Interreg
EUROPEAN UNION
Austria-Czech Republic
European Regional Development Fund

INFORMATICS

Networks

UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

VŠTE

EUROPEAN UNION

Contents

1. BASIC TERMS

This part offers a comprehensive definition of basic terms which students may encounter in the area of computer networks. It is also necessary to say that suggested notes may not be considered as precise definitions; it rather refers to a complex area with many notable exceptions to the rule. All the same, students should have at least a broad conception of these keywords and should be able to efficiently use them.

Client means a computer connected to a network. It usually does not have any privileged status and his opportunities are similar to those of other clients. This term may also be encountered at labelling software which communicates with the server and, in this way; it provides a user with an essential service (FTP client, e-mail client etc.).

Server refers to a computer with a privileged status in a network. He is charged to provide the clients with essential services or functions, e.g. effective communication of clients, domain name transfer to the IP address (DNS), internet connection, print, sharing files etc. However, the server may be regarded as a client with respect to a different server. They are usually computers with a specific construction (special processor, disk arrays etc.).

Router is a device securing the packet routing. It involves a network element with a detailed knowledge of its environment and, simultaneously, it secures the packet routing in the right direction. Considering a packet as a letter, the router would play a role of postal service. Nevertheless, its application goes further; it guarantees high-quality services, secures TTL (a parameter limiting the lifetime period of packets so as not for the lost packet to stray forever); it should thoroughly explore its surroundings and find out network changes. At the same time, it calculates the best route to further hubs.

Packet includes a fixed dataset sent via network. Data are usually (almost never) not sent as an uninterrupted flow of information, but as datasets, i.e. packets. This elaborate system strengthens its security, secures right routing and effective use of the network capacity. Although the packet has a rigid structure, it usually contains sender's and receiver's address, information about the protocol, data or other supplementary information.

Network card is a hardware component (nowadays, usually integrated in the motherboard) which secures network connection. Contained information is transferred to packets and packets are collected to data. The card may carry out a specific protocol of data transfer (usually Ethernet) and also contains a port for cable connection (twisted pair, optic fibre, coaxial cable). Moreover, it contains a specific MAC address, which is unique all around the world and serves as the computer identification in the network, or alternatively, it generates a local address.

Port includes a number from 0 up to 65535, which identifies an application currently used as a means of communication. Individual applications are identified within TCP or UDP protocol. The ports enable an application servicing; secure (to a certain extent) the quality of services etc. As a matter of fact, there are fixed port numbers, e.g. SMTP contains 25, and POP3 110, HTTP 80 or FTP 21. All the same, however unusual is it, users or applications may agree on a different number of ports.

Medium represents a physical environment by which a network communication is carried out. It involves led media, i.e. classic cabling (optic cable, metallic cable, twisted pair) or wavelength media (air, vacuum), which use technologies such as Wi-Fi or GSM.

Protocol is a formal language defining the way of communication (IP, TCP, and IMAP4). It accurately describes the packet, i.e. the speed it should be sent; furthermore it defines security elements, corrects errors etc. Almost each layer of ISO-OSI model contains its own group of protocols. They are usually bound only to one layer.

Switch means an active network element connecting its parts. In contrast to a bridge, it allows connecting more than two network circuits. Smaller networks parts have a better access to the medium, as a result of which a higher transfer speed and network usage is secured.

Repeater refers to a simple device securing the signal transmission in a longer distance. It is situated within a certain distance from the transmitter and strengthens the incoming signal. In this way, it operates straight on the physical layer.

I.I. What is a computer network good for?

Companies install computer networks mostly in order to share resources and enable a direct communication. Resources include data, application and peripheral devices, e.g. external floppy disk drive, printer or modem. Direct communication involves sending messages, replying to messages or e-mail.

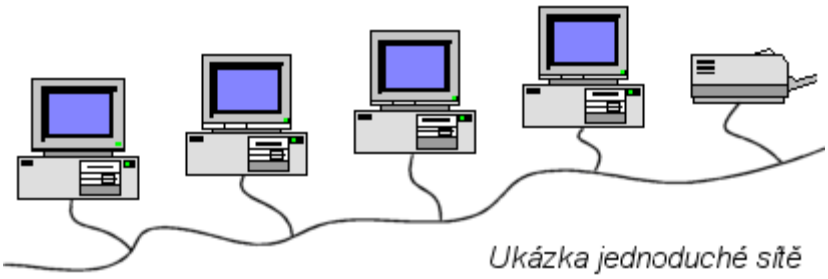


Illustration of a simple network 1

Computer network is a general term for technical devices by means of which a connection and data exchange between computers is carried out. In addition, it enables users to communicate according to the rules. The soundest reason for the network connection is sharing information and technical devices.

Picture 1: a star shaped network connection

According to the vastness, four computer networks may be distinguished:

- **PAN** (**Personal Area Network**) is a network covering a very small area (smaller than LAN area); network includes communication devices such as mobile phone or laptop,
- **LAN** (**Local Area Network**) is a local network covering a small area, i.e. an area larger than PAN, but smaller than MAN,
- **MAN** (**Metropolitan Area Network**) is a network larger than LAN and smaller than WAN,
- **WAN** (**Wide Area Network**) is a network covering a huge area, i.e. an area larger than MAN,
- **VLAN** means a virtual LAN (network). It is a virtual network created within LAN network which operates within one hardware component (cable). VLAN runs on the grounds of interpreting data, which are transmitted via the network. The data are interpreted according to the appropriate network.

2. NETWORK TOPOLOGY

Network topology describes the physical connection. To put it more precisely, it is possible to discriminate between a logical and physical computer connection.

Ring topology refers to a circular connection of computers. In this way, one computer is always connected to two others. The biggest advantage of this model is that as long as one element falls out, the network may (supposed it is duplex) go on. Likewise, the nearest computers (in LAN network) usually communicate the most often.

Mesh is probably the least used topology. As a matter of fact, there are not any cardinal rules; thus, it is created ad hoc by progressively connecting computers. On the other hand, of interest may be its description, which is actually very simple. Logically, it is possible to say that Mesh is an internet considered as a whole.

Star represents one of the most common models of connecting; its individual stations are connected to one central point (e.g. a server), which provides all the communication. A big advantage is its effective management and clear direction; on the other hand, a weak point is the server.

Tree refers to another frequently used topology. As a matter of fact, there is a complex structure of computers connected to a structure of a mathematical tree. In this way, individual computers may (unless end-to-end or root computers are to be dealt with) play the role of the server and client at the same time.

Bus concerns a model in which stations are progressively connected to one medium; thus, a concept of a shared medium is to be dealt with.

Naturally, there are other important topologies – linear, interconnection or an extreme case of a point-to-point connection. Usually, it is something in between.

2.1. Computer networks and their services

Computer network is a general term for technical devices by which a connection and data exchange is carried out. Furthermore, it enables users to communicate according to the rules. The main reason for the network connection is to share information and technical devices.

Picture: computer network

2.2. Network topologies

Topology refers to the way of connecting computers. In addition, it contains the information about the particular connecting computers and their communication. Possible methods of connecting are depicted below.

Bus topology Star topology Ring topology Unlimited topology

Picture: Topology – possible connecting computers networks

The connection of bus topology is provided by a transfer medium called bus, to which all end-to-end computers, i.e. network hubs, are connected.

Star topology refers to a star shaped network connection. It is the most frequent method of connecting computers based on a computer in the middle called a central computer. It is connected to other computers around. It is possible to imagine that one or more end-to-end computers are replaced with the central computer. Thus, the whole network is progressively growing.

Ring topology refers to a connection where one hub is connected to other two hubs in the way of a ring. However, this topology is not very fast since a huge number of hubs prevent fast data transferring to the target computer. Moreover, supposing one of the hubs does not work, the data transfer is not possible; thus, the whole network stops working. This sort of connection is not much used nowadays as the star topology is much more reliable. On the other hand, the costs of building up this network are lower.

3. WHAT IS THE INTERNET?

The internet is a global network similar to a common computer network. Computers are interconnected as a result of which they may communicate and share information. The internet consists in connecting already existing networks with a coherent structure and distribution.

The internet may also refer to computer system containing information and networks which provide us with the particular information.

Computers within the internet play the role of clients or servers. Servers provide internet services; subsequently, clients make use of these services. In addition, internet services secure data transfer to a client upon request.

3.1. Origin of the internet

During the Cold War, the US needed a functional management system able to connect the most important academic, government and strategic computers (countries, military bases etc.). The key requirement was to build up a strong network which would be running despite falling out of several network hubs and at least a partial communication would be secured.

As of 60s of 20th century, RAND Corporation Company was asked for solving the problem which lay in smooth running of computers even after a nuclear war. The main task was to devise a stable system despite a possible destruction of its parts.

In 1964, the same company came up with a comprehensive solution, which was based on two central principles.

- Network does not contain any central component
- Network is running although some of its parts are out of order

With all that said, the American army, i.e. Pentagon may be considered as the Internet creator. In 2010, 2 billion active internet users were registered.

3.2. The internet development

Zero phases

A zero phase began when the American army needed to establish an effective communication between government departments in case of nuclear war during the Cold War. The US Department of Defence, i.e. ARPA Agency (Advanced Research Projects Agency) set up ARPANET Network and managed financing of this project.

First phase

The first phase allowed access to the then most powerful computers, mainly to those of universities in the USA. In the late 1969, the first network hubs of ARPANET Network were placed at those universities. The main goal was to connect not only one computer, but the entire network. The development took place in all possible organizations; subsequently, local computer networks started to run. The beginning of 80s saw a rapid development of ARPANET which also went on in other networks. Thus, networks such as Usenet or BITnet were created. As a result, all the networks were connected to ARPANET. In 1987, more than 10,000 network hubs were registered; two years later, it was more than ten times more.

80s and 90s expanded services that people of today are familiar with and make a use of; it was mainly e-mail (1971), telnet (1972), TCP (1974) and its updates on TCP/IP (1978), DNS (1983) and its start in (1984).

In 1980, Pentagon decided that preferred protocols for the Defence Department would be TCP/IP protocols and 2 years later, all the computers connected to ARPANET network had to change for TPC/IP protocols. In this way, ARPANET became an incipient network and a conglomerate of co-existing and newly established networks, which was called the Internet, began.

Second phase

The second phase goes through the internet development in 1983-1992. This period is characterized by a dramatic growth of the internet and, mainly, its huge expansion beyond American continent. ARPANET also connected other networks such as NFSNET, EUNET, EARN, JUNET etc.

In November 1983, DNS domain system which allowed numeric addresses allocating domain names was introduced.

In 1989, WWW (World Wide Web), which afterwards became an integral part of the internet, was established.

The year 1990 saw decommission of ARPANET and its subsequent cancellation. As of then, NFSNET became the key internet network.

In 1991 the Czech Republic was connected to the internet. As of 1993, common users start to use it.

3.3. What is the internet good for?

Owing to the internet, its users may use a large number of services. These services are provided by computer programs and programs which communicate to one another by protocols. The basic internet services are as follows.

- **WWW** – a system of websites displayed via a browser; it uses http/HTTPS protocol.
- **E-mail** – electronic mail
- Sending messages via SMTP protocol
- Receiving messages via POP3 and IMAP protocol
- **IM – Instant messaging** – online, live communication ICQ, Jabber, Skype
- **FTP –** file transfer
- **DNS –** domain name system used for their better remembering
- Furthermore, plenty more protocols may be mentioned, e.g. file sharing (NFS), protocols used for connecting to a remote computer (telnet, SSH, VNC) etc.

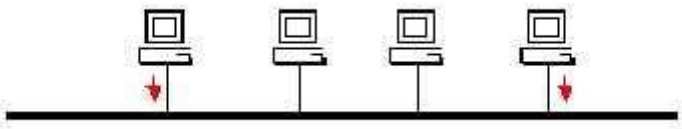
3.4. Ethernet

Ethernet is a technology for computer networks. It represents a set of technologies which deal with data transfer mainly in LAN networks. The most of its versions is subjected to IEEE institute standardization. Ethernet is implemented by the first (physical) and second (bond) layer of ISO/OSI reference model. Furthermore, Ethernet mostly uses a twisted pair or optical cable as a transfer medium; in the first versions, coaxial cables were dealt with. The next integral part is RJ_45 connector. There are several types of Ethernet depending on the type of cabling and transfer speed; the transfer speed was from 10 Mbit/s up to 100 Gbit/s.

Nowadays, Ethernet has become the most frequent network technology. This technology is based on a very simple principle called CSMA/CD irrespective of it being a common 10 Megabit Ethernet, or its faster mutation (Fast and Gigabit Ethernet).

A well-structured cable system may use various kinds of network technologies based on different transfer methods, e.g. Ethernet, Token Ring, CDDI, ATM etc.

CSMA (Carrier Sense Multiple Access) is a station ready to transmit data and "checks" whether the transfer medium (cable) is used by another station. In such a case, the station tries to access it later until the medium is free. The moment the medium is free, the station starts to transmit its data.



CD (Collision Detection) refers to a station which, during transmission, observes whether the medium shows a signal corresponding to transmit levels (i.e. so as not to transmit signal 1 the moment it transmits signal 0). Such a case of a complex signal interaction is called **collision**. In case of **detection**, the station collision sends out JAM signal and both (all) stations at the same moment of transmission generate a random time value after which they will try to repeat the transmission.

As a matter of fact, such effectiveness brought down prices of AC adapters and active elements and, consequently, Ethernet considerably expanded. All the same, the effectiveness of such a solution brought one grave disadvantage; with an increasing number of network hubs, simultaneously, a number of collisions increase; therefore a theoretical network throughput decreases. The set of hubs of which the common activity may cause a collision is called **collision domain**. Logically may be deduced that the collision domain should be as small as possible. Applied active elements have a different relation to the collision domain; on the one hand, some extend the collision domain and, on the other, some separate it. Therefore, by carefully choosing them, the network throughput may be controlled.

In addition, apart from the collision domain, a term **broadcast domain** has been applied. The computer network contains two kinds of packets; these are unicasts and non-unicasts. Unicasts refer to packets with a particular addressee provided by the network address. On the other hand, non-unicasts tend to use a group address and are either for all network users (broadcasts), or selected group of users (multicasts). The main issue is that a computer has to occupy itself with non-unicast even though it is not meant for it. Therefore, with an increasing number of network hubs, simultaneously, a large number of non-unicasts increases in the broadcast domain. For that reason, it is necessary to keep the broadcast domain in the reasonable size. Applied active elements have a different relation to the broadcast domain; consequently, by carefully choosing them, the network throughput may be controlled.

Packet format

As has been said before, all Ethernet speed modifications follow the same communication method CSMA/CD. However, they also use the same packet size and format. Ethernet packet is defined on the 1st and 2nd OSI layer.

