

Jihočeská univerzita v Českých Budějovicích

Pedagogická fakulta – Katedra aplikované fyziky a techniky

Počítačové sítě – výukový materiál pro žáky základní školy

Diplomová práce

Vedoucí práce: Ing. Michal Šerý, Ph.D.

Autor: Bc. Jindřich Sikora

Anotace

V této diplomové práci vysvětluji žákům přístupnou formou princip počítačových sítí, způsob jejich ochrany a monitoringu. Vytvořil jsem interaktivní výukový materiál pro žáky základní školy, který je seznámí s touto problematikou tak, aby měli představu, jak taková počítačová síť funguje, jak ji můžeme zabezpečit proti útočníkům a jak můžeme monitorovat provoz v této síti.

Abstract

In this thesis, I explain to pupils principle accessible form of computer network, the method of their protection and monitoring. I created an interactive teaching material for primary school pupils, who is familiar with this issue so that your concept of what a computer network works, how it can be secured against intruders, and how we can monitor the operation of the network.

Prohlašuji, že svoji diplomovou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

Datum: 26.6.2013

Podpis:

Touto formou děkuji svému konzultantovi p. Ing. Michalu Šerému, Ph.D. za cenné rady a připomínky při zpracování mé diplomové práce.

Obsah

1	ÚVOD	8
2	POČÍTAČOVÉ SÍTĚ – TEORETICKÁ ČÁST	8
2.1	CO TO VLASTNĚ POČÍTAČOVÁ SÍŤ JE	8
2.2	HISTORIE POČÍTAČOVÝCH SÍTÍ.....	8
2.3	VÝHODY POČÍTAČOVÝCH SÍTÍ	9
2.4	TYPY POČÍTAČOVÝCH SÍTÍ.....	9
2.4.1	<i>Sítě typu klient - server</i>	9
2.4.2	<i>Sítě typu Peer to peer (rovný s rovným)</i>	10
2.5	ROZDĚLENÍ DLE TOPOLOGIE	11
2.5.1	<i>Lokální počítačová síť - LAN (Local Area Network)</i>	11
2.5.2	<i>Metropolitní síť - MAN (Metropolitan area network)</i>	12
2.5.3	<i>Rozlehlá síť - WAN (Wide Area Network)</i>	13
2.5.4	<i>Bezdrátová lokální síť - WLAN (Wireless Local Area Network)</i>	14
2.6	HARDWARE POČÍTAČOVÝCH SÍTÍ	15
2.6.1	<i>Kroucená dvojlinka</i>	15
2.6.2	<i>Konektory</i>	17
2.6.3	<i>Optický kabel</i>	18
2.6.4	<i>Síťová karta</i>	20
2.7	STRUKTUROVANÁ KABELÁŽ.....	24
2.7.1	<i>Požadavky na strukturovanou kabeláž</i>	26
2.7.2	<i>Topologie strukturované kabeláže</i>	26
2.8	AKTIVNÍ PRVKY	26
2.8.1	<i>Switch</i>	26
2.8.2	<i>Router</i>	27
2.8.3	<i>WIFI router</i>	28
2.8.4	<i>Gateway</i>	29

2.8.5	<i>Přenosové protokoly</i>	29
3	OCHRANA POČÍTAČOVÝCH SÍTÍ	30
3.1	FIREWALL	30
3.2	PROXY SERVER	31
3.3	ŠIFROVÁNÍ	31
3.3.1	<i>Symetrické šifrování</i>	31
3.3.2	<i>Asymetrické šifrování</i>	32
3.4	VPN – VIRTUAL PRIVATE NETWORK	32
3.5	ANTIVIROVÁ OCHRANA	32
4	MONITOROVÁNÍ POČÍTAČOVÝCH SÍTÍ	33
4.1	MONITORING SÍTĚ	33
4.2	CÍLE MONITORINGU	34
4.3	CO MONITORUJEME	34
4.4	PRINCIPY MONITORINGU	35
4.4.1	<i>Monitoring využívající agenta</i>	35
4.4.2	<i>Monitoring bez agenta</i>	35
4.5	REPORTING MONITORINGU	36
4.6	MONITOROVACÍ SOFTWARE	37
4.6.1	<i>ZABBIX</i>	37
4.6.2	<i>NAGIOS</i>	38
5	VÝUKOVÝ MATERIÁL	39
5.1	ZÁSADY PRO TVORBU VÝUKOVÝCH MATERIÁLŮ	39
5.2	INTERAKTIVNÍ VÝUKA	39
5.3	CO TO JE INTERAKTIVNÍ PREZENTACE	40
5.4	PREZENTAČNÍ SOFTWARE	40
5.4.1	<i>MS PowerPoint</i>	40
5.4.2	<i>Impress</i>	41
5.4.3	<i>Prezi</i>	42

5.4.4	<i>Smart Notebook</i>	43
5.4.5	<i>Macromedia Flash 8</i>	44
5.5	TVORBA INTERAKTIVNÍHO VÝUKOVÉHO MATERIÁLU	45
5.5.1	<i>Výběr vhodného software</i>	45
5.5.2	<i>Interaktivní výukový materiál - scénáře</i>	46
6	ZÁVĚR	62
	POUŽITÁ LITERATURA:	63

1 Úvod

Počítačové technologie dnes již zcela zásadním způsobem ovlivňují všechny oblasti naší společnosti a prosazují se v běžném životě většiny z nás. Usnadňují práci, zrychlují tempo přenosu informací a tím umožňují rychlejší komunikaci. Propojení nejen počítačů, ale i dalších zařízení do počítačových sítí umožňuje jejich vzájemnou komunikaci a výměnu informací. Skrývá to však také některá úskalí jako je například otázka bezpečnosti a ochrany počítačových sítí. Pro bezpečnou správu těchto sítí je nutné monitorovat jejich provoz, vyhodnocovat jej a na základě těchto informací je chránit před nebezpečnými útočníky.

2 POČÍTAČOVÉ SÍTĚ – TEORETICKÁ ČÁST

2.1 *Co to vlastně počítačová síť je*

Pod pojmem počítačová síť si můžeme představit nejenom spojení jednotlivých počítačů, ale také dalších elektronických zařízení jako například terminálů, multifunkčních tiskáren, zálohovacích zařízení, diskových polí, pomocí přenosového média. Jako přenosové médium může sloužit kabelová nebo bezdrátová technologie, umožňující komunikaci těchto zařízení.

2.2 *Historie počítačových sítí*

Historie počítačových sítí sahá do 50. let minulého století. Tehdy se počítače propojovaly pomocí sériových a paralelních portů. Následně v 60. letech nastupují terminálové sítě, které jsou založené na terminálech připojených k centrálnímu počítači. V 70. letech se objevuje mnoho firemních sítí, které se začínají propojovat. Vzniká též základ dnešního internetu experimentální síť ARPANET. Ta byla založena v roce 1969 jako čtyřuzlová síť na amerických univerzitách. Měla za úkol ověřit techniku přepojování paketů a umožnit přístup k nejvýkonnějším počítačům. Zajímavé bylo, že síť byla využívána především ke komunikaci a předávání zkušeností než k přístupu k výpočetnímu výkonu centrálních počítačů. K ARPANETu se připojují další počítačové sítě a ten se stává spíše pátevní sítí, která propojuje lokální sítě. Koncem 70. let se začíná experimentovat s přenosovým protokolem TCP/IP. Tento protokol je plně využit od počátku 80. let v technologii sítě Ethernet.

2.3 Výhody počítačových sítí

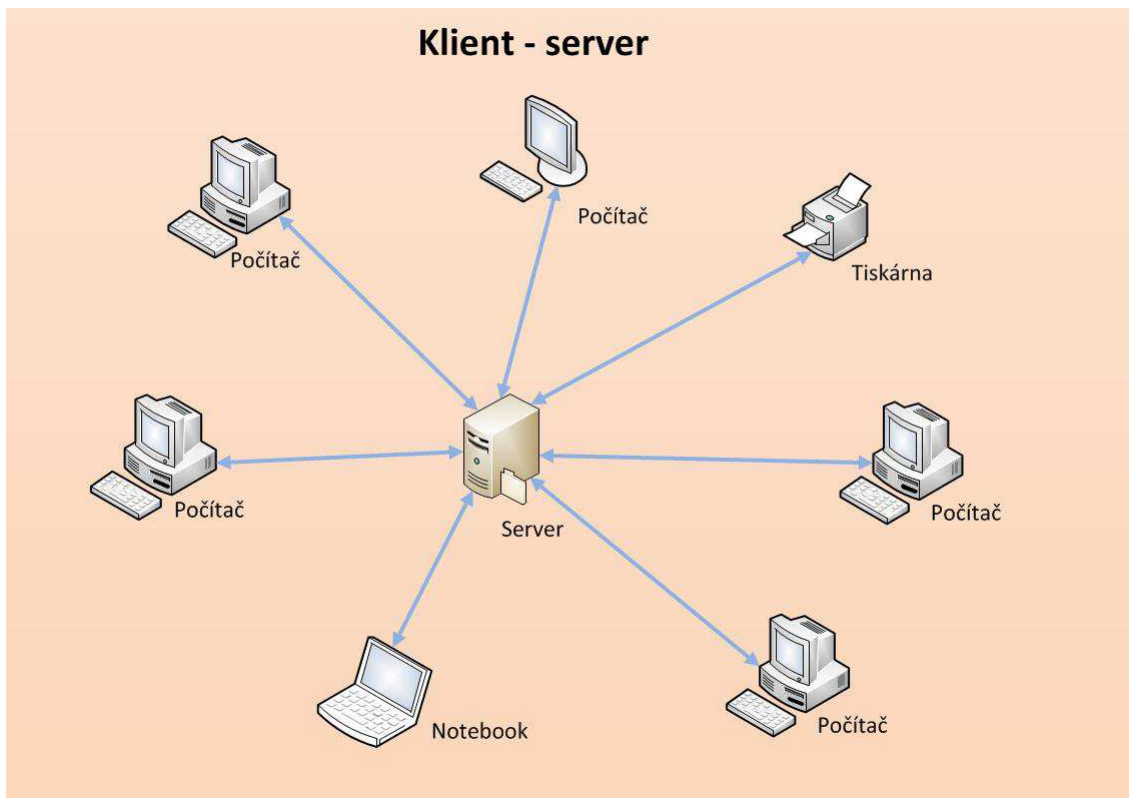
Mezi výhody počítačových sítí řadíme tyto:

- ✓ Sdílení dat a aplikací
- ✓ Sdílení diskového prostoru
- ✓ Sdílení multifunkčních tiskáren, zálohovacích zařízení
- ✓ Jednoduchý a rychlý přenos dat
- ✓ Přístup k informacím v Internetu
- ✓ Komunikace mezi uživateli – e-mail, sociální sítě, ICQ, chat
- ✓ Ochrana dat
- ✓ Zálohování dat
- ✓ Řízení provozu na síti

2.4 TYPY POČÍTAČOVÝCH SÍTÍ

2.4.1 Síť typu klient - server

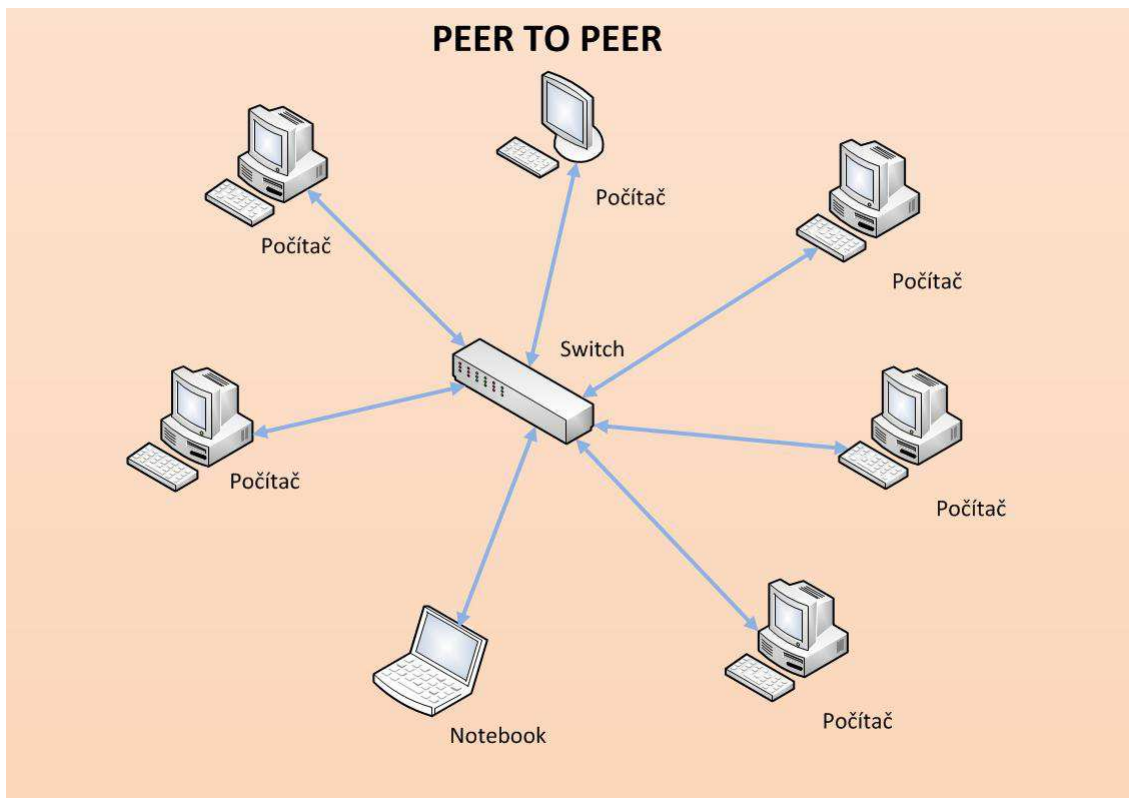
Tento model je jednou z hlavních myšlenek počítačových sítí. Klienti tzn. uživatelé zasílají žádosti o data na server a ten jim požadované informace předá. Servery mají v počítačové síti různou úlohu, podle toho jaké služby poskytují. Mohou to být tiskové servery, e-mailové servery, souborové servery, webové servery, databázové servery, proxy servery a další. Tento typ počítačových sítí je dnes nejrozšířenější.



Obr. 1 Ukázka sítě typu klient – server [autor]

2.4.2 Síť typu Peer to peer (rovný s rovným)

V těchto počítačových sítích jsou navzájem propojeny jednotlivé počítače, přičemž žádný z nich nemá dominantní úlohu, počítače jsou si rovny. Navzájem si vyměňují data a využívají svých prostředků, které mohou sdílet. Tento typ počítačových sítí se uplatňuje v tzv. výměnných sítích, kde si připojení uživatelé vyměňují data. Výhodou těchto sítí je, že s rostoucím počtem uživatelů roste i přenosová kapacita celé sítě.

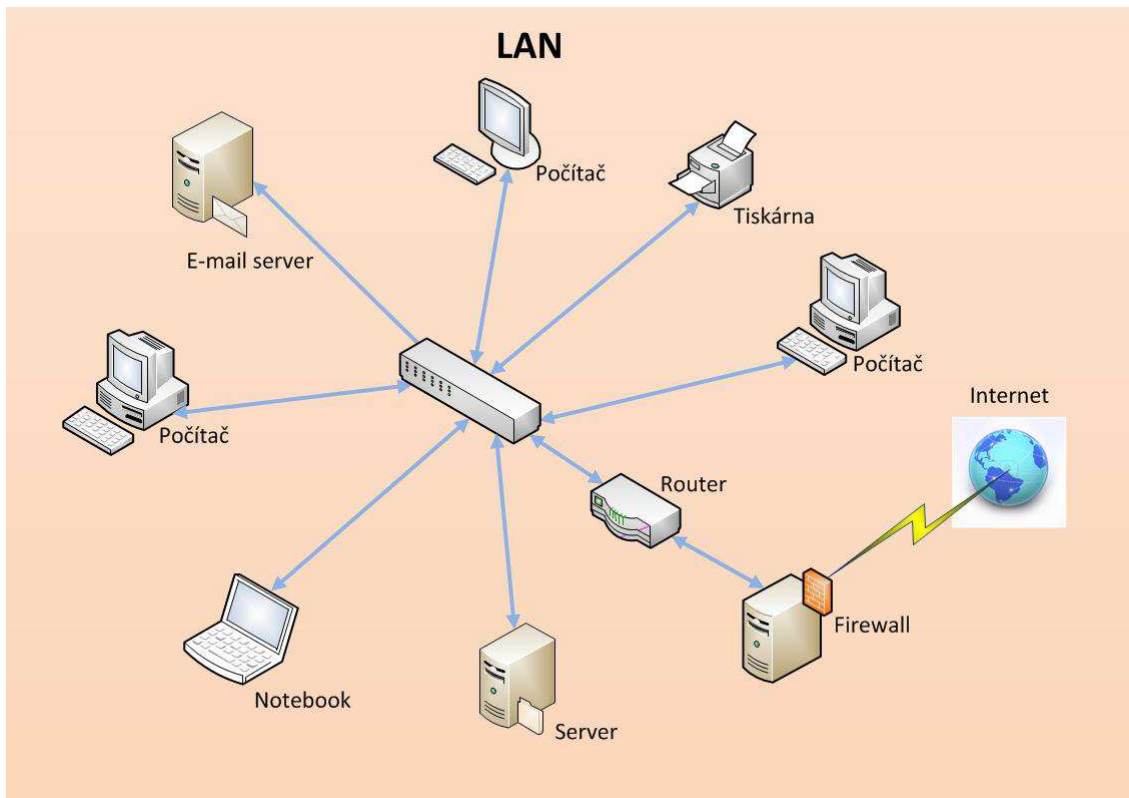


Obr. 2 Ukázka sítě typu peer to peer [autor]

2.5 ROZDĚLENÍ DLE TOPOLOGIE

2.5.1 Lokální počítačová síť - LAN (Local Area Network)

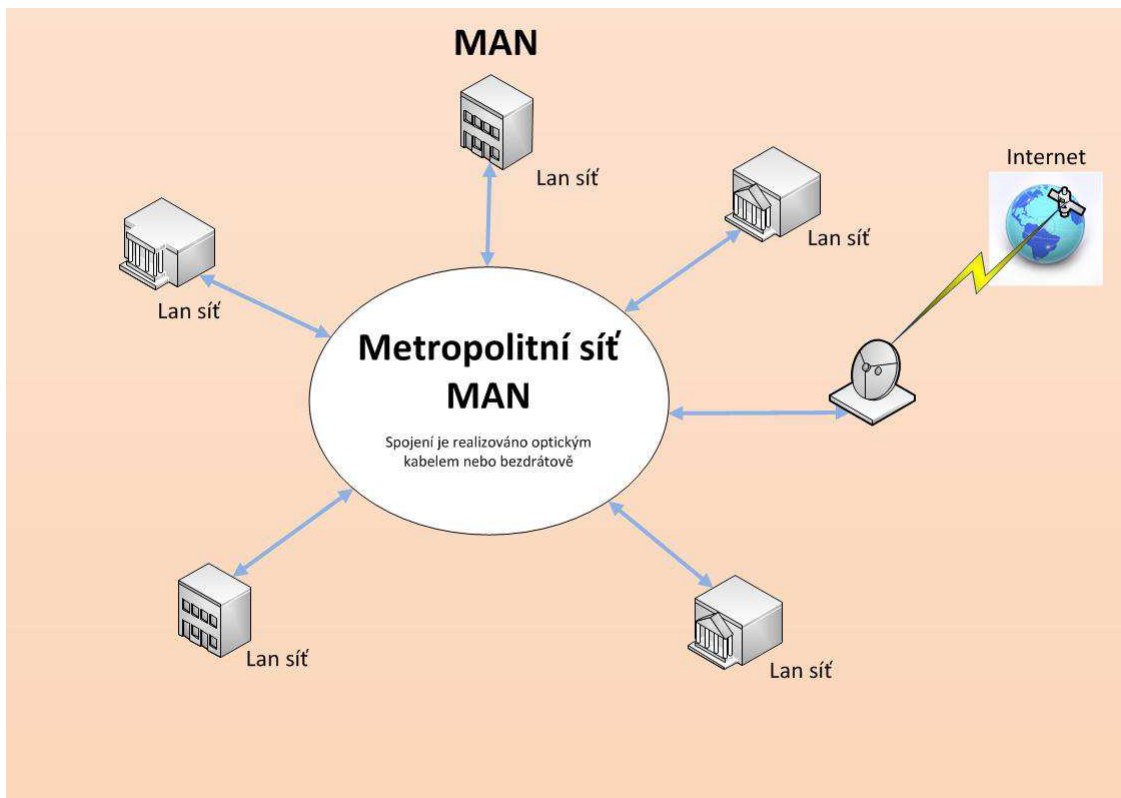
V lokální počítačové síti jsou její prvky propojeny na menším území např. uvnitř firmy, budovy nebo místnosti. LAN jsou určeny k propojení serverů, pracovních stanic, síťových tiskáren a dalších zařízení v budovách nebo podobných oblastech. Pro tyto počítačové sítě se nejvíce používá technologie přepínaného Ethernetu nebo technologie bezdrátová. U přepínaného Ethernetu je propojení realizováno metalickými kabely a případně optickou páteří. Jedná se o vysokorychlostní síť s propustností mezi 10 Mb/s až 1 Gb/s. Může to být samostatná síť, které propojuje řadu zařízení, ale dnes je již zcela určitě propojena do internetu, tedy WAN sítě.



