcasting, as the frame is sent to all devices except the sender. The device to which the frame is not addressed discards it, while the receiving device responds and sends the frame to the switch. The switch reads the MAC address of the sender from the frame and stores it in its table. The whole process of learning and flooding is shown in the video tutorial.

Ethernet frame

Since the Ethernet standard operates on the second layer of the OSI model, you can guess, that it also creates its own frames. Of course, yes, Ethernet encapsulates its own frame, called an Ethernet frame. You can see an example frame below:

Field size in bytes	**7**	**1**	**6**	**6**	**2**	**46 - 1500**	**4**
Field name	Preamble	Frame start marker	Recipient's MAC address	Sender MAC address	Length/Type	Data and filling	Frame Control Code (FCS)

- Preamble and Frame Start Marker - these fields are used to inform the target device that it is ready to receive frames;

- The target MAC address, which is the physical address of the recipient of the frame;

- The source MAC address, which is the physical address of the sending host;

- Length/Type - The length field specifies the size of the frame, while the type specifies the protocol used by the higher layers, the most common of which is IPv4;

- Data - this is the packet received from the network layer. The minimum size of this field must be 46 bytes and the maximum size must be 1500 bytes. If the packet is smaller than 46 bytes, it is supplemented with random data to increase the size of the entire frame to the required minimum, i.e. a maximum of 64 bytes.

- Frame check code - field containing frame checksum, used to detect possible frame errors. The device sending the data calculates the checksum and places it in the frame, the data receiver also calculates the checksum after receiving the data; if both checksums are correct, the frame is accepted, if they are different, the frame is considered damaged and rejected.

The total frame size can be up to 1518 bytes (the preamble and start of the frame signal are not taken into account when calculating the frame size). There is also an Ethernet frame frame with a maximum length of 1522 bytes. Such frames are used in virtual LANs, in so-called VLANs.

13. Basic issues of VoIP communication

Key definitions

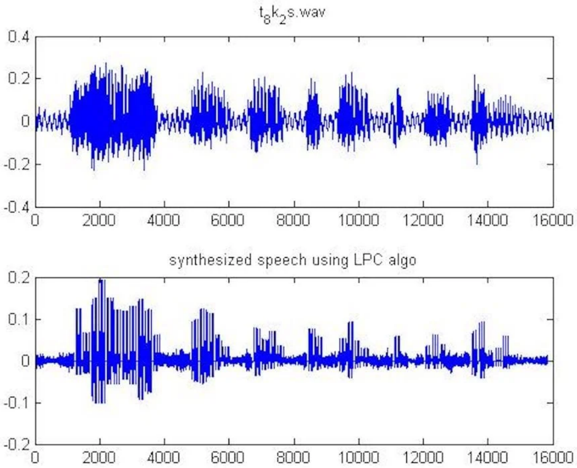
VoIP - https://pl.wikipedia.org/wiki/Voice_over_Internet_Protocol
PBX - https://pl.wikipedia.org/wiki/PBX
Codec - https://pl.wikipedia.org/wiki/Kodek
SIP - https://pl.wikipedia.org/wiki/Session_Initiation_Protocol

What is VoIP?

VoIP is an acronym for Voice over Internet Protocol. It is a technology that allows audio to be sent and received over a computer network, this technology is used to make 'phone calls' in real time.
Although VoIP technology has become very popular over the past decade the history of VoIP begins nearly 100 years ago at the Bell Labs research institute.

In 1938, Homer Dudley, a Bell Labs engineer, created the first electronic speech synthesiser, known as the Vocoder. The concept of operation was similar to today's packet transmission (IP), which records voice samples on one phone and plays them back on another. Today, the same technology is used not only in VoIP telephony, but also in cochlear implants.

It is not possible to make calls over the Internet without a computer network. The history of computer networking begins in 1969 at the Advanced Research Project Agency - a US government agency. The agency's work led to the development of the TCP/IP network protocol and the launch of the first computer network, ARPANET. This network continued to operate formally until 1990.
In 1973, at MIT, Bob McAuley, Ed Hofstetter and Charlie Radar developed the first voice packet transmitted over ARPANET.


t_8k_2s.wav

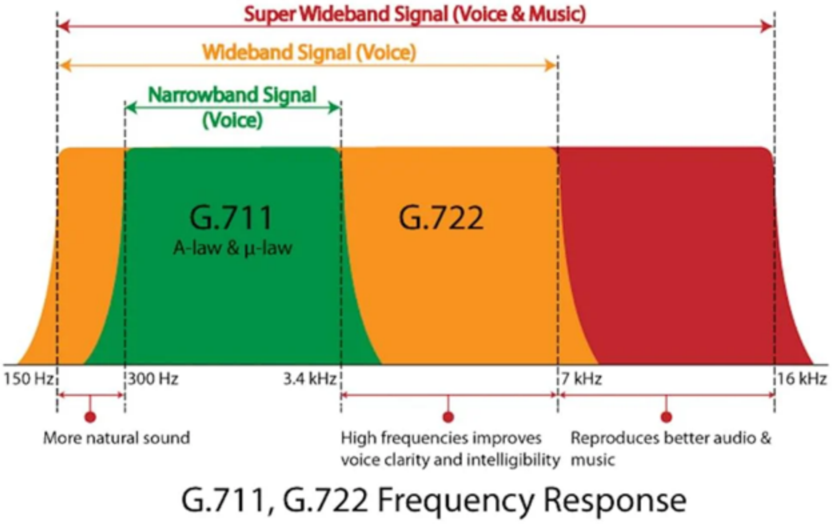
synthesized speech using LPC algo

(Source: https://www.mathworks.com/matlabcentral/fileexchange/13529-speech-compression-using-linear-predictive-coding)

This voice transmission was made possible by LPC, or Linear Predictive Coding - the foundation of modern VoIP technology. LPC is a speech analysis technique that relies on a linear predictive model to process and re-synthesise compressed digital forms of voice and speech signals.

At the time, ARPANETs could not be used privately. The first 'technical' cybercriminal was Leonard Kleinrock, who in 1973 sent a message over ARPANET regarding his missing electric razor.

In 1974, Lincoln Lab and Culler Harrison Inc. successfully transmitted test voice data packets between them. In 1976, Culler Harrison and Lincoln Labs conducted a teleconference via LPC. In 1982 they made significant progress, using the LPC to connect over the local cable network, mobile packet network and interface with the PSTN (Public Switched Telephone Network).


