Department
of Telecommunications

Faculty of Electrical Engineering and Computer Science, VŠB-TU Ostrava

Telecommunication Networks
Internet

Date:	22. 3. 2017
Author:	Ing. Petr Machník, Ph.D.
Contact:	petr.machnik@vsb.cz
Subject:	Telecommunication Networks

The Internet

Ing. Petr Machník, Ph.D.

Introduction

- The Internet is not just a unique network, it is also a phenomenon of contemporary civilization. It brings a wide area of benefits:
  - The web service has radically changed the method of presenting information by combining text, graphics, and sound within web pages.
  - The Internet transport – inexpensive and available to practically all companies and individuals – it has significantly simplified the task of building enterprise-wide networks.
- The TCP/IP stack, on which the entire Internet is based, has become the most popular protocol stack.

Main Features of the Internet

- It is the largest network in the world by number of users, covered territory, total amount of transmitted traffic, and number of connected networks.
- The Internet is a network that has no single control center. Nevertheless, it operates according to rules, providing all its users with the unified set of services. The Internet is the network of networks, but any network connected to it is managed by an independent operator known as an Internet Service Provider (ISP). Some central authorities exist, but they are responsible only for the unification of technical policy, a coordinated set of technical standards, and for the centralized assignment of parameters vitally important in such a giant network. This includes the domain names and addresses of computers and networks connected to the Internet.

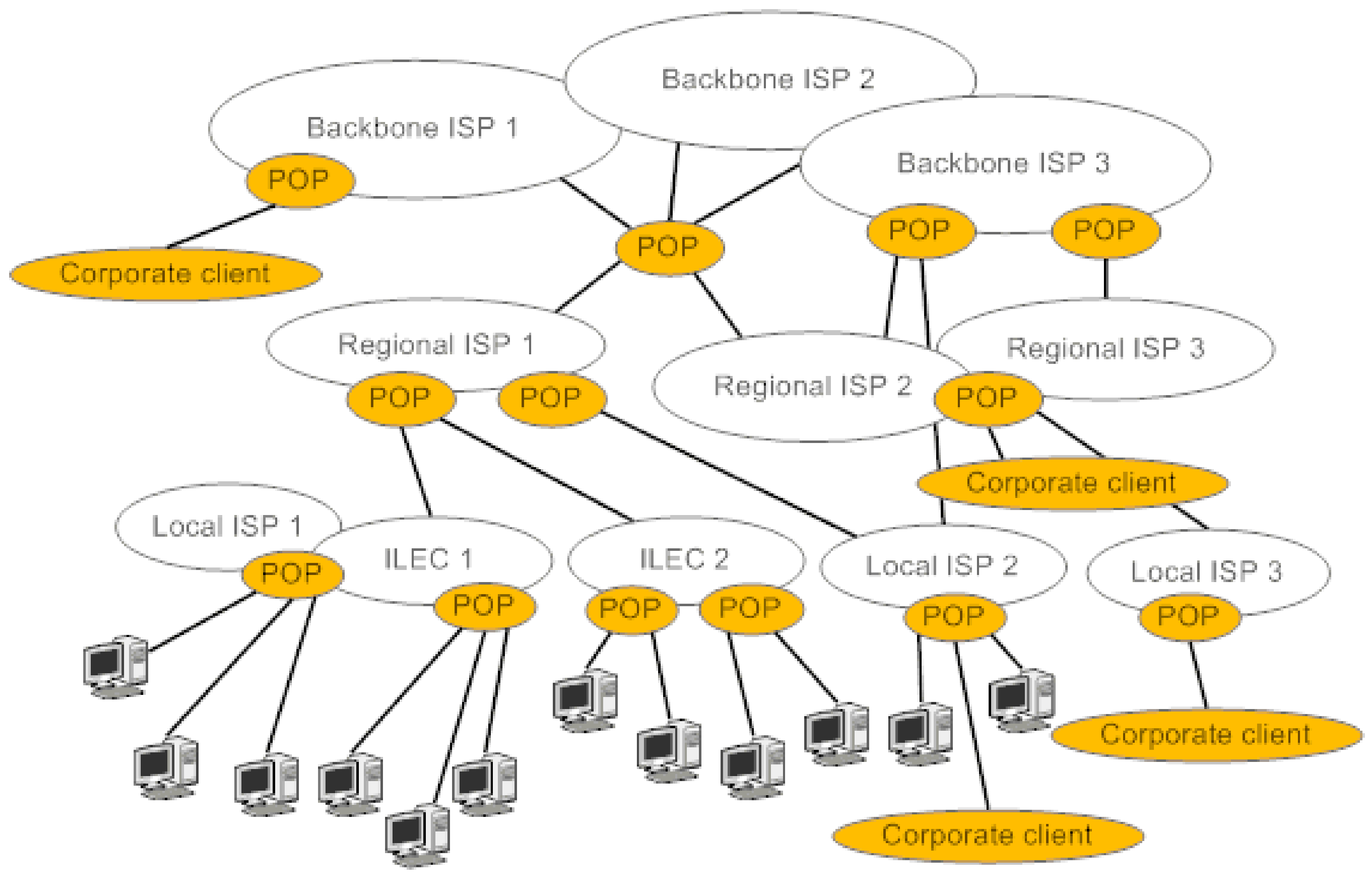
However, they are not responsible for day-to-day maintenance of the Internet or for supporting it in a usable state.

