evropský sociální fond v ČR

EVROPSKÁ UNIE

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

OP Vzdělávání pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PřF UHK“

Registrační číslo: CZ.1.07/2.2.00/28.0118

Computer Network

Jiří Jelínek

Hradec Králové 2012

Introduction

The purpose of the presented text is to provide the basic material for people interested in studying a Computer Networking Course.

This course introduces the principles on which current information and communication technology is based. Students get an idea of how a computer network functions during common tasks that are often used nowadays, such as file transfer or loading a webpage. Students also learn (receive an overview about) the abbreviations used in computer network terminology. Lastly students get a preview in the entire computer network field, its history, meaning development from the very beginning to the present time.

This text is designed as an introduction to the different areas of this field but its aim is not to make people experts in computer designing and computer network management. After studying the presented material, one will have the basic knowledge and skills needed to build a computer science or programming course, for which the knowledge of a computer network is needed.

Table of Contents

3 Topology and Types of Computer Networks 15 pages total

4 Physical Layer of Computer Networks 20 pages total

5 Ethernet 26 pages total

6 Internet 23 pages total

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PřF UHK“

Registrační číslo: CZ.1.07/2.2.00/28.0118

1 The Development of Computer Networks

1.1 Motivation for the Development of Computer Networks

Communication between people is stated to be the initial goal for creating the network. The starting point, similar to the majority of other fields, was in military, scientific and academic environment.

In the 1940s-1950s, the idea of interface for programming computers was gradually coming into existence. The original arrangement of the computer (processor controlling a programmable memory) with punched cards as input and output of the computing tasks was heading for the current model, using a monitor and a keyboard for interactive work. A printer can be, for example, an output. The mouse was invented by Douglas Engelbartem at the Stanford Research Institute in 1963. It took another 5 years before the device was presented to the public and another two years, before Douglas Engelbart got his invention patented (in 1970).

In effort to build a machine for the processing of information in the amount allowing, for example, numerical computation, sorting data or searching for it, large machines with large power consumption, high acquisition and operating costs were built by scientists.

These machines had only limited usage. The solution was to create multiple terminals meaning "monitors with keyboards". The transfer of information between the terminal and the main device was gradually universalized to a model where the terminal consists of simple computer processing information from the keyboard and generates the signal to the monitor.

Information between the terminal and the main device were gradually transferred by a more general communication line (port), (for example, through a telephone network).

The term “user account” comes from this period. It was a paid service to work with a supercomputer and assign a calculation to it. Computers were soon equipped with a multi user environment and the information in them and multiple people had access to them. The result of it was that they could communicate with each other.

The arrangement of the supercomputer and a terminal was not computer network yet, but even then, it was used for communication among people (for example, sending an e-mail with an option to attach a file with required results delivering to the addressee).

We can say that computer networking started when people managed to link then supercomputers together. Linking four computers was implemented in 1969. The aim was to test the proposed multi-layer architecture and a technique of data frame works (packets, packages). That type of network was named ARPANET. The gained experience resulted in a proposal for building Internet as we know today.

1.2 The Use of Computer Networks

1.2.1 The Use of Large Computers

The original motivation for creating computer networks is still valid. (assigning the computing tasks to large computers). From today's perspective, it is just an application of current networks.

1.2.2 Communication

We talk about communication among users. The dominant usage of global computer network, communication among programs, distributed applications

1.2.3. Resource Sharing

Data sharing and common disk space. In the 1980s and 1990s idea of diskless workstations, simple modern diskless terminals, data on the target network, was widespread.

Availability of the storage media relegated this vision indefinitely. However, nowadays, the amount of data which are stored outside of the computer with which we are working at the moment as been increased (maps, timetables, social networks, Google doc etc.).

Sharing technical resources, expensive peripherals, printers and large capacity is timeless (was used in the past and today).

1.2.4 Higher Reliability

Backing up, deliberate redundancy implemented through computer network.

1.2.5 Cost Savings

Fast computer network allows sharing resources efficiently. More easily accessible computers are faster and cheaper than one super machine.

We do not construct super machines as separate powerful computers anymore. There are grids and clusters built instead. The exception is the mainframe platform.

1.3 Levels of Computer Integration

1.3.1 Supercomputer

Supercomputer enables users to communicate (terminals can be geographically distant). Programs communicate directly, for example, through operating system functions.

In the case of the supercomputer it does not necessarily need to be a computer network (there is only one computer; terminals can be connected by ports without computer network, as we know it today).

Since 2000 the „Renaissance“ of the Mainframe Platform came into existence (everything is on one large supercomputer), of course, in this case, the computer network is used.

1.3.2 Separate computers

Separate computers are rarely used, for example especially programmed controlling computer (these are mostly simple computers).

1.3.3 Computer Network

It is a group of autonomous, interconnected (communicating) computers. It is a widespread version. However, it is common that today's computers with greater computing power than supercomputers used to have a few years ago, become only terminals nowadays, for example, via the Web interface.

1.3.4 Distributed System

A group of computers acts as a compact unit (the user normally does not know at which machine his task was processed).

The term cluster is used when a distributed system implemented on normal PCs with a different performance, different availability, different architecture, different operating system and does not require the machines to be constantly available and running. The term grid is also frequently used.

2 Architecture of Computer Networks

2.1 Layers as a Base of Architecture

The development of standardization of a communication network began in the 1970s, when the first major computer networks came into existence, built according to the specific conceptions of leading computer manufacturers. Soon a need for a unified standard that would have been able to link the computer systems of different types and concepts came, originating from different producers.

While computers can dynamically evolve, reversals in the development can occur relatively often. Some procedures may be revised or canceled (for example, the established ceiling of memory in the MSDOS and its subsequent withdrawal) and replaced with completely different procedures. There is nothing like that possible in the field of computer networks.

Earlier and even today, computers with completely different processors, operating systems and especially concepts developed by different companies, were connected by computer networks. If we introduce a procedure in the field of computer networks, it is clear that it will be used for a long time, because it is not going to be a matter of one producer, but it will connect the older, current and future technologies.

For example, the analog phone didn’t undergo any significant alterations despite the rapid development of electronics and the complete transformation of telephone exchange. The dialing system was changed, with better devices, for example, caller ID was added.

The rest remained essentially unchanged, except the voltage level of signals, twisted pair cable and power supply.

In case of computer networks, we can say that the network and transport layer has been basically unchanged for last 30 years, but the time for a change is coming soon. On the other hand, the physical layer and the connecting layer have been fundamentally modified many times in certain areas.

2.2 Principle of the Layered Network Model

Communication is carried out by a protocol of a given layer. A separate team of engineers can focus on the development of a given layer and can change it in a certain way. For example, the function of the telegraphers can be modified (upgraded) by replacing the translator. The whole architecture has preserved its structure even after these changes. See the picture.

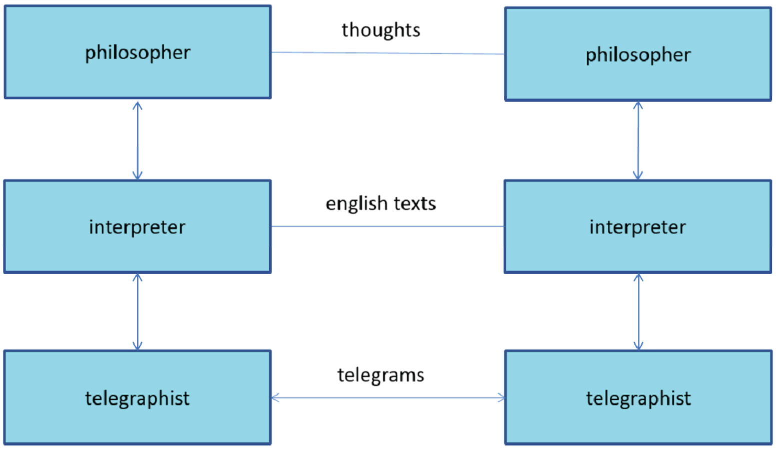


Figure 2.1 – Communication in three-layer setting-structure

2.3 Terminology Related to Segmentation into Layers

2.3.1 Protocol

Two computers on the same layer communicate though a Protocol (headers, questions, responses, etc.). Messages are passed to the child layer. The protocol is independent of the implementation and allows mutual cooperation (so called interoperability).

2.3.2 Interface

Interface is a definition of services offered to the parent layer. Implementation is directed by a protocol and the upper layer knows nothing about it. Interface depends on implementation (for example OS).

2.3.3. Headers

Every query passed to the lower layer is considered to be data with a header. We say, therefore, that we add and remove headers. A typical example from practice can be encapsulation of IP frame into an Ethernet packet (communication and transport layer interface heads down).

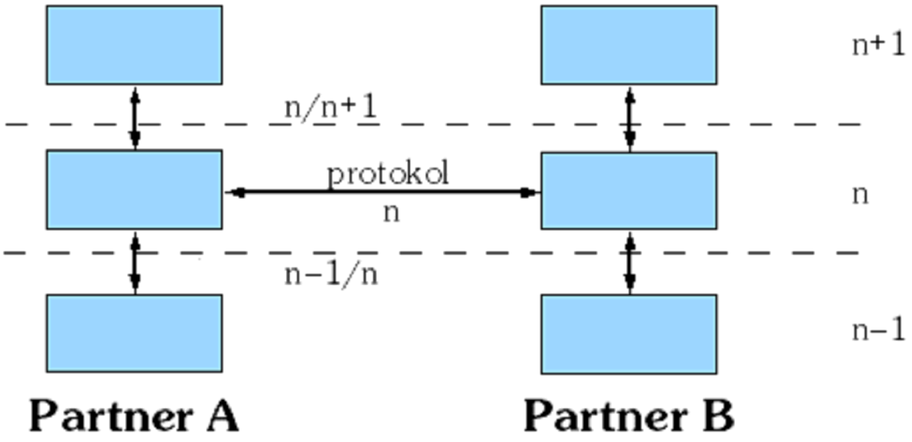


Figure 2.2-Interface and protocol in layers of a computer network

2.4 Connection-oriented and Connectionless Services

2.4.1 Connection-oriented Services

Connection-oriented Services function on a similar principle as a telephone system. If you want to speak with someone over the phone, you must first dial his number and he must answer your call by lifting up the handset. This is the way connection happens between you and another with the result of mutual communication and will cease at the end of the call when we put down the receiver.

In the case of two entities on the same level that want to communicate with each other it works the same way – they must first be connected. Once this connection is established, it basically acts as a pipe – a sender puts into it what he wishes to transmit to the side and the recipient receives it on the other side in the same order.

Connection-oriented services

- Establishes a connection and then the data run through (just as with a phone).
- It adheres to the order of frames.
- It has smaller claims (to the application layer).

2.4.2 Connectionless Services

Connectionless Service, on the other hand, can be compared to a normal service of letter delivery. This service doesn't count on the establishment of the connection between the sender and the recipient, but instead considers the individual parts of data transition (the message) as separate units, bearing the address of the ultimate consignee, and delivers them independently of other messages. Individual messages may therefore be principally transmitted through different ways, so it can happen that when you receive it, the correct order does not need to be preserved– which never happens with connection-oriented services.

Connectionless service

- Every packet is conveyed separately (as separate letters).
- It is more flexible and robust, reacting to changes in the network.
- It is more versatile and better reflects the nature of networks.

2.4.3 Theory and Practice

Transmissions in local networks usually have a connectionless character. The original version of the ISO/OSI reference model (see below), however, counted only with connection-oriented services and protocols and implementation of connectionless protocols was carried out subsequently.

2.4.4 Reliability of the Offered Service

Reliable Service is one that never loses any data.

This service is run through the appropriate mechanism of confirmation (when the recipient confirms the successful delivery and request again data that has been received incorrectly). However, it is associated with a certain overhead that may not always be desirable. Consider, for example, the transmission of digitalized sound.

It is certainly more convenient to sometimes accept bad data (i.e., somehow distorted sound) than to accept outages, caused by endorsement or retransmission of malformed data.

Therefore, unreliable services have their place, however, it is somewhat misleading designation. It is appropriate to understand them more like services which have a high degree of reliability, however, do not provide a 100 percent guarantee of the successful transfer.

2.5 Reference Model of Open System Interconnection

Model ISO/OSI is a reference communication model indicated by the acronym of the title "International Standards Organization / Open System Interconnection".

This is the recommended model defined by ISO in 1983, that splits the mutual communication among computers into seven related layers. These mentioned layers are also known as “a set of protocol layers”.

The task of each layer is to provide services to the next higher layer and not to overload the higher layer with details about how the service is, in fact, carried out. Before data is moved from one layer to another, they are split into packets.

Supplementary information is added to a packet (formatting, address) in each layer that is necessary for successful transmission over a network.

Table 2.1 – Reference Model ISO/OSI

	Data Units	Layer	Function
Host layers	Data	7. Applicational	Network processes and applications
		6. Presentational	Encryption and Representation Data
		5. Relational	Interhost Communication
	Segment	4. Transporting	End -to-End Connection and reliability (TCP)
Media layers	Packet/datagram	3. Network	Rating and Logical addressing (IP)
	Frame	2. Linking	Physical addressing (MAC & LLC)
	bit	1. Physical	Media, signal, binary transmission

2.6 Layers of ISO/OSI Reference Model

2.6.1 Physical Layer

Physical layer defines the means for communicating with the transmission medium and with the technical means of the interface. It also defines the physical, electrical, mechanical and functional parameters relating to the physical connection of individual devices. It is hardware.

2.6.2 Data Link Layer

Data link layer provides the integrity of the data flow from one network node to another. As part of this activity, data block synchronization and management of their flow is executed. It is hardware.

2.6.3. Network Layer

Network layer defines protocols for routing data, through which the transmission of the information to the desired destination node is ensured. We do not need it in the local network if there is no routing. It is hardware but when routing is resolved by a PC with two network cards, it is known as software

2.6.4. Transport Layer

Transport layer defines protocols for structured messages and ensures error-free transferring (performs some error checking), for example, the splitting of the file into packets and their acknowledgment. It is software.

2.6.5 Session Layer

Session layer coordinates communication and keeps the session as long as it is needed. It also ensures security, login and administrative functions. It is software.

2.6.6 Presentation Layer

Presentation layer specifies the way the data is formatted, presented, transformed and encoded. For example, writing accents, CRC, compression and decompression and data encryption. It is software.

2.6.7. Application Layer

Application Layer is the highest layer in the model. It defines the way in which applications communicate with the network, such as database systems, electronic mail, or programs for terminal and emulation. It uses the services of lower layers, and due to that it is isolated from the problems of network technical resources. It is software.

2.7 History of ISO/OSI Reference Model

The first computer networks as we know them today were built for routine operations on commercial principles, not for experimental purposes. Those started to be built sometime in the mid-1970s when the first products designed for these networks were seen in the market. The problem was in the fact, that the appropriate products were solely proprietary (i.e., specific for a particular producer) and did not support any interoperability.

This was the solution, offered by large companies (mostly IBM and DEC) and produced by particular interests, ideas and traditions of the appropriate companies (for example IBM conceived its network architecture SNA more like the building of large terminal networks connected to their mainframes). What the market was missing was such network architecture sufficiently open, therefore, independent of the particular producers, widely accessible in their specifications, offering the required compatibility and mutual interoperability of design from various producers, being able to open space for competition (and on the other hand not creating a dependency of the customer on a single "exclusive" supplier).

The task to create such independent architecture was eventually taken care of voluntarily by the international standards organization ISO (International Standards Organization: International Organization for Standardization), associated national standards organizations of the majority of developed countries in the world. Initially, the intention was to create a unified standard for the functioning of the open systems; that is, actually, for the operation of all computers as such, without necessarily being plugged into some network nodes. It was supposed to be called "Open Systems Architecture" (literally: the architecture of open systems), but, of course, soon it was obvious that something like that is beyond the possibilities of the time (and certainly even today, despite considering the effectiveness). Therefore, the people from the ISO adjusted their views, in particular point that they will not deal with the functioning of computers as such, but only in regards to their mutual communication.

Opulent "Open Systems Architecture" project thus become a more realistic one called "Open Systems Interconnection Architecture" (literally: “the architecture of networks interconnection”).

In the end, it was necessary to make concessions from this limited vision. The reason was the approach of people of the Organization. They were refusing to accept developed and standardized solutions from somewhere else, but only used what they themselves approved and released as their own standard (they actually didn’t trust in anyone else’s competency). Due to that and other factors, the progress of development slowed down so much that they could soon see a necessity to make other concessions: not to proclaim everything as a real network architecture, including all the protocols, but only as a certain empty frame - as an idea of how many hierarchical layers should be there and what they are supposed to do, but without specific protocols that would fit into these layers (with a plan that these protocols will be worked out gradually, depending on how the work on development will continue).

As a result of that the name had to be changed again. The temporary name "Open Systems Interconnection Architecture" has eventually changed to "Reference Model for Open Systems Interconnection" (literally: „the reference model for interconnecting of open systems").

The phrase "reference model" is used in the title for emphasizing the fact that it is a general concept, a pattern, a framework, in fact a model (not a specific and strictly defined prescript), which will be during time filled with specific directions (protocols), depending on how these will be available.

2.8 OSI RM Layers and Internet Architecture

The concept of the Internet as we know it (IPv4, see separate chapter about the Internet) dates back to the years 1974 to 1979 and standardized in January 1980.

OSI Recommendation is used only partly. However, in a very appropriate manner (the IP was designed before OSI RM). The lower layers are not standardized. From the beginning, the usage of existing technologies is expected, but there is room for dynamic development. Similarly, it is with non-standardizing of the presentation and application layers (session layer affiliates to transport and associate one).

The fundamental requirement when designing TCP/IP model was the possibility to mutually link such networks, that were built on completely different principles and transmission technologies, via TCP/IP protocol (such as Ethernet, Token Ring, later FDDI and ATM, networks with 2-points connections, etc.).

Since the beginning, there wasn't a complex network technology, but merely a bridge among existing technologies, that‘s why the Internet as we know it succeeded in the competition of other proposals.

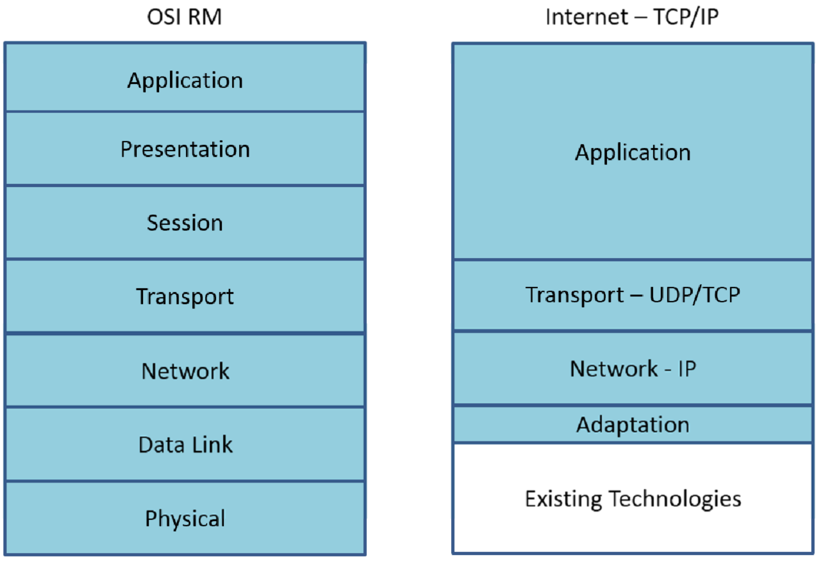


Figure 2.3 – OSI RM and the architecture of the Internet

2.8.1 Existing Lower Layers (Existing Technologies)

Main idea: its not necessary to reinvent the wheel. The developers of the Internet Protocol didn't standardize lower layers. This approach has significantly contributed to the fact that in 1983, when approximately 1000 computers were linked through IP, the phenomenon of the Internet came into existence.

It became clear that higher layers are timeless and lower (physical, linked layers) will be developing and variable as time goes (the same way as hardware and computer operating systems).

2.8.2 Adaptation Layer

This layer is sometimes called "A Network Interface Layer". A layer always resolves only the issue of how to transmit IP in the lower-layer technology.

The task is to cover up possible specifics of the particular network technologies and create for them a single environment offering a unified service and a unified way of addressing, etc.

Unlike the higher layers, it is not filled by any protocols in the framework of TCP/IP, contrarily it tries to adapt to existing solutions (e.g. Ethernet).

For a new technology, it is enough to define how to transport IP on it and it is possible to use the new technology immediately. For the higher layer then, it is irrelevant whether Ethernet is the physical layer or data frames. They had to overcome the route, for example, via ADSL, WiFi, etc.

2.8.3 Network Layer

Similarly as with the ISO/OSI model it provides routing. However, it provides a connectionless transmission using a simple datagram service. It does not deal with the reliability of the transmission. It should focus on the fastest possible data transfer.

The Internet Protocol (IP) works on this layer. It is connectionless and without warranties. It means that it tries to transmit flawlessly, but if it fails it loses or damages something somewhere and does not consider it as its duty to take care of fixing it (instead it expects higher layers to provide help).

Its connectionless nature is due to the fact that the transmission of data does not establish a direct link between the sender and the recipient; instead it sends all the data "to the middle of nowhere".

Internet Protocol Layer holds the entire Internet together, ensures the ability of different systems to interact with each other, provide services and achieve synergies (so-called Interoperability).

2.8.4 Transport Layer

It ensures communication among the end parties i.e. via the interface of the operating system directly between application programs.

According to their requirements and demands, the layer can regulate the data flow in both directions. There are two Protocols working in these layers -TCP and UDP.

Protocol TCP (Transmission Control Protocol) provides connection-oriented and reliable services, thereby changing the nature of the network layer services.

Protocol UDP (User Datagram Protocol) provides a connectionless service with no guarantees (retains the nature of network layer services).