4. STANDARDIZATION OF COMPUTER NETWORKS, TCP/IP STACK

4.1. Standardization of computer networks

The general strategy of leading producers involved creating and maintaining such specifications that provided users with compatibility strictly with products of their company. These computer networks, labelled as homogenous or closed systems, had a major deficiency in adapting to both, the manufacturer of technical equipment and the manufacturer of software (here are some of the proprietary protocols – DECnet from DEC Company, SNA – Systems Network Architecture from IBM Company, SPX/IPX – Sequenced/Internet Packet Exchange from Novell Company etc.). In contrast to these closed systems, open or heterogeneous systems refer to computer systems which were devised according to the established international standards and may be purchased from more independent producers. The application of open systems allows programs operating in local or remote network systems to closely cooperate and enables a unified communication of users of these applications.

The term OSI (Open Systems Interconnection) concerns technical equipment and computer network software. In the area of computer networks, international organizations CCITT (Comité Consultatif International de Télégraphique et Téléphonique is one of the three central committees ITU – International Telecommunications Union) and ISO (International Organization for Standardization) are the most important ones and deal with establishing adequate standards. As a matter of fact, government institutions or organizations responsible for the telecommunication in individual member countries are key members of CCITT. CCITT publishes detailed recommendations which, after a general approval from ITU, become international standards. In contrast to this organization, ISO is a voluntary non-governmental organization, whose members are standardization institutions. Other important organizations are IEEE (Institute of Electrical and Electronics Engineers), which is a prestigious American association of electrical and electronic engineers. This association issues periodicals, holds conferences and creates a professional body which establishes professional standards. IEEE 802 group of standards is notable within the area of local computer networks. In 1979, ISO organization adopted a standard labelled Reference Model of Open Systems Interconnection (RM OSI).

Network communication

The main network activity involves data transmission from one computer to another. This complex problem may be divided into these tasks.

- examining data
- dividing them into usable data banks
- supplying each data bank with useful information (source and goal)
- providing relevant information about timing and error detection
- transferring data to a network and sending them to a proper place

4.2. Basic terms RM OSI

Layer is accurately defined by its useful functions. Each layer, except for the highest and lowest, interfaces the layer directly below and above. The highest layer interfaces the application process. In addition, the lowest layer interfaces the physical media.

Entity is an object effectively operating within the particular layer. The term usually refers to a program group. Lower levels contain hardware (I/O port). Actually, the direct supplier and service user do not refer to a layer, but a particular layer entity.

Protocol includes entities in the identical layers of various open systems; they **communicate**

Service refers to entities of a particular layer performing its function; furthermore, they provide the higher layer with adequate services. In order to carry out these functions, they use services of the layer directly below. Individual services are offered by so called Service Access Points (SAP), which are identified via their addresses. These services may be divided as follows:

- **Connection-oriented Services** - two entities on the same levels must at first establish a connection before starting a direct communication. After the successful connection, the sender sends a message and the **receiver**, on the other hand, receives it. As a matter of fact, this kind of service is similar to the phone connection.
- **Connectionless Services** does not rely on establishing a strong connection between a **sender** and receiver. **Instead**, they consider individual parts of transferred data as single wholes supplied with the address of their final receiver and are delivered irrespective of other messages. Individual messages may be transferred in different ways.
- **Reliable Service** provides services that never lose any data. Usually, it involves services maintained by an effective mechanism for confirming messages.
- **Unreliable Service** does not provide confirming messages, but offers services of a high reliability.

4.3. ISO/OSI Reference Model

This popular model was designed by ISO international organization as a unified standard for interconnecting systems of various kinds and conceptions defined by different producers. The produced model contains seven layers. These seven layers create a complex hierarchy beginning with applications on the top and ending by physical connections at the bottom. OSI reference model includes two models of communication.

- horizontal – a protocol-based model by which programs and processes of different computers communicate,
- vertical – a service-based model by which layers of a single computer communicate,

As a matter of fact, an effective communication requires following elements; it requires at least two sides willing to communicate; therefore, a common language (protocol), by means of which the sides will communicate, must exist. In addition, vertical layers communicate via API (Application Program Interface).

Application layer, presentation layer, session layer, transport layer, network layer, data link layer, physical layer.

4.3.1. Application Layer

This layer precisely specifies the environment in which network applications communicate with the network services. The end user uses the networks for running the applications, file transfer, mail, remote login etc. Application layer protocols mainly contain application programs; also network superstructures, which enable the station to connect to the network, may be found there. Programs and protocols providing application layer services are as follows:

- NICE (Network Information and Control Exchange), which secures monitoring and network administration.
- FTAM (File Transfer Access and Management), which is responsible for remote file administration.
- X.400, which specifies protocols and functions for forwarding messages and electronic mail.
- CMIP, which is responsible for network administration based on the framework formulated by OSI.
- Telnet, which provides a terminal emulation and remote connection.
- Rlogin, which provides UNIX environment with a remote connection.

4.3.2. Presentation Layer

This layer manages formatting of data transfers. The data, which are transferred via the network, may be texts, digits or general data structures. Furthermore, it contains specifications for coding and decoding charsets; a data compression or their ciphering might be also carried out within this layer. In addition, presentation layer provides services to an application layer situated directly above and uses a session layer below.

4.3.3. Session Layer

This layer stimulates processes which control data transfers, detects transmission and transfer errors and files records on broadcast transmissions. In addition, the layer keeps and disturbs sessions between end-to-end participants (the user and target computer). In regard to starting the session, the layer requires establishing a connection on the transport layer by means of which a communication between both session participants is carried out. Likewise, it decides who may transmit signals or, alternatively, it disturbs the existing session. Session layer protocols are as follows:

- ADSP (AppleTalk Data Stream Protocol) allows two network hubs to make a tenuous connection for a data transfer.
- NetBEUI refers to an implementation and development of NetBIOS.
- NetBIOS uses 5th, 6th and 7th layer and offers session monitoring services.
- PAP (Printer Access Protocol) allows the access to PostScript printer in AppleTalk network).

4.3.4. Transport Layer

This layer allows functioning of appropriate connection establishment, disintegrates data to smaller parts, i.e. packets, to which the transferred data are gathered; upon receiving,

the data are taken out of the packet and folded into the original shape. Therefore, it secures transferring of randomly big messages despite individual packets having a limited size. As a matter of fact, the transport layer is fairly essential since it is situated between upper and lower layers, which are network-oriented.

4.3.5. Network Layer

This layer describes processes which route data between network addresses and check whether the complete messages have been sent on time. In addition, it secures a convenient routing of packets. Furthermore, the network layer must be aware of the particular network topology, i.e. the way of the direct interconnection of individual network hubs.

4.3.6. Data Link Layer

This layer, also called a bond layer, deals with processes which detect and correct errors on the data level during the data transfer between the physical layer and layers above the physical layer. Data link layer creates packets of relevant network architecture. All the same, the transfer route is inclined to errors as a result of which received bites are different from those that have been sent. Physical layer does not deal with the importance of individual bites; such sort of errors is detected to the data link layer; it checks whether the whole packets (sending different kinds of checksums etc.) were transferred correctly. Furthermore, the data link layer provides the sender with a direct confirmation of receipt of flawlessly transferred packets, while an error requires their repeated transmission.

4.3.7. Physical Layer

This layer imposes electric, mechanical and functional requirements for network data processing. By and large, the task seems to be easy; it secures transfer of individual bits between a receiver and sender.

4.4. TCP/IP Model

TCP/IP stands for Transmission Control Protocol/Internet Protocol; it refers to a standard file of protocols used e.g. in the Internet Network, which has become the largest network in the world.

History points out that in 1969, DARPA (Defence Advanced Project Agency) launched a research and development project aimed at creating an experimental network with packet switching. This network was called ARPANET and was designed to study techniques

allowing reliable and supplier independent data communications. On the whole, this experiment was highly successful and a large number of organizations started to use its services for a common daily communication. In 1975, ARPANET changed from an experimental network to an operating network. The basics of TCP/IP protocol were laid down when ARPANET had already been an operating network. This protocol was accepted as a Military Standard in 1983 and, at about this time, the term Internet spread all over the world.

Advantages of TCP/IP

- Open protocol standard freely available and developed irrespective of a particular technical equipment or operating system.
- Complete independence of a particular physical network hardware as a result of which it is possible to run TCP/IP within a large number of networks. Therefore, TCP/IP may run on Ethernet, token ring, phone lines and practically on each physical transfer medium.
- General addressed scheme allowing any TCP/IP device to directly address any other device in the entire network.
- Standardized high level protocols providing widely available user services.

4.5. TCP/IP Protocol architecture

Protocols draw up a formal code of conduct within data communications. In homogeneous networks, the set of rules is formulated by the system supplier. TCP/IP creates a heterogeneous network with open protocols which do not depend on differences between operating systems and architectures; they are available to everyone and their development and modifications are subject to the terms of the contract. The most precise information on TCP/IP is provided in RFC (Request for Comments); these documents contain the last updates of all standard specifications.

TCP/IP is usually considered as a model composed of fewer layers than OSI model. Most of the TCP/IP descriptions define the protocol architecture by three to five functional levels.

Network Interface Layer

This layer deals with everything associated with controlling a particular transmission path, direct transmission and reception of data packets. Moreover, it depends on a particular transmission technology (i.e. all industry standards – Ethernet, IEEE 802.x, and FDDI).

Internet Layer

This layer is sometimes called IP layer, in regard to IP protocol, and secures for individual packets to be sent from the sender to their actual receiver irrespective of there being a

direct connection between them. With respect to the unconnected character of the transfer (IP protocol), a basic datagram service is provided on the level of this layer.

- Internet protocol is a cornerstone for the internet. Its functions include:
- Datagram definition, which is the basic transmitting unit,
- Definition of the internet addressing scheme,
- Data transfer between the network and transport layer,
- Directing datagrams to distant destinations
- Providing fragmentation and datagram composition

Datagram refers to a packet format (packet is a data block, which contains information necessary for its delivering) defined by the internet protocol.

Transport layer

This layer is also called TCP layer according to the protocol. The layer is responsible for securing transmission between end-to-end participants, which, in case of TCP/IP architecture, are represented by application programs. According to their requirements, the transport layer may regulate the data flow in both directions, secure the transmission reliability and also change the unconnected character of the transfer to the connected one within the network layer.

Application Layer

Application layer is the very up layer of TCP/IP architecture; its entities represent individual application programs, which, in contrast to RM OSI, communicate directly with the transport layer. Possible presentation and relational services are provided by application programs themselves.

4.6. Architecture of communicating systems

Definition of terms

- **System**
  an independent whole able to stimulate processes and transfer information
- **Network architecture**
  system of layers, services, functions and protocols
  correspond to the structure of network equipment
- **Open architecture**
  adequate standards describing the architecture is publicly accessible
  all systems meeting the standards are inter-connectable
- **Layer protocol**
  rules of cooperation of entities on the same layer and other systems

- **Interface protocol**
  SW interface
  rules of cooperation of adjacent layers
  service primitives are used
  communication via Service Access Points (SAP)

5. ISO/OSI MODEL, SELECTED PROTOCOLS

5.1. Computer networks – ISO/OSI Model

ISO/OSI model refers to a communication model labelled 'International Standards Organization / Open System Interconnection'. It concerns a recommended model defined by ISO organization in 1983, which divides a common communication between computers into seven interconnected layers. The concerned layers are referred to as a Set of Protocol Layers.

The main task of each layer is to provide the following upper layer with particular services and not to burden the upper layer with details about the particular service provision. Before transferred from one layer to another, data are divided into packets. Subsequently, in each layer, all packets are supplied with additional information (formatting, address) necessary for a successful transmission over the network.

The suggested model shows the following layers (each upper layer uses functions of the lower one).

A brief description of individual layers – the individual layers appear in the same order as mentioned above

1. Physical layer

It defines means of communication with a portable medium and technical means of the interface. Furthermore, it defines physical, electric, mechanical and functional parameters concerning physical interconnection of individual components; i.e., it deals with hardware.

2. Data link layer

It maintains the integrity of the data flow from one network hub to another. This activity involves data block synchronization and their flow management; i.e. it also deals with hardware.

3. Network layer

It defines protocols for data directions, by means of which the information transfer to the required target network hub is secured. As a matter of fact, the appropriate direction, unless used, does not have to be in the local network. It also refers to hardware; however, when the PC deals with the direction between two network cards, it concerns software.

4. Transport layer

It defines protocols for structured messages and secures a flawless transfer (carries out some of the error checks). Moreover, it secures a partition file into packets and confirmation. It deals with software.

5. Session layer

It coordinates the communication and maintains the session as long as needed. Furthermore, it performs security, login and administrative functions. It concerns software.

6. Presentation function

It explores the way of data formatting, presentation, transformation and coding; i.e. it deals with diacritics, punctuation, compression and decompression and data encryption. It concerns software.

7. Application layer

It represents the uppermost layer. It explores the way of communication of a network with applications, e.g. database systems, electronic mail or programs for terminal emulations. It uses services of lower layers as a result of which it is isolated from problems of technical networking resources. It is software-based.

5.2. ISO/OSI Reference model – seven layers

Designers of ISO/OSI reference model concluded that an optimum number of layers of network software are seven. However, which layers and tasks are to be dealt with? Let's proceed from the lowest to the uppermost.

1. Physical Layer

Its main task seems to be very simple – to make a transfer of individual bits between the receiver and sender via the physical transfer path, which is under a full control of this layer. Nevertheless, a lot of issues of technical character must be dealt with – e.g. the voltage level of logic 1 and logic 0; how long one bit "lasts"; how many contacts and which shape cable connectors should take on; which signals are transmitted via these cables; of which importance they are; their time course etc. Therefore, these issues rather belong to the area of electro-engineers and technicians.

2. Data Link Layer

Physical layer usually provides means of individual bit transferring as its standard services. Using these services, the right above data link layer (sometimes called **bond layer**) must secure a flawless transfer of data blocks (in the scope of hundreds of bits) labelled as **frames**. Since the physical layer does not interpret individual transferred bits, the data link layer must correctly define the beginning and end of the frame and its individual parts.

In fact, a various disturbances and failures may occur on the transfer path as a result of which received bit values differ from those that have been sent. Since the physical layer does not deal with individual bits, these errors are detected up to the data link layer. This layer checks whole frames whether they were correctly transferred (according to the checksum; see 3rd part of our series). Furthermore, it provides the sender with information about a flawless frame transfer while, in case of damaged frames, it requires their resending.

3. Network Layer

Data link layer secures transferring of whole frames; however, only between two network hubs, where a direct connection is established. Nevertheless, what to do supposing the connection between a receiver and sender is not direct, but it goes through one or more intervening hubs? As a matter of fact, network layer must take an action and secure a convenient routing of transferred frames – labelled as packets. The network layer chooses the correct path (or route) via intervening hubs and, also, secures progressive transferring of individual packets from the original sender to the end receiver on the route.

Therefore, the network layer must "consider" a particular network topology (i.e. the way of direct interconnecting of individual hubs).

4. Transport Layer

Network layer provides the right above layer with services securing packet transfer between two random network hubs. As a result, the transport layer is screened out of the actual network topology and creates illusion of every network hub having a direct connection to any other network hub.

Consequently, the transport layer only secures an end-to-end communication; i.e. a communication between the original sender and end receiver.