Obr. 3 Ukázka sítě LAN [autor]

2.5.2 Metropolitní síť - MAN (Metropolitan area network)

Metropolitní síť propojuje jednotlivé LAN v rámci města nebo městské oblasti. Z tohoto důvodu dostala název metropolitní neboli městská. Pro tyto sítě používáme bezdrátové spojení nebo optická vlákna. MAN může být vlastněna jednou organizací, ale většinou se jedná o propojení několika nezávislých objektů. Můžeme mít například několik poboček firmy v jednom městě propojených do MAN sítě. Propojení jednotlivých LAN sítí je většinou realizováno pomocí kabelových optických rozvodů, bezdrátových a satelitních spojení.



Obr. 4 Ukázka sítě MAN [autor]

2.5.3 Rozlehlá síť - WAN (Wide Area Network)

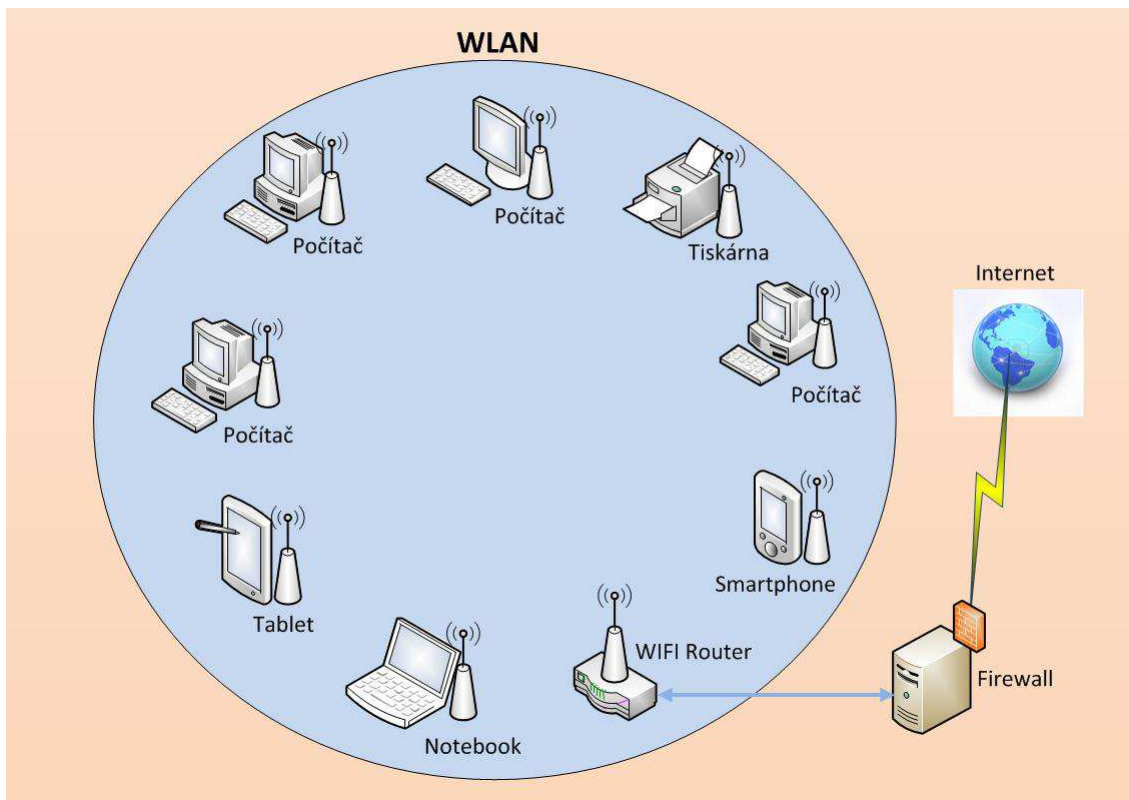
Tato počítačová síť pokrývá rozsáhlé území, jako je spojení zemí či kontinentů. Přes WAN síť se spojují jednotlivé LAN sítě tak, aby se zajistila komunikace na velké vzdálenosti. Dnešní nejrozsáhlejší a nejznámější WAN sítí je Internet. Vzhledem k obrovskému rozmachu datových sítí se dnes výraz WAN prolíná s pojmy jako intranet nebo Internet. Jako WAN sítě bývají označovány privátní sítě rozprostírající se přes různé geografické oblasti, což odpovídá rozsáhlému intranetu



Obr. 5 Ukázka sítě WAN [autor]

2.5.4 Bezdrátová lokální síť - WLAN (Wireless Local Area Network)

Tato počítačová síť je obdobou běžné LAN, ale jednotlivé prvky nejsou fyzicky propojeny metalickým nebo optickým kabelem, ale jsou propojeny bezdrátově. Pro přenos dat se využívají rádiové vlny. Výhoda bezdrátových sítí je rychlé zprovoznění počítačové sítě, kdy není nutná montáž žádné strukturované kabeláže a možnost začlenění mobilních zařízení do této sítě. Nevýhodou těchto sítí je to, že se velice špatně omezuje šíření signálu. Případný útočník se může velice snadno připojit do této sítě, pokud je nedostatečně zabezpečena a nemusí získat přímo fyzický přístup k zásuvce, jako v případě kabelových sítí.



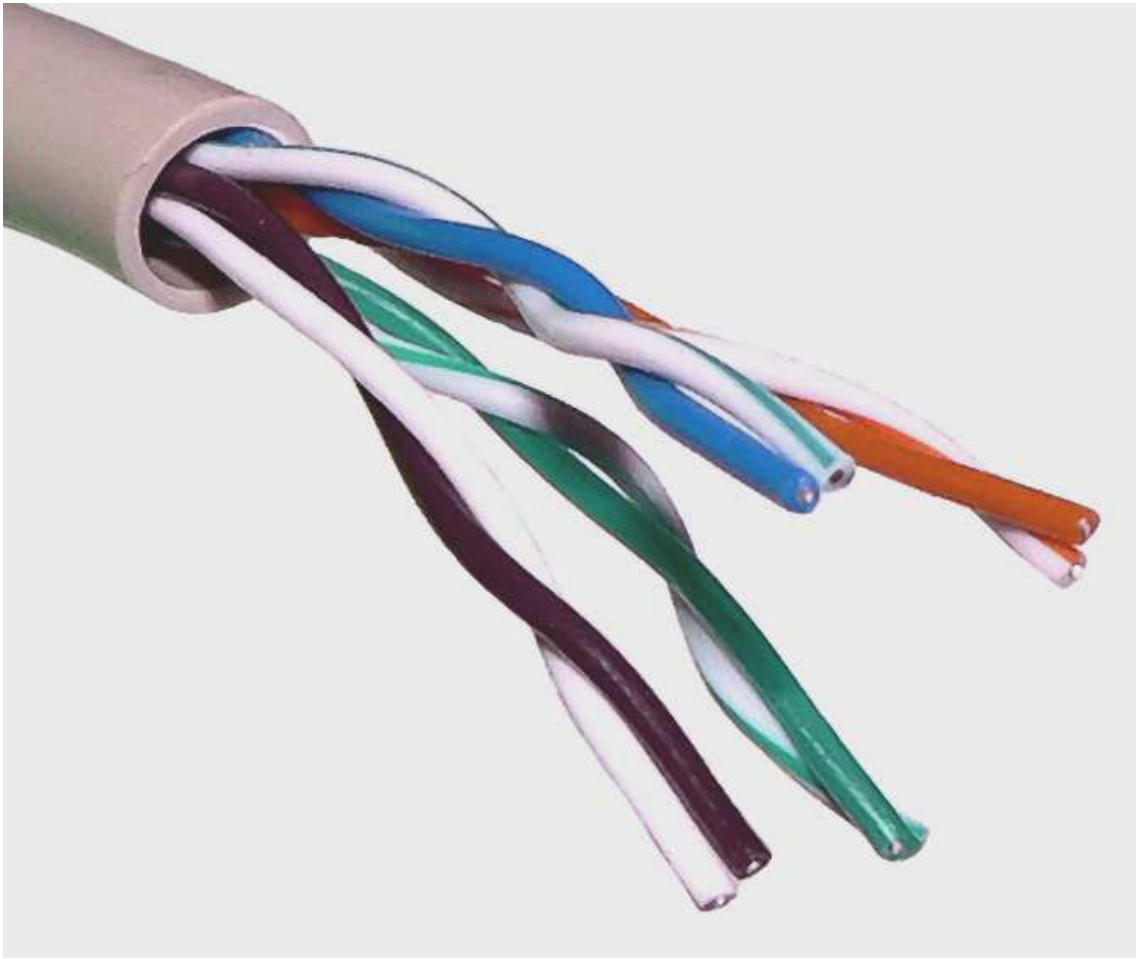
Obr. 6 Ukázka sítě WLAN [autor]

2.6 *HARDWARE POČÍTAČOVÝCH SÍTÍ*

2.6.1 Kroucená dvojlinka

Kroucená dvojlinka je v dnešní době nejrozšířenější typ přenosového média. Skládá se ze 4 dvojic navzájem zkroucených vodičů. Vodiče jsou zkroucené z důvodu omezení jejich vzájemného působení. Používají se 2 typy kroucené dvojlinky:

- Nestíněná - UTP (Unshielded TP) – zkroucené páry jsou uloženy v plastické izolaci. Používá se v běžných počítačových sítích, tam kde se neočekává výraznější elektromagnetické rušení.