2.8.5 Application Layer

Internet Architecture is very strict compared with the reference ISO/OSI model. These are protocols of specific applications.

The authors of the TCP/IP came to the conclusion that the requirements for supportive services (such as services for the conversion of transmitted data, correct sessions course, etc.) will be less frequent and that applications that will not use from these services, will be more common.

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PřF UHK“

Registrační číslo: CZ.1.07/2.2.00/28.0118

3 Topology and Types of Computer Networks

3.1 Technical Resources for Computer Networks

3.1.1 Connected Computers and Servers

This group includes: peripherals, data storage, measuring instruments, security devices, VoIP phones equipped with a network adapter (which is also called a network interface card or NIC-Network Interface Controller).

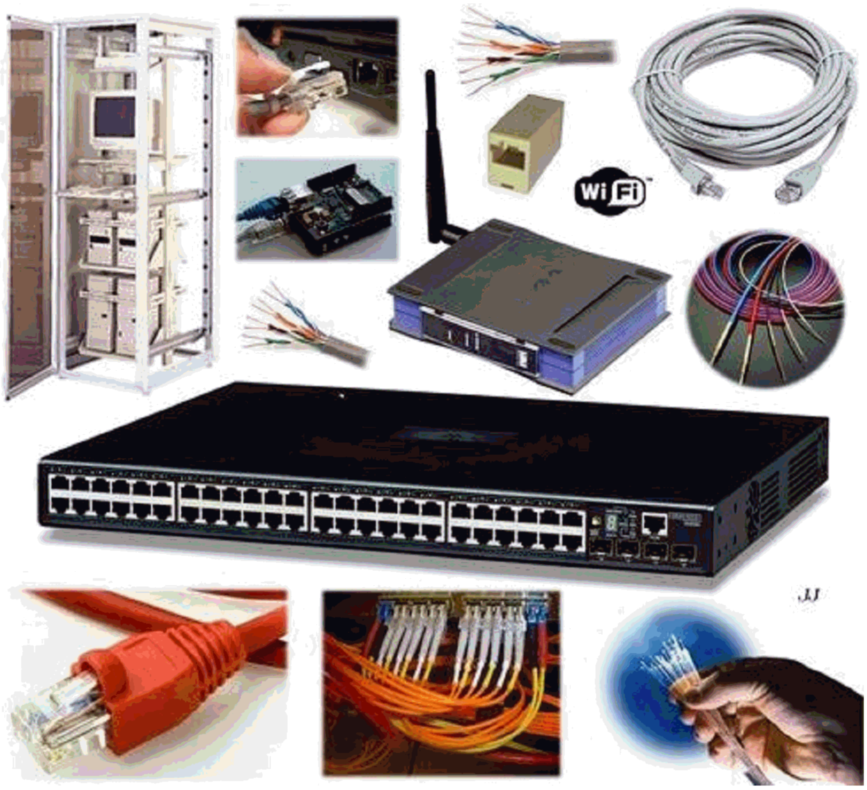


Figure 3.1 – Typical hardware items that form a computer network

3.1.2. Connections (cables, lines, channels)

This group consists of copper wires (twisted pair cable, coaxial cable), optical cables, radio wireless connections, wireless optical connections (mostly laser ones, infrared). More will be said about this field in a separate chapter - the physical layer of computer networks.

3.1.3 Active Elements (Switching Elements)

Network hub (hub, a concentrator) - only amplifies the signal and allows implementation of a bus (bus topology) despite the fact that connections are two-point and physically connected in the star. It has almost zero delay out of all active elements. It combines several network segments into one. The operation in one part of the network is transferred to the other parts and therefore unlike the switch, it engages the entire network. This group also includes the network bridge – it connects two physically separated network segments, it can change the interface (mediaconvertor), for example, Ethernet - WiFi, Ethernet - DSL. Hub is commonly used in the industrial Ethernet.

Switch -connects at least two devices within a single network segment or in the frame of multiple segments, separates the network traffic and delivers packets to specific addresses, which unlike the hub does not burden the other parts of the network. Compared to the hub, it complicates network monitoring (higher class switches allow monitoring and diagnosis by using a special port).

Router - redirects the communication to another segment of the same network type, for example, it can transfer data between two physically separate Ethernet networks through TCP/IP level of communication (it acts as a computer in both networks - with a different IP address in each of them and with a different address of the physical layer). It can easily become a firewall.

Repeater – it fixes and amplifies a damaged signal and passes it further properly timed.

Modem (modulator and demodulator) as well transceiver (transmitter and receiver) is technically more complicated version of the media convertor. Modem is used for overcoming the difficult route (telephone line). Transceiver links a long two-point connector, for example, among buildings.

3.1.4 Terminology - Framework and Packet

Framework is a link-layer level block of data consisting of a header, footer and transferred data. The header contains the MAC address of the sender and the recipient.

Packet is a network level block of data, possibly of a higher level. Packet includes a network address (typically an IP address) of both the participants and information needed for confirmation and the control flow.

3.2 Types of Networks According to their Range

3.2.1 LAN (Local Area Network)

The local computer network is characterized by the fact that computers are linked/connected at the smaller geographical territory (i.e., within the company, the building, room, etc.).

LAN mostly uses switched Ethernet (a twisted pair cable, optical fiber) extended by WiFi (IEEE 802.11).

- Since its origin has been working at high speed (10 Mb/s to 10 Gb/s).
- Primarily intended for sharing resources.
- Low error rate.

3.2.2 WAN (Wide Area Network)

It is a communication network that covers a large territory, as is the connecting of countries and continents.

Internet is the largest and best known public WAN. The physical layer consists of rented cabling (fiber optic, microwave links, satellites), the most today used technology is Frame Relay.

- Large range of speeds (64 Kb/s to 10 Gb/s).
- The error rate is dependent on technology.

3.2.3 The Differences between LAN and WAN

Various literary sources compare LAN and WAN networks. They consider speed, range, reliability, etc.. Various other acronyms can be found – PAN, MAN, etc. (see additional text).

The benefits and importance of such divisions are questionable (for example, it cannot be claimed that local networks are faster because the speed of backhauls are usually even higher).

Designation LAN and WAN is nowadays often used for routers providing security protection of local area network (firewall). (see Figure 3.2).

Generally, it can be said that LAN network is linked through WAN network to ensure a communication over great distances with servers located in the WAN (Internet).

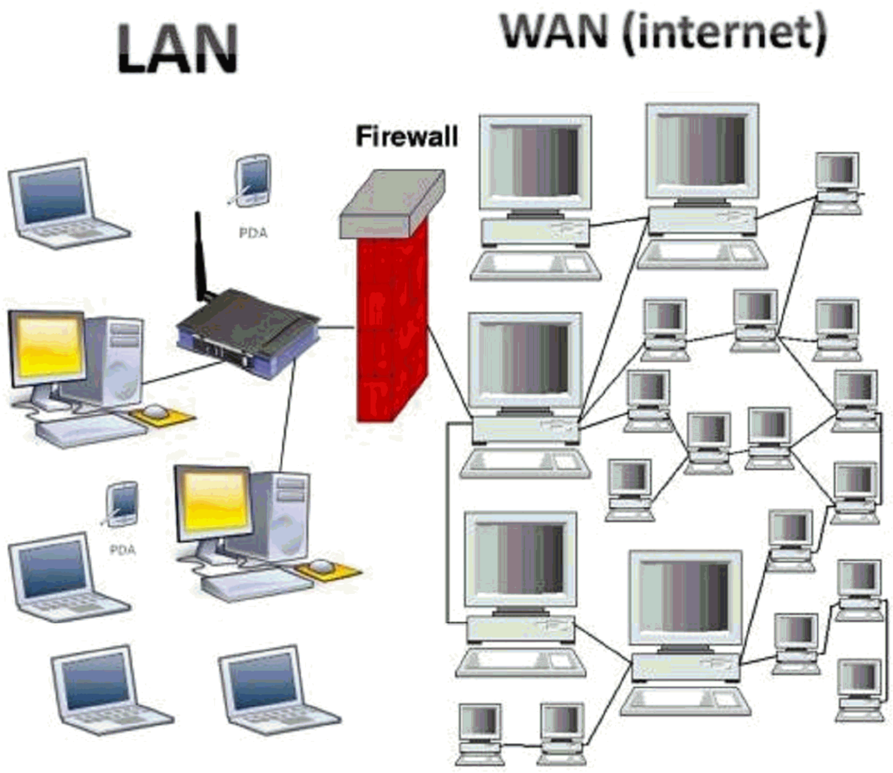


Figure 3.2 – Typical arrangement of LAN connected to the Internet

3.2.4 WLAN (Wireless Local Area Network)

Wireless local area network is similar to a regular LAN, but the individual elements are not physically connected by a wire (twisted pair cable, optical fiber), but they are connected wirelessly.

The disadvantage is, for example, that it is hardly possible to limit signal propagation, and that an intruder does not need to get physical access to the socket (for example, school buildings or companies), like with wired networks.

Most multipurpose devices (e.g. router/firewall-Ethernet, Wi-Fi, ADSL, 3G) use this abbreviation for indication of configuration of wireless part of network. For example, you can set a different level of security for the wireless part of the network.

3.2.5 VLAN (Virtual Local Area Network)

Not only in the school area it may be interesting to operate, for example, two, to a certain extent, separate LANs (on the twisted pair cable) and supplement the entire system with Wi-Fi. This arrangement allows you to set different security rules (classrooms x offices).

Classic Ethernet would require double cabling between buildings and a limited flexibility in configuration. More advanced network elements allow to implement more (virtual) local networks on one infrastructure. A computer can be connected to another local area network, to a different address and provide other options by mere remote configuration.

Each Ethernet frame is equipped with the information to which local network it belongs. It loses this information at the end network element and it is sent to the particular network computer card. Virtual LAN is similar to Classic local area network (LAN) except that LAN depends on the physical layout and links, while VLAN logically arises within the physical LAN.

3.2.6 MAN (Metropolitan Area Network)

Network which connects individual LANs but does not reach outside of the city or a metropolitan area. It often uses wireless connections or optical fibers.

MAN may be owned by one organization, but mostly it is a link between several independent objects. For example, we may have several branches of one company in one city. In the past, technologies such as ATM and FDDI were used, but nowadays Ethernet (known as metro-Ethernet) is dominating.

It is possible to deploy VLAN technology on one infrastructure and create local networks of individual city units (transportation company, municipality, municipal police).

3.2.7 PAN (Personal Area Network)

Personal area network is a very small computer network used to connect personal electronic devices such as mobile phone, PDA, laptop, etc. The range of these networks is the smallest (about 10 meters). An example of it is the Bluetooth in the office, in the car or the networks of measuring systems (Bluetooth 100 meters).

3.3 Computer Network Topology

3.3.1 Star Topology

- It is the most widely used method of connecting computers to a computer network. Computers are connected by cable segments (UTP, STP) to a central control - switch.

- There is only one way between any two stations. This system of connecting comes from the beginning of using of computer technology, when computers were connected to the central computer (mainframe).

- It was temporarily pushed away by bus arrangement in local networks (1980-1994) - Ethernet on coaxial cable.

- Currently this topology dominates in LAN thanks to Ethernet on twisted pair cable.

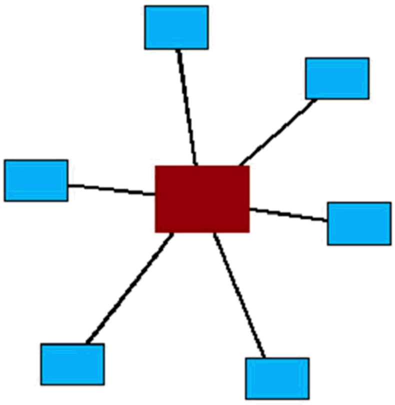


Figure 3.3 – Graphical representation of star topology

Advantages

- If one computer or cable fails, the connection will not work only for one station and other stations can still send and receive.

- Allows parallel operation –higher performance compared to bus topology at the same nominal bit rate. This relates to the fact that one cable is connected to only one computer, that's why there are no collisions between packets and it also can simultaneously transmit data of multiple computers.

- Allows separate traffic - the central element that can bring security

- It is easy to set up and extend

- Defects can be easily found

Disadvantages

- There is a large amount of cables required - one for each computer.
- There is a need of extra hardware compared to a bus topology (this might be cheap).
- In case of a central network element failure, the entire network stops working. Therefore, it is good to protect it from the power outage by a backup power source (UPS).

3.3.2 Bus Topology

Connection is provided by a single transmission medium (bus), to which all network nodes (terminal computers) are attached. Physically it can be a coaxial cable or terrestrial radio wireless connection.

The bus is a simple connection, has a low acquisition cost, but it also has disadvantages. The problem occurs when two clients want to broadcast on the network at the same time - a collision arises.

In the view of the fact that this situation happens quite often, the systems using a bus topology for communication have implemented a scheme for avoiding such collisions - Random access system (CSMA) is used in computer networks, which prevents collisions, and if it happens then fixes them.

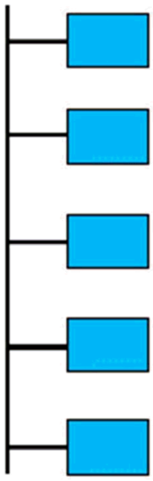


Figure 3.4 – Graphical Representation of the Bus Topology

Advantages

• A simple implementation and easy extension of the already existing network.

• Does not require as much wiring as e.g. star topology.

• Suitable for small or temporary networks that do not require high speed transfer.

Disadvantages

- Difficult troubleshooting
- Limited cable length and number of stations.
- If there is a problem with the cable, the entire network will work no longer
- The performance of the entire network is rapidly decreasing with larger numbers of stations or operations.

3.3.3 Ring Topology

For connecting computers in a circle trivial network control protocols can be used - simple succession.

The common solution of communication is an implementation of token (the authorization for action), that the stations pass in the circle and which allows its holder to broadcast, while other stations are just listening.

The message passes through all intermediate computers in the circle, and its delay at each node is just one bit (i.e. right after loading of the incoming signal, the signal is sent further).

Communication break up happens when the circle interrupts therefore some technologies work with a backup circle (for example, FDDI).

The system cannot be distinguished at first sight from the star because generally a central element tends to be used, the concentrator, which realizes the circle using two-point connections on the twisted pair cabling.

Ring topology is, therefore, a logical arrangement. Physically, looking at wiring, it is the star topology.

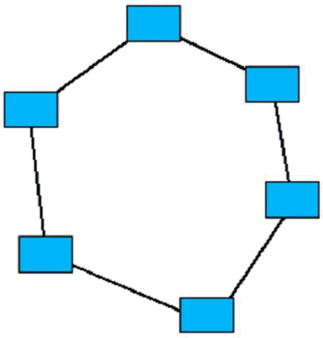


Figure 3.5 – Graphical Representation of the Ring Topology

Advantages

- Data transfer is relatively simple, because packets are sent in one direction.
- Adding another node has only a small impact on bandwidth.
- There are no collisions.
- Minimum delay (in bits, according to the number of nodes).
- For the above reasons, the network throughput is the highest during stress comparing to all other topologies,.
- Ease of implementation to guarantee the amount of data transferred per unit of time.
- There may be less cables than in a star topology.

Disadvantages

- Data must pass through all the members of the circle, which increases the risk of failure.
- Breaking the circle means a problem.
- When you add a new node, it is necessary to temporarily interrupt the circle (with token ring this is only for a negligible moment).
- Input and output (on and off) of a station is logically and implementally complicated operation.

3.3.4 Tree Topology

Tree Topology derives from the star topology by joining the active network elements that are in the centers of each star.

Such link is used primarily in large computer networks in large companies. Each Star often represents particular/individual Departments of the company, floors of the building, or entire buildings. These Stars are also linked in a star way.

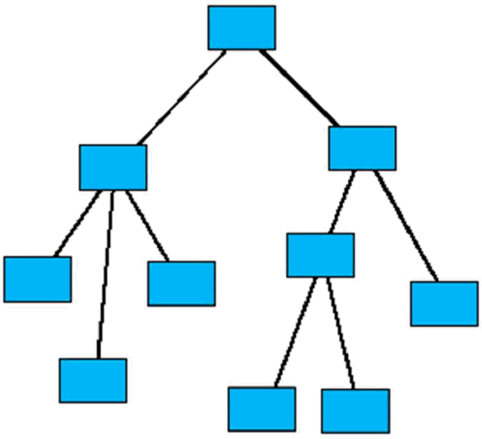


Figure 3.6 – A graphical representation of the tree topology

Advantages

- If one active network element fails, the other parts of network can continue.
- Reduces the required amount of cabling.
- Increased security - the difficulty of network communication eavesdropping rises.
- It is possible to separate traffic, to create virtual local area networks by configurating active elements.

Disadvantages

- The real performance depends on arrangement
- There are vulnerabilities. If they fail, the entire network is paralyzed.

3.3.5 General Graph Topology

It is sometimes called looped, mesh topology.

It provides redundant connections (WAN network, Internet, etc.).

Each device is linked with each other (full mesh). The common alternative is that some connections are omitted (partial mesh).

Routing in the Czech Republic.

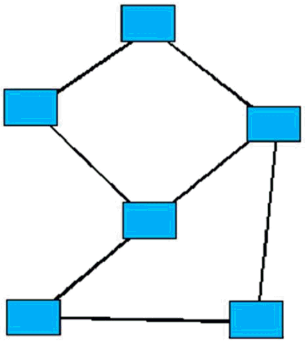


Figure 2.3 – Graphical representation of the General graph topology

Advantages

- High reliability. When some connection fails, the data find a different path.

Disadvantages

- Greater number of active elements.
- Large demands on the active elements (they must search for optimal routing settings).

3.3.6 Stand-alone Computer (Virtual Network)

It is not obvious, which of the above mentioned topologies characterize the situation more properly. If it is a multiprocessor computer with a high quality OS, then the application layer reaches full mesh.

3.3.7 Satellite Network

The setting is identical to the star network. The participants don't "hear" directly. It requires neither cables nor other infrastructure in its vicinity.

There are large delays (> 0, 5 sec) which mean that it does not support interactive work. Commonly used protocols, typical for other networks, may fail.

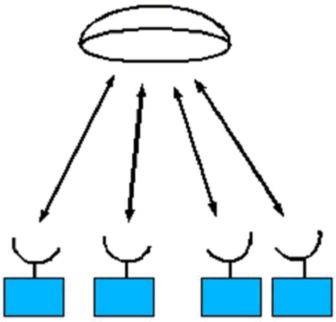


Figure 2.4 – Graphical representation of the topology of the satellite network based on Wireless Network

3.3.8 Wireless Network Based on a Close Infrastructure

It enables mobility near the access point, it does not require completely free line of sight (for example, to the sky compared to the satellite arrangement).

It has higher energy demands. Lower bandwidth compared to metallic wires or optics.

There is a lack of frequencies and authorization to broadcast power that is able to cover a larger area. In mode without a central element it is close to the bus topology (these devices compete).

In the central element mode it resembles a circle and a star. Central element grants permission. In a simpler variation, the individual devices can communicate only via the central element.

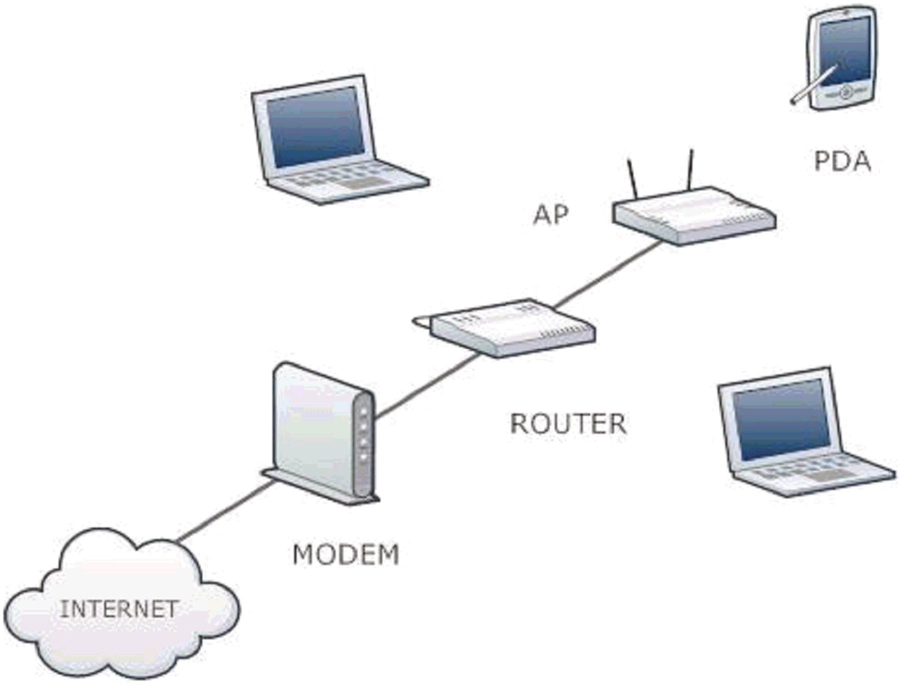


Figure 2.4 – Graphical representation of the network topology based on infrastructure

The session and presentation layer is not implemented (mentioned support functions must be handled by the application itself). Similarly, as in case of the lowest layers it was a prudent decision for TCP/IP design.

The original services of the application layer are electronic mail (SMTP, POP, IMAP), file transfer (FTP) and remote login (TELNET), additionally DNS and DHCP are joining and after a long time there are others that were added (WWW came after ten years in 1991).

Applications are able to implement two-point communication or even the more sophisticated peer-to-peer one (communication on the level equal to equal, meaning among multiple computers or applications), and client-server one (one or more servers control other network clients).