Moreover, the transport layer secures building up individual packets upon the data transfer into which the transferred data are divided; analogically, the data are taken out of the packets and built up into their original shape upon receiving. In this way, a transfer of any large messages is secured despite the individual packets having a limited size.

5. Session Layer

This layer establishes, maintains and breaks off **sessions** between end-to-end participants. While establishing a session, this layer requires a connection to the transport layer through which a communication between both session participants is established. This layer is responsible for an occasional communication management (i.e. outlining transmission timetable when two participants simultaneously occur). In addition, the layer is responsible for everything needed to close the session and break off the actual connection.

6. Presentation Layer

The data transferred via the network may be, apart from others, textual, numeric or general data structures. All the same, individual hub computers may use different internal representation of these data; i.e. central computers of IBM Company use EBCDIC character code while most of the others work with ASCII code. Likewise, one computer may display integers in the supplementary code while another one may work in a direct code etc. – this layer is responsible for required conversions of transferred data.

The layer also carries out potential compressions of transferred data, alternatively their ciphering.

7. Application Layer

End-to-end users make use of computer networks via various network applications – electronic mail systems, file transfer, remote login etc. As a matter of fact, incorporating all the different applications directly into the application layer would not be relevant due to their enormous variety. For that reason, the application layer involves only a part of these applications which provide common, i.e. generally applicable mechanisms. For example, considering electronical mail, the particular part which secures network messaging is also an essential part of the application layer. For all hub computers which use the same electronic mail system, this part is identical. The user interface of the electronic mail system, i.e. the particular part which is actually employed by the user and which enables a user to read messages, replies to them, create new ones and submits them for sending, is no longer considered as a part of the application layer since it may significantly differ in each particular hub; e.g. controlling (by means of line commands, various kinds of menu, with or without windows etc.). Another typical example may be a terminal emulation needed for remote login. On the whole, there are a large number of various terminals and to make a required adaptation between two random kinds of terminals is quite impossible. As a consequence, only one 'reference' terminal – so called virtual terminal – is implemented. Each particular type of terminal contains only one adaptation between this virtual terminal and the actual terminal. Nevertheless, the means for working with the virtual terminal are included in the application layer (since they are the same) while means for its adapting to the particular terminal are not involved in the application layer.

6. WIRELESS COMMUNICATION TECHNOLOGIES

Wireless networks; principles, standards, components, communication mode, application and properties,

Standards

A development of wireless networks took place similarly to cable networks; initially spontaneously, then it was necessary to define standards which would ensure a common network cooperation. Main producers of the wireless technology formed WECA Alliance (Wireless Ethernet Compatibility Alliance), which imposed requirements for its effective management and in this way ensured a common compatibility. Upon complying with the conditions, the product is awarded Wi-Fi certificate, which confirms the compatibility with products from other producers. The wireless standard itself was based on Ethernet; therefore they have similar features; i.e. CSMA/CD access method and a similar packet composition. There are several standards for LAN wireless networks, of which the properties are suggested in the table. 801.11g standard is backward compatible with the older and slower 802.11b (they may cooperate; however only on a lower speed). 802.11i standard was based on 802.11g standard, the former of which uses a safer authentication and ciphering algorithm.

Components

Wireless components communicate in two useful ways:

- Ad hoc, this refers to a direct connection of several computers – from two to five. Each computer communicates with another one on the equal level; i.e. they are equal (the organization is similar to a peer to peer network). The main advantage is a quick installation and a very low price (except for client network adapters, other hardware is not required). It allows sharing files and the Internet, print over the network and other things commonly occurring in LAN networks. On the other hand, the key disadvantage is that all connected devices must be in range; i.e. everyone has to see everyone. The next shortcoming is a ridiculously easily-established connection as a result of which its security may be compromised.
- Infrastructure mode is based on Access Point (AP). It functions as a server through which all data flow between network clients (the organization is similar to client/server network). The key advantage of its application is a possibility of filtering and supervising the operation including making networks available to different clients. Thus, the elimination of unconscious attempts to establish ad hoc connection is secured; the entire flow must be directed to AP, which provides an adequate network protection. The access point is definitely not needed supposing a wireless

connection is established only occasionally and only between several devices. However, provided a small home network is built up or shared in a household or small office, an access point is usually required (tighter network security).

Access Point

AP is a base of a wireless network. It establishes a connection between wireless end-to-end points and a server by means of placing it within a metallic LAN network. For that reason, AP contains a radio part – transmitter/receiver and a cable part – RJ-45 socket for a twisted pair connection. AP involves hubs transmitting the signal. A lot of producers offer powering of AP by a twisted pair, through which the point is connected to the fixed network. Thus, the access point (in a hardly accessible place) does not have to bear two cable lines. The access point and its counterparts – client adapters work only unless there is an obstacle – between AP and computers placed in the wireless network must be clearly visible. As a consequence, access points may be found in the uppermost parts of rooms. Their positioning must consider possible sources of radio signal interference; i.e. metal constructions (even in walls), electrical interferences (e.g. microwave ovens operate in the range of 2.4 GHz, wireless phones, wireless speakers etc.). As long as a direct wireless interconnection is required, Wireless Bridge (WB) may be applied – access points of a bridge function, filtering packets between networks.

Client adapter

It refers to a unit through which a PC is connected to an access point. Basically, it refers to a network card (with an aerial). It is designed for PCI and USB slots. Laptops may apply a wireless network card according to PC Card standard; however, a lot of laptops run on an already integrated wireless network interface (which facilitates and marks down a wireless network set-up).

6.1. Wireless network properties

6.1.1. Speed

In contrast to metallic networks, its speed is considerably lower. As a matter of fact, theoretically maximum attainable speeds are suggested in the table, which also provides adequate standards. Actually, these standards are hard to achieve, the fact of which is caused by a weaker accessibility of the signal between radio stations, which results in a skip to a lower transmission speed.

On the whole, it means that a longer distance (e.g. over 20 metres) or an obstacle (e.g. a quality metal frame) dramatically decreases the speed by half or quarter. As long as the group of receivers is connected to the same access point, and thus they are physically

located within one network segment, the capacity must be divided by an adapter. As a result, a lot of collisions occur (CSMA/CD character). The next variable bringing down the feasible speed is a careful management of protocols within upper layers as a result of which the actual bandwidth for pure data considerably decreases again. All the same, under favourable conditions, the maximum bandwidth for a useful data load is about a half of the nominal values; i.e. 5 Mb/s B line and 25 Mb/s G line.

6.1.2. Security

SSID (Service Set ID)

It refers to an access point which is visible to all the clients who are located within its range. For that reason, SSID serves as a logical indicator of a particular wireless network. It may be manually fixed to the station, or the access point regularly transmits the information about SSID, or SSID transmission may be switched off in the situation of which the client himself asks for SSID.

WEP (Wired Equivalent Privacy)

It refers to an old security system of wireless networks according to original IEEE 802.11. Standard. The aim of WEP was to provide wired computer networks with a top security (e.g. twisted pair) since the radio signal may be easily picked up even within a long distance without a physical contact with the computer network. However, WEP was broken through in August 2001; therefore, it should be replaced with WPA2 according to IEEE 802.11i standard.

WPA (Wi-Fi Protected Access)

This refers to a security system of wireless networks. In order to break WEP security system through in 2001, Wi-Fi Alliance improved WPA security system as a part of the then prepared standard IEEE 802.11.i in 2002. In addition, Wi-Fi Alliance holds the rights for Wi-Fi and WPA trademark and certifies their products.

WPA2

It implements all necessary components of IEEE 802.11i. It uses Advanced Encryption Standard (AES) block cipher while former WEP and WPA use the current cipher RC4. 802.11i; the architecture contains the following components: IEEE 802.1X for authenticating (i.e. Extensible Authentication Protocol – EAP).

Wireless PAN

WPAN connects individual devices in a relatively small area, which is very easy to access for a person connected to this network. For example, headphones may be connected to a laptop by Bluetooth or infrared light; in this way, a small private wireless network may

be created (WPAN). Zig Bee also supports WPAN applications. As a matter of fact, private Wi-Fi networks became a commonplace for an ordinary consumer to the extent of the integrated equipment within a large scale of electronic devices. In addition, devices such as 'My Wi-Fi' from Intel and 'Virtual Wi-Fi' from Windows 7 facilitate setting and configuration of a private wireless network.

Wireless WWAN

A large wireless network WWAN refers to a wireless network covering large areas. These networks may be used for connecting office branches or as a public access system. Wireless connection between access points is usually carried out by a point-to-point microwave line using a parabolic reflector of 2.4 GHz frequency. A typical system runs on entrance gates of basic stations, access points and wireless signal bridge. The other configuration consists of network systems where each access point passes the signal.

Wireless MAN

Wireless metropolitan networks WMAN refer to wireless networks which are connected to several local networks. WiMAX is a type of MAN wireless network and is defined by IEEE 802.16 standard.

6.1.3. Application

Its application includes mobile phones, which are an integral part of the everyday wireless communication and facilitate the communication, intercontinental network system, which employs satellites for communication all over the world. Common people and salesmen use wireless networks for fast sending and sharing data irrespective of them being in a small office, or anywhere in the world

7. VIRTUAL NETWORKS (VLAN).

VLAN concerns a Virtual Local Area Network. It refers to a functional LAN network within which another one, a virtual network, is created; it runs on only one hardware device (physical cabling). On the whole, VLAN operates on an individual pre-setting of already active network components of a new virtual mode and model.

VLAN works on a principle of tagging data transferred via the network. The data are tagged according to the appropriate virtual network. The key goal is to properly interconnect more local LAN on the level of the second network layer of ISO/OSI model. Moreover, a great advantage is a good configurability.

Regarding a high-quality network security, VLAN easily discerns users of individual end-to-end stations and ever-running applications (e.g. Linux Demon) independently on the active network device.

In this way, unauthorized access of a non-ethical hacker to a computer network is entirely eliminated. Thus, the most common kind of a cyber-attack aimed at computer networks – DDoS may be resisted in the very beginning.

7.1. What is LAN network good for?

First launches of VLAN technology took place in the middle of 90s of the last century. One of the main reasons was to form a group of particular users which will successfully communicate and access their files and information in an easier way. The next reason was stagnation in the development of Ethernet technology.

Of importance is also the fact that VLAN technology easily discerns a network communication which has recently shared a network on an appropriate network device – switch.

As a matter of fact, using a switch port offers the most effective and practical solution.

VLAN technology developed in 1995; however, it was based only on a close source technology; yet, it has been only a couple years ago since it developed mainly to middle-sized and large companies although an adequate standard has already been defined.

Main reasons of VLAN creation:

- ***dividing network users*** into groups, sections or by particular services instead of a physical position and communication sections between these groups
- ***reducing network broadcasts*** which became a problem a couple years ago
- ***reducing the collision domain*** in time, when hubs were used instead of switches

The idea of a logical group of users, which is mentioned in many materials, and therefore a creation of VLAN observes:

- ***Organizational structure*** – provided most of the communication is carried out within the section with printers, file servers etc.; provided there is no communication between individual sections; only a few services (mail) are common.
- ***Services –*** VLAN associates workers who use the same services (accounting, DB etc.).

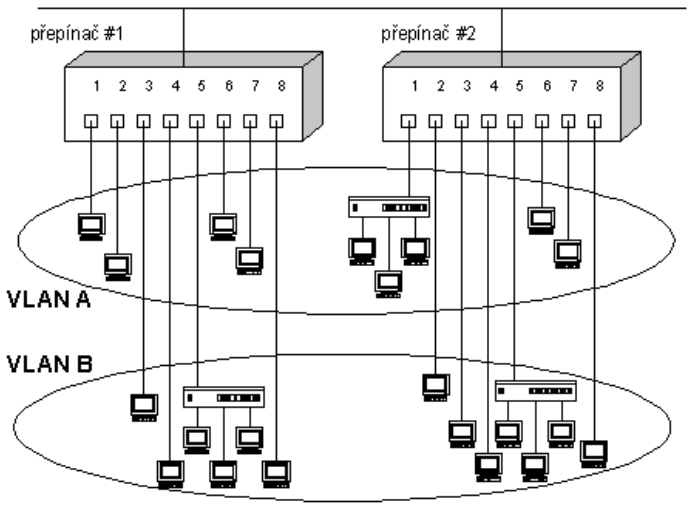
Major advantages of VLAN

Since VLAN membership may be defined in different ways, VLAN are typologically divided into networks with port-based and policy-based memberships. A more distinct division distinguishes four types of VLAN membership:

- ports;
- MAC addresses of hubs;
- network protocol or network addresses of hubs;
- Group of IP broadcasting.

Port-based VLAN

This historically first type of virtual networks defines a network membership for individual switch ports (group of ports). The first VLAN implementations did not allow expanding of virtual networks to more switches; they focused only on one switch. Yet, the next generation did not allow it; thus defined network is depicted in the picture below.



Picture – a port-based VLAN membership

Grouping ports is the principal method of creating virtual networks. Although very clear and simple, its basic limits consist in redefining a membership in relation to any moving

of the user station between individual switch ports (i.e. such changes which would cause a change in the membership in the virtual network).

MAC address-based VLAN

MAC address is "hard-pressed" in the network adapter circuit; therefore, thus defined virtual networks may be considered as user-based VLAN. Supposing a user changes his connection (relocates his station to another switch port), his VLAN membership remains the same.

This method involves a rigid manual definition of a membership for all networks of the station. Another huge disadvantage is a risk of a substantial power reduction in case of a shared segment with stations in different VLAN being connected to the switch port. The next, rather a minor, problem may be a situation in which users, and their laptops, change their position and connect by a steadily-connected docking stations. Thus, a definition MAC address changes with a location (network adapter is mostly a part of the dock). Although it poses only a minor problem, certain VLAN limits, which are imposed by MAC address-based membership, are clearly illustrated.

However, the possibilities of user redefining of own MAC address directly in the operation systems adds a further complication, e.g. in regard to the security.

Protocol or address-based VLAN

Thus defined virtual networks are based on the information from the third, OSI-based network layer. In multiprotocol networks, hubs may be divided into individual VLAN according to operating network protocols, or e.g. in networks with TCP/IP protocol according to the subnetwork address.

Although information about the network layer is concerned here, it is important to realize that its utilization for routing is not dealt with. Despite the fact that the switch must examine the packet to specify the IP address and in this way VLAN membership, no routing calculations are carried out. The switch does not use routing protocols (such as RIP, OSPF); as a consequence, VLAN defined according to the information from the third, network layer, must be regarded as a network with a flat topology interconnected by switches or bridges.

Switching even in the third, network, layer and implementation of switches with a built-in router capability slightly alleviate the problem at the first glance. However, it refers to different functions – on the one hand, merely determining VLAN membership based on a network address; on the other, a full use of router capabilities based on routing protocols and calculations. It is also necessary to say that the communication between individual VLAN requires using routers – regardless of it being classic ones, or built-in in the switches with routing functions.