- This high degree of decentralization has advantages and drawbacks. One advantage is the ease of scaling. Negative consequences of decentralization include the complications related to the modernization of the Internet technologies and services. Radical changes require coordinated efforts by all ISPs (e.g. IPv6 implementation). Because of these complications, many new, promising technologies are used only within the network of a single provider. Another drawback is the relatively low reliability of the Internet services.
- The Internet is an inexpensive network. This is the case of the Internet telephony (VoIP technology).

- The Internet has a vast information content that is easily accessible.
- It offers a lot of services – web service, FTP, E-mail, chatting, social networks, Internet shopping, Internet banking, etc.

The Internet Structure

- Nowadays, the Internet is supported by practically all traditional telecommunication carriers. Furthermore, many new companies have created businesses exclusively on the basis of providing the Internet services.
- Different ISPs are classified according to their coverage, territory and the set of provided services:
  - Backbone ISPs are similar to international telecommunication carriers. They own backbones covering large territories (specific countries, continents or the entire world).
  - Regional ISPs provide the Internet services within the limits of specific regions.
  - Local ISPs usually work within the limits of a city.



ISP Internet Service Provider
POP Point of Presence
ILEC Incumbent Local Exchange Carrier

The Internet structure

- Relations between ISPs are based on peer-to-peer commercial agreements for the mutual transmission of traffic. Backbone providers usually have such agreements with all other backbone providers (since they are not numerous). Regional providers usually make such arrangements with one of the backbone providers and several other regional providers.
- To simplify the process of organizing interprovider communications for regional providers, there are special exchange centers on the Internet, where the networks of many providers are connected. Such exchange centers can be supported by specific, sufficiently high level providers for lower level providers connected to the network.

Exchange centers can be supported by companies dedicated to accomplishing this task. Such exchange centers have special names – usually Internet Exchange (IX) or Network Access Point (NAP). There also exist centers, known as clearing houses, that act as a stock exchange for wholesale bandwidth trading. All ISPs connected to such centers declare their cost for data transmission and the center plays the role of mediator when making arrangements.

- Another popular ISP classification divides them into four categories – Tier 1, Tier 2, Tier 3 and Tier 4. Definition of the Tier 1, Tier 3 and Tier 4 ISPs coincide with the backbone, regional and local ISPs. A Tier 2 ISP provides the Internet services to a large number of end users in a specific country or even on an entire continent. It provides a range of information and communication services.

A Tier 2 ISP is similar to a local ISP in that it works directly with the Internet users. However, the scale of the coverage area distinguishes it from local providers.

Other types of providers

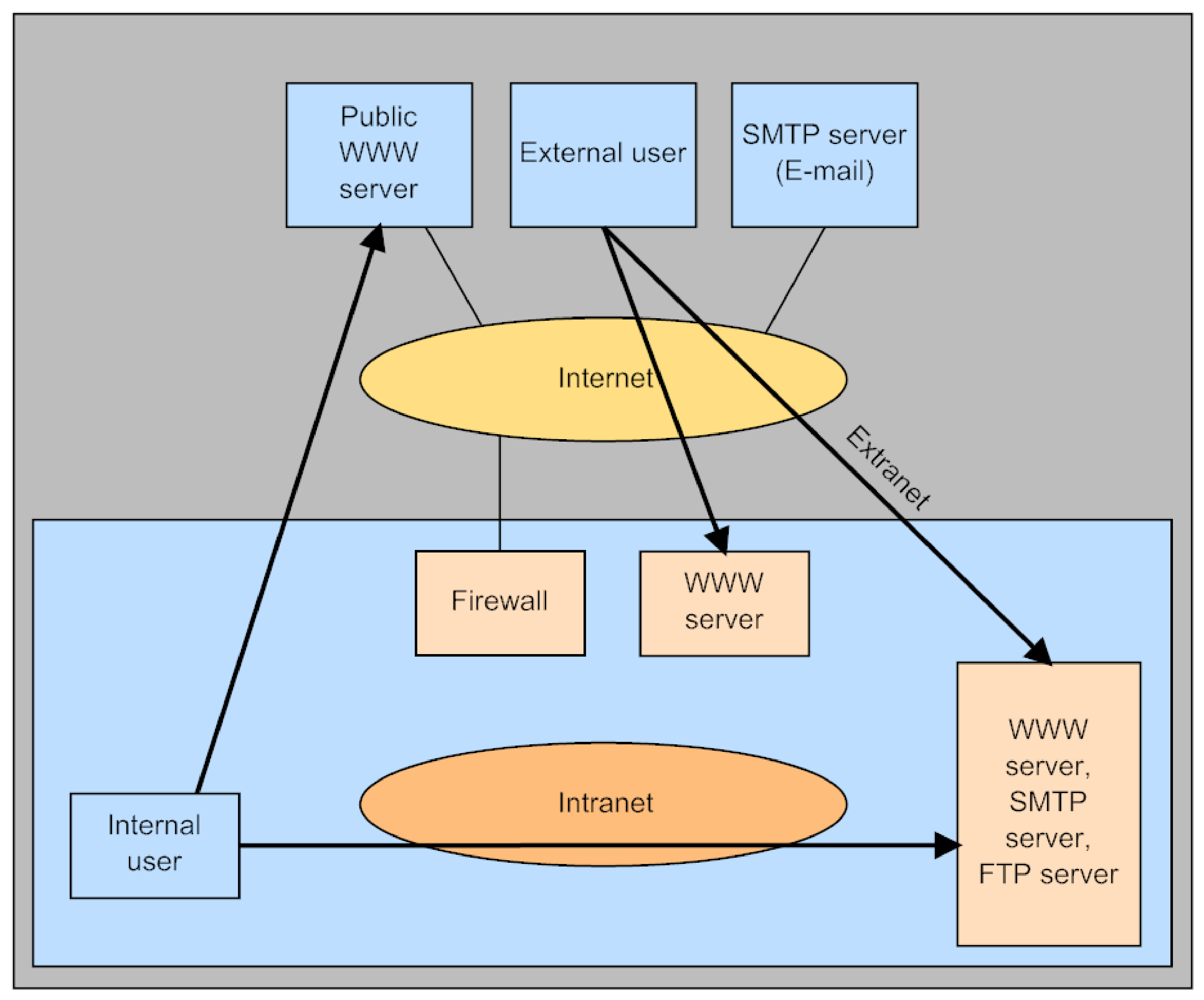
- If an ISP has its own web sites and fills them with content, it is referred to as the Internet Content Provider (ICP).
- If the company provides premises, links and servers for content created by other companies, it is called a hosting provider.
- There are also Content Distribution Providers (CDPs), which do not create content but they are involved in hosting content in multiple locations closest to the users to increase the speed of user access to the information.
- Application service providers (ASPs) provide clients with access to large scale, universal software products that are difficult to support (e.g. company management applications).