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PřF UHK“

Registrační číslo: CZ.1.07/2.2.00/28.0118

4 Physical Layer of Computer Networks

4.1 Twisted Pair Cable

4.1.1 History and Physics of Signal Transmission

The pair cable was historically the first cable used as a medium for signal transmission. The first technical experience comes from telecommunications. The physical nature of electric current, electromagnetic field and electromagnetic radiation already became evident with voice transmission where frequencies 3 to 4 KHz max were supposed to be used.

The so-called crosstalk effects occurred on long telephone connections. Each pair transmitted one phone call and crosstalk effect was a phenomenon causing other phone calls to be heard in the background as a result of radiation and feedback reception of electromagnetic waves.

This effect can be removed by the separate twisting of each pair. The twisting of the pairs in the cable is not random; it must be elaborated so well that the attenuation of the signal is the smallest.

Each signal must have its own pair of conductors and the transmitting current must be symmetric (the sum of the currents in the two conductors of the pair must be zero).

The cables are made in various qualities, e.g. the telephone cable requires much lower quality of twisting of the individual pairs.

If it is an end connection, i.e. one pair, it is not even necessary to twist the cable to minimize radiation and interference. It is achieved just by keeping all the wires during the whole route in close proximity. For Gbit/s transmission, the requirements are extreme.

In industrial applications, where large currents can be induced on the cable (i.e. the whole pairs of conductors) and put the input circuits of network interface out of service it is necessary to protect all pairs by the common screening (TNCS). In special applications, it is even necessary to shield each pair separately.

If the twisted pair cable should transmit a high-frequency signal, it must be properly adapted concerning impedance. The best results can be achieved when we use a two-point connection (the bus can be used when there are lower bandwidth requirements - for example, in communication buses RS485 or telephone line with two or three phones connected).

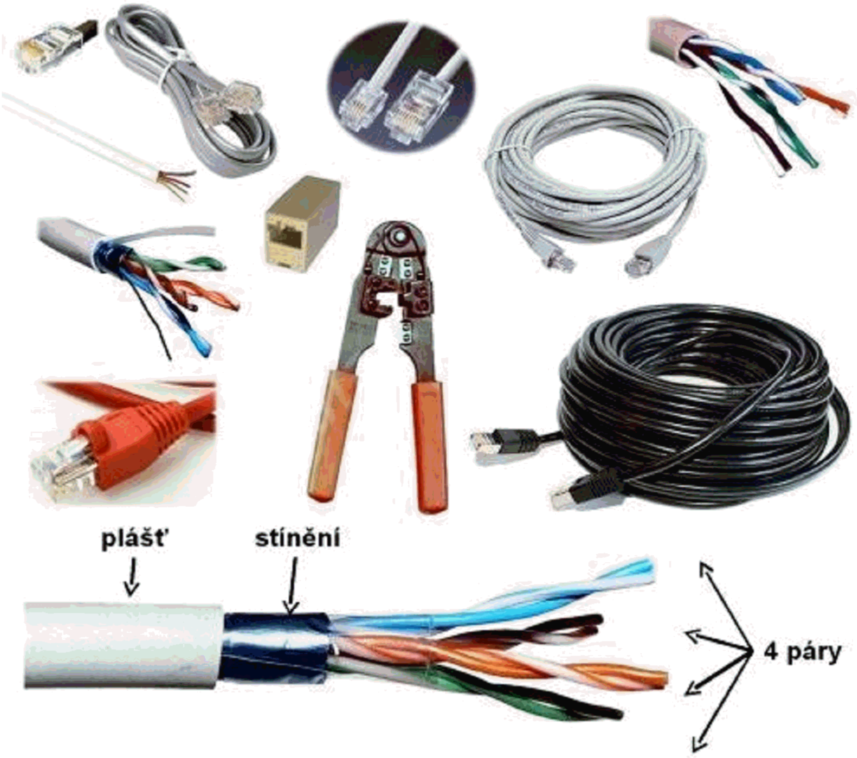


Figure 4.1 – Twisted pair cable - Hardware

4.1.2 Twisted Pair Cable in Computer Networks

It was used for the first time in the IBM networks (Token Ring), connectors RJ11, RJ45 were used. Unscreened is called Unshielded Twisted Pair, UTP. Screened Shielded Twisted Pair is called, STP. It is typically two-point connection - star, tree and ring topology.

Very popular and today classic and standard media of the connections can be easily made by using special pliers. Machine-made plugs have guaranteed mechanical resistance.

The connection terminated by the RJ45 connector must be wired to ensure a backward compatibility of the socket when using the RJ11 connector, for example, for the telephone line.

The plug designed for connecting two network interfaces of "the same type", which means two computers or two network elements are connected by crossing the RX and TX pairs. There is usually no need to use a crossover cable for network elements (they switch inputs and outputs automatically), but in the case of two computers or other special applications (network bridges) the crossover cable can be useful.

Quality is expressed by the link category.

Category 1

- This type of distribution is not intended for data transfer, it can be used, for example, for telephone wiring network.
- The transfer speed rates up to 1 Mbit/s, suitable, for example, for analog telephone wiring networks, ISDN, and so on.

Category 2

- Designed for data transfer with a maximum bandwidth 1.5 MHz.
- It is used for digital audio transmission and primarily for the IBM Token Ring wiring.
- The transmission speed is about 4 Mbit/s.

Category 3

- Designed for data distributions and voice with a 16 MHz bandwidth and transfer speed up to 10 Mbit/s.
- It is used for data transfer known as 10 Base-T Ethernet

Category 4

- Designed for data transfer in the Token ring networks with a 20 MHz bandwidth and transfer speed up to 16 Mbit/s

Category 5

- It works in a bandwidth of 100 MHz.
- Wiring for computer network with a transmission speed of 100 Mbit/s, or 1 Gbit/s in the case of the use of all 8 threads.
- Used for 100 Mbit/s TPDDI and 155 Mbit/s ATM. It currently is replaced with the 5e standard.

Category 5e

- It also works in bandwidth to 100 MHz, however, it requires new ways of parameters measuring and it is more strict in certain parameters.
- The objective is to operate 1 Gbit/s. It is used for TPDDI 100 Mbit/s, 155 Mbit/s ATM and Gigabit Ethernet.

Category 6

- It works with a bandwidth of 250 MHz. It is used for ultrafast backbone applications in an area of local networks.
- This is currently the most popular cabling for newly built distributions. It is used, for example, for transferring images on a large screen.

Category 6a

- It works with a bandwidth of 500 MHz. It is used for particularly fast backbone applications in the area of local networks.
- It is also used for 10GBASE-T Ethernet (10 Gbit/s).

Category 7

- It works in a bandwidth of up to 600-700 MHz.
- The first experiments with this standard are being currently carried out.
- The cable is fully shielded - each pair is shielded separately by Al foil and the cable itself has an extra complete shield.
- Fully shielded construction has resulted in a greater weight, greater outer diameter of the cable and smaller cable flexibility than UTP or STP.
- It is used for transmissions of the full-scale video, teleradiology.
- For the time being, the cable and components is not widespread because of high cost.

4.2 Structured Cabling

By gradual building of ever larger and more modern networks, a comprehensive and sophisticated notion has been developed about how computer network distributions should be done.

Today, practically all new network distribution systems are built according to the principles of the "structured wiring".

Current type of structured cabling is based on the twisted pair cable (for a certain transitional period, there were also installations based on a coaxial cable).

Wires from all sockets are led into one center, the socket then can "move with the user."

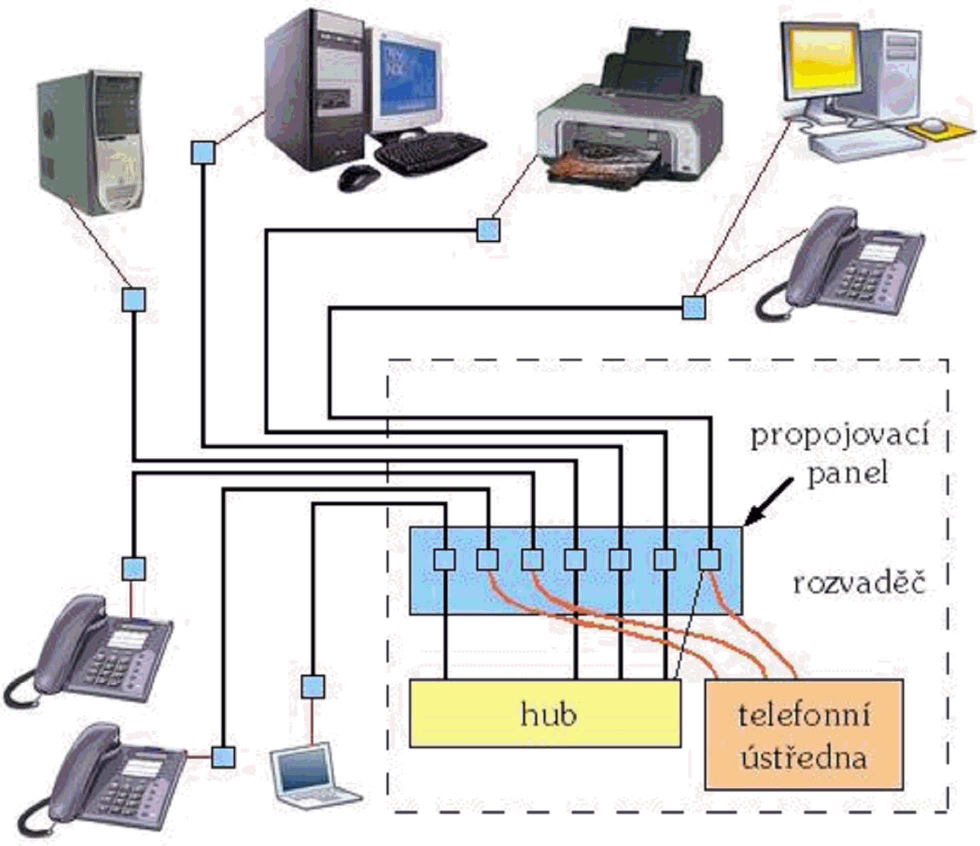


Figure 4.2 — Typical usage of structured cabling

4.2.1 Requirements for Structured Cabling

Cable networks are installed the way so that they do not interfere with anything. The lifetime of cables is generally much longer than the lifetime of the device that will be using them. Cabling implementation is very expensive (nowadays even more expensive than the price of the hardware that is connected to this line).

Network wirings are deliberately designed excessively large. There is also a tendency to install the network wiring even in such rooms or parts of the building where no connection is yet required.

Quality distributions are designed in such way to minimize the risk of failures and defects which are achieved by using high-quality cables, connectors, plugs and other installation elements, as well as the appropriate installation procedures (for example, hiding cables in rails, etc.).

The universality of the structured cabling - wiring can be used for multiple different purposes (for example, telephone wiring, wiring for security devices, etc.). The used materials are already so reliable and durable, and the methodology of the structured cabling building is already so highly-developed, that companies are willing to provide very long warranties – commonly 15 years.

4.2.2 Structured Cabling Topology

For a proper understanding of the structured cabling nature it is beneficial to remember that the wiring is purely passive. Neither end nodes (the user workstation) nor a variety of servers or active network elements are components of the structured cabling.

The whole system of structured cabling topology is inspired by the philosophy of Ethernet on twisted pair cable, but on the other hand, it is so universal that it can be used also for other networks and their combinations.

Structured cabling topology is basically a tree topology (in the basic version it is a star topology, see the picture).

The distribution cabinet is an important design element of structured cabling and all connecting elements must fit into it (interconnecting cable, hub, switch etc.).

Systems based on the twisted pair cable are used in the lowest "levels", limited by its range up to 100 meters. These distributions "collect" the end connections in their range and they "combine" them into larger units (by a standard switch in the case of classic Ethernet).

From the distribution points of the lowest level there are other connections going "upwards" (so called: uplinks, typically optical fibers) to the interconnection points of higher levels - there may be several "levels" and in each of them the individual units of lower levels can merge or interconnect with each other - through bridges, routers and switches, etc.

Everything is intentionally universal, so that individual connection places (implemented through the standardized boxes) can be filled by various active elements according to specific needs, and this way create almost any logical (and to some extent even physical) computer network topology.

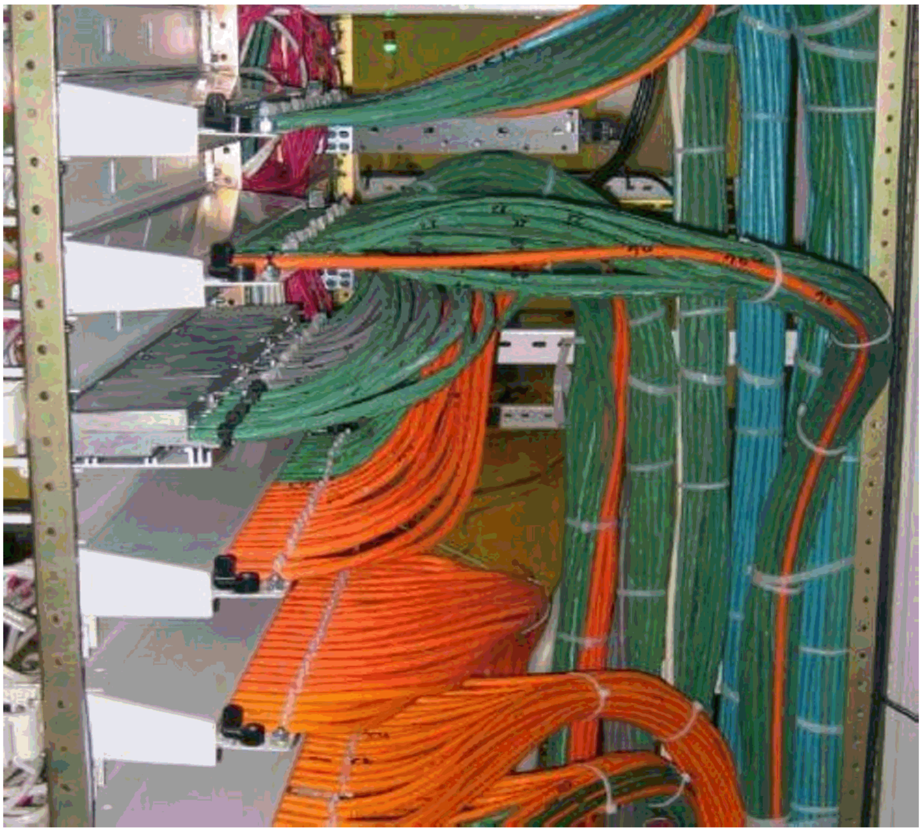


Figure 4.3 – Example of wiring in a distribution box

4.3 Coaxial Cable

4.3.1 Coaxial Cable Properties

Coaxial Cable is an asymmetric electric cable with one cylindrical outer conductor and with one wire or tubular inner conductor.

The outer conductor is often called a shielding and the inner wire a core. The inner and outer conductor is separated by a non - conductive layer (dielectric).

The most common function of a coaxial cable is the transfer of electromagnetic waves of high frequency (up to 50 GHz), for high frequency signal, it is a kind of a waveguide.

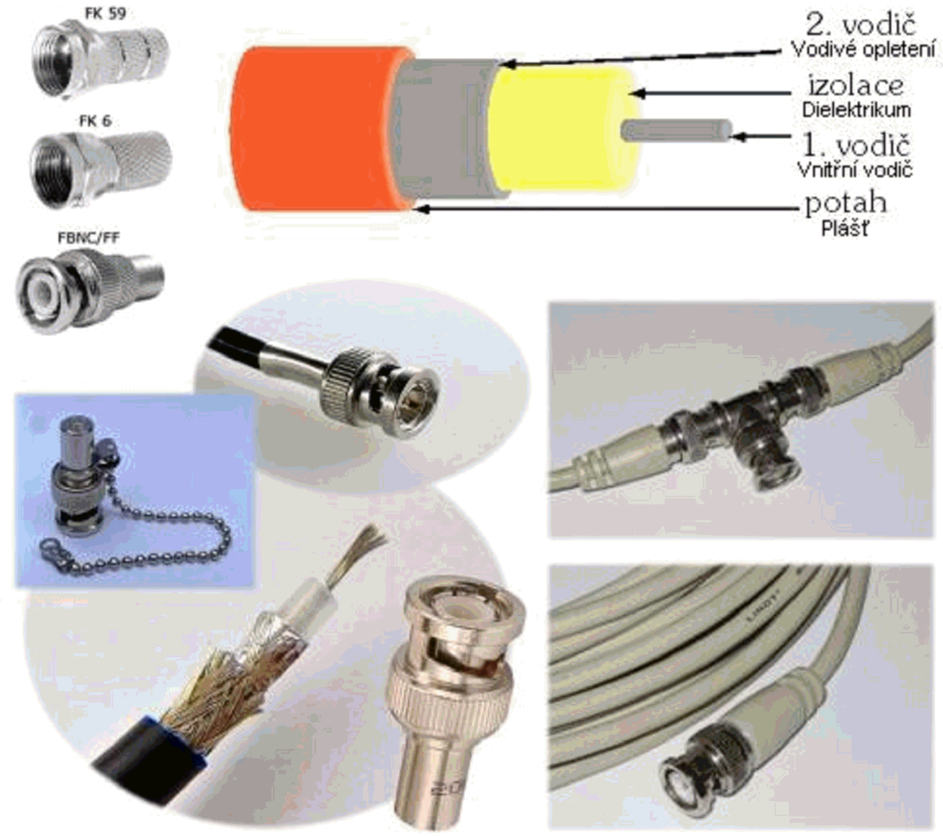


Figure 4.4 — Coaxial cable and the used connectors

Coaxial cable is the oldest type of cable used in computer networks. It had a great influence on computer network development (LAN). The motive for its application was not only a huge bandwidth, but the elimination of receiving multiple signals with minimum interference and noise.

A cheaper twisted pair cable could be used after the development of new methods of integrated circuits, which provided ways to modulate/demodulate a signal enabling it to cope with receiving multiple signals and noise (even the best category 7 allows to transmit the signals only slightly exceeding 600 MHz, and it is already beginning of the coaxial - shielding, dielectric).

Coaxial cable is also irreplaceable in antenna systems and is also used in computer networks of cable television operators (combined systems of the digital television, internet 100 MB and higher, phone).

In the context of Ethernet technology it is claimed by various sources that its transmission rate is only 10 MB/s and twisted pair cable produces 100 times higher speeds. However, it is only the specific Ethernet, rather than a characteristic of this media!

The basic difference among coaxial cable, twisted pair cable or optical fiber is the fact that a coaxial cable can be used for branching and it is therefore possible to use it for multipoint connections (each connects more end nodes using the T-connectors).

On the other hand, neither the twisted pair cable nor the optical fiber can used for branching, that's why these transmission media are therefore applicable only for two-point connections (the required "branching" must be provided electronically, in appropriate hubs).

The problem, however, occurs when one of the computers, connected to a coaxial cable, fails. With the failure of one computer all that are connected to the broken network segment lose the ability to communicate at the same time.

To find out the exact location of the fault was very difficult. It is a different case with a twisted pair cable. When a failure occurs, only one end node usually loses the possibility of communication, but others can continue to work.

Using a coaxial cable for the two-point connection and for a transfer of digital signal is currently a matter of luxury and special applications. Furthermore, it is necessary to realize that two coaxial cables must be used (RX, TX), the original Ethernet was only half-duplex.

4.3.2 Coaxial Cable Connectors

BNC Connector (British Naval Connector)

- Soldered down/pressed at the end of the cable
- It is used mostly in the measuring technique (in the past also in the Ethernet and therefore it is known.)
- Designed for frequent connecting and disconnecting
- T-plug/connector BNC, I/connector BNC, both allow connecting and branching.
- The terminator - the common/ordinary resistance of 50Ω absorbs energy of the VF signal

FK Connector

- It is used for more permanent installations.
- It is simple and therefore suitable for the highest signal frequency.
- It is widespread nowadays in satellite and television technology.

Other High-frequency Connectors

- Large versions in power transmission technology.
- Miniature for GSM, Wi-Fi applications.

4.4 Optical Cable

It consists of one or more optical fibers, which are together with a suitable lining stored in the outer sheath. The diameter of the kernel is several units to tens of micrometers and it is usually made of different kinds of glass.

This type of cable is based on a different principle than the previous ones. Data are not transmitted electrically in metal conductors by moving with electronic packaging of atoms, but by photons, light impulses in the translucent threads.

For light signal execution, a full reflection is used which is a phenomenon that occurs at the interface of the core and the shell when the appropriate material of the core and shell is chosen.

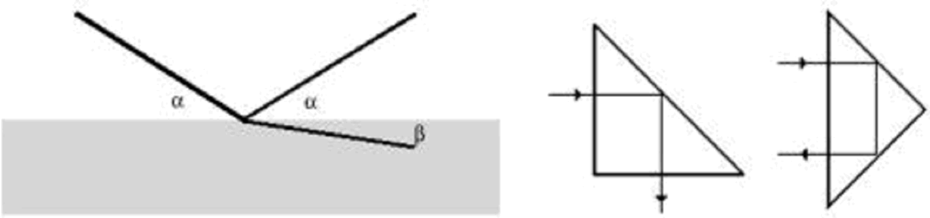


Figure 4.5 –Impact, refraction and reflection of light

The illustration shows the principle of the impact and reflection of light. The optical density of the fiber must be significantly higher compared with the wrapping of light conduct so that the refraction β, indicated at the picture, does not occur.

Photons remain "trapped" in the thread and spreads without significant losses to the other end of the cable (a similar effect can be observed with the naked eye, for example, under water the surface appears to us to look like a mirror from a certain critical angle).

Optical cables allow signal transmission over long distances (up to 10 km when using single-mode optical fiber, see below) without the use of active elements.

The advantage of optical cables is absolute resistance against electromagnetic interference (photons are electrically neutral particles unlike electrons). They have very low losses and high transmission speed.