Obr. 7 UTP kabel [převzato a upraveno z 14]

- Stíněná - STP (Shielded TP) – zkroucené páry jsou zabaleny do kovového stínění, které zajišťuje ochranu proti vnějšímu rušení. Tato stíněná kroucená dvojlinka se používá tam, kde se očekává vyšší úroveň elektromagnetického rušení. Tento typ přenosového média je finančně náročnější.



Obr. 8 STP kabel [převzato a upraveno z 15]

Kroucená dvojlinka se dnes používá k budování tzv. strukturované kabeláže. Pro připojení k počítači je zakončena konektorem s označením RJ45. dovoluje přenos dat přenosovou rychlostí až 1000 Mb/s. Této přenosové rychlosti se dosahuje současným využitím všech 4 párů.

2.6.2 Konektory

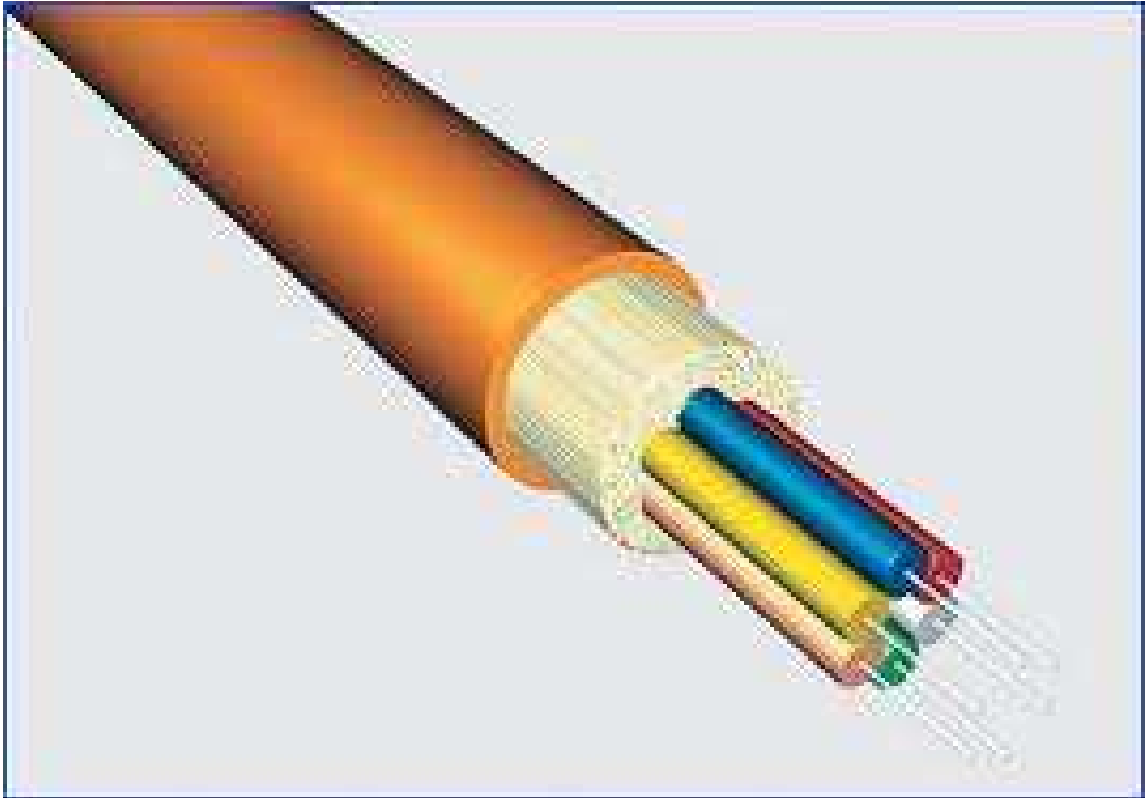
Pro připojení kroucené dvojlinky do počítačových zařízení slouží konektor RJ45. Pro přenos rychlostí 10 Mb/s a 100 Mb/s se používají pouze 2 páry vodičů. Pro přenos rychlostí 1GB/s se používají všechny 4 páry vodičů kroucené dvojlinky.



Obr. 9 Konektor RJ45 [převzato a upraveno z 16]

2.6.3 Optický kabel

Optický kabel se skládá z jednoho nebo více optických vláken, která jsou uložena ve vnějším plastickém obalu. Jádro má průměr jednotky až desítky mikrometrů. Data jsou přenášena světelným signálem ve skleněných vláknech. Světelný signál se šíří v optickém vlákne na základě fyzikálního jevu nazvaného úplný odraz, ke kterému dochází na rozhraní jádra a pláště. Před optickým přenosem se elektrický signál převádí na signál optický. To zajišťuje LED nebo laserová dioda, která generuje světelné impulsy na základě přiváděného elektrického proudu, jedná se o tzv. generátor optického signálu. Na konci optického vlákna je třeba optický signál převést zpět na signál elektrický, což zajišťuje fotodioda. Jedná se o detektor optického signálu.



Obr. 10 Optický kabel [převzato a upraveno z 12]

Optická vlákna dělíme na:

- Mnohovidová (angl. multimode) – při průchodu optickým vláknem se světelný tok dělí na více paprsků tzv. vidů. Na konec kabelu dojdou jednotlivé vidy s časovým odstupem, což vede ke zkreslení signálu. Tyto kabely jsou levnější, ale mají horší optické vlastnosti. Jádro má průměr 50, 62,5 nebo 100 mikrometrů. Mnohovidová optická vlákna mají dosah, maximálně dva kilometry.
- Jednovidová (angl. singlemode) – optickým vláknem prochází pouze jeden paprsek, který se neláme. Jednovidová optická vlákna mají jádro o velmi malém průměru 8 až 10 mikrometrů. Tato vlákna mají lepší optické vlastnosti než vlákna mnohovidová, dosahují vyšší přenosové kapacity a data přenášejí na větší vzdálenost až desítky kilometrů, ale jsou dražší.

Přenosová rychlost optických kabelů se pohybuje mezi 10 – 40 Gb/s. Optické kabely umožňují přenos signálu na kilometrové vzdálenosti, aniž musíme používat aktivní prvky. Výhodou optických kabelů je odolnost vůči elektromagnetickému rušení, nízké

ztráty a vysoká přenosová rychlost. Optické kabely se používají nejčastěji v páteřním vedení a dnes již také přímo pro spojení zařízení, která vyžadují přenos velkého množství dat, jako jsou zálohovací zařízení a diskové pole. S příchodem gigabitových spojů se stává nepoužívanějším konektor typu LC. Na konci každého kabelu musíme použít převodník pro převod elektrického signálu na světelný signál a naopak. Dále používáme konvertor, pro napojení optického kabelu na kroucenou dvojlinku.



Obr. 11 Optický konektor LC [převzato a upraveno z 26]

2.6.4 Síťová karta

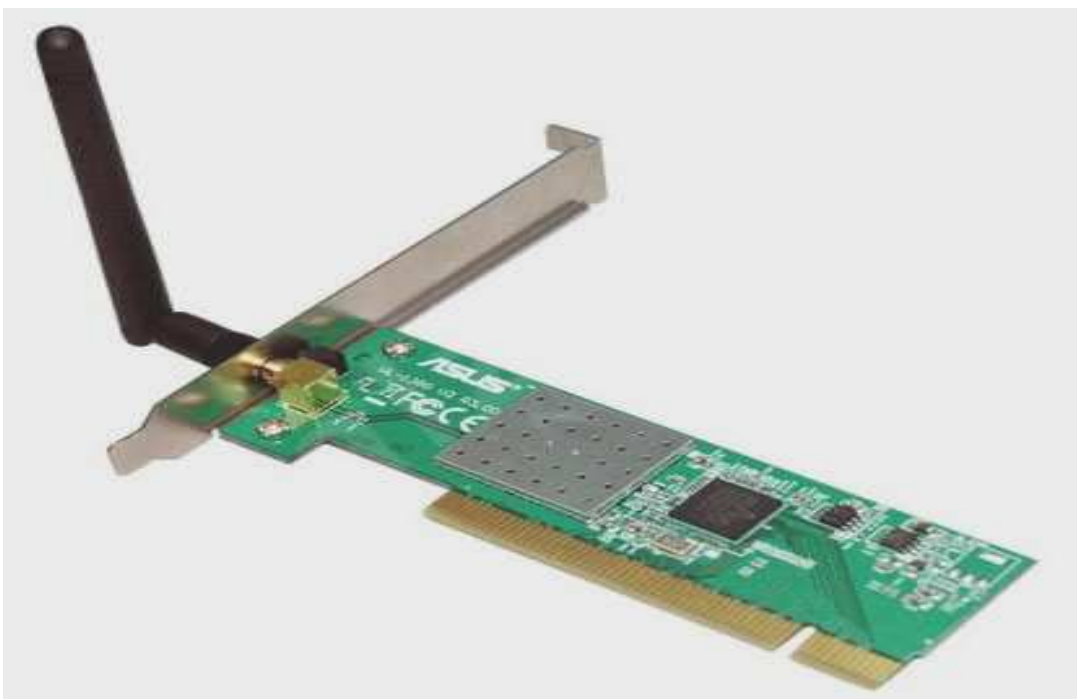
Síťová karta umožňuje komunikaci počítače s dalšími zařízeními v počítačové síti. Převádí data do podoby datových paketů a přenáší je po přenosovém médiu k dalším počítačům. Ke každé síťové kartě je k dispozici ovladač síťové karty. To je program, který slouží k její instalaci a nastavení. Zajišťuje také komunikaci mezi počítačem a kartou. Dnes již jsou síťové karty obvykle součástí základní desky počítače.