All the same, defining network layer-based VLAN has a lot of advantages, e.g. users' mobility or, to put in more precisely, their stations without a necessity of reconfiguring VLAN membership, a possibility of forming groups which provide particular services or applying and eliminating the need of packet tagging containing the information about VLAN membership when communicating with each other (see the following).

Group broadcasting-based VLAN

Group broadcasting in IP networks (IP multicast) works the way in which a packet designed for group broadcasting is sent to a special address, which functions as a proxy for an explicitly defined group of hubs (IP addresses). The packet is delivered to all hubs which are members of a particular group. The group is formed on the dynamic basis; within this group, the hubs continuously log in and out.

Consequently, all the stations may be considered as members of one virtual LAN since the group forms one domain of omnidirectional broadcasting. Nevertheless, it significantly differs in two distinctive characteristics – the group is dynamically formed only for a limited period; thus, it is very flexible and its range is not limited by routers; i.e. it may expand, for example, to a vast WAN network.

Why did VLAN develop?

VLAN technology started to develop around 1995; at the beginning it involved only close source-based activities. Actually, these activities did not expand until a couple years ago, namely in middle-sized and large companies although an adequate standard has been defined long ago.

Main reasons for VLAN development were as follows:

- group or section-based grouping of network users or service-based instead of physical position or section-based communication between these groups
- reducing network broadcasts, which have become a big problem since a couple of years
- reducing collision domains in the time when hubs were used instead of switches
- idea of a logical grouping of users, which is mentioned in many materials, and which creates VLAN consists in
- Organizational structure – provided most of the communication is carried out within the section with printers, files servers etc. and there is no communication between individual sections; only a few services (mail) are common to all.
- Services - VLAN associates workers who use the same services (accounting, DB etc.).

7.2. Major advantages of VLAN

The way of integrating the communication in VLAN

VLAN integration is usually set up on a switch (only is special cases, a tagged communication goes through trunk from another device). Switches supporting VLAN always include at least one VLAN. It refers to a default VLAN NO 1, which is not possible to be deleted or switched off. Unless set up in a different way, all ports (i.e. the entire communication) are integrated in VLAN 1.

There are four principal methods of integrating a communication in VLAN; however, mostly the first method is employed in practice.

1. port-based method

Switch port is manually and tightly integrated (configured) in a particular VLAN. The entire combination going through this port belongs to the particular VLAN; i.e. as long as another switch is added into the port, all devices connected to that will be in the same VLAN. As a matter of fact, it is the fastest and most frequently used method. In addition, there are no specific requirements in regard to VLAN integration; its definition is local-based on each switch. Moreover, it is clearly arranged and easy to administer.

2. MAC address-based method

Ports are integrated in VLAN according to the source the MAC address. Therefore, a detailed table containing a list of MAC addresses for each device, together with a particular VLAN, needs to be drawn up. The key advantage is its highly dynamic integration; so if a device is connected to a different port, it will be automatically integrated in the appropriate VLAN.

There are two ways of using this method; either port integration in VLAN is set up according to the MAC address of the first frame – the setting remains the same until the port switches off, or each frame is separately integrated in VLAN according to the MAC address. Nevertheless, this method is very performance demanding.

However, Cisco found out a solution called VLAN Membership Policy Server (VMPS), which requires a special server administering MAC address tables. Moreover, this method integrates ports in VLAN; as a consequence, provided more devices (20 max.) are connected, all of them must be in the same VLAN.

3. Protocol-based method = according to the information from 3rd layer

This method determines protocol-based integration of the transferred packet, e.g. separation of IP operation from Apple Talk, or IP address or scope-based integration. However, it is not very common in practice. A device must contain a strictly defined IP address and

the switch must operate as far as the third layer (it usually operates as far as the second), which means a considerable slow-down.

4. authentication-based method

This method verifies a user or device by IEEE 802.1x protocol, and according to the provided information, places it in VLAN. Primarily, it refers to a safety method which controls the network access (NAC); however, when expanded, it also serves to VLAN. The method is also effective due to its versatility; i.e. neither a physical device, nor a place of connection is important. RADIUS server, which verifies the user's identity, also allows mapping of VLAN users; subsequently, after a successful authentication, this information is sent. This method also allows a special setting that in case of a user not being authenticated, he is integrated in a special host VLAN.

Cisco switches may encompass a single-host port, which allows connecting only one device, or a multi-host, which, on the one hand, allows connecting more devices to one port, but after the first authentication, the port itself is authenticated as a result of which all devices may communicate.

7.3. Principles of VLAN communication

Actually, there are two situations dealing with VLAN membership. The first one deals with communication within one switch; the second one deals with communication between several switches.

One switch-based VLAN

VLAN communication within one switch is actually very easy. In its operation memory, the switch retains information about a particular communication (port) belonging to a particular VLAN; as a consequence, only one correct routing is allowed within one switch. In such a case, individual ports are integrated in one VLAN, namely, either statically, or dynamically as has been mentioned above (options 2, 3, 4). Cisco refers to these ports as access ports.

Multiple switches VLAN

As a matter of fact, a more complicated situation arises on condition that the information about a particular VLAN integration must not get lost upon transferring to another switch; i.e. in order for the entire network to use identical VLAN irrespective of a particular switch-device connection. Moreover, may be interconnected on two switches, then integrated in the same VLAN, and required information may be transferred. However, this procedure is very ineffective.

8. URL, X/HTML, HTTP

URL is an acronym of Uniform Resource Locator. It is used for correctly identifying documents on the internet. An example of URL website is

http://www.adaptic.cz/znalosti/slovnicek/url/

Where the address of our server consisting of the top-level domain (cz), second level domain (adaptic) and the third level domain (www), which are separated by dots, may be seen. Furthermore, URL contains a path to a website of a directory of the structure (/znalosti/slovníček/url/) separated by slashes. The last part of the URL is a protocol which allows asking a server for this website; in this case, protocol HTTP (ono http:// at the beginning) is to be dealt with.

In addition, URL may contain:

- a title of the website including its ending (e.g. index.htm),
- port number, which identifies a required service (written behind TLD and separated by colon, e.g.:80),
- name and password when required (written right behind the protocol – username:password:@).
- URL tabs referring to a particular place on the website (written as #tab at the very end of URL)
- website parameters (written behind the website name and separated by a question mark, e.g.? logged=true) may also be an integral part of URL.

8.1. Types of URL

The form of URL mentioned in the example above refers to the **absolute URL**; in contrast to **a relative URL**, which refer to a particular position of a current document (website containing its links).In such a case, some parts might be left out; i.e. provided a referenced website is located on the same server, the name of the server (domain) may be left out within the particular URL. On the other hand, as long as the website is located in the same directory as the referenced website, there is no need of writing a path in URL either.

A well-treated URL is called **cool URL** (also in Czech). Provided only applicability is of our interest, we refer to a so-called **user friendly URL**. On the other hand, provided only search engines are considered, **SEOfriendly URL** is to be dealt with.

8.2. The importance of URL form

URL form heavily influence the visibility and applicability of the web. For example, if a domain name is short and comprehensible, visitors are more likely to remember it and, moreover, it is easier to be dictated via phone. On the other hand, supposing a domain name contains a keyword (or different parts of URL); it is highly useful for a search engine optimization. However, URL containing a large number of parameters works in the opposite way in both cases; i.e. URL written in capital letters or a longer URL (they are also slashed in e-mails and the e-mail program renders them illegible).

URL

URL is written either as an absolute address, or a relative one. While the absolute address precisely corresponds to URL, the relative address refers to a certain abbreviated address entry, which is based on a search engine understanding the entry from the address of the current website. Caution – URL considers capital letters.

Absolute URL

Each absolute address consists of a protocol and domain name. It is mostly followed by a directory path and file name. Sometimes, the address contains a port number, tab name and query string.

Protocols

Http or https protocols most often transfer HTML websites. These are written as http:// and https:// into URL.

All the same, a big difference does not arise as far as the server communicates with the search engine. Http is transferred un-encoded via the internet; https is an encrypted protocol.

As a matter of fact, http and https should not be swapped since both of the protocols may not work on a particular server, which means as long as absolute addresses are used, it must be found out which protocol works on the particular web.

Domains

Each internet server has its domain name. It consists of three parts separated by dots.

- name of the virtual server, mostly www (third level domain)
- second-level domain name (registration required)
- top-level domain, mostly cz, sk or com

Port

Generic domain is not usually followed by a colon or port number.

Directory path

The target file is usually stored either in a directory, or directly in the root of the server. Directories should be written in URL after the generic domain. A forward slash (not a back-slash) comes before the name. Multi-level directories are written one after another separated by slashes.

Files

File name is written after the directory path (if it exists). A slash is written before the file name.

Tabs

A direct link may connect to a tab in a referenced document. A hashtag '#' and tab name is written in URL after the file name.

Query

Input data for a certain script may also be a part of URL. These are written after the question mark at the end of URL. The syntax in name=value&name2=value2.

Example

A typical example of absolute URL may be as follows:

http://www.jakpsatweb.cz/html/url.htm#priklad

Part of the address	Example	Other possible values
protocol	http://	ftp:// , mailto: etc.
3rd level domain (server)	www.	www. , anything.
2nd level domain	jakpsat-web.	seznam. , mujweb. etc.
top-level domain	cz	com, sk, gov etc.
port	nothing	:80 , :*number*
path (directories)	/html/	/, /anything/directory/
file name	url.htm	index.html etc.html

tab	#example	#tabname
query	nothing	?variable=value

Relative addressing

As a matter of fact, writing the entire absolute address is often a needless and lengthy process. Therefore, there is a way of facilitating by means of a relative address.

The idea of relative addresses is based on existing files, which are interconnected, stored in the same server. Each file which requires another URL file has an absolute URL. For that reason, only a file path, slash and file name needs to be written in the address, all of which means a relative URL.

Relative URL = path/file_name

Directories are separated by slashes. On condition a target file is situated higher in the directory hierarchy (thus a certain "jump-up" is required), two dots must be written for the superior directory.

Example: inserting a picture with logo "Jak psát web" (How to write a web) into this website would be carried out using a relative address as follows: <img src="../images/jakpw.png">

8.3. XHTML

XHTML refers to a modern mark-up language having replaced already old HTML language. XHTML also applied through XML language as a result of which it differs in several ways; e.g. requirement for coding declaration, more strict rules concerning entries (they must be closed) and attributes (small letters in quotation marks).

Nowadays, XHTML exists in two versions. The first is XHTML 1.0, further divided into three variants, Frameset (for websites using frames), Transitional (facilitates transition to XHTML) and Strict (the most strict variant). The second version is XHTML 1.1. As a matter of fact, it does not significantly differ from XHTML 1.0 Strict variant; it is merely divided into several modules.

Although opinions about this issue vary, Strict XHTML presents the most practical way concerning www websites. In fact, XHTML 1.1 is not compatible with older browsers; on the other hand, two remaining variants XHTML 1.0 are too unrestricted, which means, like HTML, issuing high demands on a coder's discipline.

What is XHTML

XHTML is a different, then newer, HTML standard. By and large, HTML did not develop for a long time; it was in HTML 4.01 version when the first attempt XHTML was made.

The 'X' at the beginning of XHTML means eXtensible; however, practically, it rather refers to its "narrowing" and "cutting".

On the whole, XHTML support is completely identical with that of HTML in current browsers (written in 2004 and applies to 2012 as well). Although estimated that future XHTML support would be better than that of HTML, there is no sound reason for assuming, based on experience of browser development, that it would come true.

Differences between XHTML and HTML

XHTML, in contrast to HTML, must have all the tags including unpaired tags such as <meta>, <link>,
, <hr> or <img> terminated. The entry may bear more forms; either classic (valid) <img></img> or abbreviated <img/> or slightly modified <img />. Nevertheless, the first method is not recommended to use on condition XHTML document with text/html type is sent. The second way, without a gap, is not recommended to use due to older browsers, which might leave out the last attribute as long as entered.

Furthermore, XHTML, in contrast to HTML, must have all the tags and their attributes written in small letters for the reason of case sensitivity of thus declared and referenced DTD and X (HT) ML; in other words, it considers font size. Provided an own DTD is declared, capital letters may be greatly used.

All attribute values must be put in quotation marks.

In addition, a document must begin with XML declaration, although its use is not mandatory if the document is encrypted in UTF-8, or the encryption is provided by a higher protocol (e.g. http).[14]

As long as frames are needed, XHTML 1.0 Frameset, and for individual websites XHTML 1.0 Transitional, may be declared.

XHTML document should be sent via another MIME type than common HTML documents.[15]

8.4. HTTP

HTTP refers to an internet protocol originally designed for exchanging hypertext documents between a server and browser (i.e. www service). In fact, the current HTTP version is able to transfer any files and is used for many more functions (e.g. running remote applications). There is also a secure version of HTTPS for HTTP.

HTTP is based on a query → response principle; individual queries are not discernible from the point of view of the server. Therefore, HTTP is also called stateless protocol. In fact, it was a great advantage in times of internet presentations; however, when programming more complex web applications, thorny problems occur since, for example, HTTP does not allow saving a basket content in the online store. Consequently, effective methods of breaking it, 'Cookies' for example, need to be applied.

HTTP protocol

Http protocol explores a way a browser communicates with the server while downloading websites.

Effective use of HTTP

On the whole, in order to create a website, knowing http protocol is not required. However, as soon as more complex issues arise or a more advanced search engine optimization is to be dealt with, a greater familiarity with activities between the server and client is required.

Http headers provide information about e.g. redirects, cacheting, cookies, compression or referrer.

As long as server scripts or more complex web programs are written, it is good to know where and how to send a particular http response.

The abbreviation HTTP means Hyper Text Transfer Protocol (Hypertext is a text with links).

Functioning of http protocol

A client talks to the server; i.e. client wants something and the server provides it.

- A client is usually represented by an internet browser (Explorer, Mozilla, Opera); however, a search robot or another program may represent a client as well.
- Http server involves a program running in a server room on a computer (although this computer is also called 'server', it does not refer to 'http server'). The most frequent http server is a program called Apache.

Thus, http protocol is a sort of language by which two programs talk; they talk via a network, mostly the Internet.

A client usually requires a particular website – he connects to a server and asks the server for URL websites. Such a request is formulated within HTTP protocol (the connection itself is carried out via TCP protocol). Subsequently, the server submits the request and sends back a response also written in HTTP protocol. For instance, it sends http headers to a client followed by a website text in HTML. The client receives the response, reads the headers and displays the website.

An example of http communication

For instance, a reader wants to read this website. Its URL is as follows

https://www.jakpsatweb.cz/server/http-protokol.html.