Before the transfer, it is necessary to ensure conversation of an electrical into an optical signal, which is provided by LED's or laser diodes that generate light pulses according to the incoming current (so called generators).

On the other side of the line it is necessary to convert the optical signal back to electrical power, which is provided by photodiodes or phototransistors (so called detectors).

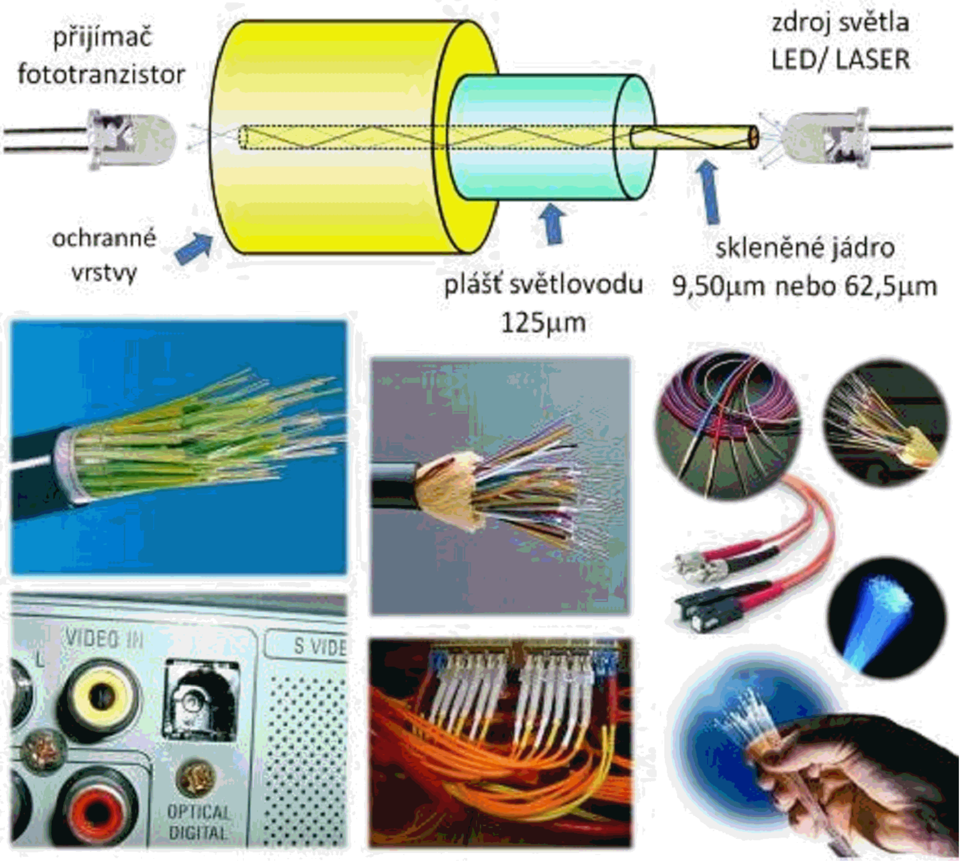


Figure 4.6 — The application of the optical fiber

4.4.1 Optical Fiber Characteristics

- The core dimension and its wrapping are usually stated.
- There is a huge bandwidth (terabits).
- No interference, received and transmitted (it does not radiate and does not induce electrical magnetic waves).
- It is a standard for outdoor services.
- It cannot be intercepted ("tapping").
- Two-point connection, branching has not been satisfactorily resolved.
- It is relatively expensive, but now available for common applications.
- It is less flexible.

4.4.2 Multi-mode Fiber

- Multimode (MM) - the light energy is divided into multiple beams while passing through the fiber (so-called modes), the individual modes reach the end of the cable with time lag which causes a distortion of the signal.
- Intersecting rays travel various distances – in the figure you can see where there are rays travelling a different distance represented by a different color.
- The response to the downward edge is dimming on the receiver side.
- The light source is a luminous semiconductor diode (LED).
- It reaches the distance of hundreds of meters, up to 2 kilometers.
- These cables are cheaper, but have worse optical properties.
- Their core has a diameter of 50, 62.5, or 100 micrometers (the wrapping has 125 microns).

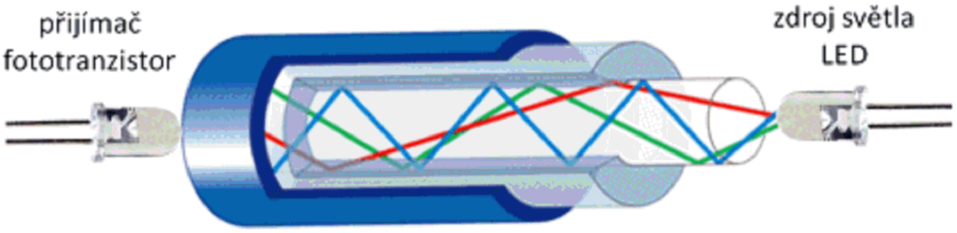


Figure 4.7-The propagation of light in the multi-mode thread

4.4.3 Single-mode Fiber

- Single-mode fiber (SM) – only one ray passes through the cable (without different refractions and routes).
- Single-mode optical fibers have a core with a very small diameter (typically 9 micrometers).
- The laser is a light source.
- These cables have better optical properties, higher transmission capacity, transfer signals to a larger distance (now it is from tens to hundreds of kilometers), but they are more expensive.

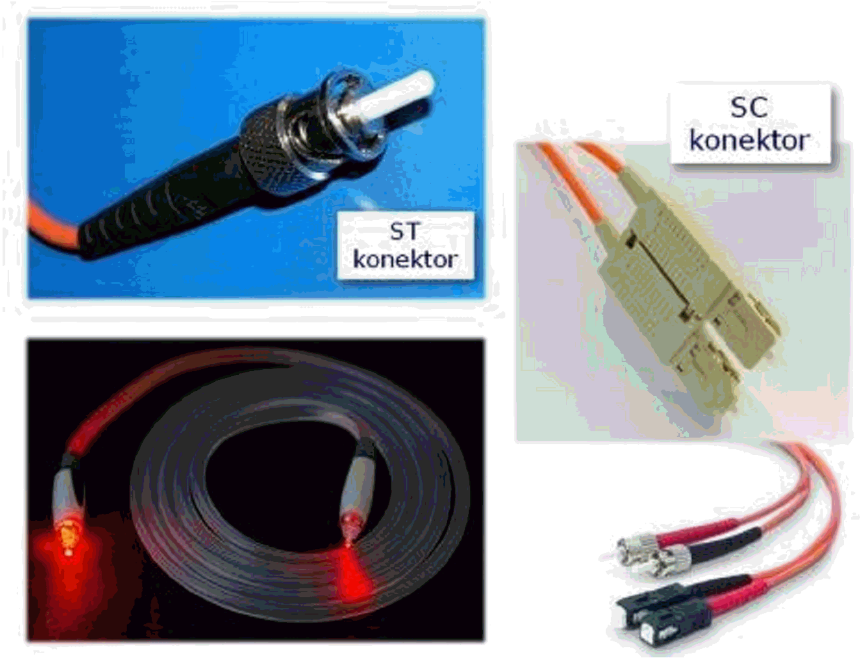


Figure 4.8-Connectors of optical lines

4.4.4 Use of Optical Fibers, Connectors

Optical cables can be used in all topologies, mostly as the backbone.

Two types of ending of the optical cable are used - round plug ST and square plug SC (see the previous figure 4.8).

Transceiver is required at the end of each cable for converting electrical impulses into light rays and vice versa.

The next element is a converter that allows connection of the optical line to a twisted-pair cable.

The ending of the optical cable requires special and expensive equipment. The end is carried out by a service company (a user cannot do it alone).

The transmission speed of the optical cables ranges from hundreds of megabits to many gigabits per second, thanks to technological progress; the anticipation of further achievable increases in transmission speed can be expected. On the other hand the realization of optical networks is costly and technically demanding.

4.4.5 Wavelength-division Multiplexing (WDM)

Wavelength-division multiplexing is a technology, which during the transmission multiplexes multiple optical signals in a single optical fiber by using different wavelengths (colors) of LEDs or lasers.

The principle is illustrated in the following figure 4.9. This is how it is possible to increase the capacity of the media, or to perform two-way communication on a single optical fiber.

The concept of wavelength-division multiplexing is most commonly used in the transmission of information optically (the signal is described by its wavelength). Frequency-division multiplexing is typically used in radio transmission of information (the hallmark of the signal is usually frequency).

As well as at the frequency-division multiplexing there are different frequencies used for different signals, for communication over optical fiber we use WDM with different supporting wavelengths.

Indeed, the wavelength is inversely proportional to the frequency of the waves, moreover optical and radio signal are only two of the possible forms of electromagnetic waves.

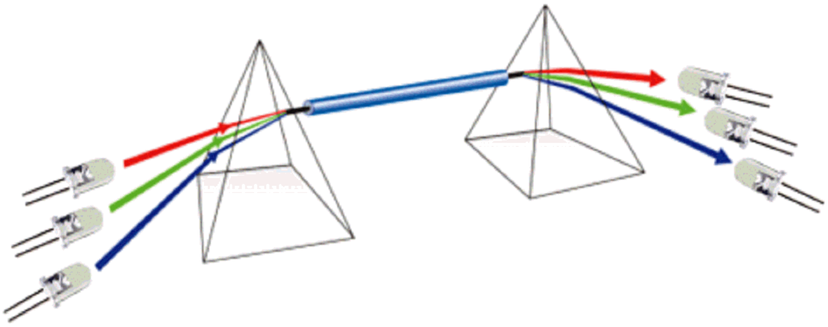


Figure 4.9 – The principle of wave multiplexing (WDM)

The concept was first published in the 1970s, and in 1978 WDM was implemented in laboratories. The first WDM was able to combine two signals. Modern systems can handle up to 160 signals and can extend to 10 Gbit/s optical systems on the theoretical capacity to 1.6 Tbit/s over a single optical fiber pair.

WDM is popular in the telecommunications companies because it allows expanding the network capacity without laying more fiber. Using WDM and optical amplifiers, they can place multiple generation technologies in their optical infrastructure without having to overhaul the backbone network. Capacity can be incremented by a simple extension of the multiplex at each end.

The most commonly used are optical-electric-optical converters at the very edge of the transport network, thus maintaining interoperability of the existing equipment with optical interfaces. Most WDM systems operate on the single-mode optical fibers which have a core diameter of 9 μm, but WDM optical fibers are also possible on the multi-mode.

4.5 Comparison of the Optical Cable, Coaxial Cable and Twisted Pair Cable

Optical cable is in principle similar to the two-line cable. The difference is mainly in the materials and size. Coaxial cable, as an electric conductor, can be compared with two-line cable.

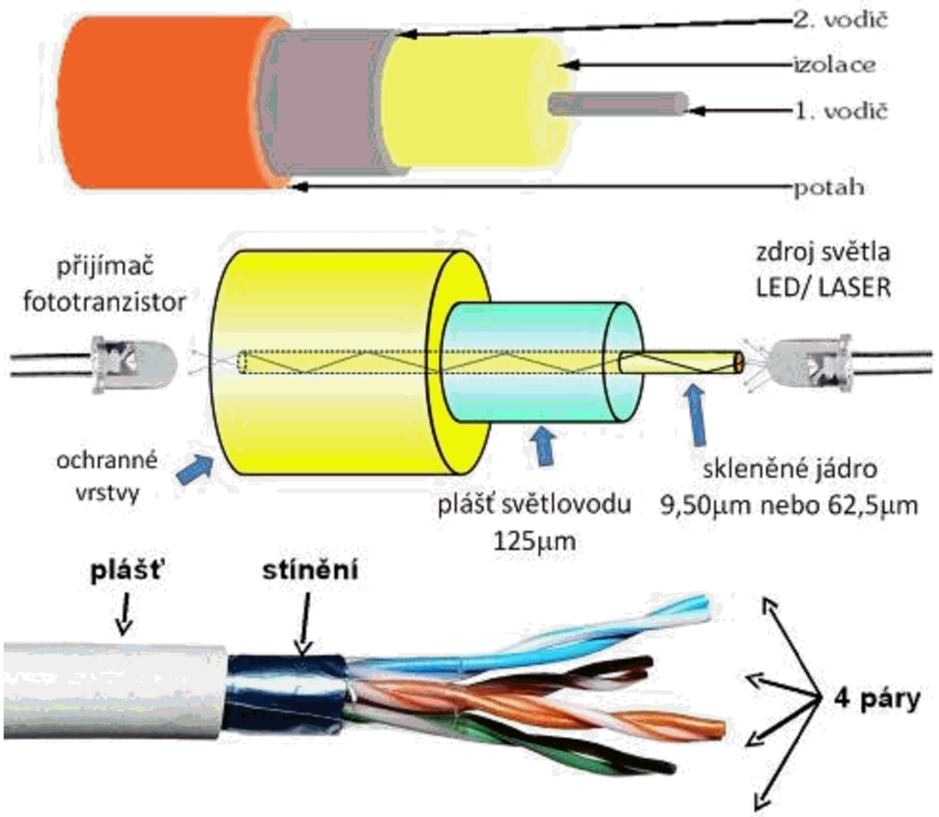


Figure 4.10 – Comparison of the optical cable, coaxial cable and twisted pair cable

Coaxial Cable

- In the case of coaxial cable, the electromagnetic wave (size of waves approximately 1 meter) is created by the electric current on the surface of the middle conductor.
- Depending on the structure (dimension and used material) of the coaxial, signal attenuation occurs with the increase of frequency. If everything is set correctly, wave impedance is adapted to the signal source and receiver impedance (50Ω or 75Ω usually), the signal transmission is in principle possible to relatively large distances (hundreds of meters up to the unit km-cable TV).

Optical Fiber

- In case of the optical fiber there are electromagnetic waves (photons) brought into the input area without metallic wires from a source such as LED or Laser (the size of electromagnetic waves is approx 0. 0005mm).
- Distortion of the conditions of full light reflection leads to loss of signal. Branching at the optical fiber has not been resolved yet. Another difference between the coaxial and the optical cable is that the optical cable is strictly two-point joint.
- Unlike coaxial cable, optical fiber offers attenuation independent on the frequency of electromagnetic waves, i.e. from immediate infrared to a visible spectrum.
- Bandwidth (maximum frequency of modulated signal), however, decreases with the length of the cable (see previous chapters considering single-mode and multi-mode fiber)
- Optical fiber can therefore offer transmission speeds in terabits or it can be just slightly better than the high-quality (and very expensive) coaxial cable.

Twisted Pair Cable

- The basis for signal transmission at the twisted pair cable is an electric current. Energy of the radio signal transforms into electromagnetic waves and back to electric current (in both conductors of the single pair the same current flows, only in the opposite direction).
- As each pair of conductors creates a magnetic field in the rhythm of the given signal there is a need to twist the pair cable (in the case of a cable, each pair with different number of twisting per unit length)
- Signal attenuation grows rapidly with length, facing a multiple signal reception (for example, phone line and DSL modem), attenuation grows with the frequency of the AC power supply.

- The various applications, different lengths and different transmission speeds by using a twisted pair-cable:
  - SATA - 1 meter
  - USB - 5 meters
  - Various ports - 10 meters
  - Ethernet - 100 meters
  - DSL - 2 kilometers
- The medium has also the highest requirements on the signal modulation and demodulation. Similar methods are used with wireless transmission. Great development → investment into modulator and demodulator pays off, because the twisted pair cable is the cheapest and most flexible (connectors, cable handling, etc.) and partly replaces coaxial from other fields (like TV technologies).

5 Ethernet

5.1 The Origin of Ethernet

A network fundamentally similar to today's Ethernet was assembled and tested for the first time by Robert Melancton Metcalfe at XEROX Company in the 1970s.

The network transferred data at a speed of 3Mbit/s and was called "the experimental Ethernet".

The first standard was created in 1976 and it's name was IEEE 802.3. In 1980, a consortium of three companies (Digital, Intel, Xerox) was founded which established the first parameters of the oldest Ethernet system with the transferring speed 10Mbit/s. This is how the classical Ethernet, under the name we know it today (sometimes also known as DIX) came into existence.

In 1985 Ethernet was gradually standardized first at IEEE organization under the standard IEEE 802.3 and later at ISO organization under the standard ISO 8803.2 (Ethernet II, DIX).

All devices manufactured after 1985, comply with both of these standards. DIX Ethernet and IEEE 802.3 standard are functionally compatible, there is a difference in meaning of a single frame field (see chapter „Access to Medium“).

From the very beginning, Ethernet was based on the access method CSMA/CD. This way of (no) traffic control diverged from other technologies, that is why it broke through in general competition.

The basic concept for this "traffic control" method is a collision - a situation where two or more stations broadcast at one time. Ethernet notices a collision and fixes it by repeating transmission attempts, similarly as sometimes people do in a discussion group.

Figure 5.1 – The origin of Ethernet, hardware once and today

From the beginning, Ethernet was developed for office applications and it is used for these purposes still today. Its massive expansion and reducing price of the cables and network elements, push it through to technical and industrial applications.

In both, the office version and industrial applications, the original algorithm CSMA/CD is now being replaced by different methods (see chapter „Hub versus switch“).

5.2 Ethernet Topology

5.2.1 Bus Topology Based on Coaxial

Ethernet topology has always been strictly of the bus type. The original electric implementation was based on the so-called thick coaxial that could be up to 500 meters long without any active element. Coaxial formed space (ether) for the signals transmission without reflexions and multiple receiving. The network elements listened with electrically high internal resistance (they transmitted to a load of 50 ohm).

The signal energy was thwarted by a so called terminator (HF resistor 50 ohms). It was possible to increase the distance of the network for up to 2 km by strengthening the signal, (the length of the backbone network). This distance was not possible to further increase (problem of a collision window, see the article „Access to medium“). The transmitting speed was relatively high for 1980s (10 Mb/sec).

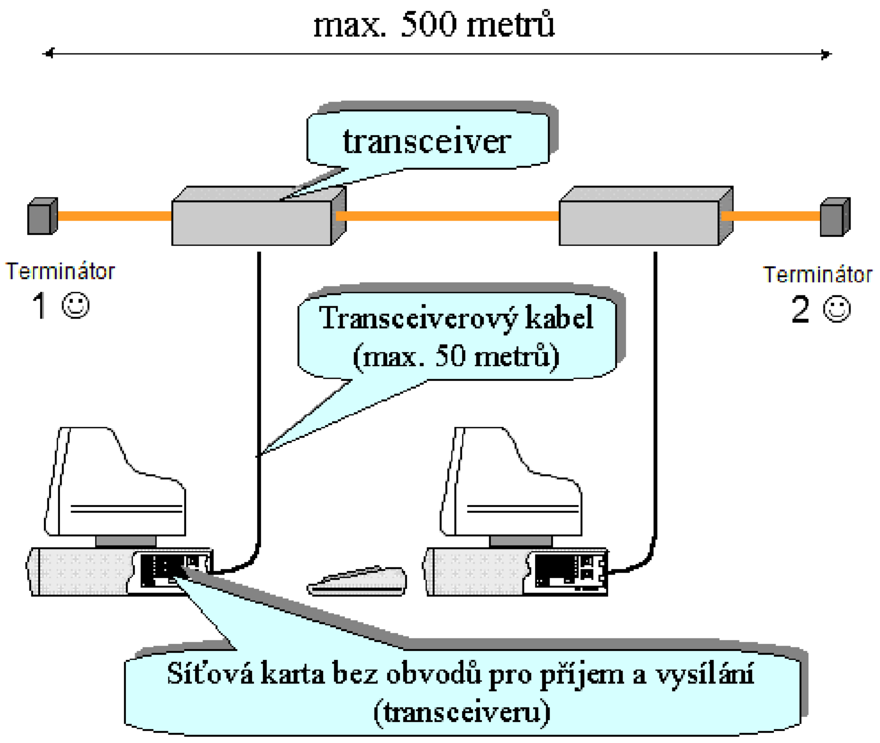


Figure 5.2 – The original Ethernet based on thick coaxial

The thick coaxial cable was an uninterrupted cable (usually of a yellow color), which was connected to a transceiver by special "vampire" pliers (the central wire has not been damaged, the shielding minimally).

The advantage of this topology has been the ability to connect a computer up to 50 m from the backbone. The backbone was usually "interweaved" through the whole building. The physical arrangement can be seen in the previous figure 5.2.

Thick coaxial required special equipment (very special pliers), and skills (cable disruption was fatal).

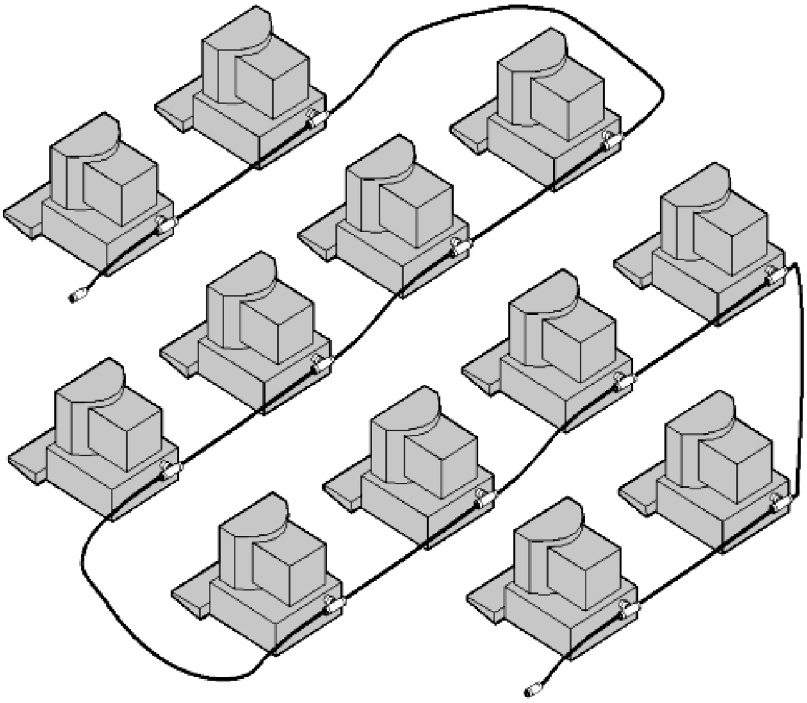


Figure 5.3-Ethernet-based and thin coaxial- in a classroom

Thin coaxial cable is simply a replacement of the thick cable by the common coaxial with BNC connectors (used then and today in the measuring broadcast technology).