Obr. 12 Externí síťová karta [převzato a upraveno z 17]

2.6.4.1 Bezdrátová WIFI síťová karta

Slouží pro připojení zařízení do WLAN počítačové sítě. Datové pakety se přenášejí pomocí radiového signálu na frekvenci 2,4 GHz. Můžeme si vybrat z klasických externích WIFI síťových karet pro stolní PC nebo USB WIFI síťových karet, které můžeme připojit do USB portu.



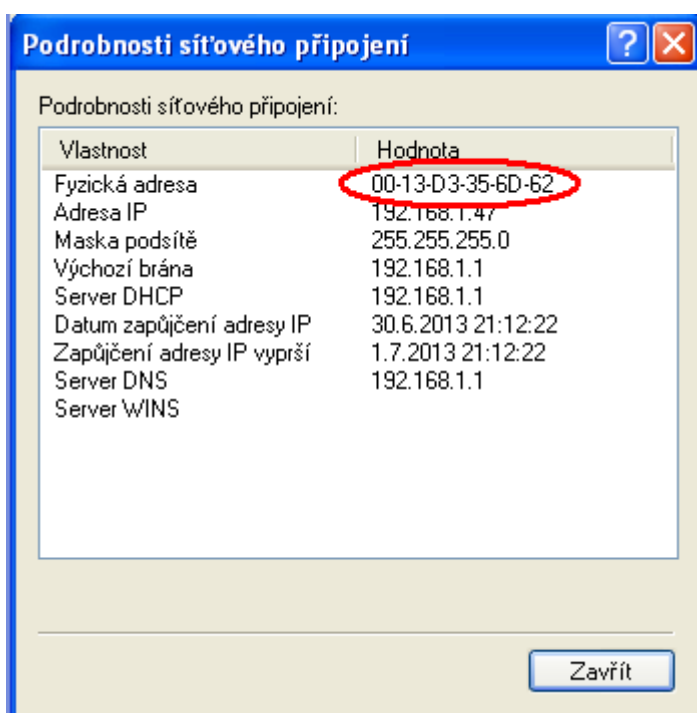
Obr. 13 WIFI síťová karta pro stolní PC [převzato a upraveno z 18]



Obr. 14 USB WIFI síťová karta [převzato a upraveno z 19]

2.6.4.2 MAC adresa síťové karty

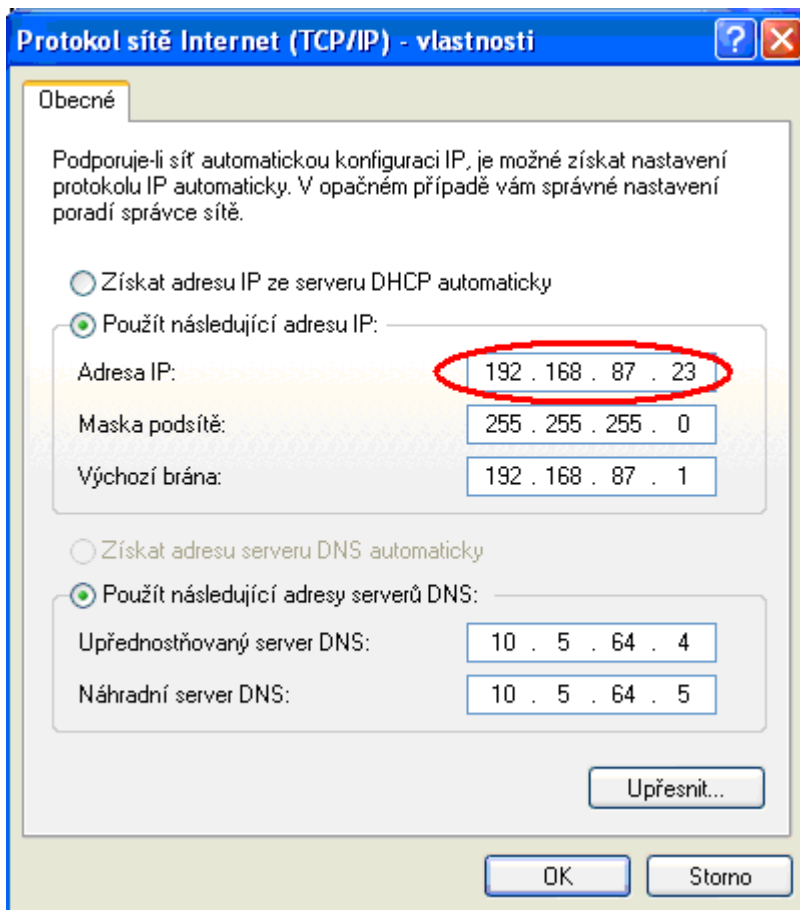
MAC adresa síťové karty slouží pro její jednoznačnou identifikaci v rámci počítačové sítě. Tuto adresu zapisuje do paměti na síťové kartě výrobce. Je zajištěno, že na světě se nevyrobí dvě karty se stejnými MAC adresami. Pro MAC adresu se používá číslo ve dvojkové soustavě, které je uloženo v paměti na desce síťové karty. MAC adresa převzatá z datového paketu se porovná s MAC adresou uloženou v paměti adaptéru a rozhodne se, zda přijatý datový paket je určen danému síťovému zařízení. Dnešní počítačové sítě používají MAC adresu o délce 48 bitů, která umožňuje adresovat až dva trilióny MAC adres. MAC adresa je rozdělena na dvě poloviny, kde první část má délku 24 bitů a obsahuje mezinárodně přidělený kód výrobce. Druhá část obsahuje identifikační číslo adaptéru, který mu přiděluje výrobce. Na obr. 15 můžeme vidět MAC adresu.



Obr. 15 Ukázka MAC adresy [autor]

2.6.4.3 IP adresa

IP adresa je jednoznačná adresa počítače nebo jiného síťového zařízení nejenom v rámci LAN sítě, ale i Internetu. Dnes se používá verze IPV4 což je 32 bitové číslo ve tvaru 4 bytů oddělených tečkami, které je zapisováno v desítkové soustavě. Tímto způsobem můžeme přidělit 4 miliardy síťových adres. Na obrázku 16 vidíme, jak vypadá IP adresa.

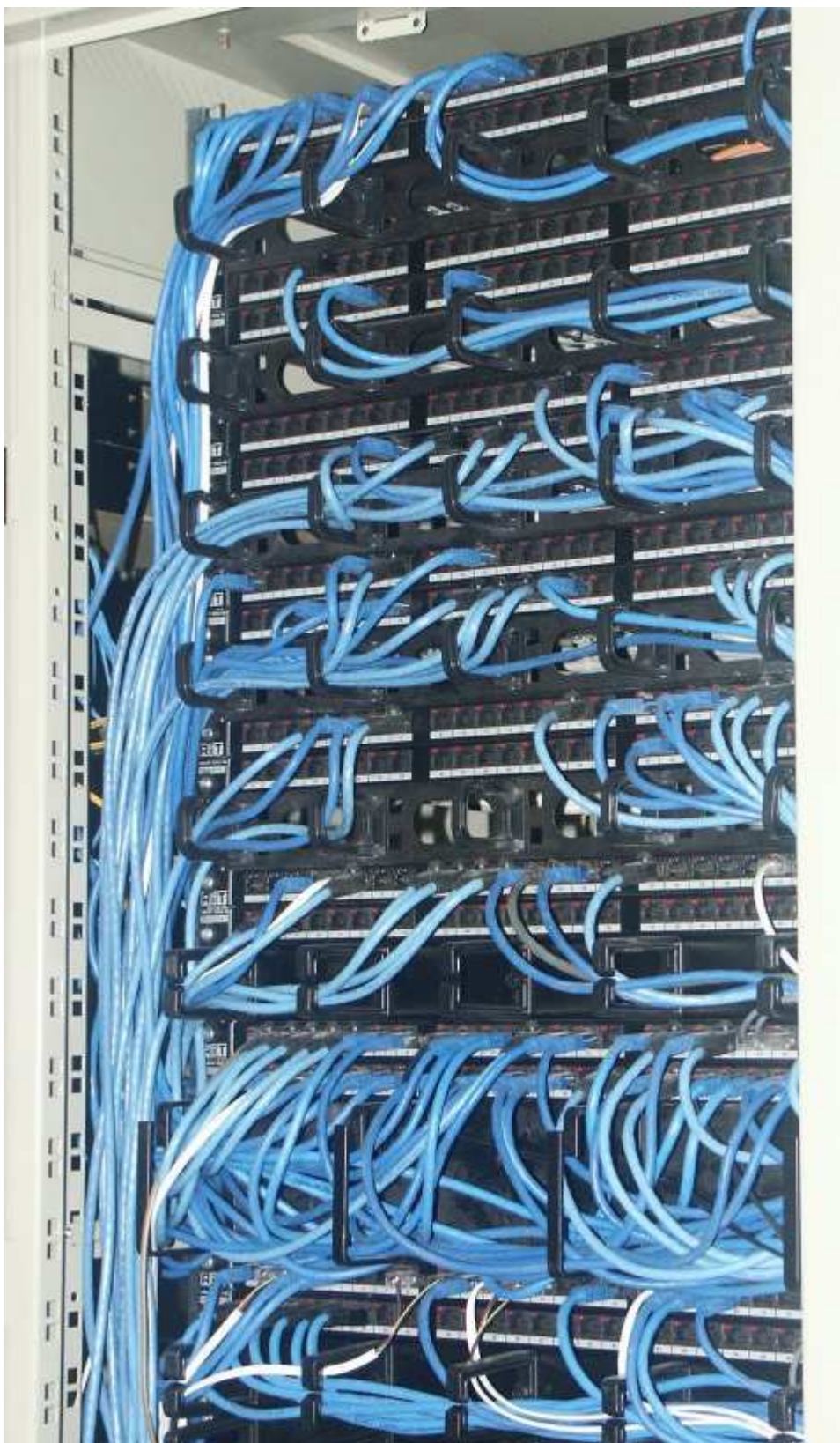


Obr. 16 Nastavení IP adresy [autor]

V budoucnosti bude rozsah IP adres vyčerpán a je již připravena verze IPV6, kde je již délka síťové adresy 128 bitů která umožňuje přidělit až 3.4×10^{38} unikátních síťových adres.