Super Wideband Signal (Voice & Music)
Wideband Signal (Voice)
Narrowband Signal (Voice)
G.711
A-law & µ-law
G.722
150 Hz
300 Hz
3.4 kHz
7 kHz
16 kHz
More natural sound
High frequencies improves voice clarity and intelligibility
Reproduces better audio & music
G.711, G.722 Frequency Response

Rysunek 2: Pierwszy szerokopasmowy kodek audio

(Source: https://www.gl.com/newsletter/g722-wideband-audio-codec-support-across-tdm-voip-platforms-newsletter.html)

In 1988, the ITU-T approved the G.722 wideband audio codec, a programme that allows audio to be converted into 'digital' language and, once transmitted over the network, converted back into an audio signal. The G.722 codec offered significantly improved speech quality compared to its predecessors. G.722 offers data rates of up to 64 kbps, making it ideal for VoIP communication - especially in local area networks (LANs).

In 1989, developer Brian C. Wiles created RASCAL, the first system that successfully transmitted voice over Ethernet networks - the first VoIP application.

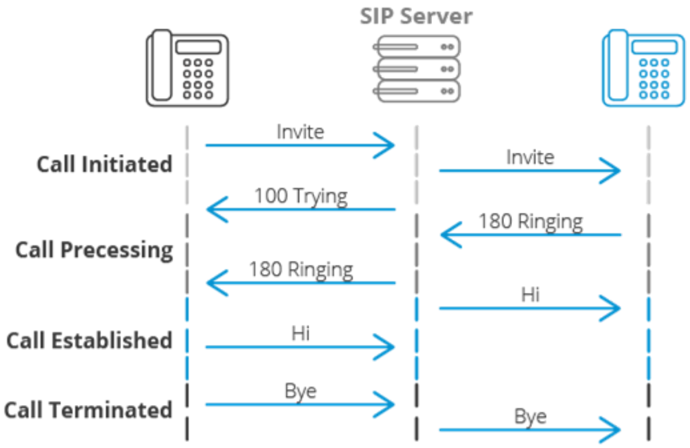
In 1991, John Walker of Autodesk wrote and released NetFone, later known as Speak Freely, the first software-based VoIP phone.

1993 brought the first video conferencing system, Teleport. The developers of Teleport were David Allen and Herold Williams, who sold their product to Hilton Hotels.

The first commercial VoIP application became the VocalTec Internet Phone programme in 1995. The programme used the H.323 protocol, the requirements were a 486 processor, 8 MB of RAM, a 16-bit sound card and an SLLP or PPP internet connection. VocalTec was cheaper than traditional telephone calls for international and long-distance calls.

In 1996, SIP (Session Initiation Protocol) was developed. The first version of SIP had only one command - 'make a call' - but by 1999 the capabilities of SIP had been expanded to six commands. VocalTec Internet Phone programme. The programme used the H.323 protocol, the requirements were a 486 processor, 8 MB of RAM, a 16-bit sound card and an SLLP or PPP internet connection. VocalTec was cheaper than traditional telephone calls for international and long-distance calls.

In 1996, SIP (Session Initiation Protocol) was developed. The first version of SIP had only one command - 'make a call' - but by 1999 the capabilities of SIP had been expanded to six commands.

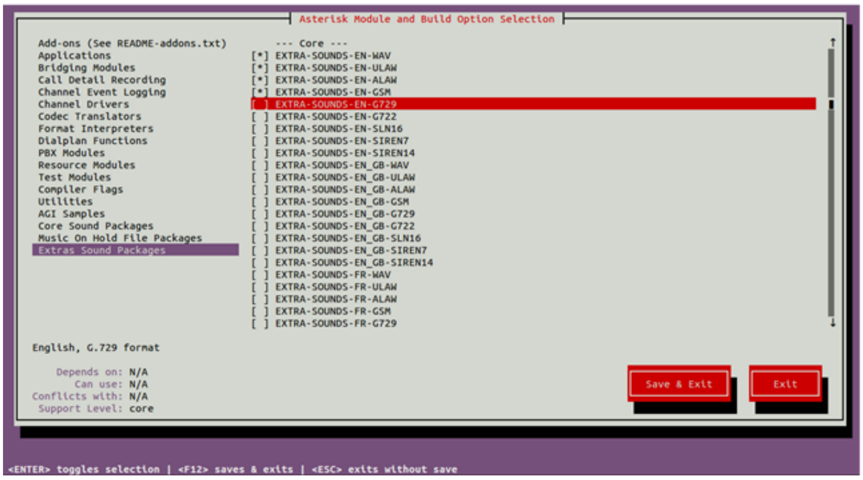


Rysunek 3: Protokól SIP

(Source: https://www.3cx.pl/voip-sip/sip/)

SIP has become the preferred protocol for mobile VoIP telephony.

In 1999, Mark Spencer decided to program his own IP-PBX system, a program that acts as a telephone exchange, and call it Asterisk. Asterisk is an open source program that quickly gained popularity and is still being developed and improved today by thousands of developers.



```
                    Asterisk Module and Build Option Selection

 Add-ons (See README-addons.txt)        --- Core ---
 Applications                       [*] EXTRA-SOUNDS-EN-WAV
 Bridging Modules                   [*] EXTRA-SOUNDS-EN-ULAW
 Call Detail Recording              [*] EXTRA-SOUNDS-EN-ALAW
 Channel Event Logging              [*] EXTRA-SOUNDS-EN-GSM
 Channel Drivers                    [ ] EXTRA-SOUNDS-EN-G729
 Codec Translators                  [ ] EXTRA-SOUNDS-EN-G722
 Format Interpreters                [ ] EXTRA-SOUNDS-EN-SLN16
 Dialplan Functions                 [ ] EXTRA-SOUNDS-EN-SIREN7
 PBX Modules                        [ ] EXTRA-SOUNDS-EN-SIREN14
 Resource Modules                   [ ] EXTRA-SOUNDS-EN_GB-WAV
 Test Modules                       [ ] EXTRA-SOUNDS-EN_GB-ULAW
 Compiler Flags                     [ ] EXTRA-SOUNDS-EN_GB-ALAW
 Utilities                          [ ] EXTRA-SOUNDS-EN_GB-GSM
 AGI Samples                        [ ] EXTRA-SOUNDS-EN_GB-G729
 Core Sound Packages                [ ] EXTRA-SOUNDS-EN_GB-G722
 Music On Hold File Packages        [ ] EXTRA-SOUNDS-EN_GB-SLN16
 Extras Sound Packages              [ ] EXTRA-SOUNDS-EN_GB-SIREN7
                                    [ ] EXTRA-SOUNDS-EN_GB-SIREN14
                                    [ ] EXTRA-SOUNDS-FR-WAV
                                    [ ] EXTRA-SOUNDS-FR-ULAW
                                    [ ] EXTRA-SOUNDS-FR-ALAW
                                    [ ] EXTRA-SOUNDS-FR-GSM
                                    [ ] EXTRA-SOUNDS-FR-G729

English, G.729 format

    Depends on: N/A
       Can use: N/A
Conflicts with: N/A
 Support Level: core                                  Save & Exit      Exit

<ENTER> toggles selection | <F12> saves & exits | <ESC> exits without save
```

Rysunek 4: Instalacja asterix w systemie Linux

(Source: https://www.howtoforge.com/how-to-install-asterisk-17-on-ubuntu-2004/)

In 2003, Skype was created and soon became the most widely used voice communicator. Over time, Skype developed into a video instant messenger with file transfer capabilities. Today, it is owned by Microsoft.