The distance was significantly shorter depending on the implementation method (50-200 m according to the quality of the implementation).

This method was later standardized (10Base2) and the transceiver was integrated directly into the computer interface (absence of transceiver cables reduced the network size).

The installation of such local networks was very popular, for example, in classrooms - see previous figure 5.3. In administrative buildings a small range of the network was compensated by repeaters - see fig. 5.4. and 5.5.

Branching was admitted during the physical realization. It was still one area, though, without one so called collision domain with a maximum length 910 m instead of theoretical 2 kilometers.

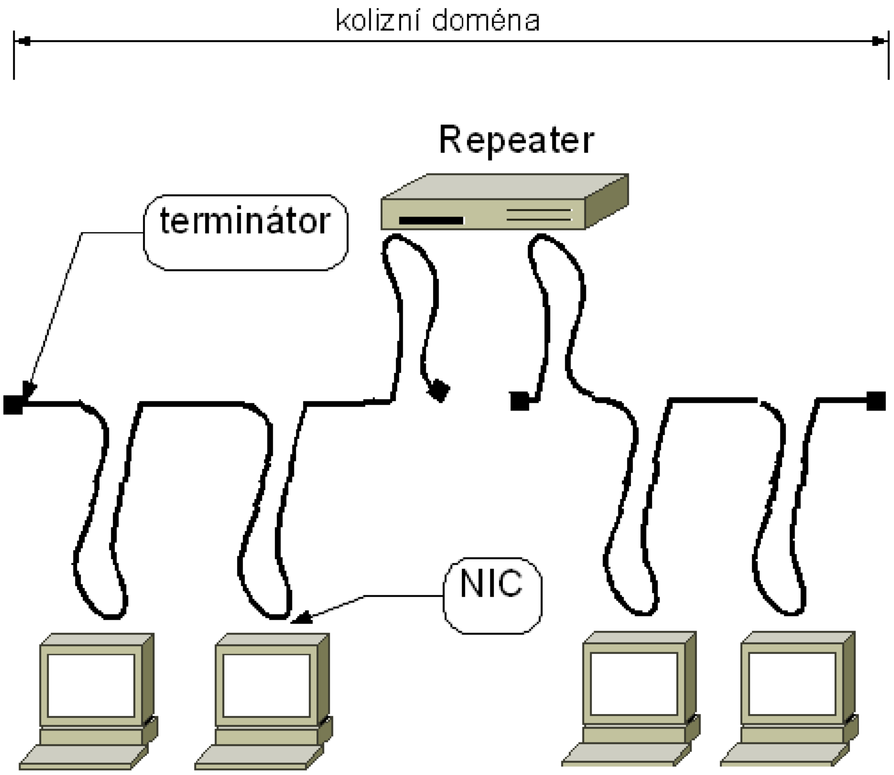


Figure 5.4 –Ethernet-based on a thin coaxial – in an office setting

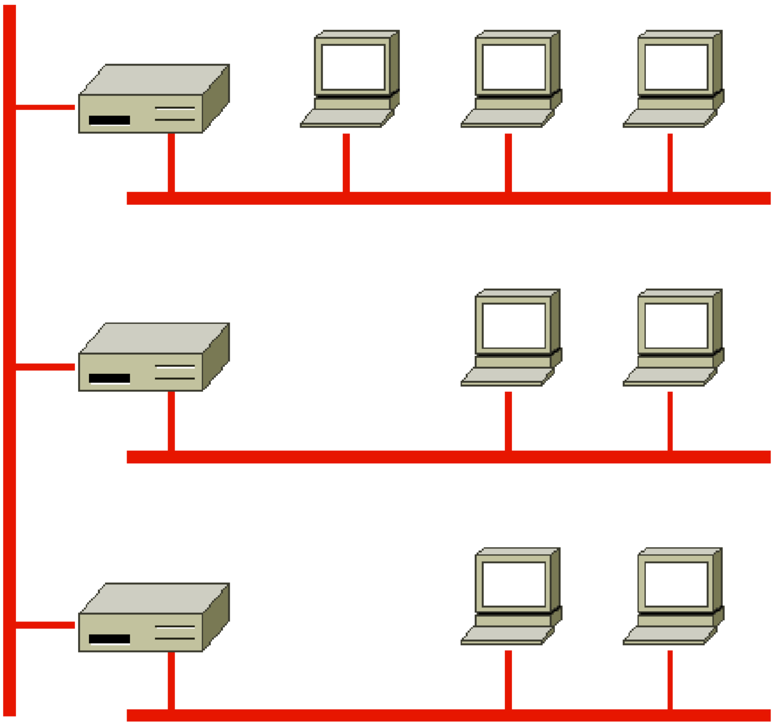


Figure 5.5 – Ethernet-based on a thin coaxial – in an office setting with branching

5.2.2 Structured Cabling Based on Coaxial

Abandoning the thick coaxial cable resulted in a difficult network implementation (branching from the backbone was no longer possible). To be able to return at least a bit to the original options, it meant finding an alternative for transceiver-branches socket, the EAD sockets have been developed.

EAD sockets enabled a physical connection of computers into one infrastructure, seemingly a star topology. The signal had to pass all of the drawers. Each drawer meant a distortion of the backbone and its extension to further meters of coaxial cable to the computer and back to the outlet.

The disadvantage was a lower reliability, the structured cabling served only for a computer network (e.g. phone needed its own infrastructure).

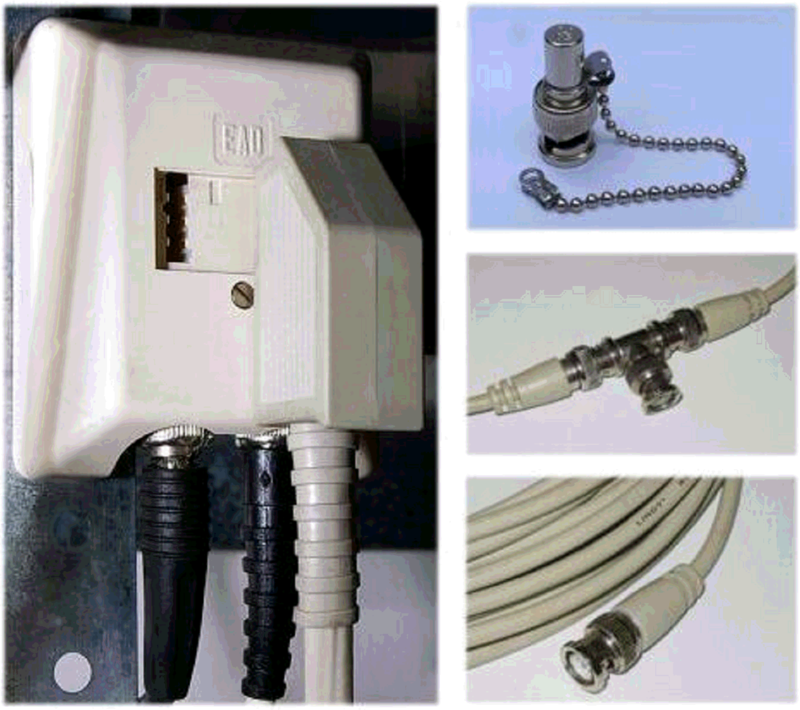


Figure 5.6 – Structured cabling based on thin coaxial

5.2.3 Bus Topology Based on a Twisted Pair-cable

Bus topology based on a twisted pair cable is illustrated in the figure. Yes, you understand it correctly. It is logically a bus topology.

The bus is seemingly physically plugged into a star or tree topology, it is true, but the signal from each interface is distributed throughout the whole network to all participants, as if they were connected to one good old thick coaxial ☺.

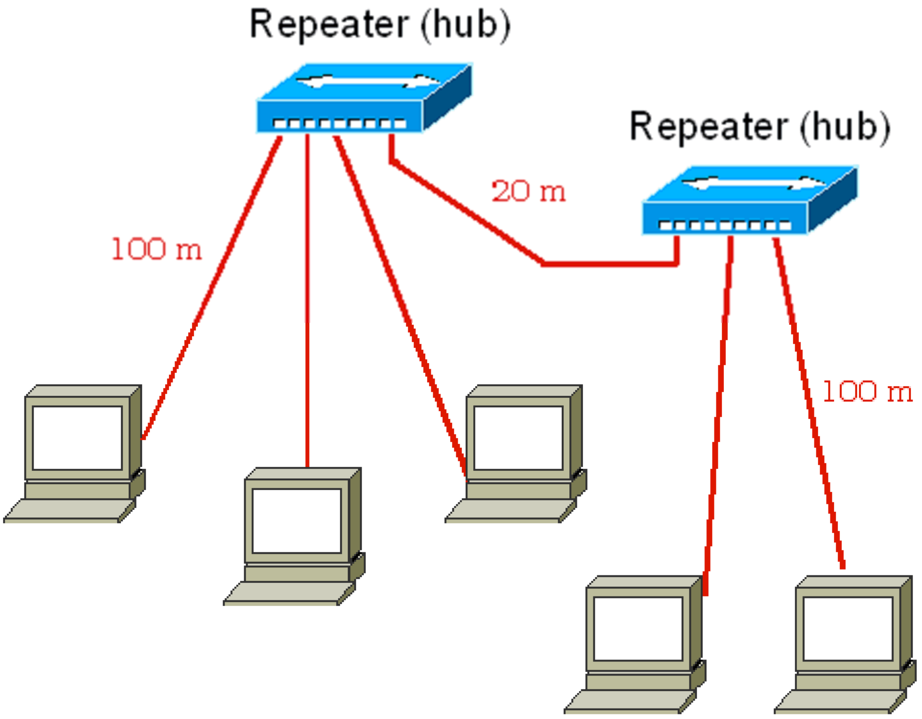


Figure 3.5 – Ethernet network connection using hubs and twisted pair cable

Connections are two-point only because a twisted pair cable is used and each network interface has a built-in terminator. This way reflections and multiple receivings are prevented similarly as with coaxial. The picture also shows the lengths. Maximum length of one connection can be 100 meters. The whole network must not exceed the 220 meters. This length reduction is based on a ten times higher transmission speed (speed of 10Mbit/sec to 100 Mbit/sec led to the shortening of the collision domain from approximately 2 kilometers to 220 meters).

The transition from coaxial has been slow because the increase of conductors discouraged users, but substantial price reduction of UTP conductors and branches gradually forced users to transition to a twisted pair cable.

CSMA/CD algorithm is limiting in this case. The further increase of distance can be achieved by putting it out of operation (see chapter Hub versus switch).

5.2.4 Star and Tree Topology Based on Twisted Pair Cable

The office Ethernet transition to a star technology is implemented by replacing central hubs with switches. The CSMA/CD algorithm is deactivated by a network adapter and the communication becomes fully duplexed (the adapter can receive 100Mbit/sec and simultaneously broadcast –no collisions are watched, the routing on the physical layer is provided by the SWITCH).

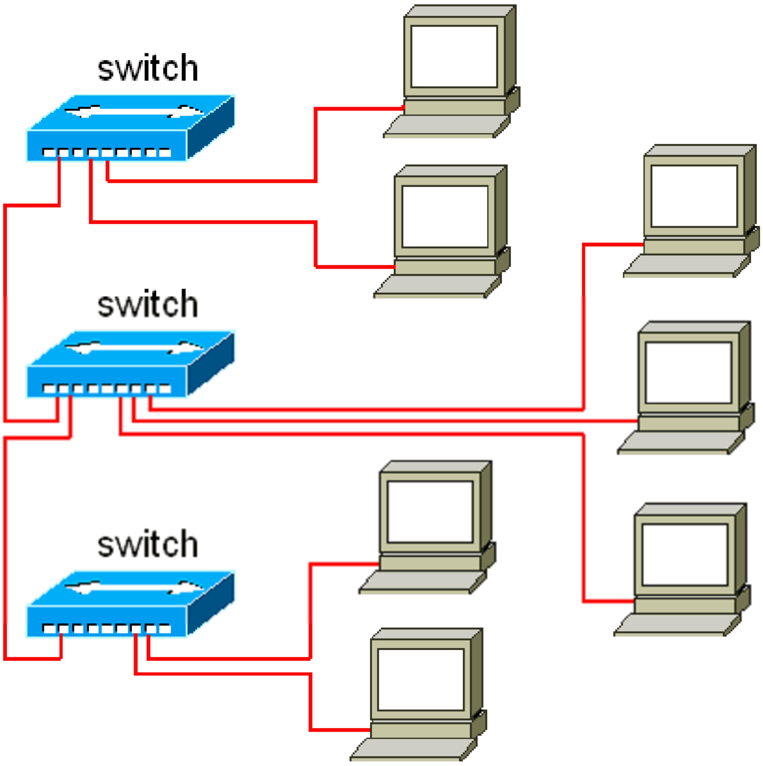


Figure 3.6 – Ethernet connection using switches and twisted pair cable

Network quality is to a large extent determined by network elements and a failure of the central element is fatal. The distance can be increased by using better quality connectors (coaxial line, multi-mode fiber, or even single-mode fiber).

5.2.5. Structured Cabling Based on Twisted Pair Cable

In construction of new buildings, it pays to invest into infrastructure without immediate need at the time of the investment. Kilometers of wires are laid down during the construction of the building. The start topology is dominating. - see figures 5.9 below.

Ethernet switches, telephone exchange or the building security system are placed in a data center (more can be read in the previous article, in the article „Structured cabling“ in the chapter „the physical layer of the computer network“).

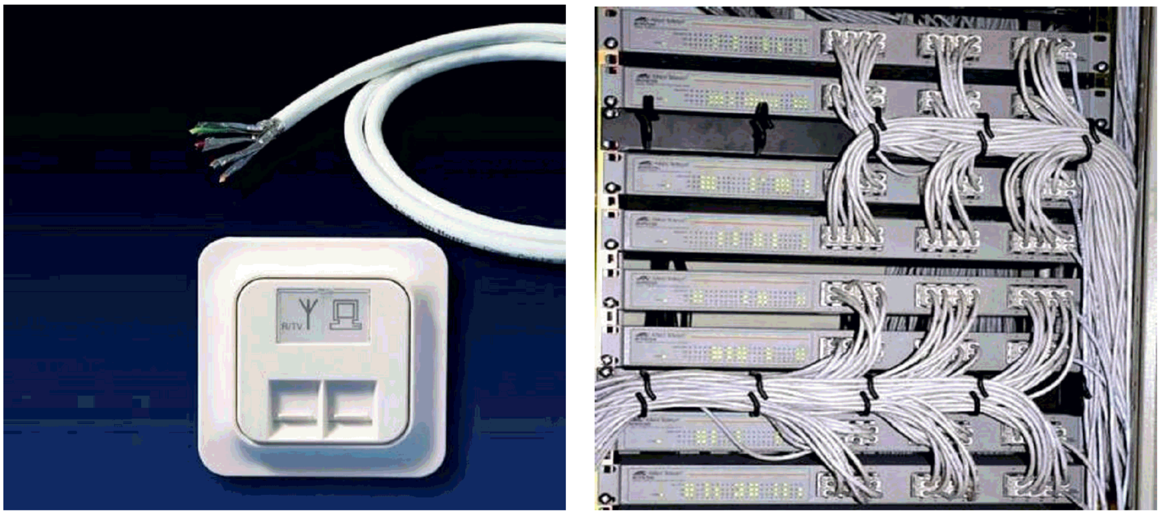


Figure 5.9 – Implementation of Ethernet Connection through RJ45 socket, production of structured cabling

5.2.6 Generic Diagram Topology Based on Twisted Pair Cable

Common switches do not allow to duplicate a link (hubs not at all) otherwise commonly used in the Internet global network.

Figure 5.10 shows the situation when it would be appropriate to implement the duplicate line. Professional switches allow operating the duplicate line, the function is mostly known under the designation "spanning tree".

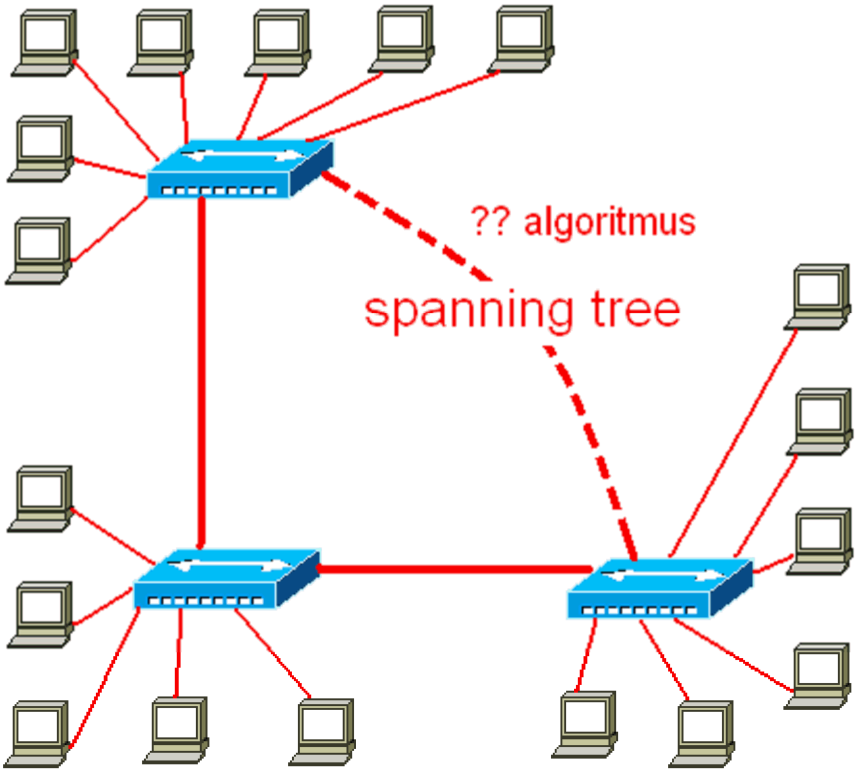


Figure 5.10 – Ethernet connection using switches and twisted pair cable with duplicate line

It is not a general diagram topology, in the true sense. The chart shows that hubs are strictly implemented as a star topology; the added lines create a "spanning tree", a backup activated with the failure of an appropriate port.

5.3 Media Access

5.3.1 CSMA/CD Access Method

The station that wants to send data is listening to whether the network is not used by another station (part of the CSMA, where CS - Carrier Sense - enables to "listen" the transfer, MA - Multiple Access - expresses the overall character of the medium transmission that is shared and all the nodes have access to it at the same time, therefore it is possible to broadcast concurrently from multiple nodes).

If the network is already used, the station is waiting for a randomly chosen interval. If the station finds that the network does not perform transmitting – it starts sending and at the same time it tries to find out whether any collision occurred (CD-Collision Detection).

Collision means that another broadcast station began to transmit at the same time – there is a conflict of signals and distortion occurs. If there is a collision, then the workstation that notices it, stops transmitting and sends a short collision signal (jam) to the network. The jam signal means that the other stations stop transmitting as well and repeat the transmitting attempt again after a randomly selected time interval.

If the broadcast is interrupted by collision 16 times, the attempt to broadcast a message is terminated (aborted) and the higher layer receives an error message. Each following interruption of transmission collisions is randomly selected from a doubled interval.

5.3.2 Access to Medium in Today's a Switched Ethernet

The station sends and receives frames according to the requirements of higher layers. Switch as a counterpart to each network adapter provides the routing according to the physical layer address - MAC (see the article Switched Ethernet, Fast Ethernet).

5.3.3 Frame Format

The frame contains first a broadcasting prelude, so called preamble: 10101010.... 10101010...10101011. (it allows the adapter to synchronize the receiving; the last number ONE (1) starts next transmission). Then addresses of the target and the sender follow: always a 48-bit MAC address (see paragraph „Addresses“).

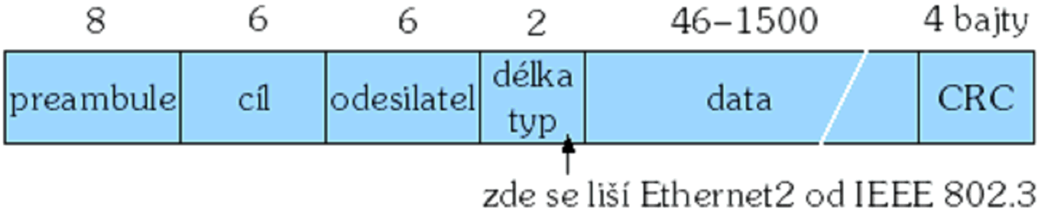


Figure 5.11-Frame format in the Ethernet network

Then follows length and type: the length of the transferred data (IEEE 802.3), the kind of transferred data (Ethernet). Then data: Transferred information (data package of a higher layer, typically IP), supplemented by the "padding" to the minimum length of 46 bytes.

Finally, there is CRC, checksum, a number calculated on the sender and the recipient side compared – when there is a discrepancy, the frame disappears – a higher layer must fix the outage by repeating.

5.3.4 Addresses

In order to be able to unambiguously identify a node in the network, it needs to be assigned a specific designation. Such a designation, so called MAC address, must be unique within the network, which allows a direct communication of computers. In the framework of networks around the world that can be mutually linked with each other it should not occur that there are two or more computers with matching addresses.