Intranet

- The network of an ISP is usually called a private IP network, since in using this network, the carrier usually provides both the Internet services and other types of services such as VPN. If this is done using the technologies on which the Internet is based (i.e. the TCP/IP transport and the web service), such services are called intranet services.

Extranet

- In the extranet, the external user (customer, business partner, etc.) have access to some internal information or services. The access is realized through the public network, it is secured and the user have to be authenticated.



The Internet, Intranet and Extranet

Secure Transport Services

- Secure transport services allow traffic transmission using a public network such as the Internet in a secure way ensuring the authenticity, integrity and confidentiality of the information being transmitted.
- The easiest tool for providing such service is the protected channel (tunnel) technology, which ensures the protection of traffic between two users of a public network according to the “point-to-point” technology. Such a protection applies the entire range of tools that use various methods of user authentication and traffic encryption.
- In IP networks, two technologies are widely used – Secure Socket Layer/Transport Layer Security (SSL/TLS) and Internet Protocol Security (IPsec).

SSL/TLS operates at the presentation layer of the OSI model, which makes it nontransparent to application. IPsec is a more universal tool because it operates at the network layer; consequently, it is absolutely transparent for applications.

- A more powerful tool of traffic protection is the Virtual Private Network (VPN). VPN is a service that creates an illusion of a private network for the subscribers of a public network. One of the most important properties of a private network imitated by a VPN is the protection of traffic of VPN users against attacks from the users of a public network. VPNs can also provide their users with the possibility of using private address spaces and QoS close to that provided by a leased line service.

IPsec (Internet Protocol Security)

- The main goal of the IPsec service is to ensure data transmission using IP networks. The application area of IPsec ensures data integrity, authenticity and confidentiality. The base technology allowing these goals to be achieved is encryption.
- For the protocols aiming at achieving this goal, the most common term is used – secure channel. The term channel emphasizes that data protection is ensured along the entire path connecting two network nodes (hosts or gateways).
- IPsec operating at the network layer is a compromise variant. It is transparent for applications, but it can operate in practically all networks, since it is based on the widespread IP and uses any data link layer technology.

SSL/TLS (Secure Socket Layer/ Transport Layer Security)

- If data protection is carried out using higher layers of the OSI model, this method of protection implementation is independent of the underlying technology (be it IP, IPX, Ethernet, or ATM) used for data transportation. This feature is an undisputable advantage of this approach. On the other hand, applications in this case become dependent on the specific security protocol because it is necessary that they have explicit calls to secure channel protocol functions built-in.
- A secure channel implemented at the application layer protects only a specific network service, such as file, web, or mail service. When using this approach, it is necessary

to develop an individual version of the protected protocol for each service.