In 2006, Truphone, the first mobile VoIP application, was launched for Nokia, iPhone, Android and Blackberry users. The app uses SIP to make calls over an internet connection rather than over mobile networks.

Between 2011 and 2015, the US saw a great increase in the popularity of VoIP telephony. Globally, there has been an increase in the number of VoIP providers, which has fostered competition and is leading or has already led to the displacement of legacy phone systems.

The COVID pandemic of 2020 has changed the nature of work to remote working overnight in many sectors of the economy. Unified communications based on VoIP technology allows teams to work remotely and contact customers through multiple channels, including: video calls, mobile apps, conference calls, team text messaging, voicemail.

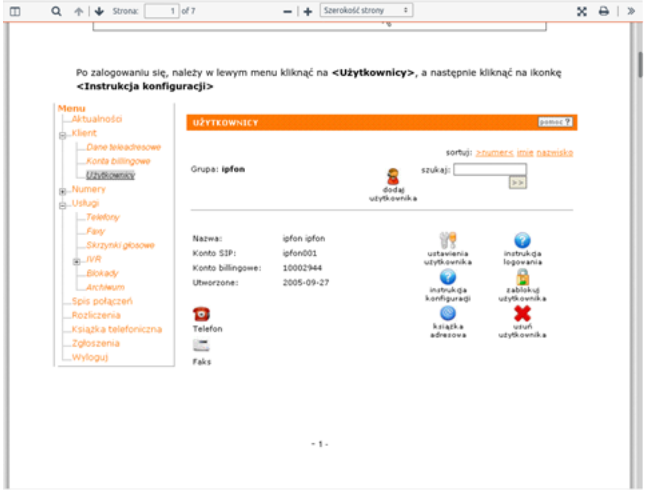
Some of the most popular software applications that use VoIP technology include: Microsoft Teams (the default messenger for the MS Windiows11 operating system), Google Meet, Zoom.

VoIP at home, VoIP for business

VoIP solutions for home users

Home users are those who generally require a single telephone number.

In order to set up a public PSTN phone number with a state and area (city) prefix, you need to register with a VoIP service provider. The VoIP provider will, in the registration process, create a SIP account - a login and password, and tell you how to configure SIP. Having the account information, we can log in to the PBX and use VoIP telephony in applications for mobile phones, applications installed in Microsoft, Apple, Linux operating systems, or finally VoIP phones.



Po zalogowaniu się, należy w lewym menu kliknąć na **<Użytkownicy>**, a następnie kliknąć na ikonkę **<Instrukcja konfiguracji>**

Grupa: **ipfon**

Nazwa:	ipfon ipfon
Konto SIP:	ipfon001
Konto billingowe:	10002944
Utworzone:	2005-09-27

Rysunek 5: Przykład uzyskania danych logowania do konta SIP

(Source: https://docplayer.pl/64633184-Uzyskanie-nazwy-i-hasla-konta-sip.html)

VoIP solutions for companies

In order to manage multiple VoIP telephones in a company, it is necessary to set up a PBX. The PBX can be either a physical device installed in the company's premises or a virtual PBX (software provided by the company selling telephony services).

In the case of a virtual PBX, the fixed telephones of the company's employees must support VoIP. The cost of a VoIP phone is comparable to a traditional phone, so for new company premises, a VoIP phone seems to be the best choice.

Companies with traditional PSTN lines and handsets can stay with the allocated telephone numbers in two ways:

- purchasing a VoIP PBX with PSTN/ISDN modules without replacing phones,
- transferring the numbers to a virtual PBX and replacing the telephones with VoIP-enabled ones.

Overview of VoIP applications

VoIP-related applications can be divided into:

- client - installed on VoIP end user's telephones/computers
- server applications - installed on regular servers or dedicated PBXs.

Client applications

Modern mobile phone technology is based on digital technology, so audio is transmitted via a codec.

On current smartphones, adding a VoIP number is possible without installing additional software. In the Android or iOS settings, we can enter our SIP account details and use VoIP telephony. There are also many VoIP apps that give additional functionality (e.g. shared address book, etc.). When choosing how we want to use VoIP telephony, it is best to follow the recommendations of the VoIP service provider. Service providers often have their own application dedicated to the use of VoIP services.

On desktop computers, laptops or tablets without the possibility of connecting to a mobile network, we can use VoIP via the Internet. So all you need to do is connect your laptop to WiFi and install a VoIP application to make phone calls.

There are many popular applications that allow VoIP telephony connections to the public switched telephone network (PSTN) : Microsoft Teams, ZOIPER, Blink, Zoom, etc. We can follow the list of VoIP client applications at: https://en.wikipedia.org/wiki/List_of_SIP_software_;

Server applications

The SIP server manages calls on the network, receives requests from VoIP clients to establish and terminate calls.

The most popular open source SIP server is Asterix (https://www.asterisk.org). To run Asterix in a company, you need to have a server with the Linux operating system installed. There are dedupe software packages in Linux distributions that contain the Asterix server. The best way to install the Asterix server is to download a specially prepared Linux distribution - freePBX (https://www.freepbx.org/downloads/). Asterix has many of the features of modern telephony including, among others: SMS, music while waiting/connecting, voicemail.

14. Network performance. Methods of reducing network traffic.

Factors affecting computer network performance

The performance of a computer network is influenced by:

1. **The passive parts** of a computer network, which are the parts of a computer network that only serve to transfer data between active network devices. Passive parts of a computer network include: copper cables, fibre optic cables, network sockets, and pathpanels.
2. **Active devices**, are the parts of a computer network that transmit/receive information or are used to transmit/enhance data on a computer network. Active devices include: network cards, switches, network amplifiers/repeaters.
3. **Electromagnetic interference**, which is what affects wireless transmission and copper (twisted pair) cables.