The problem does not occur when computers with the same MAC addresses are connected in different separated networks. The complications occur when duplicate MAC addresses appear in the same network; however, due to the fact that users can reconnect their computer to another network, it is better to keep the uniqueness of addresses throughout the world. The simplest, in terms of use and processing, is using numbers from the binary system stored directly in the network card memory.

The address taken from MAC frame can be easily compared to the address stored in the memory of the adapter and this way it can be decided whether the adopted framework is intended to the node or not.

Unambiguousness is achieved by putting the MAC address permanently into the memory of the network adapter during manufacturing. Each adapter is assigned an address different from all other addresses of each produced adapters.

The MAC address begins with a part assigned to manufacturers (this can be, for example, the first three bytes) with further supplemented serial numbers during the production. IEEE organization on behalf of ISO provides the codes allocation to producers.

Division of MAC address into two parts ensures the uniqueness of the MAC address of each adapter and the address length 48 (b) then ensures that the address space is huge, because the number of available addresses reaches approximately 0.3 trillion (approximately one address per two square meters of Earth's surface). Due to the way addresses are assigned, however, it is not an inexhaustible source. There are already estimates of when they will be exhausted.

Each of the 8-bit part of MAC addresses is usually placed as a pair of hexadecimal digits. Notation of a 48-bit address in binary system (using zeros and ones) is unnecessarily long, and therefore MAC addresses are expressed using hexadecimal digits. One 4 bit part is converted to a hexadecimal number.

Example entry: **09-28-A1-A0-D8-F3**

5.3.5 Collision Window

It is as a limiting factor of unswitched Ethernet. Information spread through medium (metallic electrical wire, optical fiber) with the final speed (0,5c to 0,9c, c = maximum speed 299 792 458 meter/sec).

It can therefore happen that computer 1 (at the picture) begins broadcasting/transmitting to a common free medium to computer 2. In a very short time, or even at the same time, computer 3 which successfully detected a free medium, begins to broadcast/transmit (signal from computer 1 hasn’t reached it yet).

If the network meets the maximum size, computer 1 and 2 detect a collision during their broadcasting. They wait randomly long time and start repeating the whole process again (until they are successful).

However, if the network exceeds standard - defined maximum dimensions in a single collision domain, there is a threat that computer 1 and computer 3 end the broadcasting without collision detection.

The signal will interfere at in computer 2 area which discards the frame because there will be a CRC discrepancy. The network will lose data frames frequently.

The condition of the conflict window: **time of media usage < time of broadcasting of the shortest time frame**, otherwise there is a threat of undiscovered collision.

Collision window cannot be overcome - a problem with networks acceleration.

There is a need for a different traffic management. It means, switching in the Office Ethernet or master slave communication – in industrial Ethernet.

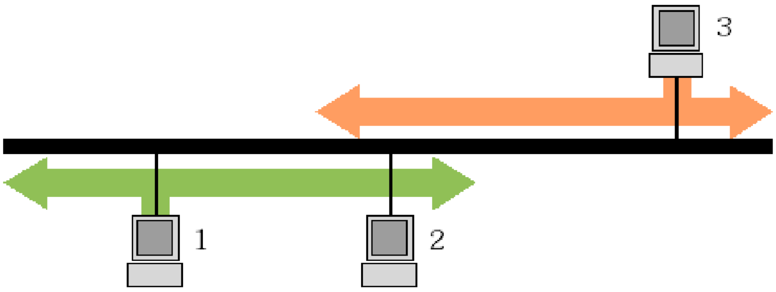


Figure 5.12 – Collision window in Ethernet network with CSMA/CD

5.3.6 CSMA/CD Consequences

Each collision means a waste of time (data is damaged; the transfer has to be repeated).

At the time of greatest interest number of collisions is increasing and the efficiency of media usage decreases.

5.4 Hub vs. Switch, Routers

5.4.1 Hub

It came into existence from the original repeater during the transition of Ethernet from coaxial cable to twisted-pair cable. The picture shows the classic combined design.

The real Hub is a signal amplifier, regenerates the signal back to readable "0" and "1", when it distinguishes between 0 and 1, and sends it further to all ports (not able to relate elements of the different speeds).

It is a basic component in the current industrial Ethernet. However, in offices it was gradually replaced by switches.

Combined devices are often sold under the name of Hub (or even Switch). The principle of one combined device (forming only one single collision domain) is evident from the Figure 5.13.

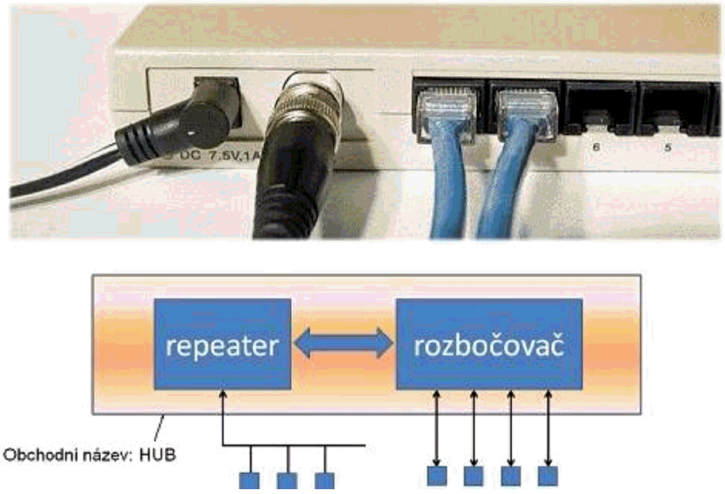


Figure 5.13 - Ethernet Hub with a repeater

Another such device is shown in Figure 5.14, it creates two separate collision domains divided by a switch.

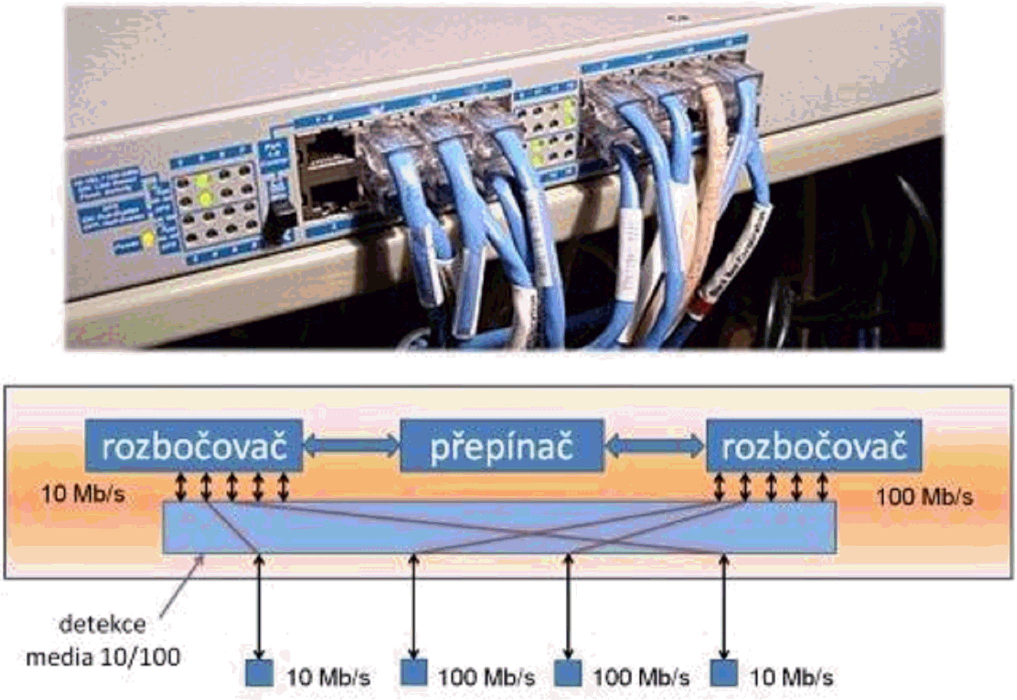


Figure 5.14 - Ethernet Hub with a switch

5.4.2 Switch

Significantly more complex equipment with an auto-configuration allows one to associate devices with different data transmission rates (see Figure 5.15). From the sender's addresses it can gradually learn “who is located where ".

Frames that are destined for yet unknown addressees are sent to all (it finds out very soon from the response where it is located).

There can be problems with cycles and network redundancy, because as a common switch does not allow it, there must be a star or a tree topology and a general diagram is not possible.

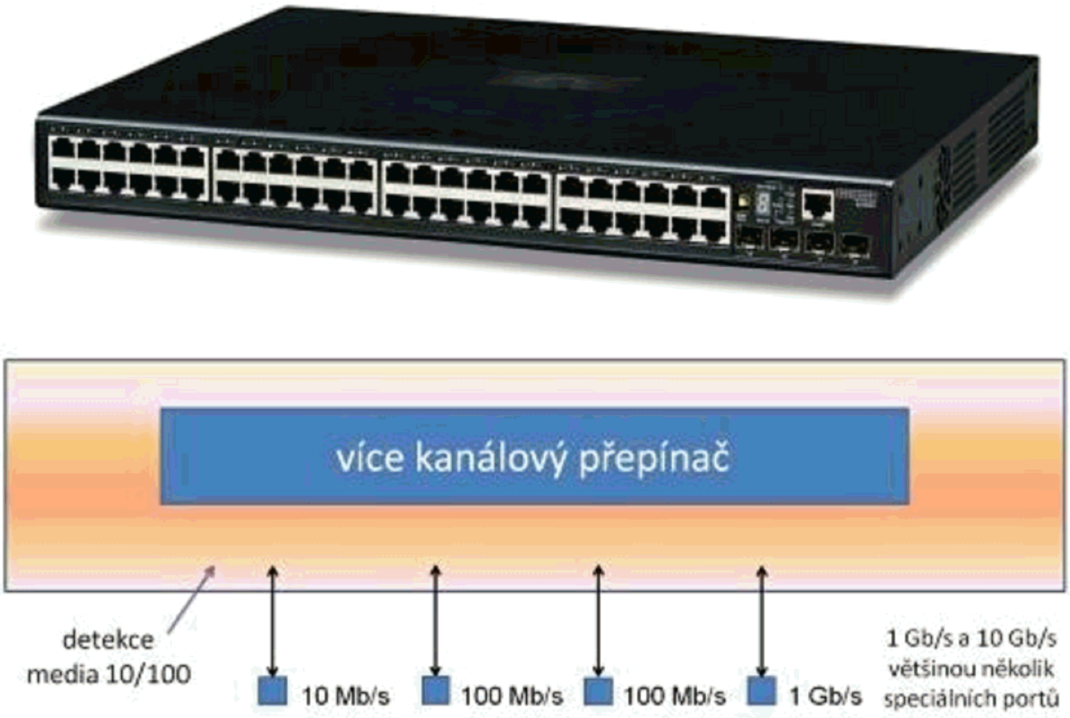


Figure 5.15 - Ethernet Switch

More complex Ethernet devices designed for large-scale LAN allow for redundancy through special technology called "spanning tree". Redundant links are deactivated and it marks a tree in the general diagram. During outages, it restores deactivated lines. In practice we notice problems and incompatibility among various producers. More information is provided in the paragraph „Switched Ethernet, Fast Ethernet“.

5.4.3 Bridge (Media Converter)

This is a switch predecessor. It has two or just a few ports. In fact, it carries out two functions – it filters frames and links of two different networks - network segments (previously collision domains).

These are mostly networks with the same structure of packets in the linking layer, i.e., either the Ethernet or Token Ring or current wireless WiFi networks. Such bridges are called homogeneous.

It is an active element that can distinguish whether the data will remain in the segment, from which it was sent, or whether they should be transferred to another network segment. The bridges are used in the case when we want to combine two or more LAN networks, extend the length of a segment (or increase the number of connected stations) or we want to reduce the load of the network.

The bridge must be able to recognize its immediate surroundings and for that reason it maintains a table of addresses of connected stations. Currently, the so called "self-learning" is used for creating and updating the table of addresses almost exclusively - switch (bridge) itself gradually creates the table based on detected links. It is the most common case.

The bridge is able to function even when such information is not available. Then it will work similarly as a repeater and distribute each accepted frame to all the parties – this way the transfer will not be effective, but it can be acceptable for a short period. It is used during the learning process.

Bridges are currently replaced by switches. Nowadays, under the term bridge we understand rather a conversion between technologies (such as Ethernet and Wi-Fi or Ethernet and DSL).

5.4.4 Router

Similarly to bridge, the router connects two or more networks. The information transfer among networks is carried out, however, on a higher layer (typically on IP level).

The router acts in both networks as a computer with a different IP and MAC address.

The router must know the actual topology of the entire network (in fact all the networks). The volume of the necessary information is significantly greater than at the link layer.

The router's task is to select the appropriate way for that particular frame from the network node, send it to another network node, while both networks can be separated by several other networks, or by a great distance.

It has a built-in packet filtering extended by intelligent routing using IP addresses.

Router is dependent on the protocol of the network layer. The router can link different network architectures (Ethernet, Wi-Fi, Token Ring, FDDI, ...).

Routers are a typical part of the vast WAN networks, but they are also used in LAN networks, for example, for connecting local area networks to the Internet.

Router is mostly designed for professional applications, but there are now commonly available combined devices for small businesses and households under the name of router (Figure 5.16).

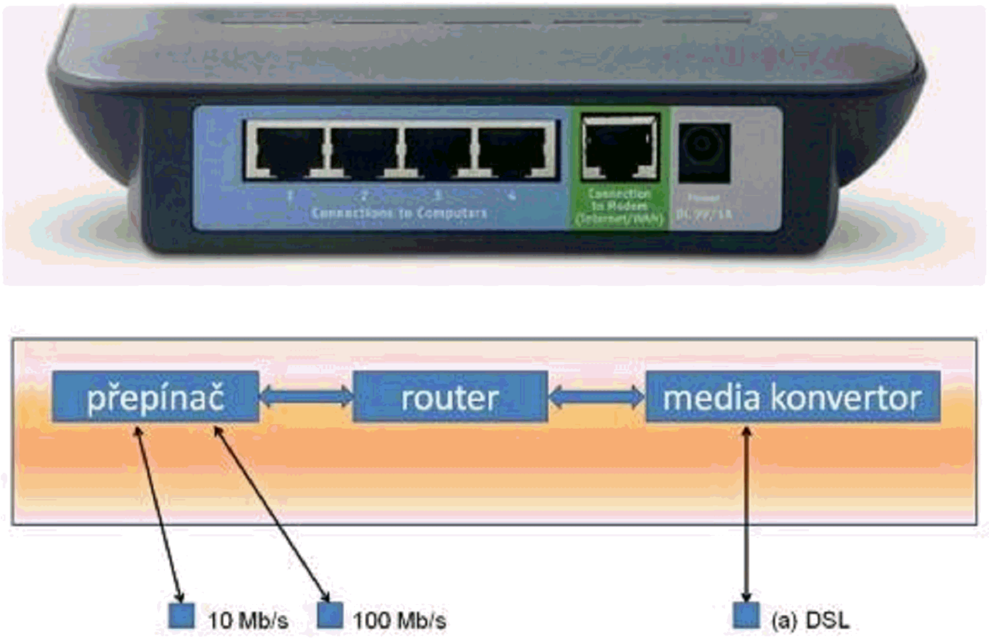


Figure 5.16-Router with an integrated switch and a bridge

Such a router usually executes not only routing, but also assigning a non-public IP address in an internal local area network, more sophisticated ones allow filtering and provide security. The advantage is mainly an integrated media converter for DSL or GSM and 3G modem.

These are mostly devices with relatively low performance, which is barely sufficient to handle the transmission of frames on today‘s offered connection in the range of tens of Mbits. Some female users might appreciate, for example, the appearance of an appliance that can match a laptop – see the picture ☺.

Figure 5.17 – A small GSM travel router

5.4.5 Gateway

Bridges, switches and routers do not care about the data content of the frames, respectively packets. They need to know only addresses. They can link only such systems that "pack" in to the frames/packets, the same data, i.e. the same systems or systems differing in transmission technologies of lower layers.

For cooperation of different systems, it is necessary to understand the transmitted data, and to be able to carry out their conversion. It is a gateways' job. The gates are always application-oriented, which means they understand only the data from a specific application and they operate work at the application layer. It serves for connecting one computer network to another one in some foreign environment. The gates are implemented in software and are always application-oriented, e.g. gateway for the transmission of electronic mail, a different one for printing, etc. The gateways are necessary for the collaboration of different systems.

5.5 Switched Ethernet, Fast Ethernet

5.5.1 The Access to Medium in today's Switched Ethernet

Ethernet passed a significant milestone in its development starting with the collision domain with CSMA/CD algorithm, reaching switched network requiring central elements.

The station broadcasts and receives frames according to the requirements of the higher layers. The switch, a counterpart to a network adapter, provides routing according to the physical layer MAC addresses. If it does not have the information of which port is the target computer with a specific address located, it sends a frame to all, it "learns" with the first response, i.e. makes its routing table.

Switches differ in their algorithms for routing. The simplest switch version "store and forward" saves each frame, finds the target, and then sends the frame to chosen port, or promotes it by using the CSMA/CD algorithm in a mixed network into the appropriate collision domain. Each switch can also function as a multichannel bridge among collision domains (if we use a combination of switches and hubs).

Switches for large networks work more efficiently. They begin to send data framework immediately when they receive the preamble and the header with the MAC of the addressee. Other features of switches focus on security (locks of ports for specific MAC, filtering frames according to the content of a data package of the higher layer - typically IP, VLAN function etc).

In general it may apply that a network based on a switched Ethernet has a higher permeability. Figure 5.18 shows a situation where two groups of computers communicate intensively mainly between themselves.

Switch manages to serve groups so that the sum of the Mb/s may significantly exceed the nominal speed (for example, 100 Mb/s).

Due to collisions, on the other hand, if a hub is used then there would be a transfer with an effective speed that is lower than the nominal speed.

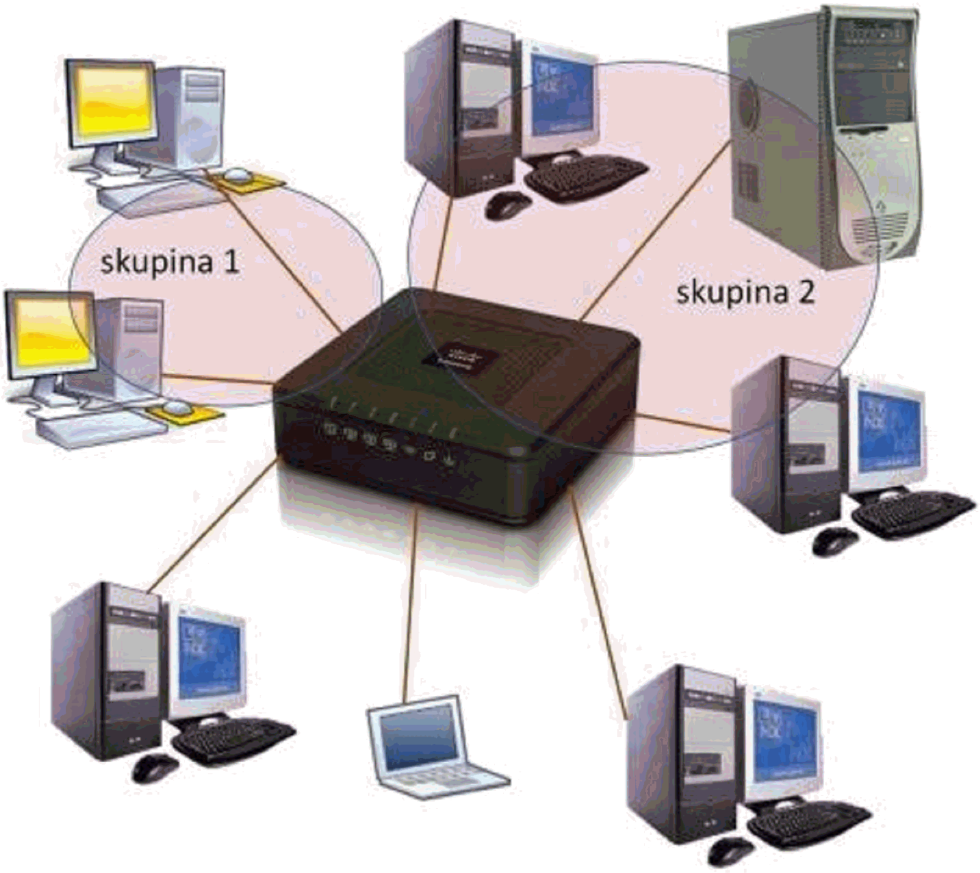


Figure 5.18-Router with an integrated switch and bridge

At the same time it holds that if all of the computers communicate exclusively with one machine (for example, with a router providing and access to a global network, which is the usual situation) using a switch does not bring anything fundamental, in case the switch will be basic type "store and forward" we can expect even worse outcome!

5.5.2 Full-duplex Operation

If we put together a network consisting only from switches, media sharing disappears, each participant may immediately broadcast and does not have to simultaneously listen during the broadcast to detect a collision. In fact it cannot at the twisted pair cable as it is connected to the switch, because the switch sends the data only to a recipient not even back to the sender as a hub does. The receiver of the sending participant is free and can work completely independently and receive different data in one moment (CSMA/CD is completely eliminated).

At present, all Ethernet interfaces support full duplex mode and the mode is usually automatically detected by the interface.

5.5.3 Fast Ethernet

This standard is labeled as 100BaseX and works according to the same rules as in the original Ethernet 10BaseT.

An access to a common media (if it is common and unswitched) is controlled by the CSMA/CD data transfer method.

The same frame format and MAC addresses, the same logic – the software of higher layers without changes.