1. Reader writes this URL in the browser.
2. The browser (client) evaluates the domain and finds out via DNS which IP addresses should be asked for.
3. The client establishes a connection with the server on the found-out IP address via TCP protocol; henceforth, HTTP begins.
4. Browser sends this HTTP command to the server:

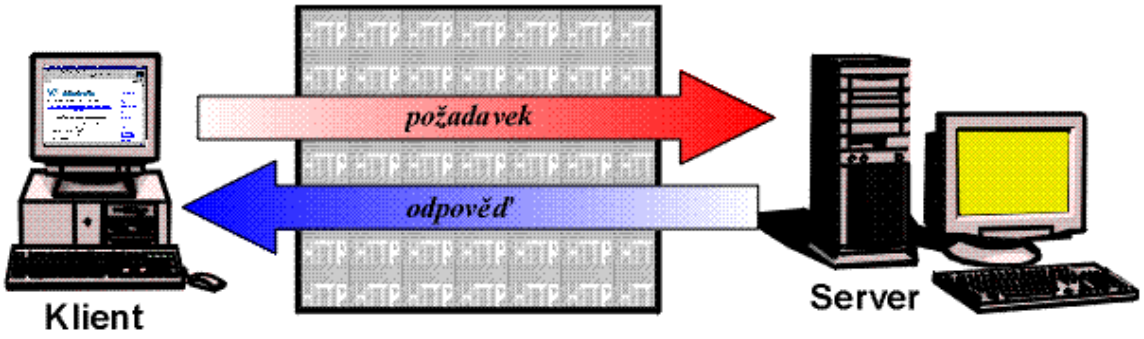
GET /server/http-protokol.html HTTP/1.1
HOST: www.jakpsatweb.cz

HTTP protocols

World-Wide Web service is based on three principal technologies – HTML, URL and HTTP. HTML refers to a mark-up language used for a standard description of the content and structure of websites. URL concerns specific addresses used on Web – each website has its own definite address in the form of URL. HTTP – Hypertext Transfer Protocol – is a protocol used for communication between browsers and web servers by means of which URL websites required by a user (via a browser) are transferred to the server. On the other hand, the server sends back a website written in HTML to the user by HTTP protocol.

For a full understanding of CGI-scripts principles, at least a rudimentary knowledge of HTTP protocol is necessary. Therefore, basic characteristics of HTTP protocol will be looked at in the following text.

HTTP protocol results from client/server architecture. Client, in this case a browser, connects to the server and sends a request. In response, the server sends a response. The standard format of the request and response is defined within HTTP protocol. All the same, the whole situation complicates the fact that there are three protocol versions – 0.9, 1.0 and 1.1. As a result, the request and response format significantly differs in the individual versions.



Picture 1: The course of communication between a client and server

Basic characteristics of HTTP protocol

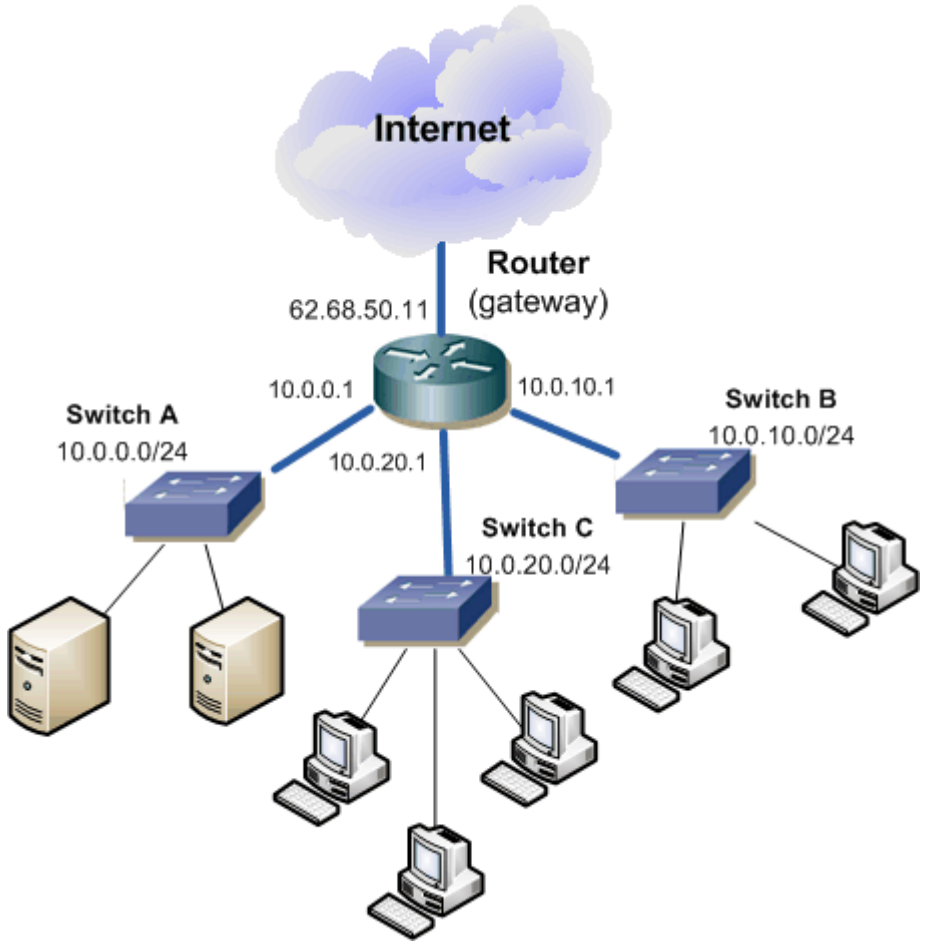
To fully understand the article, a more comprehensive knowledge of basic characteristics of HTTP is required; i.e. the actual operation of the protocol. HTTP protocol refers to an application level for distributed hyper medial information systems; i.e. this internet protocol is generally used not only for the data transfer between the client and server, but also many more operations. As a matter of fact, HTTP protocol is stateless so that it does not discriminate between clients from which it receives requests. For example, if one client sends two requests simultaneously, the server will not recognize that the same client is to be dealt with.

HTTP exists in three versions, namely 0.9, 1.0 and 1.1. The first one, referred to as HTTP/0.9, existed as a simple protocol able to transfer data on the internet in a limited way. In fact, HTTP/1.0 version allowed the protocol to transfer information in MIME format so that it could contain meta-information about the transferred data. All the same, the most significant improvement was achieved by making all connections permanent; it was implemented in HTTP/1.1 version, which is the last updated version. It means that a connection is not closed until one of the client-server pair sends a closing header. Formerly, HTTP closed a connection after each individual server response. By this huge improvement, a transfer speed significantly increased since the server does not have to open a new connection for each picture, frame and applet.

9. ROUTING PROTOCOLS

Routing refers to a technique focused on interconnecting individual networks (subnets). The original device designed for routing was a router, but nowadays L3 switches, firewalls or merely servers/computers are applied more frequently. Router forwards communication from one network to another.

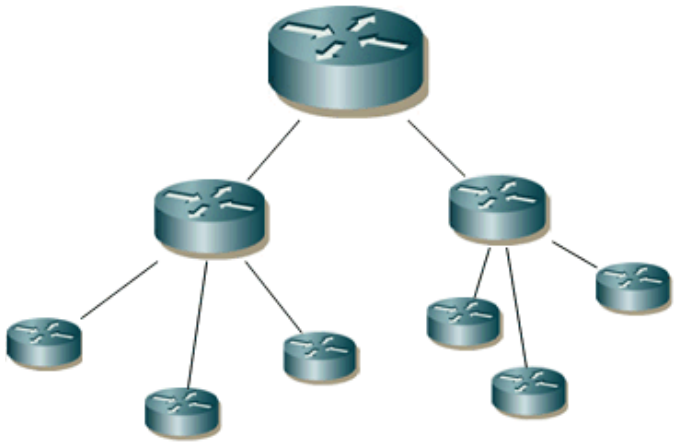
The following picture illustrates a simple example of a network with A, B and C subnets. These subnets are interconnected through a router and thus to the internet. Consequently, provided B subnet station wants to communicate with A subnet server, it sends data to the router and this secures their delivering to A subnet. On condition the station wants to communicate on the internet, the router will send the data to a different interface.



Dividing the network into subnets is based on a hierarchy and all the interconnections must have a router. The communication is carried out upwards to the nearest layer, which interconnects particular subnets, and then it goes down again. The path length is calculated by **hops,** which refers to individual transits from a device to device; i.e. a number of

routers in the way + 1. A direct connection between two computers amounts to 1 hop. A term '**next hop'** is also frequently used and refers to the address of the next router in the way.

The next picture illustrates the above-mentioned situation. There is a small (only schematic) section of a wider network or internet. Small routers are on the leaves of the tree and are connected to switches and computers. These routers associate to other (larger) ones on different levels. As a matter of fact, bigger routers are always redundant in order for the network to resist a blackout or balance the load.



9.1. Routing – technical terms

Router

A device performing routing

Routing

The process of forwarding data between networks

Route

An applied path written in a routing table

Routing table

Contains records on individual routes

Routing protocol

Manages directing of a routed protocol; defines the best route towards the target and sends routing information to other routers

Routed protocol

IP, IPX or Apple Talk

Eventually, one more important and frequently used term

Router on stick

refers to a router connected to a switch by one trunk port; i.e. only one router and one line are available, which causes a considerable strain on both, the router and line and brings about failure problems

Division of routing protocols

The routing table shows several records on routes, which depends on their origin. Accordingly, packets are routed in one of the alternative ways of routing:

- static routing – manually entered routes (records in the routing table), secure and high-quality, but it does not reflect changes in the network topology
- dynamic routing – the network is automatically adapted to changes in topology and transport; routes are automatically calculated by a routing protocol
- default routing – unless there is another way, default routing is applied

Dynamic routing protocols are divided into two distinct types

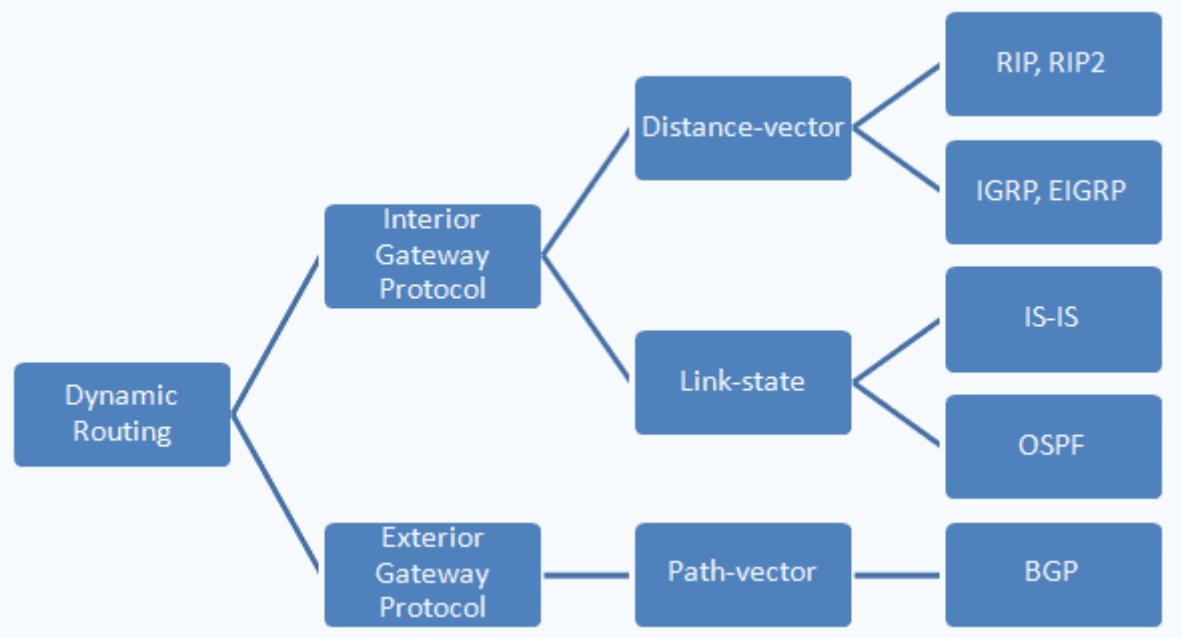
- distance-vector routing protocol – routers maintain the routing table containing information about the distance (vector) from a particular network; furthermore, they send the routing table to their neighbours, which draw up their own routing table which is further sent on; for calculating the most convenient route, one (number of hops at RIP) or more metrics (line throughput and IGRP delay) are used. In addition, an upgraded type of a distance-vector protocol is represented by a path-vector protocol.
- Link-state routing protocol – routers maintain a comprehensive network topology database (created by means of LSA), change link-state advertisements (LSA); LSA are caused by a certain event on the network. This protocol also sends Hello packets, which contain information about the protocol, quickly responds to changes of topology; all the same, it expands through a greater range and uses more resources on the router; moreover, its metric is complex-based and the most convenient route is calculated by Dijkster algorithm Shortest Path First (SPF).

Note: actually, there is one distinct type based on distance-vector protocol which has some characteristics of link-state protocol; it concerns a hybrid routing protocol or advanced distance-vector protocol. Its only representative is EIGRP.

Furthermore, dynamic protocols are divided thus; whether they are designed for being set inside a local network (to put it more precisely, inside an autonomous system (AS),

which may consist of several LAN), or they operate throughout networks (they link AS together).

- interior gateway protocol - IGP - routing inside Autonomous System (AS)
- exterior gateway protocol - EGP – routing throughout AS



10. SECURITY AND ENCRYPTION

10.1. Network security

Risks:

eavesdropping, modification of transmitted data, unauthorized access to a local network

Adequate protection:

- Protecting data from unauthorized acquiring, exchanging or deleting
- Computing capacity of individual hubs
- Cutting back on functioning or disturbing the service traffic

Passive attacks

- "Eavesdropping" in order to get unpublished information which might be abused
- Traffic monitoring – analyses of thus operated contacts

Active attacks

- Data modification
- Providing false data
- Active attacks cannot be 100% avoided; however, in contrast to passive attacks, they are easier to detect

Objectives of security services

- Securing data confidentiality – by means of encryption of the entire communication channel, or selected sensitive data
- Securing authentication of network users (revealing a masked intruder)
- Securing data integrity
- Securing the refusal of messages – to secure the impossibility for a user to deny sending the message and for the receiver to deny receiving the message
- Allocation of access rights in order to control the access to the computer, data and applications; identification and authentication of applicants for access are also its integral parts
- Securing the availability of network services; attacks on the availability of services may be prevented by authentication and encryption

10.2. Firewall

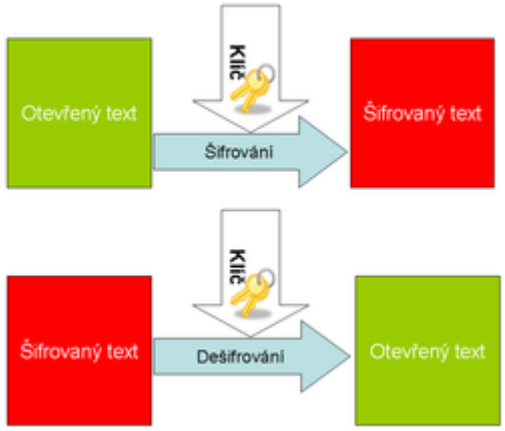
- It refers to a set of measures (implemented by HW and SW) which protect the network against an unauthorised access from the outside and, simultaneously, against information leakage
- It allows, e.g. controlling the user access from external and internal networks, setting up access rights, filtering out dangerous services, channelling security to one communication hub, blocking a hostile mapping of the internal network, auditing legal and illegal operations.
- It provides security when entering and exiting the network
- It serves as a filter; i.e. it decides what and to where it will be allowed.