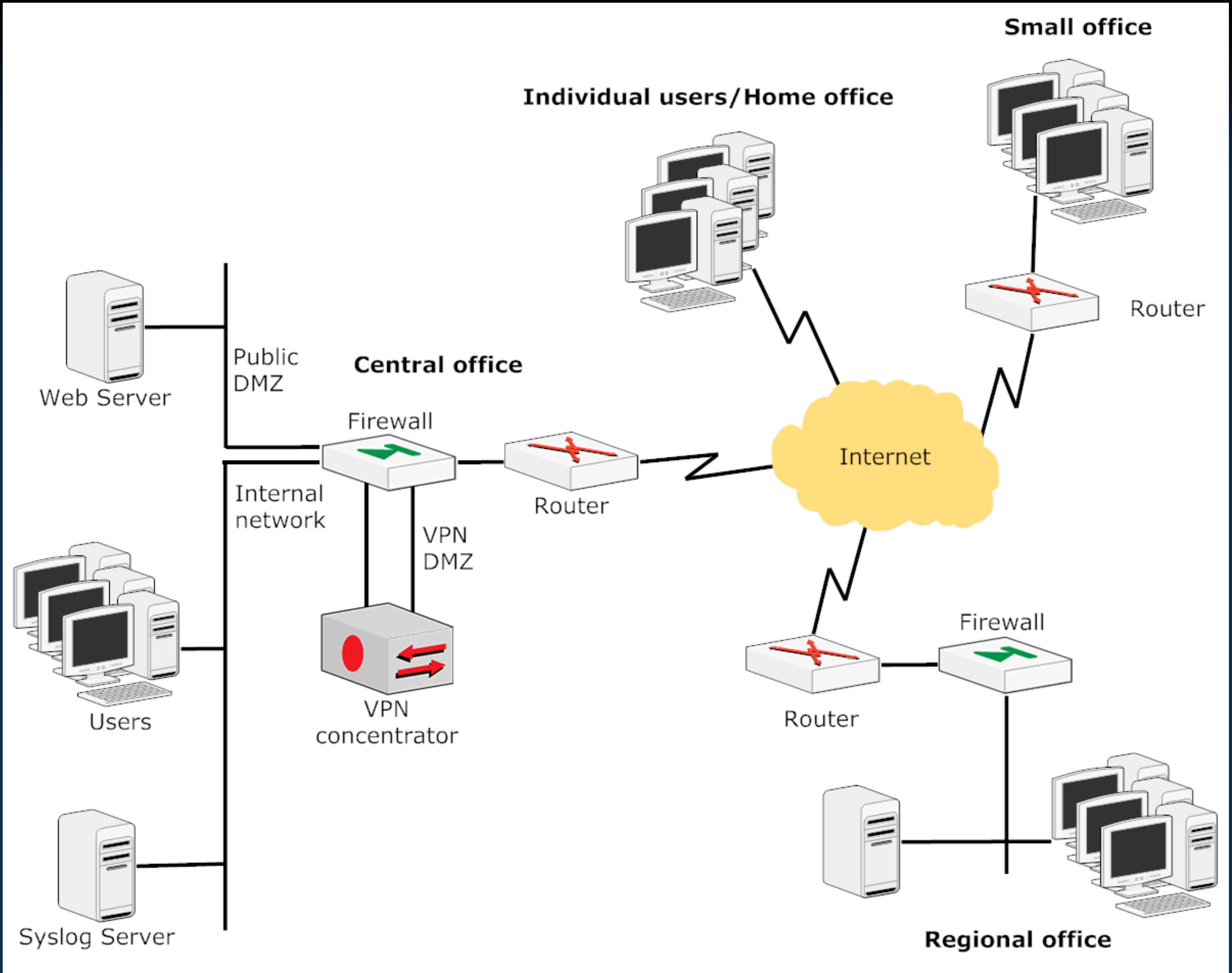
- The Secure Socket Layer/Transport Layer Security (SSL/TLS) protocols protect the PDUs of any application layer protocol or individual application. These protocols are a more universal protection tool than the secure protocols of the application layer, because any application can use them. However, for this purpose, it is necessary to rewrite applications to include explicit calls to API functions of the secure channel protocol, which operates at the presentation layer.

PPTP (Point-to-Point Tunneling Protocol)

- PPTP protects frames of point-to-point protocol (PPP) that operates at the data link layer.
- On one hand, this makes the PPTP service universal because the client can use any network protocol (IP, IPX, …). On the other hand, when PPTP is used, only PPP can be used at the data link layer.
- PPP is used in access lines, but it is being replaced by Ethernet.

VPN (Virtual Private Network)

- The term VPN means that such networks reproduce the properties of truly private networks. The network can be considered private only when the company owns it and has full control of all network infrastructure. The main feature of the private network from shared or public networks is its isolation from any other network. However, a private network is an extremely uneconomical solution.
- The VPN technology allows a medium shared by several companies to be used to implement services whose QoS characteristics are comparable to those of a private network (including security, availability, predictable bandwidth and independent choice of the addressing system).



VPN network example

- VPNs are classified into two types, depending on who implements them:
  - In the customer provided VPN (CPVPN), all problems related to VPN support must be solved by the client. In this case, the ISP provides only the traditional services of accessing the public network to connect the client’s end nodes. Network specialists employed by the company configure and manage the VPN tools.
  - In the provider provisioned VPN (PPVPN), service provider uses its own network to build a private network for each client, which is isolated and protected from other networks.
- In another classification, VPNs are divided by the location of the devices that carry out VPN functions:
  - customer edge based VPN (CE-based VPN) or customer premises’ equipment based VPN (CPE-based VPN),