Defined by the IEEE 8023u (1995).

The same medium - twisted pair cable or optics. Only option to use coaxial cable disappeared.

Differences from the original Ethernet:

- 10 x faster data transfer (100 MB/s), and as a result, 10 times smaller size of the collision domain.
- The maximum size of the network on the twisted pair-cable is 220 meters (100m+10m+10m+100m), therefore, we have to calculate with two hubs (standards allow even for three when we lower the range).
- The optical segment cannot be longer than 412 meters.

Media pro Fast Ethernet:

- 100BASE-TX - two pairs UTP category 5.
- 100BASE-T4 - four pairs UTP category 3, 4, 5, 5e, 6.
- 100BASE-FX – optical fiber.

5.5.4 Gigabit Ethernet

Defined as IEEE 802.3 (optics), IEEE 802.3 ab (UTP)-1998.

Speed 1 Gb/s, the same frame format and same CSMA/CD (rather symbolical, "full duplex" is used).

Gigabit Ethernet can be understood as a reaction to the growing demands of modern applications that have increasingly greater demands on data transmission.

Gigabit Ethernet is not just a ten-fold "blow-up" something that already exists - it is a solution that generates enough power to meet specific needs in the area of quality service guarantees. On the other hand, Gigabit Ethernet is a solution, which consistently builds on compatibility with existing Ethernet versions.

Media for Gigabit Ethernet:

- 1000BASE-TX - for twisted pair cable category 5 (UTP and STP), using four pairs, length 25 m, length 100 m.
- 1000BASE-SX - for multi-mode optical cables of 50 micrometers, the length of 200 m.
- 1000BASE-SX - for multi-mode optical cables of 62.5 micrometers, the length 500 mm.
- 1000BASE-LX - for multi-mode optical cables 1300nm - 500m.
- 1000BASE-LX - for single-mode optical fiber cables 1300nm - 2 kilometers (maximum to 5 km).
- 1000BASE-CX - coaxial cable STP (twinax) - length of 25 m.

5.5.5 Ten-gigabit Ethernet

It again preserves the frame format and CSMA/CD disappears - communication is always fully duplexed.

Defined by the IEEE 802.3ae (2002).

Mostly optical and laser fibers (for multi-mode), if UTP, then category 7.

Media for the Ten-gigabit Ethernet:

- 10GBASE - multi-mode fiber of 62.5 micrometer - 30 m (with a special design up to 300 m).
- 10GBASE - single-mode 10 kilometers (up to 40 km).

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PřF UHK“

Registrační číslo: CZ.1.07/2.2.00/28.0118

6 Internet

6.1 The Origin of the Internet

In 1958, the grant agency (Defense) Advanced Research Projects Agency ARPA-(D) was founded in order to support small teams of scientists who should recover the technological status of the US which, at that time, was partly in a shadow of success of the USSR famous achievements (Launching Sputnik).

On October 29, 1969, under the terms of the supported project ARPANET, the first computer network was launched that interconnected four large university computers in various states of the United States. The main goal was to create decentralized stations where the individual nodes were equally important which excluded the possibility of an easily destructible center.

Figure 6.1 – The Origin of The Internet

6.2 History of the Internet

- **1962** - the project ARPANET supported by the grant agency ARPA - implementation of a decentralized network
- **1969** - ARPANET put into operation (four nodes)-see fig. 6.1
- **1972** - ARPANET expanded to about 20 routers and 50 computers, Network Control Program (NCP) used
- **1972** - Ray Tomlinson is developing the first e-mail program (the effort from the beginning to use the network for communication among people)
- **1973** – the beginning of preparation of the new Protocol TCP/IP replacing the existing NCP/ as replacements for existing NCP
- **1979** - experimental operation of IPv4, the same way as it is still used today (1980 released RFC 791)
- **1983** - Unix version 4.2 supports only TCP/IP v4, Network MILNET (Military Network) separated from the ARPANET, the origin of the Domain Name System (DNS), the first commercial application from SUN, the Internet has already nearly 1,000 nodes
- **1984** –1,000 nodes exceeded, DNS implemented (BIND for DNS program has been developed)
- **1987** – 10, 000 nodes exceeded, the concept of "The Internet" is coming into existence
- **1989** – 100, 000 nodes exceeded, the scientist Tim Berners-Lee from Swiss CERN publishes a proposal of the development WEB (WWW) (Information Management: A Proposal)
- **1990** – ARPANET ends, Tim Berners-Lee and Robert Cailliau published the concept of hypertext.
- **1991** –the deployment of WEB (WWW) in the European laboratory CERN (Scientists Bulletin Board).

- **1992** - 1 million nodes exceeded, the White House connected (Government enters the Internet), the Czech Republic officially attached (on February 13, ČVUT in Prague 6-Dejvice attached)
- **1993** - establishment of the academic network CESNET, Marc Andreessen is developing the first Web noncommercial browser Mosaic
- **1994** - the Internet is commercialized, Netscape Navigator browser developed
- **1996** - 10 million nodes, 500 thousand web servers, Ivo Lukačovič establishes an Internet portal - Seznam.cz
- **1997** - Czech projects, TEN-34 and TEN-34CZ (34 MB/s)
- **1998** - project TEN-155
- **1999** – Napster expands
- **2000** - 100 million nodes, 250 million users, the first 2 GB/s in the Czech Republic
- **2001** - GEANT (10 Gb/s) and the CESNET2 (2.5 Gb/s)
- **2005** - 900 million users, the word Internet begins to be written in lowercase in the Czech Republic
- **2010** - over 2 billion users, Finland as the first country in the world where people can claim the Internet by the law
- **2007** - a work group established, a working version of HTML5
- **2011** – exhaustion of IPv4 addresses on a global level occurred - IANA (Internet Assigned Numbers Authority) granted the last two free IP/8 (the prediction of exhaustion on February 2012), the international IPv6 Day elected –June 8.
- **2012** - HTML5 specification in the "Candidate Recommendation" phase
- **2013** - the exhaustion of IPv4 addresses at RIRS (Regional Internet Registries), individual RIRS work with the last assigned IP/8 addresses. A real lack of addresses was estimated for the year 2020.

6.3 Internet Standardization

The standardization is based on RFC documents - Request For Comments. Although these are not classical standards, they describe the Internet protocols and control the vast majority of the Internet.

Individual RFC documents are published by a RSF editor, according to the commands of the Internet Architecture Board. Each RFC is assigned a number during the publication. The issued RFC is never cancelled; it can only be edited in the future by releasing newer RFC. There are already over 4000 documents.

The RFC draft can be submitted only by selected organizations, but independent submissions are also accepted. The approval process of the documents before publication is quite complicated and differs according to the document source and the categories.

6.3.1 The Typical RFC Proposer - Internet Engineering Task Force (IETF)

- Large community of designers, operators and researchers.
- Participation is voluntary, organized into thematic working groups.
- Develops new protocols, services, etc.
- The working document (draft) is valid for half a year.

6.3.2 Issued RFCS with Granted Status

- **Proposed standard**: proposal (stabilized, without implementation).
- **Draft standard**: at least two (2) independent implementations, sufficient operational experience
- **Internet standard**: matured stable.
- **Experimental:** being examined.
- **Informational**: purely for the users‘ information.
- **Historic**: replaced by an updated document.

6.3.3 RFC and Classic Standard Authorities (ISO, ANSI)

- Unlike conventional norms and standards issued by the classic standard-making institutions (such as ISO, ANSI, etc.) RFC came into existence in a different way.
- The original RFC authors are usually specific experts, who try to solve a specific problem and its solution will be offered to public as a RFS proposal (such as an Internet Draft).
- If a given solution (often already well functioning in the framework of a pilot operation) is considered beneficial, the document is issued as RFC.
- This pragmatic solution of standards established by individuals or small groups on the basis of practical experience has many advantages over the more formal processes of standardization committees like ISO.
- The standards created by the RFC are (due to the absence of any real power on their enforcement) mostly adhered to, with small exceptions. RFC helped the Internet to be developed to today's global proportions.
- Comparing with other conventional standardization authorities, the RFC process is less formal. For example, it is a tradition to issue a fun numbered document in April. The process itself is documented in RFC 2026.

6.4 Internet Protocol

Internet protocol is a basic protocol of network layer and the entire Internet. It performs datagram transmissions where the direction is controlled by IP addresses contained in the headers.

It provides the network service to the higher layers without a designated connection. Each datagram is a self-contained data unit that contains all the necessary information about the addressee and the sender and the order number of datagram in the message.

Datagrams travel through network independently from each other and their delivery sequence does not always correspond with the sequence in the message, a network with a "generic diagram" topology does not guarantee that the individual datagrams will travel through the same way.

The datagram's delivery is not guaranteed, higher layers must ensure reliability (TCP connection or the application itself).

This protocol also deals with segmentation and datagrams rebuilding to and from frameworks according to a lower-layer protocol (e.g. Ethernet).

Protocol IP, version 6 and IP version 4 is currently used.

6.4.1 RFC 791 and RFC 2460

- Holds the Internet together - support for a unified IP, head of the TCP/IP family (IPv 4, today IPv6).

- Allows any device to communicate with each other.

- Without connection (independent datagrams).

- No warranties (best effort).

6.4.2 IP Addresses

- Each interface has its own address.
- When using IPv4, a 32-bit number (2^{32} = 4,294,967,296), approximately 4 billion different IP addresses (in the eighties of the last century when the Internet started it was a big stock, currently it is an insufficient number).
- When using IPv6, 128-bit number ($2^{128} \approx 3.4 \times 10^{38}$), it is approximately 6.7×10^{23} IP addresses on 1m^2 of the Earth's surface.
- Hexadecimal Record 2001:0587:2d03:0115:0391:00ff:5ce8:0a15(IPv6) there used to be a dotted decimal notation, e.g. 195.211.105.5 (IPv4)
- Globally Unique, Distributed Allocation.
- Considering the fact that the first 64-bits and the second 64-bits part themselves are unique (see paragraph Subnets, Table) there is actually 2^{64} addresses, i.e.. 1.8×10^{19} and **per/to 1m^2 of the Earth's surface there are "only" 36, 165 addresses ☺.**
- The Internet is not a network of computers with IP addresses, but a network of networks (addresses have a hierarchical structure).

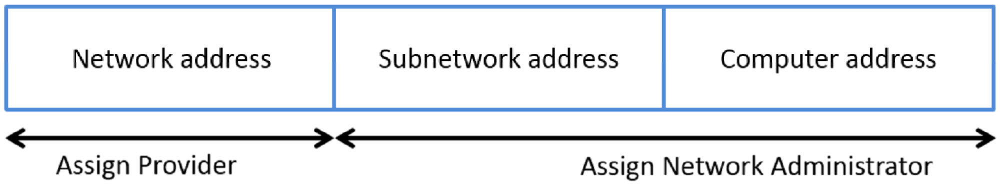
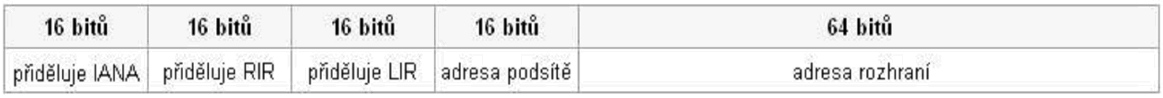


Figure 6.2 – General hierarchical structure of IP addresses

6.4.3 Address Allocation from the Central Authority Towards the Customer

- Central authority - IANA (Internet Assigned Numbers Authority).
- Regional Authority - RIRS (Regional Internet registries) - RIPE NCC (Europe and Middle East), ARIN (North America), LACNIC (Latin America), APNIC (Asia and Pacific), AFRINIC (Africa)
- Local Internet provider - LIR (Local Internet Registry)

- Customer manages the subnet address and connects devices with the interface address (the final/resulting address is 128 bits, as shown in Figure 6.3)



16 bitů	16 bitů	16 bitů	16 bitů	64 bitů
přiděluje IANA	přiděluje RIR	přiděluje LIR	adresa podsítě	adresa rozhraní

Figure 6.3 – Address allocation from the central authority - the structure of IPv6 address

6.4.4 Prefix

- Prefix is the beginning of IP address.
- The length may be different, writing it with slash – separates the address value from the specification of the relevant bits.
- Writing it with prefix dimension: 160.218.0.0/16 - how many bits from the beginning of the address are valid
- Writing with a mask: 160.218.0.0/255.255.0.0 - mask, 11...1 written at the place of significant bits, 00 ... 0 written at place of insignificant bits.
- The part of the address which is not a component of the prefixes is usually zeroed
- Prefix is used in the address allocation, routing, ...

6.4.5 Subnet

- Computers directly connected at the 2nd layer (by Ethernet), computers on the same subnet communicate directly with each other.
- The mask of subnet determines the boundary between the subnet address and computer. Contains 1 in bits of subnet and network addresses and 0 everywhere else.
- 160.218.14.153 with a subnet mask 255.255.255.0. Network 160.218, subnet 14, computer 153, the border is provided by the network administrator. In IPv6 the computer address is constructed from MAC, a subnet contains typically a 16-bit number.

6.4.6 Classless Addressing and Routing

- Classless Internet Domain Routing (CIDR) is defined by RFC 1517 RFC 1518, RFC 1519, RFC 1520.
- In 1995 it was introduced with the aim of economizing IPv4 addresses, networks received only so much space as they needed. Not necessarily IPv6 (for the time being).
- Initially there were 3 lengths of network addresses - class A/8, B/C 16/24 – it was not sufficient, there was not enough addresses in the B class, large routing tables, addresses wasting, therefore, CIDR was founded.
- It is based on sharing prefixes; ISP gets a prefix, e.g. 160.218.0.0/16, its part (e.g. 160.218.1.0/24) is assigned to the customer, outside of ISP network it is possible to summarize its entire space under a single prefix 160.218.1/16.
- There is no need to set the subnet "by bytes", the mask can be created freely (e.g. mask 255.255.248.0 creates a subnet for 2048 thousands of computers and it is not necessary to choose between 256 or 65536).
- The CIDR effect was significant, together with NAT it postponed the moment of IPv4 address exhaustion by about ten years.

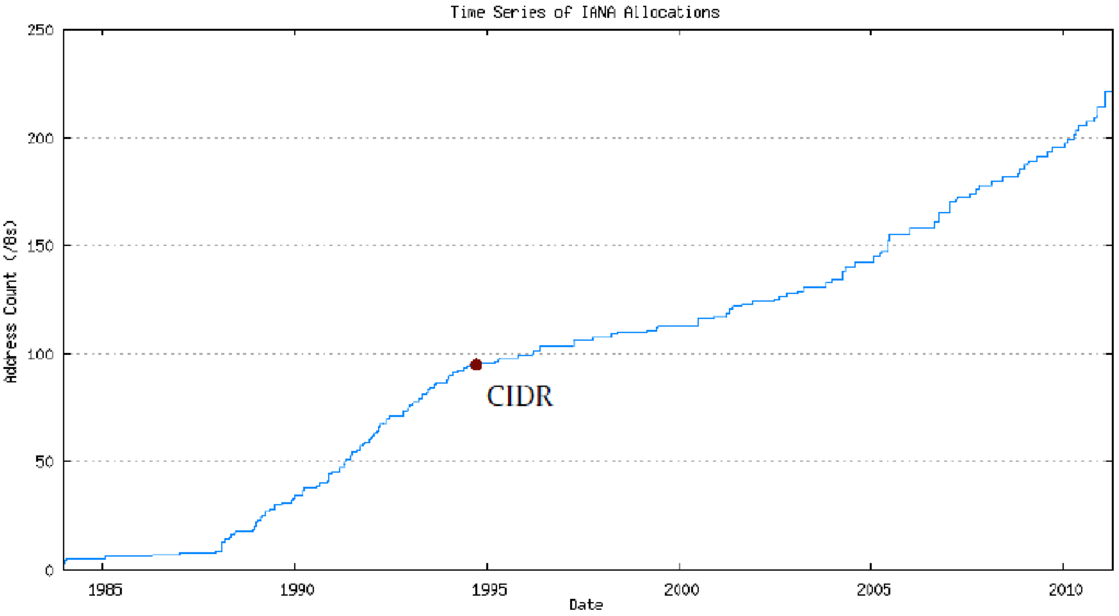


Figure 6.4 – Allocation of IPv-4addresses

6.4.7 Non-Public Addresses

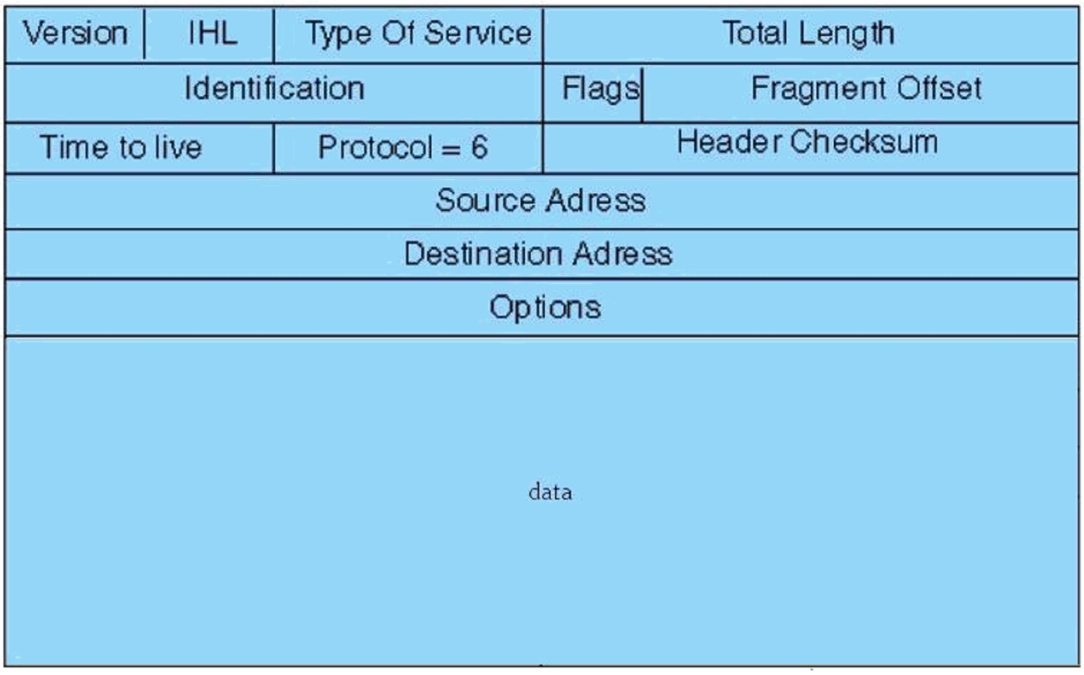
- RFC 1918 defined addresses for private networks (10.0.0.0/8, 172.16.0.0 192.168.0.0/16/16), another way to economize with addresses in IPv4.
- Non-public addresses are not routed in Internet, cannot exceed the local area network.
- Nowadays they are used for extending of the address space in combination with the NAT

6.4.8. Non-Public Addresses Translator

- Network Address Translation (NAT), RFC 3022.
- Translates addresses between two parts of the network, changes IP addresses and ports in passing IP datagrams.
- Typical example: the local network with non-public addresses connected by NAT into Internet – for the whole network only one IP address is used.
- It is commonly implemented in ADSL modems.
- A record in the conversion table is created when a computer "from the inside" sends a packet to the “outside".
- Communication needs to be established from inside - until there is a record in the table, internal computers are unreachable (they do not have public addresses).
- Interferes with the direct communication (video conferencing, iptelephone) – it is necessary to go through an intermediary with a public address.
- The limitation of internal network availability has a positive impact on security, even in IPv6 where NAT is not needed; security substitution was provided (RFC 4864 - Local Network Protection for IPv6). We can also use a state firewall that by default allows entry only to datagrams from addresses used recently from the end network. IPv6 users may only dream about earlier anonymous when using NAT system in IPv4.

6.4.9 IP Datagram

- Version 4, 6.
- The length of the header: in 32-bit words (max. 60 B).
- TOS: Type of Service, the requirements for the transport.
- The total length: max. 65 535 B.
- TTL: Time to Live, each router decreases by at least 1, discards it after reset - loop protection.
- Protocol: Protocol of the 4th layer of the data (TCP, UDP).
- CRC: does not include data (this safety lock is managed by lower layers)
- Displayed on the following figure/ image



Version | IHL | Type Of Service | Total Length

Identification | Flags | Fragment Offset

Time to live | Protocol = 6 | Header Checksum

Source Adress

Destination Adress

Options

data

Figure 6.5 – TCP Datagram (packet)

6.4.10 Fragmentation

- IP protocol is adapting to the existing technology of the lower layers through fragmentation
- IP datagram can be significantly larger than the frame (MTU, Maximum Transmission Unit) transmitted by a lower layer (it is typically Ethernet).
- If the datagram > MTU, it will be divided into fragments.
- All the fragmented datagrams have the same identifier; fragment shift indicates which position of the original datagram data of this fragment start.
- All fragments except the last one have the setting "More Fragments" in flags. The total length is updated.
- Fragments are separate datagrams transmitted independently, they can be further fragmented, the datagram receiver composes them together.
- There is a setting among flags with a command "Don't fragment", which prohibits the datagram fragmentation.
- MTU paths - the sender tries to find the largest possible size that does not cause fragmentation, which itself is ineffective (today it is realistically possible to place one whole IP datagram into an Ethernet frame).

6.5 Protocols for Work with the Physical Layer

The network layer implements auxiliary protocols for identifying errors and assigning IP addresses to physical addresses.

In IPv6 neighbors' discovering (Neighbor Discovery) dominates, using a sequence of several ICMPv6 messages.