10.3. Encryption

1. Symmetric encryption

Encryption and deciphering using a single key. Symmetric encryption, sometimes also called 'conventional', refers to a cryptographic algorithm that uses a single key for encryption and deciphering. Thus, it differs from public key-based algorithms using a pair of keys – a secret and public one.

The great advantage of symmetric ciphers consists in their low calculation complexity. Public key-based algorithms may be hundreds of times slower. On the other hand, the main disadvantage consists in the necessity of sharing a secret key; therefore, the sender and receiver of the secret message must agree on a particular secret key.



Picture 2: symmetric encryption

Open text → *encryption* → *encrypted text*

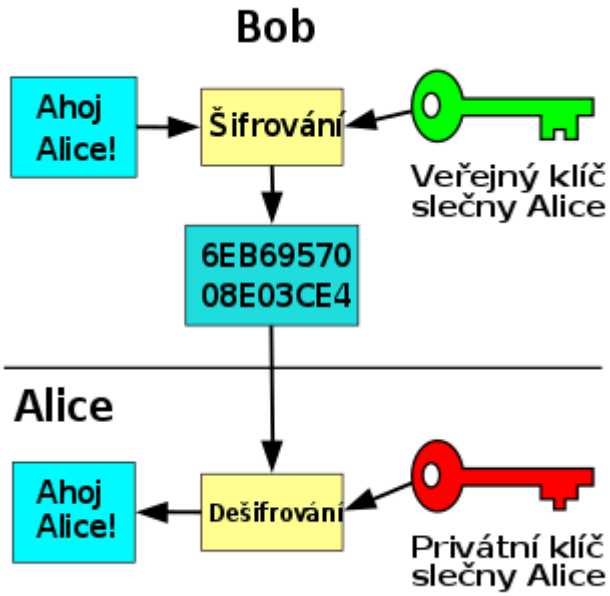
Encryption → *deciphering* → *open text*

'klíč' – 'key'

2. Asymmetric encryption

Examples of asymmetric encryption. **Asymmetric encryption (public key-based encryption)** concerns a group of cryptographic methods which use **different** keys for encryption and deciphering. On the whole, this is the main difference from the symmetric encryption, which uses a single key for encryption and deciphering.

In addition, apart from an obvious possibility of a secret communication, asymmetric encryption is also used for an electronic signature; i.e. a possibility of revealing the author of the data.



Picture 3: asymmetric encryption

Bob

Hello, Alice → encryption ← Alice's public key

Alice

Hello, Alice ← deciphering ← Alice's private key

Encryption key for asymmetric encryption consists of two parts; the first part is used for message encryption (the receiver of the message does not have to know this part); the second is used for deciphering (the sender of the encrypted message usually does not know it). Obviously, the one who encrypts does not have to share any secrets with the receiver who deciphers as a result of which there is no need of exchanging keys; this is the main advantage of asymmetric encryption.

The most common version of asymmetric encryption consists in using a public and private key; encryption key is public; the owner of the key publishes it so that whoever may encrypt the specified messages; on the other hand, the deciphering key is private; i.e. the owner keeps it secret and uses it for deciphering the messages (there are also other methods of asymmetric encryption which require to keep the key secret).

Obviously, the encryption key 'e' and deciphering key 'd' must be mathematically intertwined; however, in regard to the encryption effectiveness, there is impossibility of calculating the deciphering key from the encryption key.

Computer network security

In this case, the term 'network' refers to a system of several computing systems; users access the network via one of these systems.

- Sharing - a very large number of people may potentially access the network; various devices may be controlled by not necessarily secured systems
- Complexity - the network contains various operating systems communicating via a connecting mechanism, which should provide the security; however, this mechanism must be rather universal; moreover, the network as a whole cannot be subjected to testing or, even, certification.
- Unknown perimeter - we do not know all connected people; moreover, it is not clear how other devices work
- Number of vulnerable places - as a matter of fact, it is necessary to trust the security mechanisms in all the devices since many network parts are located off the operators' supervision
- Unknown path - in most cases, it is not possible to control the path of data transfer; thus, anyone may capture them without previous information. Anyway, communication protection may be provided as follows:
    - Data flow - also referred to as 'stream enciphering'; i.e. encryption of data in the way that conveys the impression of a communication channel being highly reliable with respect to a possible attack
    - Individual messages - correspond to a today's modern free binding using 'messaging'; application messages are encrypted, or encryption of the data flow is carried out either between two network hubs, or between two applications running on these hubs. Concerning Link Encryption, data are encrypted just before the entry to the communication medium, and then deciphered right after arriving at the second computer. This encryption is carried out on the level of physical layer or data-link layer of the reference model. The key advantage is that this mechanism is very transparent to the user; moreover, it may be very fast and easy to connect to other devices.

End-to-End Encryption

It provides a cryptographic protection throughout the transfer process. This encryption is carried out on the level of application or presentation layer of the reference model. All the same, the encryption is no longer transparent and, in order to be effective, it must be appropriately integrated in the entire system. Its main advantage is that there is no need of encrypting the entire communication but sensitive data. In contrast to the link encryption, it provides authentication and integrity (end-to-end). Sometimes, both methods are used simultaneously - link encryption for a common preventive data protection and end-to-end encryption for achieving a high-quality protection of sensitive data. In relation to the encryption, there is a necessity of distribution mechanism and administration of necessary encryption keys, competent authorities for securing the system operation of cryptographic protection and suitable cryptographic devices providing basic functions of the cryptographic protection. Apart from common problems of access control, other thorny issues arise.

Graded access rights

The access to sensitive data may be confined only to some network hubs. On condition an authorized user asks for an access from a different hub, his access rights may be severely limited, or the access to data may be entirely denied. After receiving the call, the silent modem does not immediately start generating, but waits until the other side tries to 'negotiate'. Thus, the access is, to some extent, limited only to users who know that the line leading the computer is to be dealt with. Furthermore, the method limits the possibility of a random location of this port. In case of IP protocol, a service available on a particular device on a different port from the usual one may be an alternative for a silent modem.

11. PEER-2-PEER NETWORKS

During last 10 years, exchange networks of peer-to-peer type increased in importance in the area of downloading files from the internet; nowadays, the most popular one is Bittorent protocol network, which has tens of millions users and tens of clients (µTorrent, Vuze/Azureus). Furthermore, in last 5 years, a recent phenomenon is represented by an increasing popularity of public commercial web servers for sharing files (filehosting), out of which Rapidshare.com is the most popular one; however, systems encouraging cooperation between more people on one document, or synchronizing files (Google Docs resp. Humyo.cz) may be included as well.

Peer-to-peer networks

The term peer-to-peer network (P2P) is rather general. As a matter of fact, it involves any network where there is a symmetric communication or interaction between computers (all of them can initiate, or on the contrary, on the grounds of external initiation/requirement, carry out necessary transactions and operations). Therefore, it is not possible to functionally divide its hubs into two common types - clients and servers. As a result, a basic central task of the server is failed; subsequently, one hybrid universal type of computer hub, so called 'servent', arises (the term 'client' is also frequently used). Decentralization of the internet, which began in the age of Usenet (1979) and Fidonet (1984, BBS systems), has been successfully accomplished by P2P networks. However, the equality of all computers in the network does not mean that the network is homogeneous in all the hubs in regard to quantitative parameters such as connection speed, mass of shared data, local configuration, processing speed etc.

On the whole, P2P label has almost become a medial synonym of internet exchange networks (i.e. systems of sharing files) recently although a lot of different types of applications may work on this principle - for example, applications for distributed calculations, spreading news, voice communication and chat (IRC, Skype, Qnext, DKMessenger) or P2P internet radio broadcasting and TV stations. As a matter of fact, medial stereotypes identified P2P networks (sharing files) with piracy. Without trying to find out the truth, it is necessary to observe that e.g. Bittorent network is efficiently used for a legal distribution of large programs and files (Linux distribution); furthermore, there are torrent catalogues and trackers which help distributing and registering only legal (e.g. film) material of a public domain quality (http://www.legittorrents.info/, http://beta.legaltorrents.com/, http://www.publicdomaintorrents.com/, http://www.jamendo.com/en/); i.e. the one which is legally free of charge.

A distinguishing mark of P2P exchange networks is that files or text messages saved on any computer connected to the internet (equipped with a running client/server of a par-

ticular network) may be shared within these networks. On the other hand, networks technically differ to the extent of the real degree of functional symmetry, i.e. homogeneity and decentralization, and relative "anonymity". In fact, a perfect anonymity is practically impossible on the internet. Different generations of these networks are distinguished by these distinguishing marks.

11.1. Generations of P2P networks

The first generations is represented by networks which saved file and computer lists and file and computer addresses on one, or more special central servers (Napster, OpenNap, chat - IRC (since 1988)/IRC@find, Soulseek - the latest works to this day and is frequently used by a smaller community of music fans). In regard to the evolution, the oldest exchange P2P networks use a centralized structure of client/server type for some of their activities. It mainly deals with a network connection and searching for resources (files). Thus, servers are not needed for a routine communication and sharing between end-to-end clients; such operations are carried out by peer-to-peer.

Networks of the second generation are most frequently used nowadays. Central servers are completely missing; all the same, these networks are usually not based on entirely equal servent-hubs; i.e. computers cannot be largely replaced by one another (except for such as Gnutella or Freenet). As a matter of fact, a perfect symmetry is often reduced in practice within peer-to-peer principles in order to increase effectiveness and reliability of searching or facilitate identifying files and thus speed up their downloading.

Today's P2P systems are characterized by 'local-central' or specially-delegated/dedicated components such as various 'super-hubs' (FastTrack network with clients such as Kazaa), hubs (DirectConnect, DC++) or search engines and indexators (OpenFT), of which may (voluntarily) become all individual computers. These special 'super-hubs' are important for their quick connection and cataloguing all other ordinary computer-hubs and their resources and preventing occurrence of 'tight throats' within data flows. The next 'asymmetric' components refer to specialized storage servers providing digital hash imprints of individual files (identification signature, e.g. torrents-BitTorrent, line magnets - mainly Gnutella, ed2k - eDonkey/Overnet lines); i.e. servers which help coordinating a sped-up 'swim' downloading of individual partial data segments between computers.

Despite this fact, newer networks use peer-to-peer structure for almost all purposes and tasks; therefore, they are also called 'real P2P networks'. Moreover, real P2P networks have a distinctive characteristic that their total transmission or communication capacity of a common user increases with the number of users/hubs; in contrast to the decreasing character of centralized systems, the fact of which is supported by technologies of segment downloading.

In addition, multi-protocol clients, which are able to search and download files within more networks (protocols) - sometimes simultaneously, are also an essential feature of the second generation; for example, these are MLDonkey,KCeasy and Shareaza. Furthermore, the integral part are so called 'overlay protocols' forming a certain 'supernetwork' within the particular network (Overnet).

Emerging of the third generation of networks and clients introduces or enhances encryption elements (masking of data traffic, which had been included in BitTorrent network), anonymity or pseudonymity; i.e. secreting IP addresses of computers/hubs (encryption of mutual routing or linking). Moreover, it seeks for a larger decentralization than nowadays (Freenet, GNUnet). Actually, some of these networks cannot be accessed without approving of other users (networks such as friend-to-friend - ANts P2P, WASTE, MUTE). Others almost have features of so called virtual private networks (VPN); e.g. I2P, which allows running of all internet activities in private. Sometimes, these networks include not only a mere file sharing, but also emphasize a protected area of communication and publication of documents without a censorship interference as a result of which they become decentralized and protected by a private groupware. On the other hand, the main disadvantage of these systems consists in a smaller user's comfort and relative slowness.

The above-discussed internet radios and TV broadcastings (internet streams) of peer-to-peer type sometimes belong to P2P applications of the fourth generation (TVUPlayer, PPLive, PeerCast, PPStream). A certain part of P2P-TV systems is based on BitTorent protocol or similar ones (in this case, however, television 'on-demand' is to be dealt with; not a real-time streaming); all the same, the main ones use their own, different, systems. On the whole, from tens up to hundreds of TV channels (often sport) are broadcasted in this way with a high efficiency (given to the fact that each receiving hub may simultaneously be a retranslation transmitter for other hubs.

11.2. Filehosting

On the other hand, filehosting (both - public and commercial) on web servers refers to a rather conservative and technologically old service yet very effective, considering today's connection speed. In this area, there are over 100 important foreign servers and, probably, up to 10 Czech ones. Conditions and systems of their use individually varies in regard to downloading and uploading; however, they often have two different downloading modes; i.e. capacity or time limited free downloading (paid by an advertisement and limited via OCR/captcha systems, temporary lines and time intervals) and "bonus" downloading, which is less limited, or practically unlimited only for a small user fee. A limited selection of these servers, without domain suffixes, which, in case of interest, may be added by a reader himself, is suggested below.

Foreign:

Rapidshare, depositfiles, filefactory, megaupload, mediafire, sendspace, uploading, zshare, ifolder, hotfile, icefile, letitbit, filefront, ifile, easy-share.

Czech:

Edisk, uloz.to, czshare, leteckaposta, quickshare, bagruj, nahraj.

In this area, there are a few programs which may, to some extent, automate and thus facilitate downloading from these servers, e.g. Universal Share Downloader (USD) or RapGet.

Other important links:

- www.filesharing.eu Filesharing via P2P networks
- www.slyck.com News and Slyck portal
- www.zeropaid.com News and Zeropaid portal
- www.filesharingz.com News
- www.p2pnet.net News
- www.p2pforums.com Discussion and news portal
- www.infoanarchy.org "Decentralizing" P2P wiki-portal
- www.openp2p.com O´Reilly's website, focusing on P2P area
- www.planetpeer.de Portal for anonymous networks not only for filesharing (MUTE, I2P, Freenet etc.)
- www.fileshareworld.com Signpost for exchanging systems and P2P clients
- www.ftc.gov/bcp/workshops/filesharing Opinions of the US Federal Trade Commission on filesharing
- http://cs.wikipedia.org/wiki/Peer-to-peer Czech password for Wikipedia
- http://p2ptv.yourglobaltv.com/ a http://www.tvavailable.com/P2P_TV/ Overviews of the most frequent P2P TV clients
- http://en.wikipedia.org/wiki/P2PTV Seminal article on P2P TV
- http://www.yourglobaltv.com/p2pchannels/ Main sport channels of P2P TV
- http://en.wikipedia.org/wiki/File_hosting_service Hosting servers in general
- http://www.dimonius.ru/dusd.php - Universal Share Downloader (USD) - automatic downloader
- http://www.rapget.com/en/ RapGet – similar to the above-mentioned USD.