14.1. Quality of twisted pair cable

Twisted pair cables carry information in the form of electrical impulses. A twisted pair cable contains 8 strands (wires) of copper coated with insulation. The conductors are twisted in pairs to ensure better data transmission. The speed and quality of data transmission in the form of electrical impulses are most affected by electromagnetic interference.
The workmanship of twisted pair cables is influenced by:

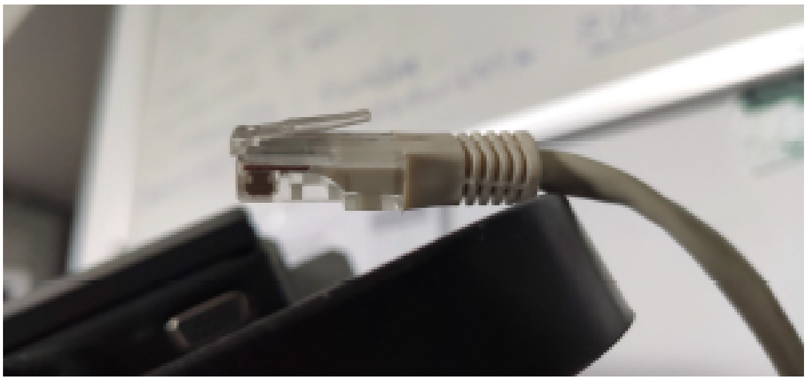
- the workmanship of the copper conductor, i.e. the purity of the metal, the retained profile dimensions
- the quality and quantity of insulation.

Depending on the amount of insulation and the shielding methods used (protection against interference), twisted pair cables are defined by category 1 to 8 and the type of shielding: U - unshielded, F - foil shielded, S - mesh shielded, SF - foil and mesh shielded. A higher category of cable ensures faster data transmission, for example: category 5 UTP, ScTP, STP ensures transmission up to 1 Gb/s; category 6 UTP, ScTP, STP - 10 Gb/s.

Network cables are terminated with RJ45 connectors. The quality of the material used and the RJ45 shielding obviously affects data transmission.

Examples of damage to twisted pair cables

In Picture 1, we see a Category 6 cable made in a factory using a specialised production line. The cable inserted into the socket retains its properties and the RJ45 termination works correctly after repeatedly connecting the computer. The protection against unwanted cable falling out works correctly - a characteristic click can be heard. Also, the cable cannot be pulled out without releasing the protection. This condition of the cable guarantees correct data transmission.



14.2. Fibre optics

Introduction

Fibre optics carry information in the form of light pulses. Thanks to the phenomenon of total internal reflection, light running inside an optical fibre is trapped there. It is therefore possible to transmit information over a much greater distance without loss than with copper cables.

Light that travels inside an optical fibre is attenuated. As no method has been invented to produce a perfectly reflective optical fibre, the phenomenon of optical power loss occurs. At present, optical fibre cables are capable of transmitting information over a maximum distance of around 100 km without loss. Thanks to the use of optical amplifiers at certain intervals, we can connect very distant locations via optical fibre networks.

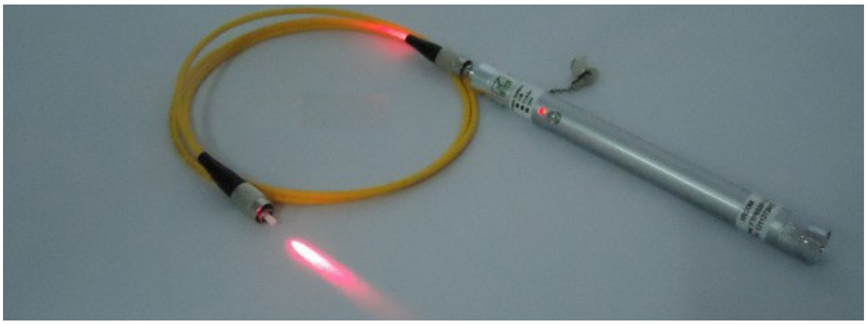
The quality of fibre-optic networks is primarily influenced by the quality of the work carried out during its laying. Attention should be paid to:

- the maximum bending radius of the cable - depending on the standard the bending radius is: 30, 10 7.5 mm,
- the quality of the cutting equipment - after cutting, the edge of the optical fibre must not be frayed,
- quality of the welding machine

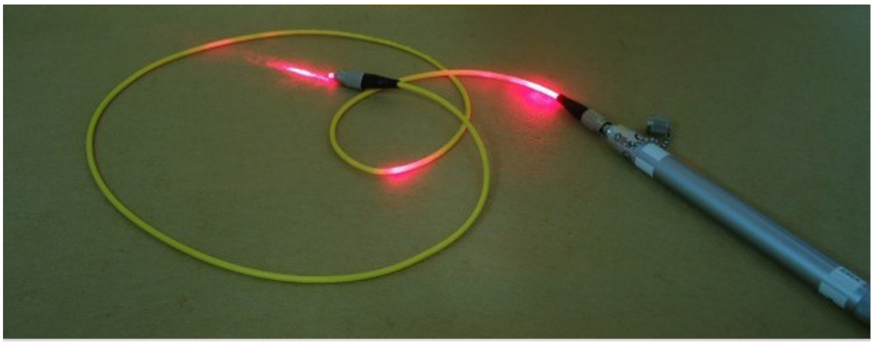
Examples of defects

One way to test a fibre optic cable is to use a visual fault locator:

- Correct optical fibre



- and damaged



The above damage most likely occurred by exceeding the bending radius of the optical fibre.

14.3. Network switches, network cards

A network switch is a device responsible for transferring data between hosts in computer networks. A host is any device connected to a computer network - a laptop, printer, television, etc.

The switch has the greatest impact on network performance. The throughput of the ports expressed in bits per second (100Mbit/s, 10 Gbit/s), i.e. how much data can be transferred to the switch in a maximum of one unit of time, is the most important factor determining the performance of a computer network.

The switch handles multiple connections between hosts simultaneously, so it is important to pay attention to parameters such as the amount of memory, processor speed and throughput. (System Switching Capacity, System Throughput Capacity).

Network cards are devices that allow a host to connect to a computer network. The basic parameter of a network card is the speed of sending and receiving data expressed in bits per second (100 Mbit/s, 1 Gbit/s, etc.). When connecting a host to a switch, it is important to remember that the network performance will be that of the device with the lowest throughput - the example of a 100 Mbps switch + 1000 Mbps network card gives a maximum throughput of 100 Mbps.

14.4. Network performance tests

Network interference

Data loss due to electromagnetic interference can occur in both wireless networks and networks using copper cables. Electrical networks, devices powered by high currents produce electromagnetic radiation.

When any part of a WiFi network is in the vicinity of equipment such as an electric traction train or tram, interference with data transmission can be expected.

Network cables made of copper are similarly affected by electromagnetic radiation. Networks where UTP cables are located too close to electrical cables can be exposed to electromagnetic interference.