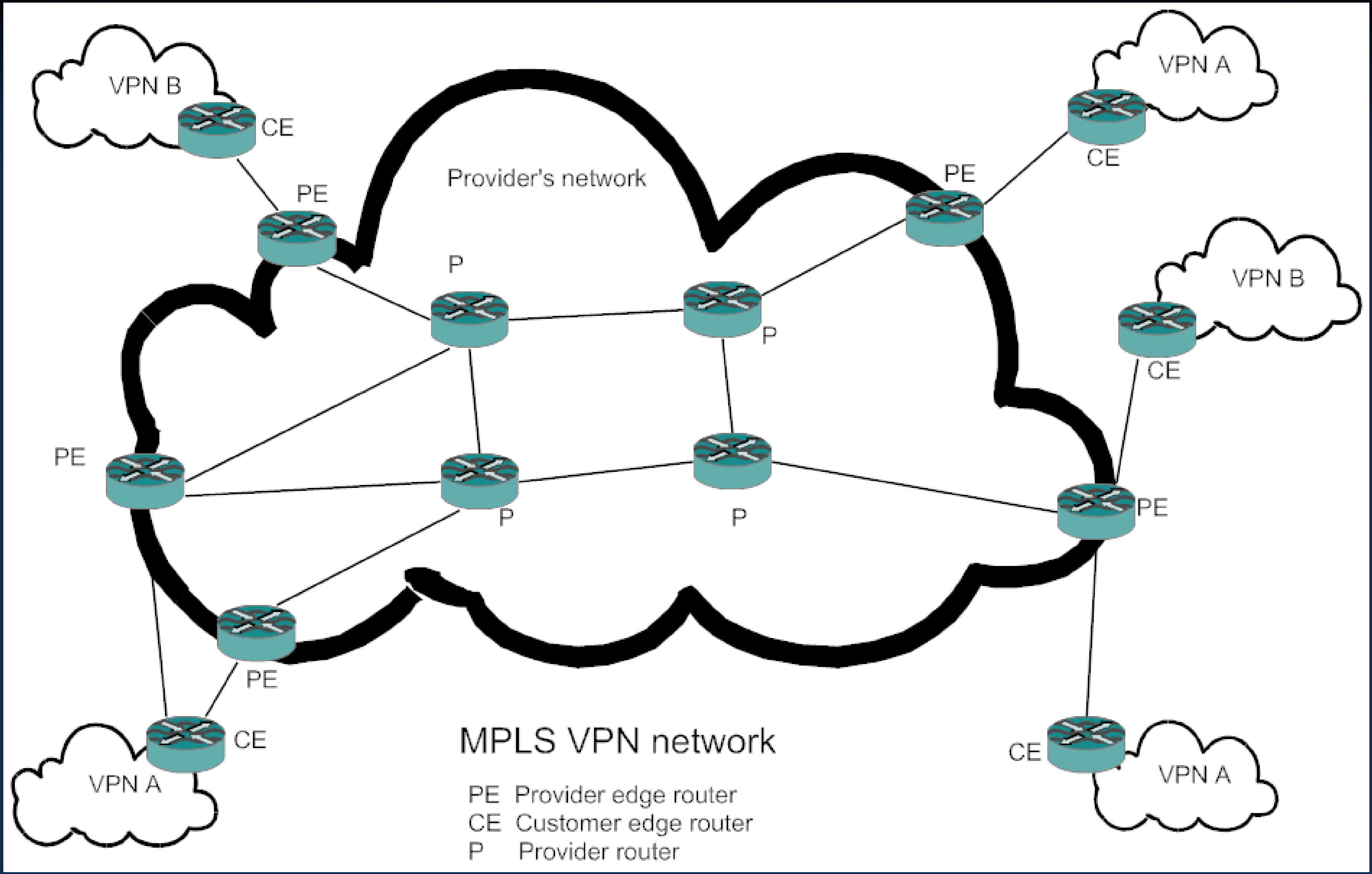
- provider edge based VPN (PE-based VPN) or network based VPN.

- VPNs are based on technologies that can be divided into two classes:
  - Technologies using data encryption – take advantage of secure channel technologies, employing them for connecting any number of client networks, not only two network users. Examples are IPsec VPN and SSL VPN.
  - Technologies ensuring security on the basis of traffic separation – use the technique of permanent virtual circuits, which ensures reliable separation of the client’s traffic from the traffic of other network clients. VPNs based on traffic separation do not use encryption because the PVC principle eliminates external attacks from other clients connected to other PVCs. Examples are ATM VPN, Frame Relay VPN and, first of all, MPLS VPN.
- VPNs implement various link topologies – for example hub-and-spoke or mesh.

MPLS VPN

- MPLS VPN is very advantageous because of its high scalability, the possibility of easy configuration and natural integration with other IP services offered by the provider.
- One of the main principles of the IP internetwork operation is the automatic interconnection of all networks into the unified internetwork. This is achieved by propagating routing information over the entire Internet using various routing protocols. This mechanism allows a routing table to be automatically created on each network router. Routing tables specify the paths along which packets are delivered to each constituent network.
- In MPLS VPN, the solution of ensuring the isolation while preserving the connectivity is achieved by automatically

filtering routing advertisements and using MPLS tunnels for transmitting client traffic through the internal network of the provider. Routing advertisements from the client’s network “jump over” the entire internal network of the service provider using the modified BGP (Border Gateway Protocol) routing protocol. As a result, the routers of different clients have no routing information about each other. Therefore, they cannot exchange packets, which means that the desired isolation is achieved.



PE Provider edge router
CE Customer edge router
P Provider router

MPLS VPN network

VoIP (Voice over Internet Protocol)

- IP telephony is the emerging communications technology arising from the convergence of the worldwide data networks and the telephone networks. Previously, the voice networks and the data networks were largely separate. Voice traffic was transmitted on circuit-switched networks where a fixed path is established at call setup and maintained for the duration of the call. Network resources are allocated to the call, leading to the logical model of time based pricing. These networks are considered to be very reliable.
- Data traffic is transmitted on packet switched networks. Messages are broken up into small packets and each packet is sent out into the network on its own, typically with header information containing the needed

destination address. Packets move through the network individually and different packets may take different paths. Packets do not necessarily arrive at the destination in the same order they left the sender, and some packets may be lost along the way. Network resources are shared, which leads to a very efficient architecture. Often, packet switched network access is priced at a fixed rate, depending on guaranteed bandwidth, but sometimes the network access is priced on a usage basis, with users charged for the number of bytes they transmit.