2.7 *Strukturovaná kabeláž*

V současné době jsou nové síťové rozvody budovány pomocí tzv. strukturované kabeláže. Je založena na principu dvoubodových spojů. Výhodou těchto spojů je, že pokud na nich dojde k závadě, možnost komunikace ztrácí většinou pouze jedno koncové zařízení, ostatní zařízení pracují dále. Jako přenosové médium se používá kroucená dvojlinka a optické kabely.



Obr. 17 Ukázka racku se strukturovanou kabeláží [převzato a upraveno z 20]

2.7.1 Požadavky na strukturovanou kabeláž

- Vysoká spolehlivost
- Dlouhá životnost kabelových rozvodů -
- Podpora standardních přenosových protokolů
- Univerzálnost - tzn. možnost integrace datových, hlasových, zabezpečovacích a automatizačních služeb
- Možnost rozšíření a zvyšování přenosové kapacity

2.7.2 Topologie strukturované kabeláže

Rozvody strukturované kabeláže jsou pouze pasivní rozvody. Její součástí nejsou koncové počítače, ani nejrůznější servery či aktivní síťové prvky typu switchů a routerů. Topologie systémů strukturované kabeláže je stromová. Na nejnižší úrovni se používají spoje z kroucené dvojlinky, které jsou omezené dosahem do 100 metrů. Tyto rozvody připojují koncové zásuvky do switchů. Ze switchů na nejnižší úrovni vedou další spoje pomocí optických vláken do propojovacích míst na vyšší úrovni, kde jsou připojeny do dalších switchů. Důležitým konstrukčním prvkem strukturované kabeláže jsou rozvodné skříně tzv. racky, v nichž jsou umístěny všechny spojovací prvky, propojovací kabely, switche, routery atd. Vše je univerzální, což nám umožňuje osadit jednotlivá propojovací místa různými aktivními prvky dle našich požadavků.

2.8 Aktivní prvky

Aktivními prvky v počítačové síti rozumíme zařízení, které aktivně působí na datové pakety přenášené po komunikačním médiu. Jedná se o switche, routery a WIFI routery.

2.8.1 Switch

Switch neboli přepínač je dnes základním stavebním kamenem LAN sítí. Zajišťuje komunikaci v počítačové síti spojením dvojice portů a těm poskytuje plnou přenosovou rychlost. Přepínač filtruje posílaná data a na základě MAC adresy zasílá datové pakety pouze danému příjemci. K tomu si vytváří tabulku MAC adres všech připojených zařízení v počítačové síti. Pro vytvoření a průběžnou aktualizaci této tabulky používá princip samoučení a to tak, že si tuto tabulku vytváří na základě realizovaných spojení.

Přepínače jsou aktivní prvky počítačové sítě, které zvyšují propustnost sítě a efektivně využívají dostupnou přenosovou kapacitu této sítě. Přepínače se liší v počtu portů, do kterých se připojují jednotlivé segmenty sítě.



Obr. 18 Ukázka 24 portového switchu [převzato a upraveno z 21]

2.8.2 Router

Router je jedním z aktivních prvků používaných nejenom v rozsáhlých WAN sítích, ale také v LAN sítích, kde slouží pro připojení do Internetu. Ukládá informace o topologii všech připojených počítačových sítích do tzv. routovací tabulky a na základě těchto informací zasílá datový paket nejvhodnější cestou na síťové zařízení v cílové počítačové síti. Směrování paketů tzv. routování zajišťuje pomocí filtrace paketů rozšířené o inteligentní směrování s využitím IP adres.



Obr. 19 Ukázka routeru [převzato a upraveno z 22]

2.8.3 WIFI router

WIFI router má obdobnou funkci jako klasický router, to znamená, že zajišťuje spojení WLAN sítě do jiných sítí např. Internetu. Spojuje v sobě několik zařízení od LAN routeru přes síťový switch až po Wireless LAN Access Point. LAN router zajišťuje spojení do Internetu pro zařízení, která jsou připojena k routeru kabelem, pomocí integrovaného switchu nebo bezdrátově k integrovanému Wireless LAN Access pointu.



Obr. 20 Wifi router [převzato a upraveno z 23]

2.8.4 Gateway

Switche a směrovače neumí pracovat s datovým obsahem paketů. Mohou propojovat jen takové systémy, které v datových paketech posílají data stejného typu. Pro spolupráci odlišných systémů je nutné rozumět přenášeným datům a provádět jejich konverzi. To zajišťují brány - Gateway, které jsou schopny rozumět datům od určité aplikace. Slouží k připojení počítačové sítě k jiné síti, k nějakému jinému prostředí. Brány jsou realizovány softwarově a jsou vždy orientované dle aplikace, např. brána pro přenos elektronické pošty, pro tisk atd.

2.8.5 Přenosové protokoly

Nejrozšířenějším protokolem je dnes protokol označovaný jako protokol TCP/IP. Je to vlastně rodina protokolů, kde každý protokol má svůj specifický úkol při zajištění přenosu informací mezi počítači v počítačových sítích.

Skládá se z těchto protokolů:

TCP (Transmission Control Protocol) – transportní protokol, který zajišťuje spojení

IP (Internet Protocol) – zajišťuje adresování v sítích TCP/IP

UDP (User Datagram Protocol) – transportní protokol, který zajišťuje služby bez spojení

ARP (Address Resolution Protocol) – transformuje IP adresy na hardwarové MAC adresy

RIP (Routing Information Protocol) – směrovací protokol, který používají routery pro směrování paketů v počítačových sítích

HTTP (Hypertext Transport Protocol) – definuje formát a přenos zpráv používaný webovými servery

FTP (File Transport Protocol) – zajišťuje přenos souborů po počítačové síti

SMTP (Simple Mail Transport Protocol) – zajišťuje přenos elektronické pošty v Internetu a IP sítích

Telnet – terminálový emulační protokol zajišťující spojení počítače se vzdálenými počítači

3 OCHRANA POČÍTAČOVÝCH SÍTÍ

3.1 Firewall

Firewall je jedním ze základních bezpečnostních prvků každé počítačové sítě. Zajišťuje její základní ochranu před útočníky. Je umístěn na hranici naší počítačové sítě, a pokud je správně nastaven, poskytuje naší počítačové síti bezpečnou ochranu. Kontroluje všechny datové pakety, které procházejí mezi naší počítačovou sítí a jinými sítěmi a pakety, které nevyhoví bezpečnostním pravidlům, které jsme na něm definovali, zablokuje. Používá metodu filtrace datových paketů, kdy na základě analýzy datového paketu rozhodne, zda bude paket propuštěn do lokální sítě. Firewall

samozřejmě nezaručí stoprocentní ochranu lokální počítačové sítě, ale sníží pravděpodobnost úspěšného útoku, který může ohrozit bezpečnost uložených dat.

3.2 Proxy server

Proxy server přijímá požadavky od počítačů z lokální počítačové sítě a předává je do externí veřejné sítě. Zpět přijímá odpovědi a předává je interním počítačům. Tím odděluje počítače z lokální počítačové sítě a skrývá je před útočníky z vnějších počítačových sítí. Proxy server umožňuje blokování nebezpečných URL a filtrování obsahu než ho předá klientským počítačům.

3.3 Šifrování

Šifrování je základní bezpečnostní prvek, který používáme pro ochranu dat proti ztrátě důvěrnosti informace. Šifrování je metoda, při které se data převádějí do formátu, který není pro nepovolanou osobu čitelný. Z původních dat se šifrováním stává nečitelná šifra, kterou můžeme přenášet od odesílatele přes veřejný přenosový kanál např. Internet k adresátovi. Adresát zašifrovaná data dešifruje, to znamená, že šifrovaná data převede do původní podoby. Šifrování a dešifrování je standardizováno a popisuje jej šifrovací algoritmus. Šifrovací algoritmy využívají pro šifrování šifrovací klíče, což jsou bitové sekvence o určité délce např. 512 bitů, 1024 bitů nebo 2048bitů i více. Čím je délka šifrovacího klíče větší, tím je odolnější proti rozluštění šifry. To jak se používají šifrovací klíče určuje typ šifrovacího algoritmu.

3.3.1 Symetrické šifrování

Jestliže se používá stejný klíč pro šifrování i dešifrování, pak šifrovací algoritmus patří mezi symetrické šifrovací algoritmy. Společný klíč se nazývá tajný klíč a musí být zajištěno jeho utajení před nepovolanými osobami. Nejpoužívanější standardy pro symetrické šifrování jsou:

- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- RC2 a RC4 (Rivest Cipher).

3.3.2 Asymetrické šifrování

Jestliže se klíč používaný pro šifrování liší od klíče používaného pro dešifrování, jde o asymetrický šifrovací algoritmus. Tajným soukromým klíčem se data šifrují a pouze veřejným klíčem, který je poskytnut příjemci se zašifrovaná data dešifrují. Přenášená data nemají chráněnou důvěrnost, neboť veřejný klíč může používat kdokoliv, avšak u dat je zajištěna autenticita, neboť v tomto případě se text určený k přenosu šifruje veřejným klíčem adresáta zprávy, tj. příjemce dat. Tato data je možno dešifrovat pouze soukromým klíčem příjemce, který je jeho majitelem a uchovává jej v tajnosti. Autenticita dat však není prokazatelná, neboť data mohou pocházet od jiného odesilatele, než je deklarováno. Pro vytvoření podvržené šifry je dostatečná znalost veřejného klíče příjemce dat.

Nejpoužívanější standardy pro asymetrické šifrování jsou:

- RSA (Rivest Shamir Adleman – jména tvůrců algoritmu)
- DSS (Digital Signature Standard)
- EC (Eliptic Curve).