If electromagnetic interference is expected in a particular location, use fibre optics as the data carrier; these are resistant to electromagnetic radiation.

Computer network performance tests

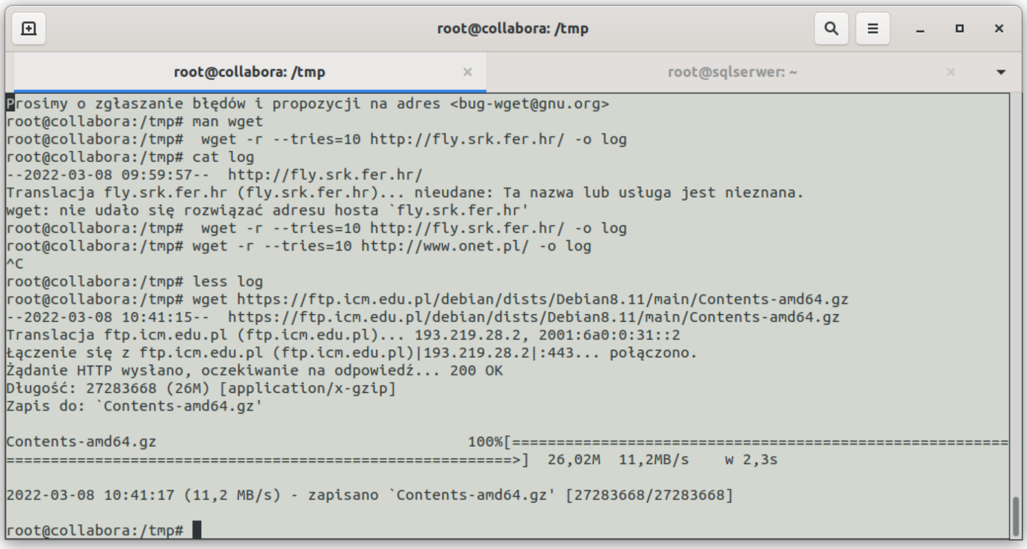
The performance of a computer network boils down to determining the throughput, i.e. the amount of information we can send over the tested network in a certain time. The simplest way to determine network performance is therefore to download/send a certain amount of data and measure the time it takes.

The results of a network performance test can be distorted by other factors that are not directly part of the computer network. When sending or downloading data, it is important to remember that it must be read and written to disk. If the computer's hard disk has a maximum read/write speed lower than the network speed, the throughput test result will not show the network performance, but only the read/write result of the data on the hard disk. In this case, we can say that the so-called "bottleneck" of our computer system is the hard disk. Another common factor that skews network performance is the download speed limits applied to file-sharing servers. Because download providers need to ensure that as many clients as possible have access to download files, they cannot allow only one client to reach the maximum download speed when downloading. File servers divide the maximum upload speed from the server to the client by the expected number of clients over a given period of time, so when downloading a file over the internet with a throughput of, say, 300Mbps the maximum transfer is, for example, 10Mbps.

To test the network throughput, we can use any program that downloads/sends data. However, in order to obtain reliable results, it should be repeated many times at different days and times. We can carry out a performance test using programmes such as wget, ping or using dedicated websites for this purpose: speeedtest.net, www.nperf.com.

wget

The wget programme is a console programme most commonly used in the Linux environment. In MS Windows operating systems from version 10 onwards, it is easy to "install" Linux using WSL (Windows Subsystem for Linux) technology. To carry out a network bandwidth test using the wget programme, issue the following command in the console (text terminal): wget https://ftp.icm.edu.pl/debian/dists/Debian8.11/main/Contents-amd64.gz , this command starts the download from the internet address: https://ftp.icm.edu.pl/debian/dists/Debian8.11/main/Contents-amd64.gz. As we can see in the image below, we get the following information: 26 MB were downloaded at a speed of 11.2 MB/s in 2.3 seconds.



```
Prosimy o zgłaszanie błędów i propozycji na adres <bug-wget@gnu.org>
root@collabora:/tmp# man wget
root@collabora:/tmp#  wget -r --tries=10 http://fly.srk.fer.hr/ -o log
root@collabora:/tmp# cat log
--2022-03-08 09:59:57--  http://fly.srk.fer.hr/
Translacja fly.srk.fer.hr (fly.srk.fer.hr)... nieudane: Ta nazwa lub usługa jest nieznana.
wget: nie udało się rozwiązać adresu hosta `fly.srk.fer.hr'
root@collabora:/tmp#  wget -r --tries=10 http://fly.srk.fer.hr/ -o log
root@collabora:/tmp# wget -r --tries=10 http://www.onet.pl/ -o log
^C
root@collabora:/tmp# less log
root@collabora:/tmp# wget https://ftp.icm.edu.pl/debian/dists/Debian8.11/main/Contents-amd64.gz
--2022-03-08 10:41:15--  https://ftp.icm.edu.pl/debian/dists/Debian8.11/main/Contents-amd64.gz
Translacja ftp.icm.edu.pl (ftp.icm.edu.pl)... 193.219.28.2, 2001:6a0:0:31::2
Łączenie się z ftp.icm.edu.pl (ftp.icm.edu.pl)|193.219.28.2|:443... połączono.
Żądanie HTTP wysłano, oczekiwanie na odpowiedź... 200 OK
Długość: 27283668 (26M) [application/x-gzip]
Zapis do: `Contents-amd64.gz'

Contents-amd64.gz                                   100%[=======================================================
=========================================================>]  26,02M  11,2MB/s    w 2,3s

2022-03-08 10:41:17 (11,2 MB/s) - zapisano `Contents-amd64.gz' [27283668/27283668]

root@collabora:/tmp# 
```

(Figure 1. Network speed test using the wget program)

We can use the wget programme to perform multiple trials simultaneously, example:

wget -r --tries=10 http://www.onet.pl/ -o log

Here we perform a recursive download (-r) of the contents of www.onet.pl , the download attempts are repeated 10 times, the results are recorded in a log file. The results stored in the log file show the time and speed of the transfer given from the web page.

ping

Another console programme available in various operating systems is ping.