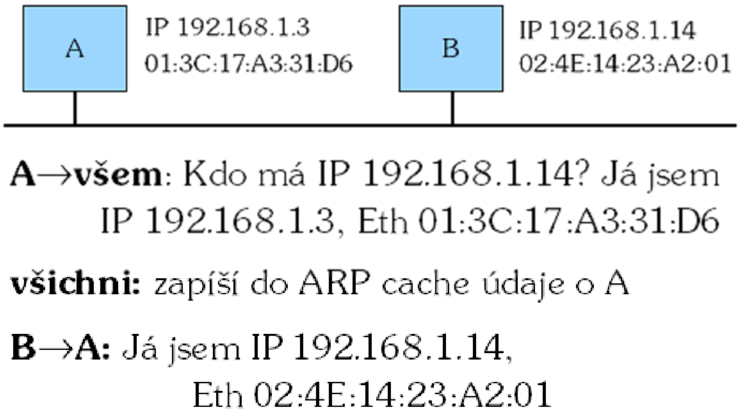
In IPv4, the connection between the physical MAC address and the IP address does not exist (IP address does not contain the MAC address), it is solved by broadcasting to all (public frame, broadcast) with the query to assign IP and MAC-ARP, see below.

6.5.1 Address Resolution Protocol (ARP)

• Protocol provides the assignment of IP addresses to physical addresses of the link-layer. The actual network communication happens using the physical addresses.

Protocol has two basic functions:

- to obtain the MAC addresses corresponding to the destination IP addresses.
- maintain assignment tables of IP and MAC address on each of the nodes in the network



A→všem: Kdo má IP 192.168.1.14? Já jsem
IP 192.168.1.3, Eth 01:3C:17:A3:31:D6

všichni: zapíší do ARP cache údaje o A

B→A: Já jsem IP 192.168.1.14,
Eth 02:4E:14:23:A2:01

Figure 6.6 – Address Resolution Protocol (ARP)

Procedure:

- When the IP protocol receives a request to send a datagram, it gets the IP address of the destination node from the higher layer, it searching in the existing ARP table.
- If the destination IP address is not listed there, it sends ARP Request. It is a public frame (broadcast) with a request for the MAC address, which belongs to the corresponding IP address.
- The ARP protocol of mode with the appropriate logical IP address responds to this request by the response frame (ARP Reply) that carries the desired MAC address.
- The ARP protocol then updates the ARP table, together with all nearest neighbors - typically computers in the local network (Ethernet). The mechanism is obvious from Figure 6.6.

6.5.2 Reverse Address Resolution Protocol (RARP)

- The protocol is used when the physical address is known to obtain the IP address. It is most common to detect IP address when you boot the system (in case of diskless workstations that need to find out their IP address from the network server).
- Station generates RARP request to a universal address with its physical address and expects a reply with information about the allocated IP address. The RARP server contains the database of hardware addresses (MAC) with the assigned IP addresses. RARP request contains specific hardware address and RARP server returns a response with a filled out corresponding applicant IP address. The format of RARP messages is identical to ARP.
- The IP address is insufficient information for full communication of a station (mask is missing, gateway, DNS, ...), that's why RARP is now replaced by more complex protocols from the application layer (BootP or DHCP).

6.5.3 The Internet Control Message Protocol (ICMP)

- Serves to transmit error and control messages between nodes and routers. Protocol messages are transmitted in exactly defined form in the data part of IP packets.
- ICMP functions include:
- Testing of availability and status of IP network destination node (Echo Request/Reply).
- Controlling of network congestion and the packet flow (Source quench).
- Updating of routing tables of IP router nodes (the Redirect).
- Sending the subnet mask (Address mask request/Reply).

6.5.4 The Internet Group Management Protocol (IGMP)

- It is used for dynamic logon and logoff from a group at a multicast router in its local network.
- It also resolves situation, when two and more multicast routers are connected in the network to prevent the dissemination of extraneous information in the network. Routers work in two modes: “requester", which sends queries about membership and “listener," which only listens and is non-active.
- Procedure:
- The station logs on to or logs out of multicast group using messages "Membership report” and "Leave group".
- Simultaneously, however, the router is sending a periodic query "General query" to workstations in the local network whether there is at least one station that wants to receive information from the group.
- If there is no reply within 10 seconds, it clears the record about the group from the table. This query solves the problem when some stations, for example before shutting down, do not make it to logoff from subscription.

6.6 UDP Communication, User Datagram Protocol

Defined by RFC 768:

- The only goal is to address applications that can send datagrams independently on one another. It is then irrelevant whether communicating applications run on one machine or whether these are two most distant machines on Earth.
- Datagram service complies with a variety of applications without warranty (DHCP, DNS, interactive - IP telephony...). Each application can send a datagram to any other in the world (except for IPv4 NAT.). Despite, this only 2 percent of data are transmitted in the network by UDP protocol.

- A port is added to the address which puts the addressing down to the application level (each application keeps track of "its" port).

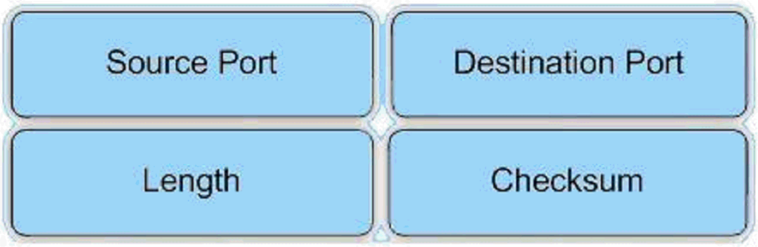


Figure 4.2 – Datagram (packet) Extension for UDP

- 65,536 ports (unlike IP address, V4 was and has always been a 16-bit timeless great number and there is no need to change it).
- Communicating applications connect to a port (OS service) and they listen, receive and send data. When sending, you need to know the application port number. The port numbers of the usual services are standardized (if the user does not enter the number, it is completed by a standard one for a given protocol). Clients use random higher port numbers. Ports 1-1023 are called well known ports. In Unixes and derived operating systems, there are root user rights needed for using it. Ports 1024-49151 are registered. Ports 49152-65535 are used for “client server“ communication.
- Due to a lack of guarantees, UDP applications must accept some losses, errors or duplications. Some applications (such as TFTP) may, if necessary, add a simple mechanism of reliability to the application layer. The applications using UDP mostly do not need a correcting mechanism, they might even be hindered by installing them (IP telephony). If the application requires a high degree of reliability, TCP can be used instead.
- As UDP lacks any mechanism of prevention and control of network congestion, it is necessary to discard redundant UDP datagrams on routers. A partial solution to this problem is DCCP Protocol (Datagram Congestion Control Protocol).

6.7 TCP Communication, Transmission, Control Protocol

Defined by RFC 793:

- Reliable transportation, required by most applications transmitting continuous data (files).
- Protocol handles a stream of bits without structure (bit pipe).
- Associated service, virtual circuits, connections are maintained at the ends, underneath the connectionless IP (datagrams travel through the network independently similar to UDP).
- Using a buffer the sender and the recipient divided group the data for maximum efficiency.
- Transfer (bit pipe) full-duplex connections, regardless of the physical layer (if the physical layer works in half duplex mode (un switched Ethernet, Wi-Fi)), the transmission parameters are slightly worse, but the application layer works the same way (only enters data into a pipe and reads incoming data).

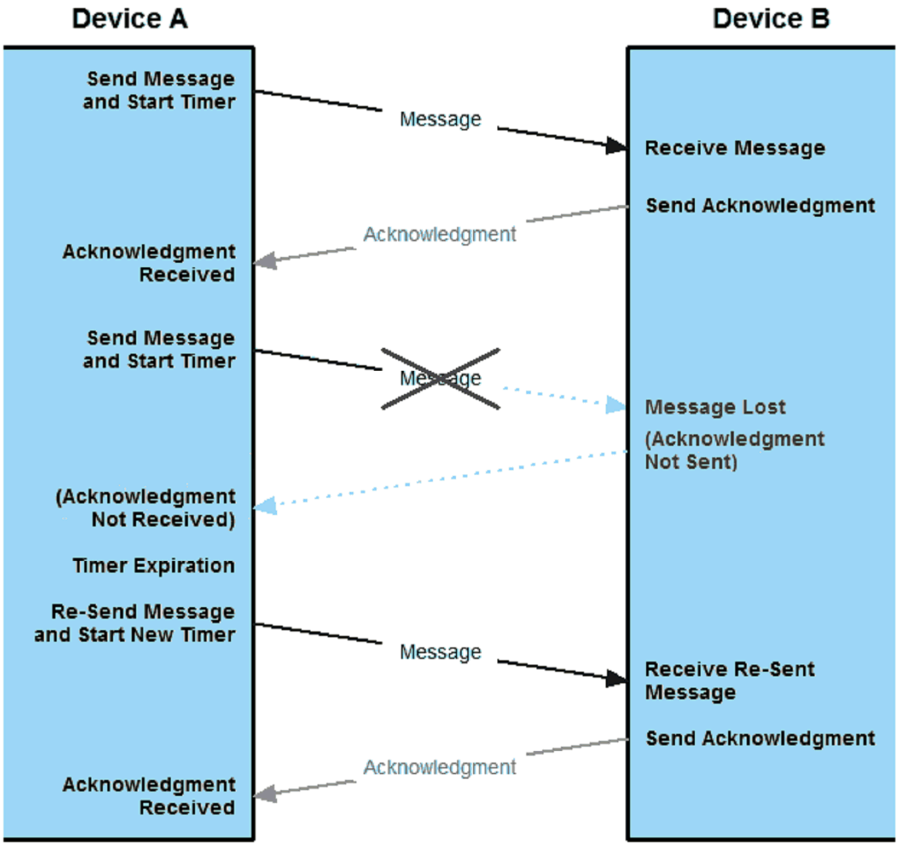


Figure 6.8 – Ensuring reliability of TCP communication

6.7.1 Ensuring Reliability

- Validation deals with losses of packets, see Figure 6.8.
- TCP tackles with reversing packets and duplications on the recipient's side, order numbers - TCP numbers bytes (octets).
- The protocol confirms the longest continuous prefix from the beginning of the broadcast (sends number of byte that it expects).
- Simple, unambiguous and optimized, the loss of the confirmation may not cause recurrence.
- Impossible to announce space.
- Checking is not as simple as the picture shows, not every datagram is validated and it is not validated immediately, see below.

6.7.2 Confirmation Timing

- Piggybacking - confirmation tries to put itself to the data in the opposite direction.
- Waiting 200 ms, if a suitable packet appears.
- Problem: how to set the timer for repeating.
- Too little - it will be unnecessarily repeating.
- Too big - a blackout will be discovered too late.
- There is no universal value; it must be adjusted to the network behavior.

6.7.3 Timer Settings

- Based on the average response time (RTT) and the average deviation (MD).
- Confirmation arrives with delay M:
  - deviation = M-RTT
  - RTT = RTT + 0,125 tolerance
  - MD = MD + 0.25 (|tolerance| - MD)
  - Timer = RTT + 4 MD
- Timer doubles for repeated packets.
- Does not count repeated.

6.7.4 Sliding Window

- Increases efficiency – no need to wait for confirmation.
- Prevents flooding of a slow receiver.
- Allowed to broadcast only up to the top part of the window, then waits, see the principle of Figure 6.9.
- The size of the window is specified by the recipient, must not "flinch".
- Empty window - must wait until the recipient opens.

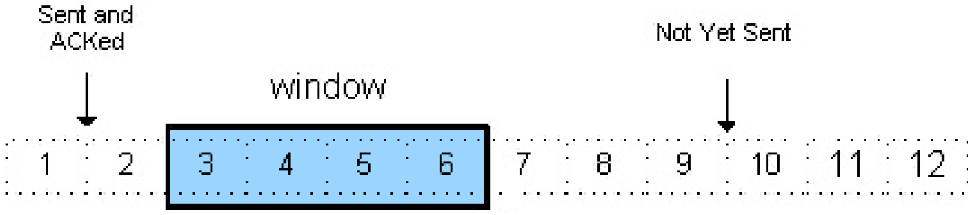


Figure 6.9 - Sliding window in the TCP communication

6.7.5. TCP Datagram, Segment, TCP Header

- Header length in IPv4 in 32-bit words, generally see Figure 6.10.
- Flags:
  - URG - the segment contains urgent data
  - ACK - contains a valid confirmation
  - PSH - pass the target application as quickly as possible (push)
  - RST – a sudden stop of connection (reset)
  - SYN – a connection restart (Synchronization of order numbers)
  - FIN – finishing of sending data, half-closing
- Checksum is calculated from the pseudo header + header + data.

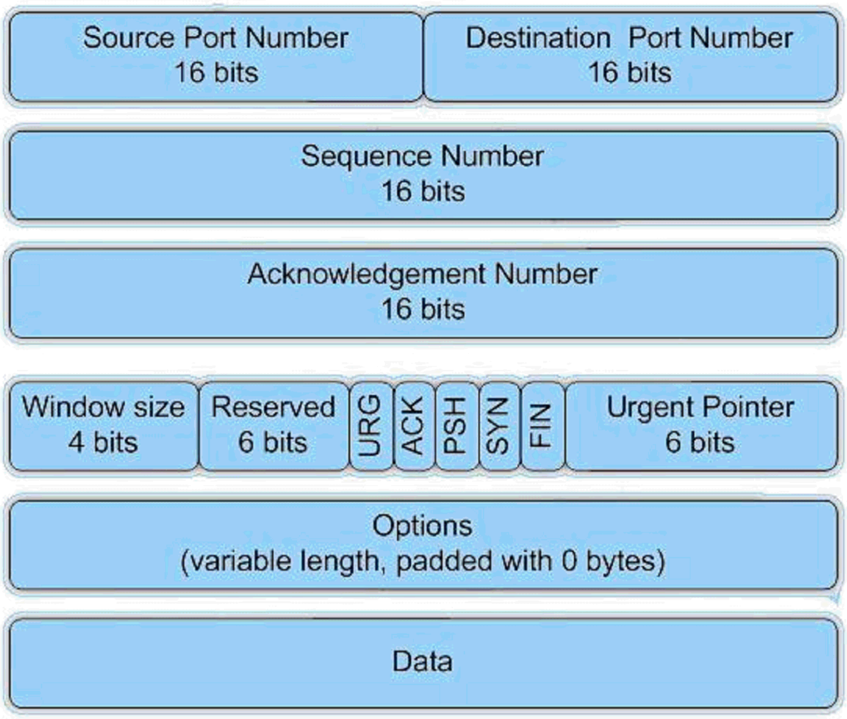


Figure 6.10 - Packet Datagram Extension for TCP segment

6.7.6 Establishing Connection

- To be able to transmit data using the TCP protocol, connection must be first established. A three-way handshake is used for establishing the connection, see Figure 6.11 on the left.
- During the connection establishment, two parties agree on a sequence number. Sequence number and acknowledgment number are 32-bit values reported in TCP header.
- Once a connection is established a TCP segment is sent that has set flags in the TCP header. These are 8 bit values CWR (Congestion Window Reduced), ECE (ECN - Echo), URG (Urgent) , ACK (Acknowledgement), PSH (Push), RST (Reset), SYN (Synchronize), FIN (Finish).
- Establishing a connection takes place in three steps:
- The client sends a SYN packet with that sequence number (x), response number is 0.

- The other party stores the sequence number (x) and responds with a **SYN- ACK**, sets its number (y) as a sequence number and inserts (x +1) into answers number – the next expected value.
- The client responds with an **ACK**, sequence number (x +1), the responses number (y +1).

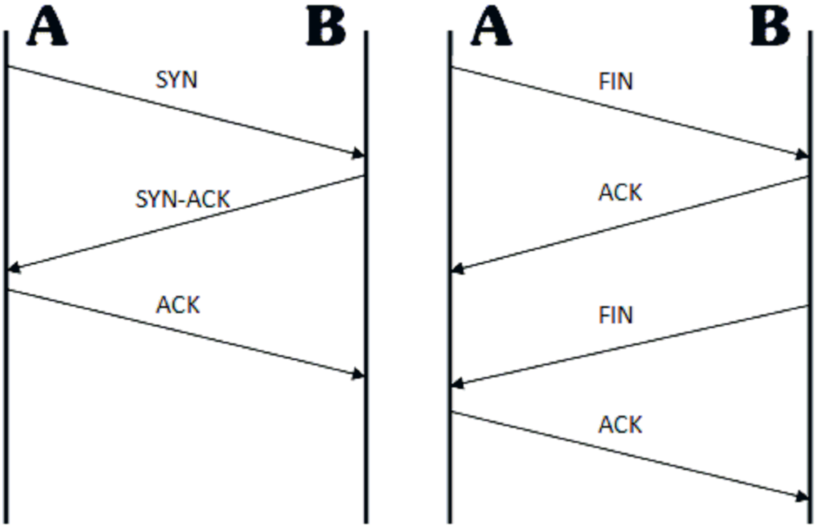


Figure 6.11 – Establishing and closing connections in the TCP Communication

6.7.7 Connection Termination

- Based on half-close.
- One party announces that it has completed the broadcast, but still accepts and acknowledges data - counterpart may finish.
- Principles for connection terminating are similar as with its establishing, it is also shown in Figure 6.11 on the right.
- The four-way handshake is commonly used, when each party closes the connection separately. Sequence **FIN** with the response **ACK** is used in this case.

6.8 Application Protocols

- Creates the application layer of TCP/IP network architecture.
- Some protocols are dependent on the TCP transport layer service (FTP, Telnet, HTTP, ...).

- Some protocols use (require) only the UDP service of the transport layer (DHCP, BOOTP, TFTP, ...).
- Protocols using TCP and UDP transport layer service "at the same time" and less frequently (DNS is used for queries when translating UDP, while for transportation of configuration is uses TCP as a supplement).
- The application layer consists also of user programs that use custom protocols (for updates of new releases, data transfer, video, audio, chat).

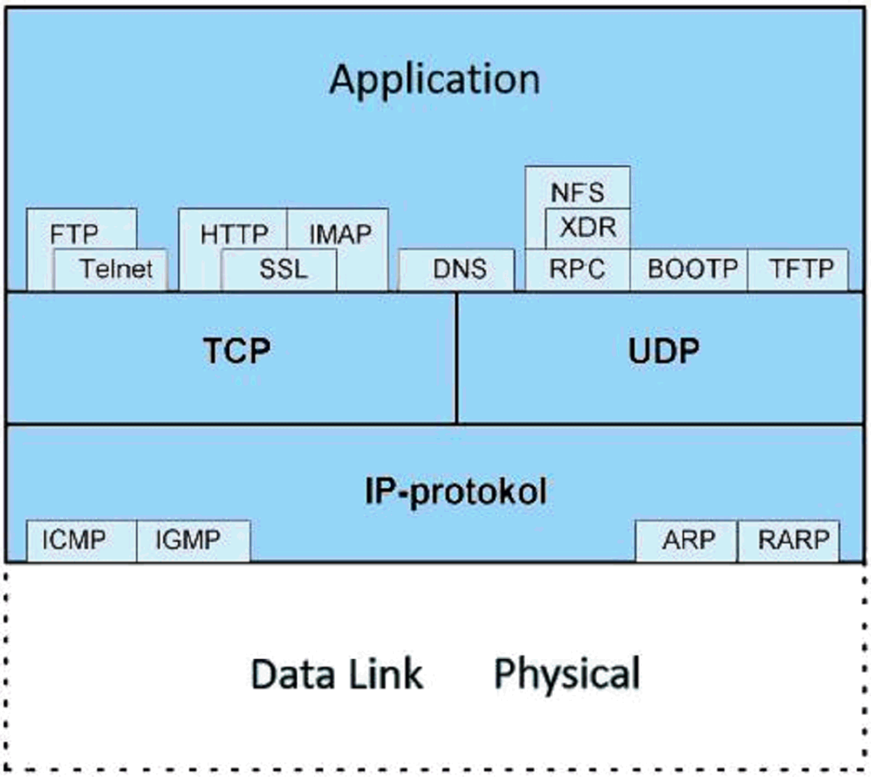


Figure 6.12 – Protocols and layers according to The Internet Architecture

Frequently used Application Protocols (some of them supported by RFC documents):

- Bootstrap Protocol (BOOTP)
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- Telecommunication Network (Telnet)
- Secure Shell (SSH)
- Remote Desktop Protocol (RDP)
- Lightweight Directory Access Protocol (LDAP)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Trivial Transfer Protocol (TFTP)
- Network File System (NFS)
- Server Message Block (SMB)
- Simple Mail Transfer Protocol (SMTP)
- Internet Message Access Protocol (IMAP)
- Post Office Protocol (POP, POP3)

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Projekt OP VK „Inovace studijních oborů zajišťovaných katedrami PřF UHK“

Registrační číslo: CZ.1.07/2.2.00/28.0118

Literature

[1] Tanenbaum A.S. *Computer Networks*. Prentice Hall 2002.

[2] T. J. Velte, A.T. Velte. *Síťové technologie Cisco*. Brno: Computer Press, 2003. 743 s. ISBN 80-7226-857-0.

[3] I. Rukovanský, O. Kratochvíl. *Bezdrátové počítačové sítě*. Kunovice : Evropský polytechnický institut, 2007. 82 s. ISBN 978-80-7314-112-7.

[4] Peterka J. Archív článků [online]. Dostupné z: <http://www.earchiv.cz>.

[5] Stevens W. R. *TCP/IP Illustrated volume 1*, Addison-Wesley 1994.

[6] R. Pužmanová. *Moderní komunikační sítě od A do Z*. 2. aktualizované vydání. Brno: Computer Press, 2006. 432 s. ISBN 80-251-1278-0.

[7] Standardy RFC, IEEE, ISO, OSI [online]. Dostupné z www: <http://standards.ieee.org/>.

[8] L. Dostálek, A. Kabelová. *Velký průvodce protokoly TCP/IP a systémem DNS*. Praha: Computer Press, 2002, ISBN 80-7226-675-6