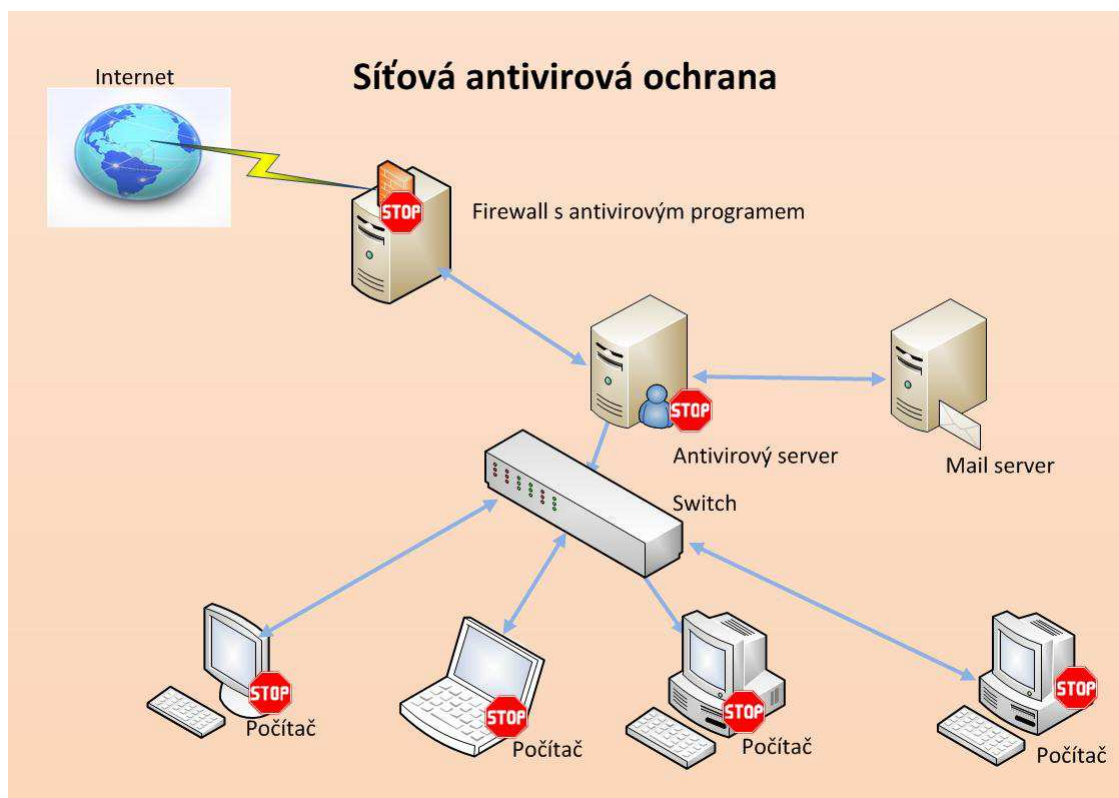
3.4 VPN – Virtual private network

Propojování sítí LAN a poskytování připojení vzdáleným počítačům přes Internet je nutné zabezpečit proti jakýmkoli útokům. Můžeme použít virtuální privátní síť VPN. Je to jednoduchý a poměrně levný způsob jak propojit privátní LAN přes Internet se vzdálenými LAN nebo se vzdálenými klientskými počítači. VPN propojí přes internet jednu privátní LAN s jinou pomocí šifrování IP paketů. Zašifrované pakety nemohou číst jiné počítače ve veřejné síti. Můžeme do nich uložit jakoukoli komunikaci, která probíhá v běžné LAN síti. Jako např. přístup k souborům a databázím, přístup k elektronické poště atd.

3.5 Antivirová ochrana

Viry se dnes mohou do počítače dostat různými cestami např. z příloh e-mailových zpráv, souborů na USB discích nebo ze souborů stažených z Internetu. Nemůžeme se proto spoléhat pouze na jednu úroveň antivirové ochrany, ale rozprostřít ji minimálně ve dvou nebo ve třech úrovních. Kromě základní úrovně představované antivirovým

programem na pracovní stanici současně použijeme antivirovou ochranu internetových vstupních bran a k tomu ještě např. ochranu na poštovním a souborovém serveru. Pokud by tedy ochrana na některé úrovni selhala, stále ještě zbývají další úrovně, které dokáží škodlivý kód odhalit a také odstranit. Princip popisovaného řešení můžete vidět na obrázku.



Obr. 21 Ukázka síťové antivirové ochrany [autor]

4 MONITOROVÁNÍ POČÍTAČOVÝCH SÍTÍ

4.1 *Monitoring sítě*

V současnosti, kdy svět je doslova protkán propojenými počítačovými sítěmi, na kterých závisí fungování naší společnosti, je nutné zajistit co nejvyšší dostupnost služeb, které tyto sítě poskytují svým uživatelům. Jakákoli nedostupnost těchto sítí má veliký vliv na její uživatele a může znamenat obrovské finanční ztráty. Z tohoto důvodu je nutné monitorovat stav zařízení těchto sítí a v co možná nejkratší době se dozvědět o problému v síti tak, abychom mohli služby, které počítačová síť poskytuje rychle obnovit. Monitoring počítačové sítě můžeme rozdělit do dvou okruhů:

- Monitoring dostupnosti zařízení a provozovaných služeb
- Monitoring aktuálních dat o určitém systému a jejich historie

Pravděpodobně neexistuje monitorovací nástroj, který by postihl všechny oblasti, které chceme monitorovat. Proto využíváme více ať již komerčních nebo nekomerčních produktů, které nám umožní sledovat všechny potřebné oblasti. Zasílané kritické události z jednotlivých monitorovacích nástrojů integrujeme do centrální monitorovací konzole.

4.2 Cíle monitoringu

Hlavním cílem monitoringu je předcházet nedostupnosti služeb poskytovaných prostřednictvím počítačových sítí a v případě že k němu dojde, zajistit v nejkratší možné době jejich opětovné poskytování. K dalším cílům patří sledování chyb na komunikačních trasách, sledování parametrů zařízení v síti, sledování dostupnosti aplikací a doby reakce na požadavky ze strany uživatelů. Na základě údajů, které monitoringem získáme, můžeme plánovat další rozvoj naší počítačové sítě.

4.3 Co monitorujeme

V počítačové síti monitorujeme tyto oblasti:

- **Dostupnost serverů a služeb**
 - dostupnost serverů
 - dostupnost služeb
 - dostupnost aplikací
 - události na serverech
 - vytížení zdrojů serveru – procesor, paměť, diskový prostor
- **Dostupnost aktivních síťových prvků**
 - dostupnost switchů a routerů
 - informace o stavech portů switchů
- **Síťovou komunikaci**
 - měření přenosu dat

- vyhodnocení statistiky síťového provozu
- zatížení komunikačních linek
- **Bezpečnost sítě**
 - informace o narušení bezpečnosti

4.4 Principy monitoringu

Monitoringem nazýváme periodické kontroly jednotlivých zařízení v počítačové síti. V případě zjištění problému se automaticky generuje výstražná událost s popisem problému, který se vyskytl na daném zařízení. Pokud máme centrální dohledové pracoviště, můžeme událost odesílat do centrální dohledové konzole nebo správci příslušného zařízení např. pomocí emailové nebo SMS zprávy. Tím zajistíme rychlé informování příslušných pracovníků o výskytu problému v počítačové síti a její rychlé odstranění. Z hlediska způsobu získávání informací rozlišujeme následující druhy monitoringu:

- Monitoring využívající agenta
- Monitoring bez agenta

4.4.1 Monitoring využívající agenta

U tohoto typu monitoringu je nutné na monitorované servery nainstalovat příslušného agenta dle typu provozovaného operačního systému, který bude sbírat data a odesílat je na monitorovací server, kde se zpracují a uloží do databáze. Toto řešení v sobě skrývá potenciální problémy s během agenta, ale poskytuje více informací o monitorovaném zařízení než řešení bezagentové.

4.4.2 Monitoring bez agenta

Tento způsob monitoringu nevyžaduje instalaci agenta na monitorované zařízení. Zde se provádí monitoring vzdáleně tak, že se využívají standardní protokoly, které běží na monitorovaných zařízeních. Jde např. o protokoly WMI, SSH, SNMP, ICMP, TCP, HTTP, atd.

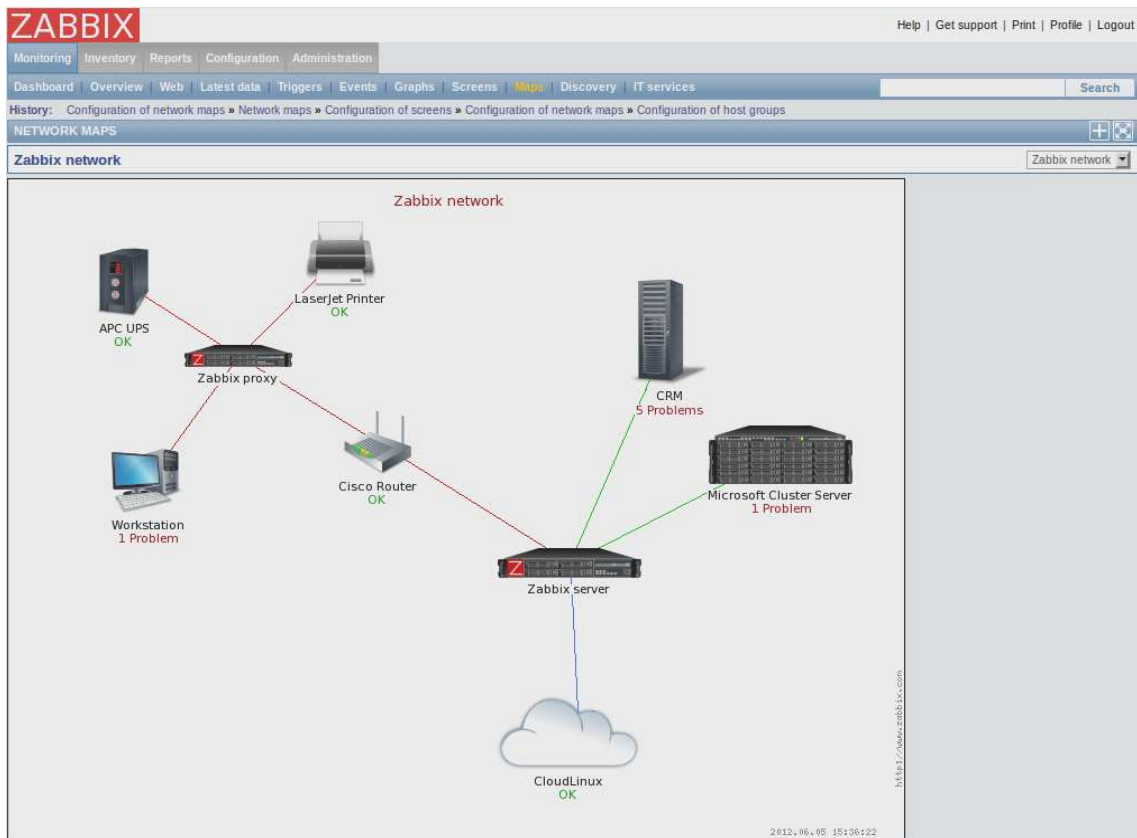
4.5 *Reporting monitoringu*

Nedílnou součástí monitoringu je též vyhodnocení a reportování výsledků naměřených hodnot a událostí. Pro informaci o stavu počítačové sítě potřebujeme přehledné a vypovídající reporty, které nám umožní identifikovat problémy v síti a rychle na ně reagovat. Reporting je též důležitý pro plánování rozvoje počítačové sítě.