12. ANONYMITY ON THE INTERNET

Anonymity on the internet has recently been a thoroughly discussed topic even by governments of developed countries. Anonymity has always been an important factor both in past and present. Nevertheless, along with the arrival of new technologies and their subsequent penetration in the society, this key topic should be more extensively discussed than ever before. On the one hand, individual countries have taken bold steps to assume control over the internet in order to identify the user due to a greater security (main concerns include terrorism, child pornography, and drug sale or money laundry). All the same, on the other hand, countries try to protect the privacy and sensitive personal data of internet users, which has been supported by enforcement of so called 'Cookie Law' by the EU.

In order to achieve a perfect social anonymity, it is necessary to ignore all seven dimensions of identification information:

- Personal name
- Location
- Pseudonym connected to a real name or location
- Pseudonym revealing other information
- Revealing behavioural patterns
- Membership in a particular social group
- Information, object or skills showing personal characteristics

Reasons for anonymity remain the same in both, the real environment as well as in the virtual one - avoiding consequences of one's own behaviour (fear of repressions, misunderstanding etc.)

Identification technologies

Modern technologies offer a lot of ways and methods of identifying the individual.

IP address

It more or less refers to a unique address of each device connected to the network. For example, IP address may reveal information about a geographical location.

Geolocation

Recently, the use of techniques which are capable of determining the location up to one meter has significantly increased, e.g.:

- **Constraint-based geolocation** is based on actively measuring the distance by a response.
- **GPS** mostly runs on mobile phones.

- **A content analysis of web posts (social networks)** refers to a method of locating users based on an analysis of publicly available posts e.g. according to cities, countries or weather in the post content. Moreover, user's activity in a view of time for locating his time zone is taken into consideration.

Cookies

Cookies serve as a permanent identifier between a client and server. However, due to their intrusion of privacy, this issue is severely dealt with by the European Union.

PRISM concerns a government project of the US secret agency NSA. This project has unlimited access to data of Google, Microsoft, Yahoo and many others with the view to the fact that the above-mentioned corporations constitute 98% of the data. Nevertheless, these corporations deny having the unlimited access to these data.

12.1. Privacy supporting technologies

Tor refers to a project based on Onion Routing concept, and thus secures user's anonymity while browsing on the internet. The program is designed for protection of personal data of users, their freedom, privacy and opportunity for a private trade in the way that protects them from tracking their activities on the internet. Nevertheless, this software may be also used for illegal activities as the use of this technology greatly complicates hunting down the offender.

Orbot refers to a Tor version for mobile phones with Android operating system.

Freenet Project - this technology is considered as a perfectly safe, anonymous and decentralized platform for sharing data directed against censorship. Each user may allow a certain space on his local disc, which is subsequently available to the entire network, for saving encrypted files from other users. In this way, an own private server is not required.

The internet comprises an extensive and complex network of communication channels, via which our data flow. Each **data packet** (hereinafter 'packet'), apart from the content itself meant to be sent somewhere, contains particular distinguishing marks, which are of a remarkable interest for "big brothers". These include **Google, Microsoft, Facebook, Twitter** etc.

As a matter of fact, they use **distinguishing marks** of our data in order to find out which websites are of our interest, the frequency of our visits, and also, our location. Subsequently, this valuable information is evaluated for targeted advertising. In addition, with the arrival of social networks, spying has gone much further.

Big brothers may successfully **combine** our web activities with those of our friends and thus draw a detailed map of the internet users. This **voluntary loss of privacy** is a price

of providing services for “free”. On the other hand, so as not to show only drawbacks of these service providers, it is necessary to say that their services display high qualities and elaborateness although they may not be evident at the first sight.

12.2. Basic principles of preserving anonymity

As has been said, the internet tracks mainly data about where our data come from and whether they belong to us. Thus, the major effort should be **masking these data**. As a matter of fact, VPN (Virtual Private Networks), Proxy servers or special internet browsers may serve the purpose. The advantages and disadvantages of individual solutions are suggested below.

Connection via VPN

Virtual private networks are mostly used at work, where they enable more computers to access network storage, printers or other servers. At the same time, they provide communication with the public internet. Furthermore, **our packets are marked by IP address** of VPN server, not our computer, in order for websites and big brothers to see them.

As long as we log in a VPN network which is located in a different country, our physical location will not be found out. Moreover, VPN server encrypts the communication so that nobody, except for end-to-end server, will be able to read our data.

There are many VPN from different places of the world which are meant for an anonymous internet surfing. Unfortunately, all of them are obliged to publish our IP address on condition they are ordered to do so by court; otherwise, they would be banned. Therefore, we cannot rely on the fact that if we subscribe VPN, nobody will be able to track down our IP address.

Connection via proxy server

Like VPN, also a proxy server **provides communication between our PC and the internet**; therefore, the internet will consider our data as belonging to the proxy server. However, in contrast to VPN, data **will not be encrypted**. Since proxy servers suggest a simpler solution than VPN, it is also possible to use proxy servers with publicly accessible web interface.

As a matter of fact, they are easily applicable when **a short-term application** is to be dealt with; the only thing is to put the appropriate address in their address bar. In this way, the proxy server provides the communication with the particular web.

All the same, it must be taken into account that all our data pass through the proxy server; i.e. in case of unreliable proxy, **the data may be abused**. Therefore, web proxy servers are not recommended to be used for visiting secured webs (http.).

Special web browsers and search engines

Anonymous web browsers focus on **layman's expectations from his common browser** when the anonymous mode is switched on; this mode does not hinder our internet activities from big brothers by any means - only from other users of the same computer. Thus, the entire communication is, as usual, tracked down.

On the contrary, anonymous web browsers are programmed in the way of preventing big brothers from tracking our data. Although this solution is not remarkably effective, it is a simple and quick resolution. In addition, using a browser with an anonymous internet search engine is highly convenient, instead of Google, Yahoo! or Bing, since this browser does not collect information on things which a user had been looking for.

The Onion Routing – Tor

Tor is a web browser and also a server network. It is often referred to as **the internet within the internet**. It works on a principle of the **onion routing** in which each packet is encrypted in layers - like an onion - and each server is able to decipher only one layer.

In this way, each packet passes through a certain number (at least three) of servers before it reaches its destination. Nevertheless, each Tor server knows only addresses of the incoming and outgoing server - not the entire cascade.

Therefore, **it is almost impossible to track down a packet as far as its home IP address**. Tor also gained an unsavoury reputation for allowing access to the black internet, which is associated with illegal activities. The key disadvantage of using Tor browser is its low speed since data travel, literally, to and fro all over the world.

12.3. TOR - totally anonymous internet

Digital footprint

Each global network user leaves a footprint of his activity; such a phenomenon has been called a 'digital footprint' since 1980s. To some extent, the footprint intensity, at least in the first phase, depends on us - our browser settings or proxy server installation, which provides communication between the internal network and internet and thus enables a large number of security settings. On the whole, it does not guarantee a total anonymity, but gives an adequate privacy protection for a common use of the internet.

A more effective protection

At the beginning of this century, a meticulous attention was drawn to the internet anonymity. A few projects in order to provide users with an adequate privacy protection were set up. As a matter of fact, a project of Tor network (The Onion Routing) was paid a special

attention since it was funded and sponsored by American government agency Naval Research Laboratory. In the beginning, it worked as a protection of the government communication in the US. Likewise, Tor received a financial support from a non-profit organization Electronic Frontier Foundation, which deals with protection of rights in the digital world.

Hub next to the hub

How does an entirely anonymous network work? The security principle is based on a large number of hubs through which the data passes. The entire communication is asymmetrically encrypted and servers share public keys and exchange generated dynamic keys for transmitting data strings with one another. Each hub is entirely autonomous and gets the information about where to send the string on only from the message header. In this way, its knowledge of the data flow ends at the next hub. To put it more simply, the server knows to whom a particular thing should be sent and to whom the response should be returned; however, other activities are beyond its capability. The more hubs are in operation, the higher anonymity is guaranteed. The network user himself chooses the appropriate path and hubs through which the data should be sent.

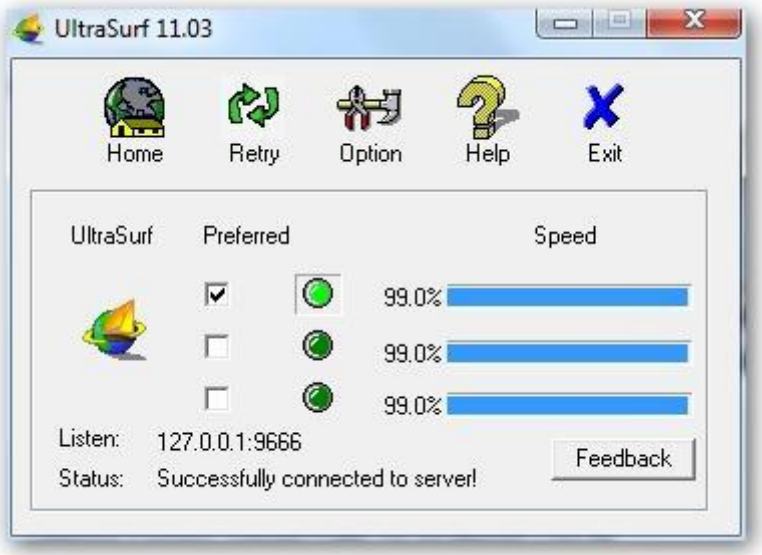
False footprints

The complexity of data transfer via anonymous servers would, at the first sight, seem highly satisfactory; however, Tor goes further. Namely, servers may send packets in a different order than have been received or false packets, which may divert a possible tracking of the data flow from the actual path, may be put in between transmitted data strings. The main disadvantage is slow response from Tor network.

In addition, there are situation in which a user, in order to protect his privacy or access some services, has to change his IP address. Nevertheless, it is not a delicate operation; a lot of services offer a solution via VPN and their own client with extra functions, an access to their own servers as a result of which the communication is redirected in the way that a user browses on the internet either anonymously, or encrypted.

UltraSurf

UltraSurf is a minimalistic program allowing anonymous browsing on the internet even to absolute beginners. This is mostly achieved by simple settings, control, low-cost operations and free availability. The program in the small window offers a connection to three different servers.



The successful change of the IP address is announced by an icon in a shape of a padlock in the toolbar; furthermore, it is possible to switch on and off controls by means of shortcuts, start the browser, automatically clear cookies and history and also set up the proxy server. In order to access American servers and services which require the local IP address, UltraSurf uses 'freekarol' reader as a result of which it belongs to the best of free-of-charge applications.

proXPN

This VPN client is very popular and widely used since it offers a fine performance, high-quality services, choice between American, British, Dutch and Singapour IP address, encryption, unlimited data transfer, limited information storage about the connection (two weeks) and a lot of other things. The program may be applied with above-mentioned services for free, or an extra charge for bonus features.

TunnelBear VPN

Users often refer to TunnelBear service and VPN application as a beautiful, very simple and user-friendly application. Moreover, it is possible to use a free-of-charge version in which 500MB may be pulled through the "tunnel" for free each month; in addition, when advertised on Twitter, 1 GB extra, together with a paid and unlimited data version for five dollars a month may, be obtained.

CyberGhost VPN

The next recommended VPN is CyberGhost, which requires an encrypted connection (1024 bit SSL 128 bit AES password) to a virtual private network VPN by a software client through which further communication passes to the internet. Program is easy to control and only a few clicks enable the connection.

CyberGhost server network is reasonably frequent and efficient. Moreover, the loss of speed, in contrast to other solutions, is significantly minor. The program and service may be also used for free although with functional limits (1 GB of transferred data per month, the speed up to 2 MB/s etc.). In addition, authors offer different paid and efficiency-graded versions. CyberGhost was recommended by *Suslikus*.

Hide My Ass

Hide My Ass is a world-known VPN which has a wide user base and wide selection of services and servers. Hide My Ass offers almost 40,000 IP addresses to hide behind in 53 different countries. As a matter of fact, free-of-charge solutions cannot compete with such a large number of IP addresses so that over 11 dollars need to be paid for a month's use;

however, the price may be reduced to six and half dollars if a long-term subscription is to be dealt with.

13. ATTACK AND DEFENSE ON THE INTERNET

13.1. Attack and defence of the PC

13.1.1. Attack

Virus

The name is derived from the analogy with biological origins. A virus is capable of self-regulation, i.e. reproduction of itself on condition there is an executable host to which it is connected. A host may involve executable files, system disc areas or files which cannot be executed directly, but by means of specific applications (Microsoft Word documents, Visual Basic Scripts etc.). As soon as the host has been executed, a virus code is simultaneously deciphered. In this moment, the virus usually tries to ensure a further self-reproduction, namely by connecting to other suitable executable hosts.

Trojan horses

In contrast to viruses, this type of harmful code is not capable of self-reproduction and file infection. Trojan horse mostly appears to be an executable EXE type of file which contains nothing (useful) but a mere body of trojan horse. Henceforth, considering that trojan horse is not connected to any host, there is only one possible form of disinfection - deleting the infected file. The older definitions say that although trojan horse appears to be useful, it is actually particularly harmful. Long ago, a trojan horse looking like McAfee virusScan program appeared although it actually disposed of files on the hard disc. Currently, several forms may be met:

- Password-stealing Trojan (PWS)
- Destructive Trojan
- Backdoor
- Proxy Trojan

Worm

Originally, the term 'worm' referred to 'Morris worm', which, in 1989, infested a considerable part of the then network, which later developed to the internet. This one and other worms (the most recent ones are Code Red, SQL Slammer, Lovsan / Blaster, Sasser etc.) work on a lower network level than common viruses. They do not spread in a form of infected files, but network packets. The packets are routed from a successfully infected system to other systems of the internet (either randomly, or by a particular key). Provided

such a packet reaches a system with a specific security hole, it may be infected, and thus other 'worm packets' may be produced. As a matter of fact, spreading a worm is based on abusing particular security holes of the operating system; its success depends on the frequency of the software containing abusive security hole. As may be derived from the above characteristics, worms cannot be detected by a common form of the antivirus software. In addition, its side effect may be a serious network infection, including enterprise LAN. The term 'worm' is often associated with a kind of infiltration spreading through electronic mail. In this way, terms 'virus' and 'worm' may overlap.

Spyware

Spyware refers to a program which uses the internet for sending data from a computer without user's knowledge. In contrast to the backdoor, only statistic data such as an overview of visited websites or installed programs are stolen. This activity is defended by trying to find out user's needs or interests and use the information for targeted advertising. However, no one can guarantee that the information or technology cannot be abused. Therefore, there are a lot of users indignant by a mere existence and legality of Spyware. Of importance also might be that Spyware spreads together with a large number of shareware programs and with a full approval of their authors.

Adware

It concerns a product obstructing a work with PC advertising. The typical symptoms are pop-up advertising windows while surfing, together with imposing websites (e.g. default website of Internet Explorer) which are of no interest to a user. A part of Adware is accompanied by 'EULA' - End User License Agreement. In this way, in many cases, the user has to agree with the installation. Adware may be a part of particular products (e.g. BSPlayer). Although the advertising provides a company during the entire activity with a particular program, its reward is a larger number of useful functions which a common free-of-charge version (advertising-free) does not include.