- The goal of the convergence is to transmit data and voice in the same network in the packetized form. Circuit switching technologies are making way for the packet switching technologies.

- These changes take advantage of the idle space in voice conversations, where it has been determined that during a conversation, only about 10 to 25 percent of the time is actually utilized to carry the voice. The rest of the time, people are in idle condition because of listening to the other end, thinking of a response to a question, or breathing between their words.
- The compression of the voice stream can reduce the circuit usage and encourage the use of a packetized form of voice. The use of a packet switching transmission system enables interleaving voice and data packets where there is an idle space. As long as a mechanism exists to recoup the information and reassemble it on the receiving end, it can be a more efficient use of bandwidth.

- It is just this bandwidth utilization and effective saving expectations that have increased the popularity of packetizing voice and interleaving it on a data network, especially on the Internet.

Basic Functioning of VoIP

- The first process in an VoIP system is the digitalization of the speaker’s voice.
- The next step is typically the suppression of unwanted signals and the compression of the voice signal. This has two stages. First, the system examines the recently digitalized information to determine if it contains a voice signal or only ambient noise and discards packets that do not contain speech. Second, complex algorithms are employed to reduce the amount of information that must be sent to the other party. Sophisticated codecs enable noise suppression and compression of voice streams. Compression algorithms include G.723, G.728 and G.729.
- Following compression, voice must be packetized and VoIP protocols added.

- Some storage of data occurs during the process of collecting voice data, since the transmitter must wait for a certain amount of voice data to be collected before it is combined to form a packet and transmitted via the network.
- Protocol headers (RTP, UDP and IP) are added to the packet to facilitate its transmission across the network. Because IP is a protocol designed to interconnect networks of varying kinds, substantially more processing is required than in smaller networks. The network addressing system can often be very complex, requiring a process of encapsulation one packet inside another, and as data move along, repackaging, readdressing, and reassembling the data.
- When each packet arrives at the destination, its sequencing is checked to place the packets in the proper order.

- A decompression algorithm is used to restore the data to their original form, and clock synchronization and delay handling techniques are used to ensure proper spacing. Because data packets are transported via the network by a variety of routes, they do not need to arrive at their destination in order. To correct this, incoming packets are stored for a time in a jitter buffer to wait for late arriving packets.
- In IP networks, a percentage of the packets can be lost or delayed, especially during periods of congestion. Also, some packets are discarded due to errors that occurred during transmission. Lost, delayed and damaged packets result in substantial deterioration of voice quality. Because VoIP systems are time sensitive and cannot wait for retransmission, in case of a packet loss, sophisticated error detection and correction systems are used to create sound to fill in the gaps.

During this process, a portion of the incoming speaker’s voice is stored and then, using a complex algorithm to approximate the contents of the missing packets, new sound information is created to enhance the communication. Thus, the sound heard by the receiver is not exactly the sound transmitted, but rather portions of it that have been created by the system to enhance the delivered sound.

Signaling Protocols

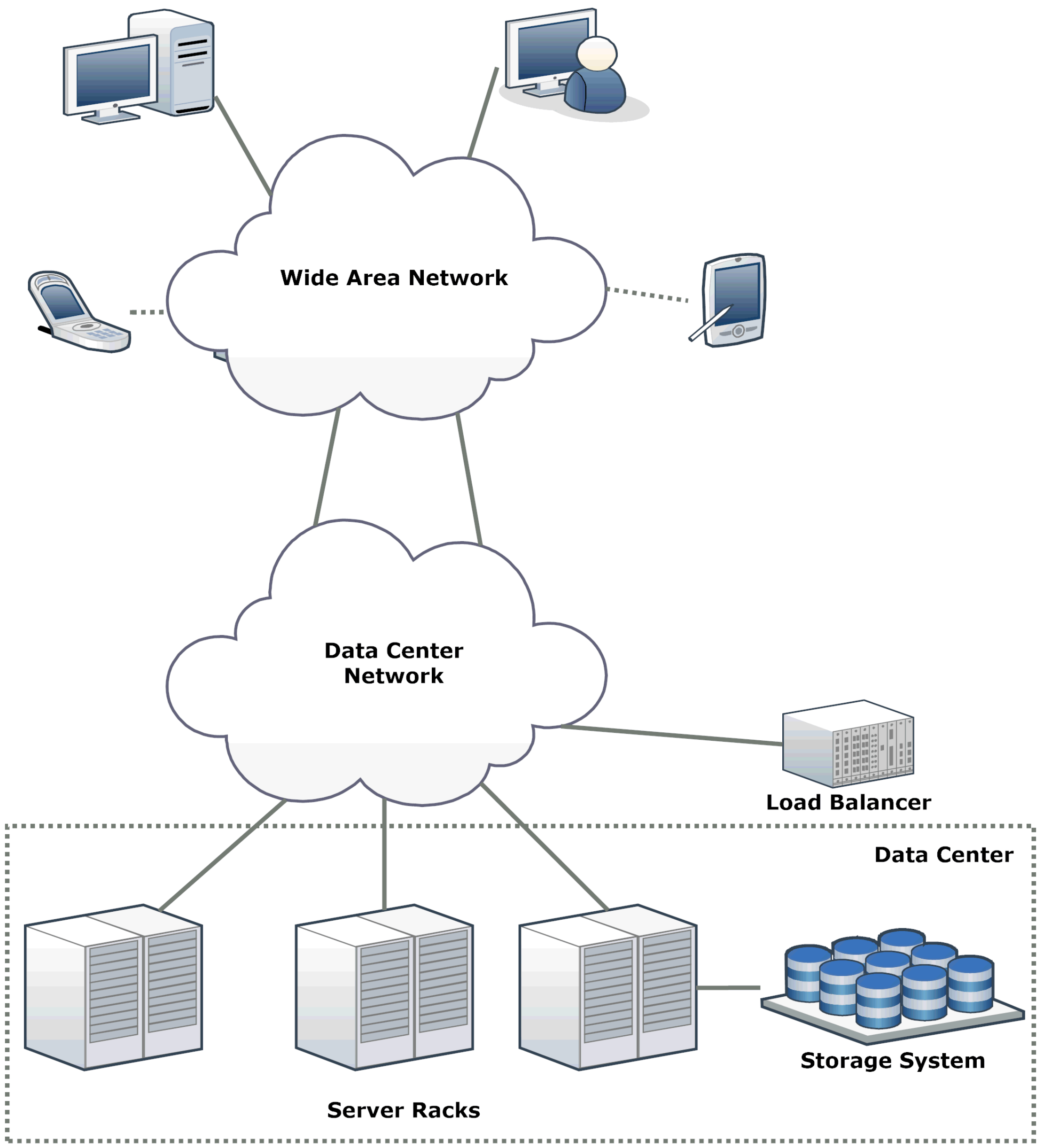
- The process of setting up a VoIP call is roughly similar to that of a circuit switched call made on the PSTN (Public Switched Telephone Network).
- When the calling and called parties agree on how to communicate and the signaling criteria have been established, the data stream over which the packetized voice conversation will flow is established. Signaling establishes the virtual circuit over the network for that data stream. Signaling is independent of the data flow. Signaling is concurrent throughout the call.
- Currently, two types of signaling are popular in VoIP, H.323 and SIP (Session Initiation Protocol).