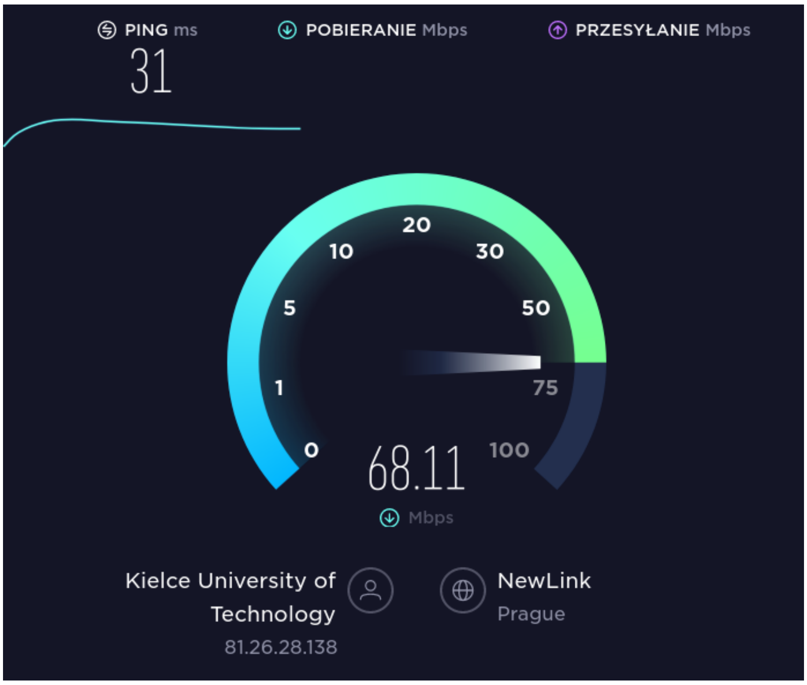
Example of network performance test using ping:

```
ping wp.pl

PING wp.pl (212.77.98.9) 56(84) bytes of data.

64 bytes from www.wp.pl (212.77.98.9): icmp_seq=1 ttl=55 time=16.0 ms

64 bytes from www.wp.pl (212.77.98.9): icmp_seq=2 ttl=55 time=15.3 ms

64 bytes from www.wp.pl (212.77.98.9): icmp_seq=3 ttl=55 time=15.2 ms

64 bytes from www.wp.pl (212.77.98.9): icmp_seq=4 ttl=55 time=15.3 ms

64 bytes from www.wp.pl (212.77.98.9): icmp_seq=5 ttl=55 time=15.2 ms

64 bytes from www.wp.pl (212.77.98.9): icmp_seq=6 ttl=55 time=15.2 ms

64 bytes from www.wp.pl (212.77.98.9): icmp_seq=7 ttl=55 time=15.3 ms

64 bytes from www.wp.pl (212.77.98.9): icmp_seq=8 ttl=55 time=15.3 ms

64 bytes from www.wp.pl (212.77.98.9): icmp_seq=9 ttl=55 time=15.3 ms

64 bytes from www.wp.pl (212.77.98.9): icmp_seq=10 ttl=55 time=15.3 ms

64 bytes from www.wp.pl (212.77.98.9): icmp_seq=11 ttl=55 time=15.2 ms

64 bytes from www.wp.pl (212.77.98.9): icmp_seq=12 ttl=55 time=15.2 ms

64 bytes from www.wp.pl (212.77.98.9): icmp_seq=13 ttl=55 time=15.2 ms

--- wp.pl ping statistics ---

13 packets transmitted, 13 received, 0% packet loss, time 12015ms

rtt min/avg/max/mdev = 15.185/15.307/16.032/0.212 ms
```

In the example above, an ICMP Echo Request packet was sent to the server with the address www.wp.pl 13 times and the same number of replies were received (ICMP Echo Reply). The last line of the example (min/avg/max/mdev = 15.185/15.307/16.032/0.212 ms) contains the result of a test of the speed of transmission of a packet through the network - the smaller the response times, the more efficient our network is.

speedtest.net

There are also web applications for testing upload/download speeds. At https://www.speedtest.net we can perform a test showing both the PING value and the upload and download speeds. The figures below show screenshots of an internet upload test between a network in Kielce (Poland) and a network in Prague (Czech Republic).



PING ms 31

POBIERANIE Mbps

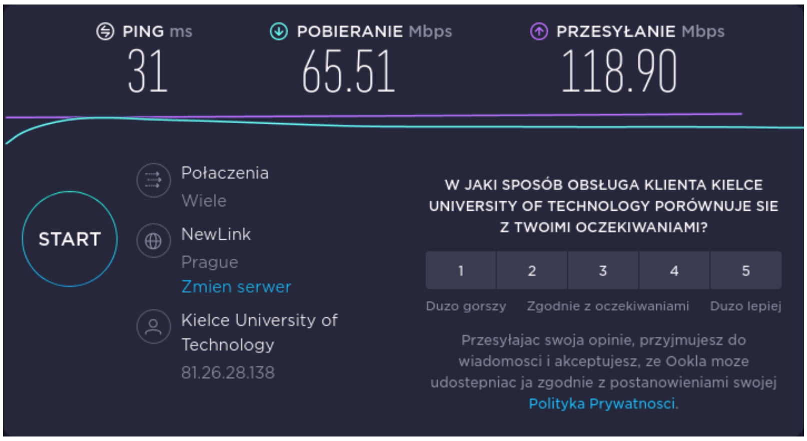
PRZESYŁANIE Mbps

68.11 Mbps

Kielce University of Technology
81.26.28.138

NewLink
Prague

(Figure 2. Network speed test using speedtest.net)



PING ms 31

POBIERANIE Mbps 65.51

PRZESYŁANIE Mbps 118.90

START

Połaczenia
Wiele

NewLink
Prague
Zmien serwer

Kielce University of Technology
81.26.28.138

W JAKI SPOSÓB OBSŁUGA KLIENTA KIELCE UNIVERSITY OF TECHNOLOGY PORÓWNUJE SIE Z TWOIMI OCZEKIWANIAMI?

1 2 3 4 5

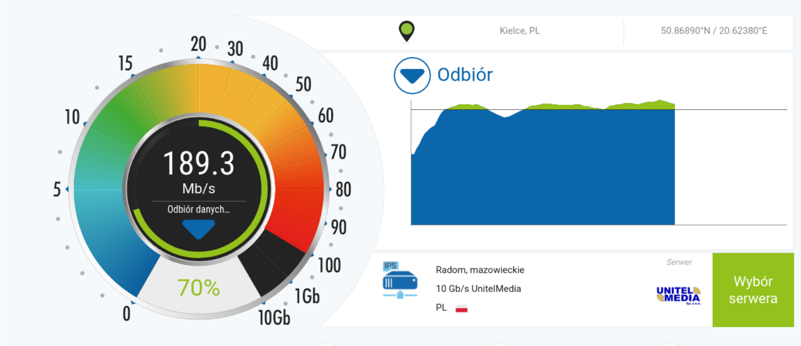
Duzo gorszy | Zgodnie z oczekiwaniami | Duzo lepiej

Przesyłajac swoja opinie, przyjmujesz do wiadomosci i akceptujesz, ze Ookla moze udostepniac ja zgodnie z postanowieniami swojej Polityka Prywatnosci.