Dialler

Dialler involves a program which changes the way of internet access via modems. Instead of a common phone number for the internet connection, it redirects the dialling to numbers with a specific tarification, e.g. 60 Kč/minute. All the same, the era of diallers concerns only analogue phone lines (dial-up) and does not involve ADSL or other modern technologies.

Phishing

This term refers to fraudulent e-mails in which fraudulent mails looking like information from a major institution (mostly banks) are sent to a large number of addresses. These mails extensively employ 'social engineering'; i.e. the receiver is informed about a supposed necessity of filing information into an elaborated form otherwise his bank account

will be blocked (in case of a bank) or alternatively, he can be disadvantaged in another way. The e-mail usually contains a link to websites with the elaborated form which as though referred to a server of this important institution. Actually, the user is redirected to an alien server created in the same design like websites of the original and true institution. Thus caught user may not spot the difference and may fill in default boxes in which confidential information, account numbers, passwords for internet banking, pin for the payment etc. are required. Thus obtained information may be easily abused by fraudsters.

13.1.2. Protection

Unfortunately, the term 'prevention' is not much considered by PC users. Nevertheless, it is necessary to realize that merely installed antivirus software (even a regularly updated and correctly set) is an insufficient prevention. **Regular updates** of at least those products associated with a computer network of the internet are absolutely vital. To put it in the nutshell, it requires:

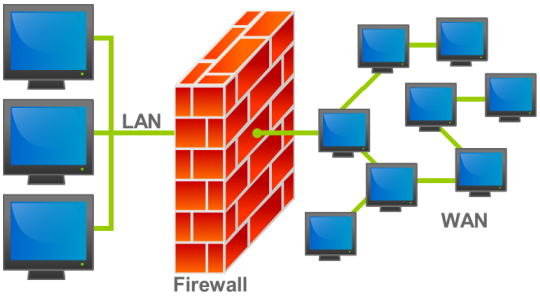
- allowing regular updates of Windows operating system and its integral parts (Start / Control panels / Automated updates)
- Regular updating of other commonly used products which might be abused from the internet (Mozilla, Firefox, ICQ, DC++); alternatively, allowing regular updates. Obviously, it also concerns various 'plugins' of particular browsers (java, shockwave, flash player)

Antivirus software

Antivirus software should be an integral part of each PC. In most cases, an essential part of antivirus software is also anti spyware. Antivirus and anti-spyware are necessary to be regularly automatically updated. In regard to the high speed of spreading bugs (mainly via electronic mail), every half an hour's update is not a luxury. On the whole, the more often the antivirus software updates the better. Likewise, it is also necessary to ensure module runs securing a continuous inspection of files manipulated by a user or application (opening /saving / running etc.). Such modules are usually referred to as 'resident shield' or, technically, 'on-access scanner'. It is also necessary to take into account that this module is the most important part of antivirus software. Although, in most cases, a module which directly inspects downloaded or sent mail is offered, it may be declined since a possible infection would be anyway prevented by on-access scanner (except for a few exceptions caused by abuse of bugs in the program). Although the virus would not be identified before put in the inbox, it would be identified at the moment of the user's attempt of opening - running the infected email attachment.

Firewall

Firewall, mostly personal firewall, is a useful supplement for the user accessing the internet. Firewall is almost vital in the moment of a user being connected via IP address and his computer thus accessible from anywhere with the internet access (a user usually gets public IP address upon dial-up connection or connection via the cable internet - Chello/UPC. Like antivirus softwares, firewall requires an appropriate use. In this way, the user should be able to discriminate between legal and illegal communication; i.e. what should be permitted or forbidden. Otherwise, firewall lacks its purpose irrespective of using a Windows integrated firewall, or a different paid firewall.



13.2. Dangerous network - resisting the attacks

As a matter of fact, networks are full of danger. There are thousands of applications that may be theoretically and practically abused. Some dangers can be relatively easily eliminated, for example, by observing appropriate safety measures such as strong passwords or up-to-date software versions. However, there are certain dangers which cannot be easily eliminated and their identification is not easy at all. These dangers will be discussed in the following text.

It mainly concerns attacks using TCP/IP protocol. This protocol is over 30 years old and it was found out that not everything had been designed and laid out correctly. On the other hand, conditions in which TCP/IP protocol was designed and created also need to be considered. As a matter of fact, its development did not foresee that within several decades the global computer network would have hundreds of millions users. However, with an utmost caution and observing appropriate measures, also the following dangers may be eliminated.

Network traffic monitoring

Network traffic monitoring is usually referred to as 'sniffing'. Basically, a network traffic analysis is to be dealt with. In the following text, basic principles and conditions on the grounds of which a possible attack may happen will be formulated. Above all, it needs to

be pointed out that this type of attacks usually occurs in LAN networks. The next condition is laid down by network not using a switched connection (this condition can be disregarded - see the further text). Now, let's see how the communication in LAN network is carried out. All the data, irrespective of from or to whom they were sent, pass through a transfer medium (cable) in a cluster called 'a frame'. Each frame is designed for a particular MAC address which means an address of each network card. Within most of the cards, the address is invariable and allocated by the producer. Furthermore, in the same network segment, each card gets all frames passing through the transfer medium and finds out whether it is meant for it. If so, the card passes the frame on to a higher layer for processing. If not, the frame is ignored. All the same, a unique situation, in which a frame is designed for all MAC addresses, may arise (broadcast).

Let's consider that from a computer connected to a LAN network you are connected to a local mail server. Further, you enter a user name, password and you download your mail without any problems. In fact, you are unaware of the fact that your colleague next to you or somebody on the opposite side of the Earth might be reading your password or mail. All the same, this situation is possible. The colleague might do it in a very easy way. As a matter of fact, there are programs allowing reading of frames even though they are meant for a different MAC address. These programs are called sniffers. You just need to install and start the program; the rest is performed by the program itself. Actually a skilled programmer finds writing of such a program very easy. The program switches the network card to so called "promiscuity" mode and monitors and analyses the entire traffic in the particular network segment. There are simple sniffers, e.g. Unix Tcpdump, or very sophisticated ones such as Hunt. The effective protection against Hunt is an adequate encryption. As long as the traffic is encrypted, the hacker will find the data useless since he would not be able to read them. The most advantageous alternatives are SSH and SSL. Therefore, it is convenient to replace current services using text passwords. Nevertheless, we need to know who is monitoring the traffic. On condition somebody from our local network is monitoring it, the adequate protection is quite hard to provide. All the same, there are programs which are able to find out network cards that are currently in the promiscuity mode.

All the same, sniffer may be installed to a computer within a certain LAN by an intruder from the outside. If he succeeds in hacking such a network, he will probably do so since there is no easier way of getting a great deal of information about various usernames and passwords. The most effective protection is to secure the network so that nobody would hack it and install the sniffer.

DNS

DNS (Domain Name Service) refers to one of the most important services that can be found within the network. This service secures transferring domain names to IP addresses and vice versa. Moreover, the service daily makes life easier to millions of users. Each

object (server, router) which is a part of a network based on IP (intranet, internet) has an exclusive identification. Such identification is represented by IP address. It refers to a number in the form of xxx.xxx.xxx.xxx.; for instance, 192.168.1.1. This number is exclusive and cannot be shared by two objects connected to the network at the same moment. However, this definite identifier has its nominal alternative, e.g. http://www.firma.cz.; and namely the transfer between these two identifiers is secured by DNS. On the whole, addresses such as http://www.pcworld.cz or http://www.google.com are easier to remember than a "bizarre mixture" of numbers. All the same, a detailed description of DNS functioning is the aim of this article; therefore a closer look at DNS abuse will be taken in the following text.

DNS spoofing

DNS spoofing is a rather dangerous activity. In order to perform it, it is necessary to meet a few requirements. Above all, the hacker has to monitor your network traffic (see above). Provided he has access to your LAN, he can start a program on his computer which captures all DNS queries and tries to respond to them according to the hacker's intention. Thus, the key goal is to subvert the DNS response and redirect the guest to another system. For instance, the hacker has a network server which is a perfect copy of, for example, a email web server - at the first sight, identical to the original. Its essential aim is to redirect all users of your network straight to that server. In this way, as long as a user enters http://www.webmail.something with the actual address 192.168.1.1 in his browser (this address is actually not available since it refers to an address from a private address block used for networks not directly connected to the internet; it is used just for an illustration), the hacker's program will try to subvert the DNS response and respond to the client in the way of the server having http://www.webmail.something 192.1691.100 address. On condition this response arrives in the user's system before the response of the actual and original DNS server, the hacker wins. How could such attacks be prevented? The first and general principle is to prevent the hacker from entering the network. Unless allowed to enter, he cannot do anything. However, if an authorised user behaves in such a way, a sniffer search engine is a comprehensible solution. In addition, there is another option - using a DNS server which signs its responses.

Further DNS abuse

There is one more type of attack which abuses a DNS server. However, this attack is rather old and effective only against older DNS versions of BIND server (Unix DNS server), still these old versions may be sometimes encountered. This attack is called Cache Poisoning and is based on subverting some authorised DNS responses. In order to pull this trick, the hacker does not even have to have access to your network; on the other hand, the solution is very simple - to use an updated software.

Routing and forwarding

Routing refers to the characteristic of IP protocol which manages the way of packets going through the network on condition that systems, which the hacker allocates on the way, allow routing. By means of routing, packets may be easily spoofed; thus, unauthorised information may be obtained. A comprehensive solution consists in switching off routing (neither Windows, nor Linux usually provide this service). Nevertheless, as long as you need routing, ACL must be correctly set in all routers.

On the other hand, routing allows a hacker to access to the internal network, which may be connected by one system and does not have to be visible to the surrounding internet on condition that forwarding rules are not adequately drawn up; therefore these rules should always be checked and tested.

Kidnapping sessions

Kidnapping sessions refers to a more advanced method of attack. The hacker has to have a sound knowledge of network communication as a result of which this attack is more dangerous. Again, the hacker has to monitor the network traffic. An ingenious device for kidnapping session is called Hunt. The hacker starts Hunt program on his computer and follows the communication between two systems. Upon considering a perfect moment for taking control over the session, he tries to take it over. In case of success, he is in a total control of the session and the target system will not find out that it is communicating with a different subject. On the whole, the hacker is allowed to do everything like the original session owner. The adequate protection again consists in an appropriate encryption and heightened network security.

Man in the middle

These attacks concerns less sophisticated methods and are possible to be easily prevented. In fact, they strongly rely on user's indifference and carelessness. These attacks may also be carried out in case of encrypted protocols such as SSH or SSL. All the same, there is no error in protocols; only users' trust was abused.

SSH

As it appears from the title of this attack, the key principle is to provide a communication medium. The hacker needs to capture the client's session, connect to the actual target server and pretend to be the end-to-end system. In this way, the client does not know that he communicates via a third system. However, there is an intricate detail. In fact, each SSH server has its own identification key. Since the hacker does not usually have this key, he has to circumvent the security. In most cases, he creates his own key. However, it results in a situation that if a client connects to the hacker's system, a warning of a change of the key displays. On the whole, this attack relies on user's indifference and carelessness. Provided a user blindly obeys and ignores all warnings, the hacker is free to follow

the traffic. Therefore, as long as you come across such a notice, contact the server administrator.

SSL

The attack by a medium may be also applied to SSL protocol. The principle is the same. However, this kind of attack is even more dangerous since SSL protocol is used within website, which associates lot of inexperienced users, who are, from image operating systems, used to blindly agreeing with every displayed notice (window). For that reason, it is very important to check SSL certificates whether they are signed by an official certification authority. A special attention should be mainly drawn to self-signed certificates.

Passwords

Even though your network is entirely secured, users observe security rules, everything is carefully monitored, controlled and analysed, yet there is a way of your network being attacked. Most servers offer certain services without which the internet would not live up to expectations. As a matter of fact, accessing these services may be offered via network and different groups of users. Some services may be available to everybody; others only to someone. Regardless of to whom the service is offered, the attack may be always carried out through the network. As a matter of fact, the hacker will try a lot of different methods and tricks; however, if proved that a network is utterly secured and most of common attacks failed, the hacker may attack your passwords. All the same, this attack is relatively time consuming and results are not guaranteed; nevertheless, it is the last possible method of getting into the system. Passwords of all protocols, which provide a particular authentication, may be attacked; e.g. SMTP, POP, FTP, SSH etc. This attack may be carried out by dozens of devices. Let's have a look at different methods of guessing the password and how to prevent it.

Dictionary attack

Dictionary attack is the most frequent method of guessing passwords. It requires a fast processor, optimized program and long wordlist. By means of an adequate program, it is possible to attack almost all passwords. However, guessing passwords does not concern only attacks through the network; passwords could also be guessed locally, which depends on specific requirements and circumstances. The main principle consists in taking a word, editing it into an adequate form (in regard to the algorithm) and comparing it with the original password. Network services aims at sending this password over the network (its form is defined by the protocol). Dictionary attack chooses such words for potential passwords which are stored in a file. Thus, different sign combinations are not tried out. Some dictionaries are very comprehensive; therefore, it is convenient to choose such a password which is not contained in the particular dictionary.

Password creation

Try creating a random password and write it somewhere. Then we will do a test whether the password was carefully chosen. Now we need a dictionary. I recommend downloading dictionaries from http://www.phreak.org/html/wordlists.shtml address. It concerns a wide selection of dictionaries of various languages. You can download dictionaries according to topics or languages. I recommend downloading all. Now, we need to find out whether the chosen password is a part of some of them. For example, UNIX uses *grep mojeheslo slovnik*. Here are a few pieces of advice on creating a strong password.

Password should contain:

- Small letters of English alphabet a-z
- Capital letters of English alphabet A-Z
- Numerals 0-9
- Punctuation marks *, #, @,] etc.
- 6 characters minimum

Password should not contain:

- any word
- any name
- combination of a name (word) and numerals, e.g. honza52
- Information about you, nicknames or wife's name etc.
- numbers related to somebody or something
- Birthdates, phone numbers, addresses etc.

It is necessary to take into account that one password should not be used twice. As a matter of fact, on condition you set up several e-mail addresses, you should supply them with different passwords. Actually, it could happen that your password will be revealed (e.g. by means of sniffer); thus a hacker would be allowed to access a lot of other systems.

14. LITERATURE

Habraken, Joseph W. Průvodce úplného začátečníka pro Počítačové sítě : není zapotřebí žádných předchozích zkušeností!. 1. vyd. Praha : Grada, 2006. ISBN 80-247-1422-1.

STALLINGS, William. *Local and metropolitan area networks*. 6th ed. Upper Saddle River: Prentice Hall, 2000. xvi, 478 s. ISBN 0-13-012939-0.

PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z : [technologie pro datovou, hlasovou i multimediální komunikaci]. 2. aktualiz. vyd. Brno: Computer Press, 2006. 430 s. ISBN 8025112780.

THOMAS, Robert M. *Lokální počítačové sítě*. Vyd. 1. Praha: Computer Press, 1996. 277 s. ISBN 80-85896-45-1.