Cloud Computing

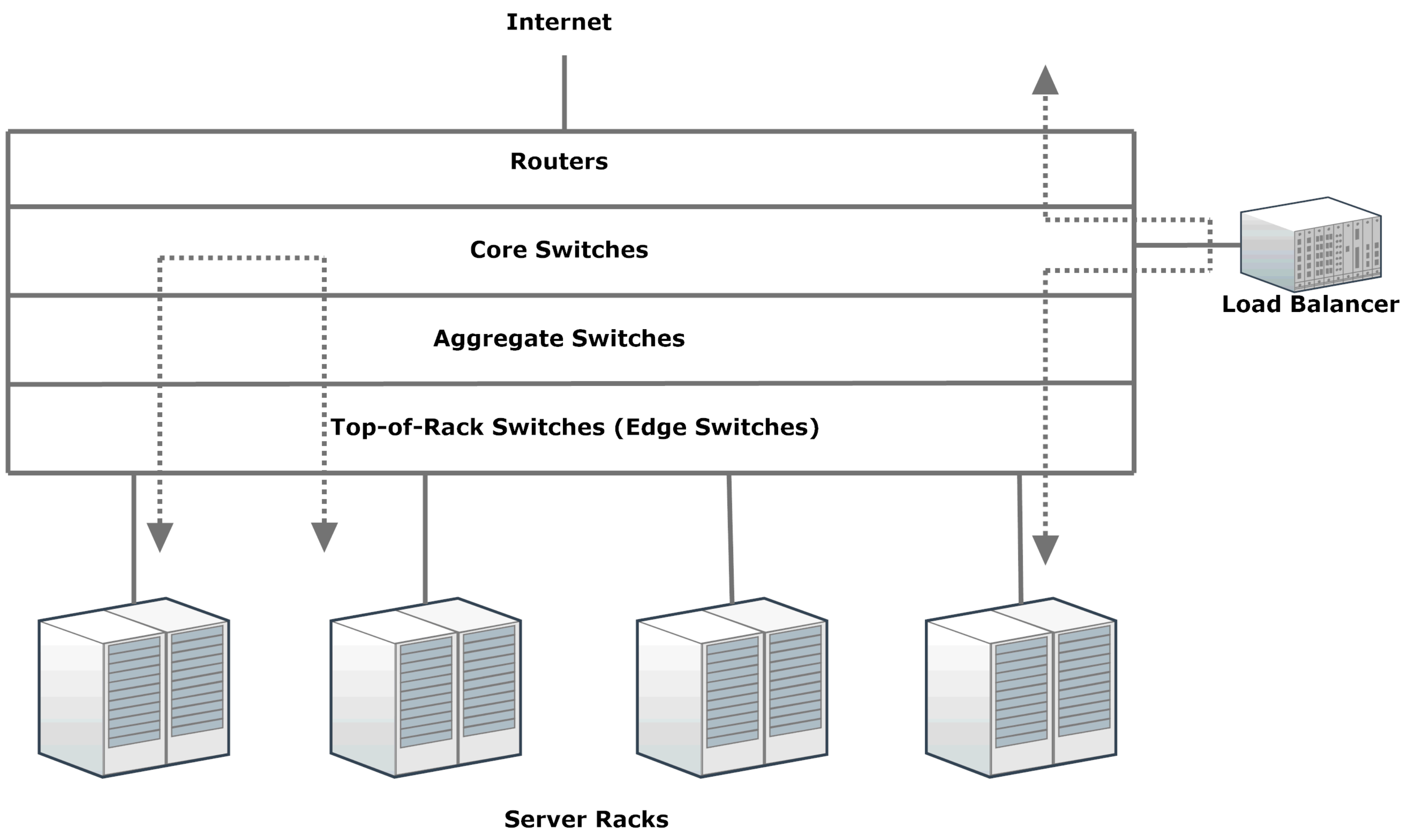
- A cloud computing or a cloud-based system is a network-based computing system in which clients use a shared pool of configurable computing resources. Cloud-based systems provide services from large data centers.
- Cloud computing means “distributed computing over a network” that runs programs or applications on numerous connected host servers at the same time. A host server in a data center is typically called a blade. Blades are normally stacked in server racks. A collection of server racks is called server farm.
- Requirements for cloud computing:
  - the possibility of creating overcapacity at large data centers,