(Figure 3. Result of the network test using speedtest.net)

www.nperf.com

The npref.com web application is similar to speedtes.net. The results are also presented in an attractive graphical form.



189.3 Mb/s
Odbiór danych...

Kielce, PL | 50.86890°N / 20.62380°E

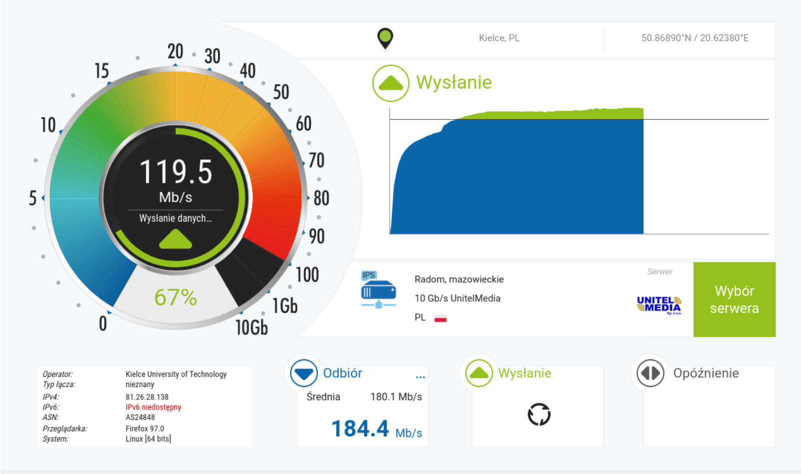
Odbiór

Radom, mazowieckie
10 Gb/s UnitelMedia
PL

Serwer

Wybór serwera

(Figure 4. Network speed test with www.nperf.com)



119.5 Mb/s
Wysłanie danych...

Kielce, PL | 50.86890°N / 20.62380°E

Wysłanie

Radom, mazowieckie
10 Gb/s UnitelMedia
PL

Serwer

Wybór serwera

Operator:	Kielce University of Technology
Typ łącza:	nieznany
IPv4:	81.26.28.138
IPv6:	IPv6 niedostępny
ASN:	AS24848
Przeglądarka:	Firefox 97.0
System:	Linux [64 bits]

Odbiór ...
Średnia 180.1 Mb/s
184.4 Mb/s

Wysłanie

Opóźnienie

(Figure 5. Network speed test with www.nperf.com)

14.5. Limiting network traffic using the example of a "home" router

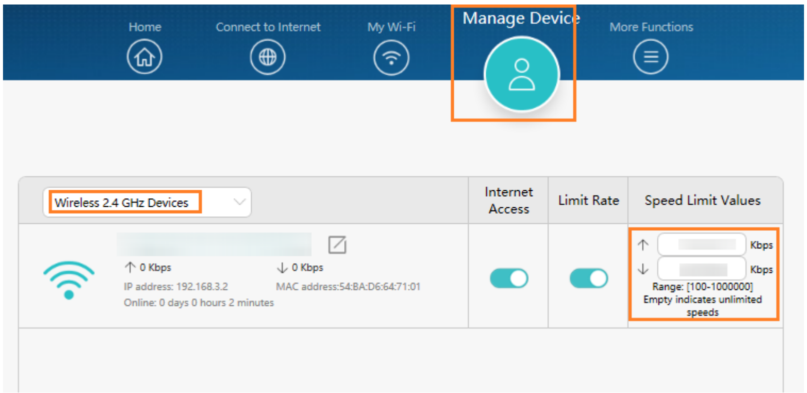
The router connects the home (company) network to the Internet. On the router, we can limit the speed, disable internet access to local hosts. Exclusions and traffic restrictions can be either permanent or activated for a specific period of time.

In a "home" router, i.e. a cheap device designed to serve a network consisting of several to several dozen hosts, we can disable access and limit download and upload speeds. The possibilities for limiting network traffic depend, of course, on the router model.

The purpose of introducing a transfer speed limitation is to protect against a drop in download or upload speeds on key hosts in our home network. For example, if we assume that our laptop, on which we are doing remote work, should have a stable connection to the Internet during a teleconference, we would introduce speed limits for all other devices.

Example of enabling speed limits in a Huawey Wi-Fi router:

1. Connect your computer/phone to the Wi-Fi router (check the nameplate on the bottom of the router for the default Wi-Fi name, no password) or connect your computer to the router's LAN port using an Ethernet cable. Enter the default IP address in the browser address bar and log in to the web-based management page (check the default IP address on the nameplate on the bottom of the router).
2. Click Manage Device, select the phone or computer for which you want to set a limit, enable the Limit Speed option and click the icon under Speed limit Values to set the maximum upload and download speed.



Wireless 2.4 GHz Devices

↑ 0 Kbps ↓ 0 Kbps

IP address: 192.168.3.2 MAC address:54:BA:D6:64:71:01

Online: 0 days 0 hours 2 minutes

(Figure - Device configuration screen, source: https://consumer.huawei.com/en/support/content/en-us15806295/)

15. Basic tests of computer networks

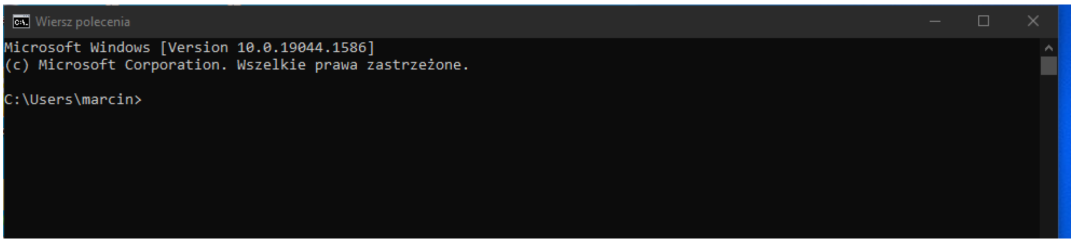
Computer network tests in MS Windows and UNIX-Like environments using programs:

- ping
- tracert
- telnet
- nc
- wget

All of the above programs are started by typing a command in the terminal / command line.

On a Linux operating system running the graphical desktop environment / macOS, you will need to start a terminal to execute commands typed in from the keyboard. Commands are entered in a terminal window.

In the MS Windows operating system, to execute a command typed from the keyboard you need to start the command line. To start the command line in Windows 10/11 click "Start" and in the search window type cmd .



```
Microsoft Windows [Version 10.0.19044.1586]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\marcin>
```

15.1. ping

The ping programme is used to diagnose network connections. We use it to check the quality of the connection between the computers sending requests and sending back a reply.