- the decrease in the cost of storage,
- the ubiquity of broadband and wireless networking,
- significant improvements in networking technologies.

- A key factor for the success of cloud computing is the inclusion of virtualization in its structure. Cloud computing is a method of providing computing services from a large, highly virtualized data center to many independent users utilizing shared applications.
- A virtual server is a machine that emulates a server through software running on one or more real servers. Such virtual servers do not physically exist and can therefore be moved around and scaled up or down without affecting the end user.



Cloud computing system



Data center network

- Cloud data centers provide a variety of computing resources and services such as database storage, computing, e-mail, voice, multimedia, and enterprise applications.
- Benefits of cloud computing:
  - Infrastructure-less – Cloud computing enables companies and applications, which are system infrastructure dependent, to be infrastructure-less and use network-based computing.
  - Flexibility – Cloud computing enables utilizing resources of all kinds: CPU, storage, server capacity, load balancing, and databases. Cloud can be scaled up or down in capacity and functionalities.
  - Availability – Services or data in the form of both hardware and software are available to the general public and companies from anywhere.

- Use of platforms – Clients can use more efficient computing platforms instead of their own desktops and laptops.
- Availability of an application programing interface (API) - an API specifies how underlying software components should interact with each other. This enables users of the cloud to have no need to know about the underlying details of the infrastructure.

- In general, a platform is a base technology on which other technologies or processes are built. In the context of cloud computing, a platform is a collection of integrated hardware, software, and Internet infrastructure that is used as a base to provide an on-demand service.

Types of Cloud

- Public cloud – Resources are dynamically available for on-demand and self-service use by the public through web applications and open APIs.
- Private cloud – It is on-site cloud of a corporation.
- Hybrid cloud – It consists of some portion of computing resources located on-site and some located off-site.
- Community cloud – It is formed when several organizations with similar requirements share a common infrastructure.

Cloud Computing Service Models

- Software as a Service (SaaS)
  SaaS, sometimes referred as “on-demand software”, is a software delivery model in cloud computing by which software and associated data are centrally hosted in the cloud. SaaS is a highly scalable software delivery methodology that provides licensed access to software and its functions remotely as a Web-based service. SaaS is usually billed based on usage and is a multitenant environment. With SaaS, the need to install and run an application on a user’s own computer is removed and no software maintenance and support are needed.
  SaaS has become a common delivery model for many business applications, such as management software, computer-aided design (CAD) software, development

software, accounting, management information system, and human resource management. One of the main reasons for using SaaS is the potential to reduce IT support costs by outsourcing hardware and software maintenance and support to the SaaS provider.

- Infrastructure as a Service (IaaS)
  IaaS is the delivery of technology infrastructure as an on-demand service. With the IaaS service model, an organization can outsource the use of any equipment needed to support operations such as storage, hardware, servers, and networking components. The service provider owns the equipment and is responsible for running and maintaining it, and a client typically pays on a per-use basis.

- Platform as a Service (PaaS)
  PaaS is a service model that provides a computing platform and a solution stack as a service. PaaS is a method of renting hardware, operating systems, storage, and network capacity online. This service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones. With PaaS, geographically distributed software development teams can collaborate on software development projects, and thus expenses can be minimized by the unification of programming development efforts. In this service models, applications must typically be developed with a particular platform in mind.

Network Virtualization

- Network virtualization is the act of decoupling networking services from network infrastructures. It enables network operators to compose and operate multiple independent and application-specific virtual networks that share a common infrastructure. To achieve this capability, the virtualization mechanism must guarantee isolation between coexisting virtual networks.
- Network virtualization components:
  - virtual links,
  - virtual network interface card,
  - virtual switches,
  - virtual LAN (VLAN).

- Bibliography:

OLIFER, Natalia, OLIFER, Victor. *Computer Networks: Principles, Technologies and Protocols for Network Design.* Chichester : John Wiley & Sons, 2006. 973 p. ISBN 0470869828.

BATES, Regis "Bud" J. *Broadband Telecommunications Handbook.* McGraw-Hill Professional, 2002. 803 p. ISBN 0071398511.

DEAL, Richard. *The Complete Cisco VPN Configuration Guide.* 1st ed. Cisco Press, 2005. ISBN-13 978-1-58705-204-0.

MIR, Nader F. *Computer and communication networks*. Upper Saddle River, NJ: Prentice Hall, 2015. 874 p. ISBN 978-0-13-381474-3.