Ping will answer the following questions:

- Is there a connection between the computers?
- What is the response time for a sent packet?

Run the program at the MS Windows command line (Linux/Mac terminal). At the command line type: ping [IP or name] and confirm by pressing Enter.

An example of how the ping program works in Linux:

```
ping 10.10.10.1

PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.

64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=0.364 ms

64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.274 ms

64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.433 ms

64 bytes from 10.10.10.1: icmp_seq=4 ttl=64 time=0.545 ms

64 bytes from 10.10.10.1: icmp_seq=5 ttl=64 time=0.380 ms

64 bytes from 10.10.10.1: icmp_seq=6 ttl=64 time=0.284 ms

64 bytes from 10.10.10.1: icmp_seq=7 ttl=64 time=0.477 ms

64 bytes from 10.10.10.1: icmp_seq=8 ttl=64 time=0.257 ms

^C

--- 10.10.10.1 ping statistics ---

8 packets transmitted, 8 received, 0% packet loss, time 7154ms

rtt min/avg/max/mdev = 0.257/0.376/0.545/0.099 ms
```

In the example above, an ICMP Echo Request packet was sent 8 times and the same number of replies (ICMP Echo Reply) were received. The packets were sent from the computer with IP 10.10.10.2 to the computer with IP 10.10.10.1. The average response time is 0.376 milliseconds.

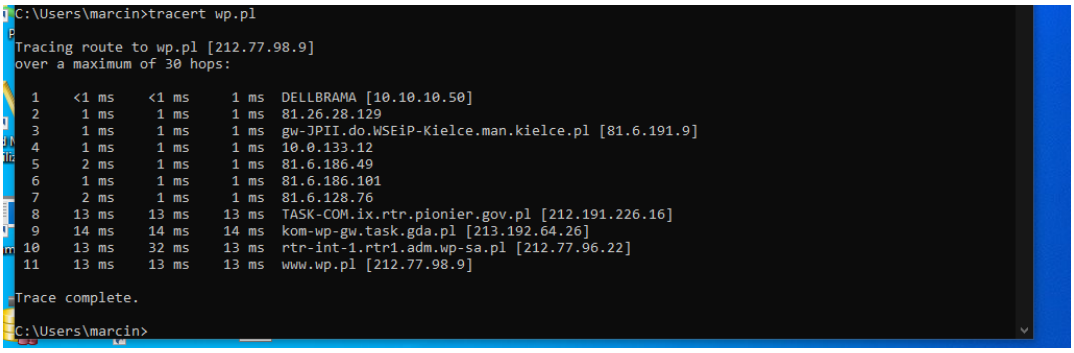
15.2. tracert

Tracert is a programme for determining the routing (route) of packets on an IP network to tracert (MS Windows) / traceroute (Linux/macOS)

Tracert/traceroute returns a list of consecutive routers on the route to the target computer on the network.

The longer the route - the greater the number of routers - the more difficult it is to communicate with the target computer on the network. If there is a badly configured router on our route, we will have difficult access to the computer in question (slow-loading website, errors when downloading files, poor quality of Internet radio, etc.).

Example of examining a route from the university premises to wp.pl server:



```
C:\Users\marcin>tracert wp.pl

Tracing route to wp.pl [212.77.98.9]
over a maximum of 30 hops:

  1    <1 ms    <1 ms     1 ms  DELLBRAMA [10.10.10.50]
  2     1 ms     1 ms     1 ms  81.26.28.129
  3     1 ms     1 ms     1 ms  gw-JPII.do.WSEiP-Kielce.man.kielce.pl [81.6.191.9]
  4     1 ms     1 ms     1 ms  10.0.133.12
  5     2 ms     1 ms     1 ms  81.6.186.49
  6     1 ms     1 ms     1 ms  81.6.186.101
  7     2 ms     1 ms     1 ms  81.6.128.76
  8    13 ms    13 ms    13 ms  TASK-COM.ix.rtr.pionier.gov.pl [212.191.226.16]
  9    14 ms    14 ms    14 ms  kom-wp-gw.task.gda.pl [213.192.64.26]
 10    13 ms    32 ms    13 ms  rtr-int-1.rtr1.adm.wp-sa.pl [212.77.96.22]
 11    13 ms    13 ms    13 ms  www.wp.pl [212.77.98.9]

Trace complete.

C:\Users\marcin>
```

In the example above, we see 11 nodes (routers)

15.3. telnet

Telnet is the program used to connect to a remote server. Telnet is installed on server-class computers, but is also widely used on all kinds of network devices (e.g. switches, AccessPoint).

You can use telnet to check whether a particular service, e.g. SMTP, HTTP, is running on the remote computer.

To check the connectivity between the client computer and the server on the command line (terminal), issue the command:

telnet [address of server under test] [port of service specified].

If you want to check if there is a working STMP server on the computer www.nasa.gov and you will be able to connect to it from your computer and send mail, issue the command:

telnet www.nasa.gov 25

where 25 is the number of the TCP port on which the SMTP service (sending mail) listens.

15.4. nc

Netcat (nc) is a command executed in a terminal. It is available on Linux and macOS It can be used to test the operation of multiple TCP ports on a remote server simultaneously.

Example:

in Linux trminal I type:

nc -z -v 10.10.10.1 22

The command returns the result:

Connection to 10.10.10.1 22 port [tcp/ssh] successful!

This means a successful connection to host 10.10.10.1 on TCP port 22

15.5. wget

Wget is a console programme that is used to download files. Wget returns the download speed so we get information about the download performance of our internet connection.

Example:

In the terminal I type:

```
wget https://download.moodle.org/download.php/direct/stable311/moodle-latest-311.tgz -O moodle-latest-311.tgz
```

This means that I will be downloading a file from the server https://download.moodle.org, I will save the downloaded file under the name **moodle-latest-311.tgz**

After issuing the command in the terminal, wget returns the following:

```
--2022-03-31 11:31:57-- https://download.moodle.org/download.php/direct/stable311/moodle-latest-311.tgz

Resolving download.moodle.org (download.moodle.org).... 104.22.64.81, 104.22.65.81, 172.67.26.233, ...

Connecting to download.moodle.org (download.moodle.org)|104.22.64.81|:443.... connected.

HTTP request sent, awaiting response... 200 OK

Length: 60212386 (57M) [application/g-zip].

Saving to: 'moodle-latest-311.tgz'

moodle-latest-311.tgz 100%
[============================================================================================
57.42M 11.0MB/s in 5.2s

2022-03-31 11:32:03 (11.1 MB/s) - 'moodle-latest-311.tgz' saved [60212386/60212386].
```

We can see the speed at which the file was downloaded - 11.0 MB/s