Z monitoringu získáváme dva základní typy dat:

- **Události** – stavové hodnoty, získáváme je z jednotlivých zařízení např. z log souborů
- **Hodnoty** – číselné hodnoty, které ukazují aktuální stav zařízení, ze kterých můžeme reportovat změnu naměřených hodnot v čase

Pro každý z těchto typů dat používáme jiný typ prezentace. Události např. aktuální stavy portů serveru potřebujeme sledovat v reálném čase a zobrazíme je v tabulce. Hodnoty např. vytížení procesoru prezentujeme v určitém časovém úseku a zobrazujeme nejčastěji pomocí přehledného grafu. Celkový stav počítačové sítě zobrazíme pomocí grafické prezentace v centrální přehledové obrazovce, kde vidíme schématický pohled na celou síť nebo její část. Jestliže se objeví problém, tak se daný prvek zvýrazní a po rozkliknutí o něm dostaneme detailní informace.

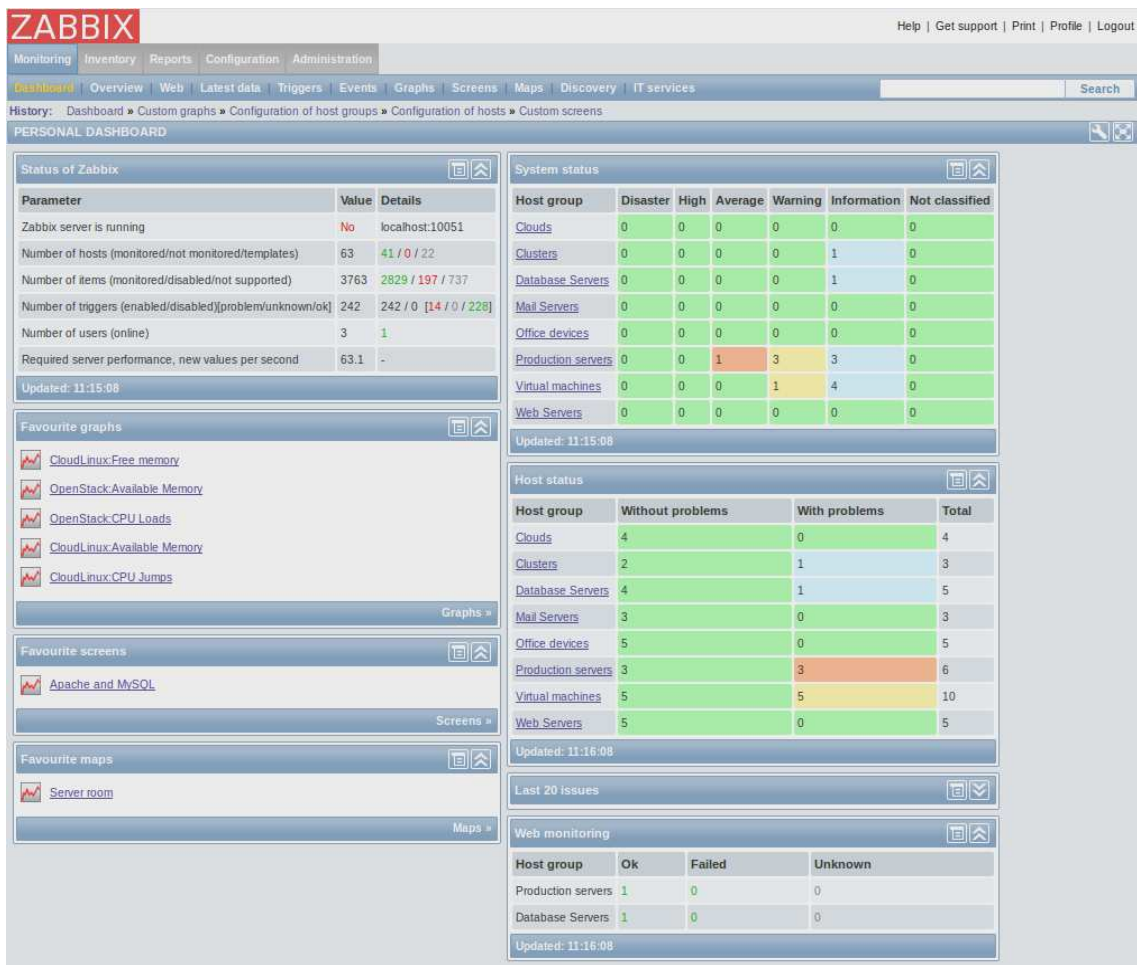


Obr. 22 Centrální přehledová obrazovka [převzato a upraveno z 13]

4.6 MONITOROVACÍ SOFTWARE

4.6.1 ZABBIX

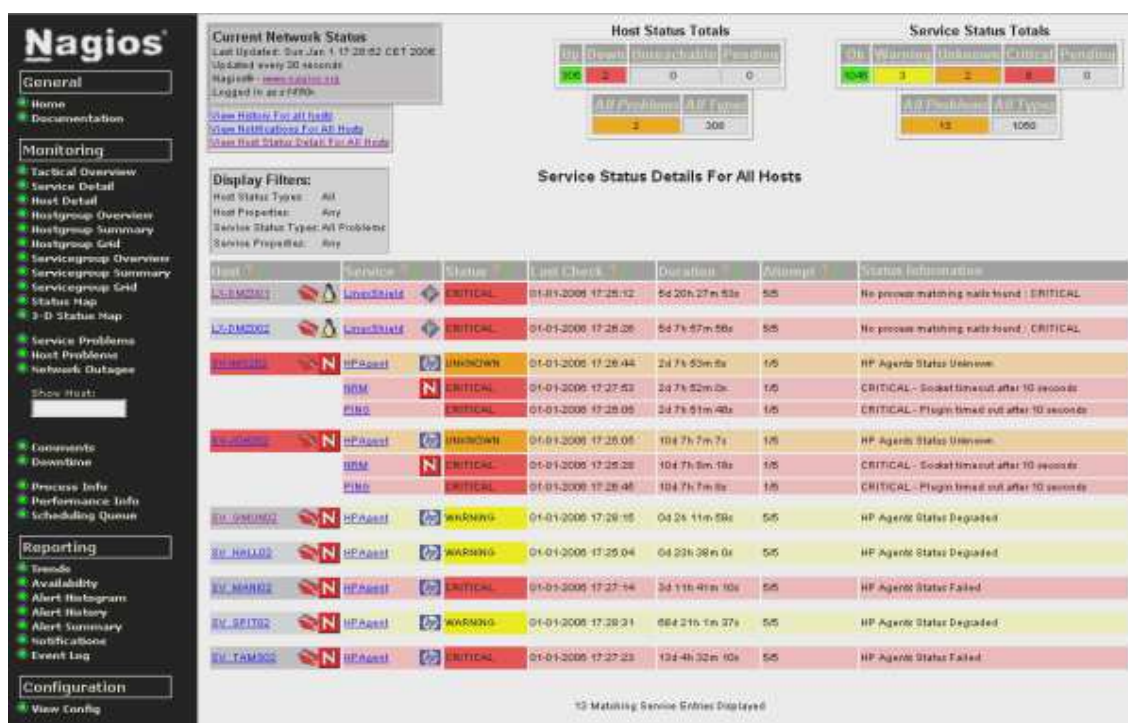
Tento open source software monitoruje zařízení v počítačové síti jako např. servery, uživatelské počítače, switche, routery, tiskárny, UPS atd. Umožňuje též monitorovat paměť, procesor, diskový prostor a také běžící služby na těchto zařízeních. Je schopen monitorovat přes 100 000 zařízení v počítačové síti. Je přístupný z webového rozhraní, které slouží také k administraci, správě a vyhodnocení naměřených dat.



Obr. 23 Přehledová obrazovka monitorovacího systému Zabbix [převzato a upraveno z 24]

4.6.2 NAGIOS

Další z open source nástrojů, který umí monitorovat hardware počítačových sítí a služby které poskytuje. Jestliže zjistí problém, upozorní administrátora.



Obr. 24 Přehledová obrazovka monitorovacího systému Nagios [převzato a upraveno z 25]

5 VÝUKOVÝ MATERIÁL

5.1 Zásady pro tvorbu výukových materiálů

Názornost – přispívá k zapamatování vědomostí, zařazení grafů, tabulek, flashových animací

Přehlednost – výukový materiál musí být přehledný, je nutné zvolit správnou velikost písma, grafika nesmí odvádět pozornost od obsahu

Přiměřenost – není nutné všechny informace umístit do výukového materiálu

Aktivita – umožnění žákům aktivně se podílet na průběhu vyučovací hodiny

5.2 Interaktivní výuka

Interaktivní výuka je moderní metoda výuky, která ji činí zábavnou a začleňuje žáky do procesu výuky. Žáci se podílejí na výuce a tím ji spoluvytvářejí. Výuka není tak stereotypní jako klasická, je názornější a poutavější. Umožňuje rozšířit znalosti

o vyučované látce o další zdroje informací dostupné na Internetu. Žáci si uvědomí, že není možné získané vědomosti separovat, ale naopak rozvíjet je o znalosti z jiných vyučovaných předmětů, které s daným tématem souvisí.

5.3 Co to je interaktivní prezentace

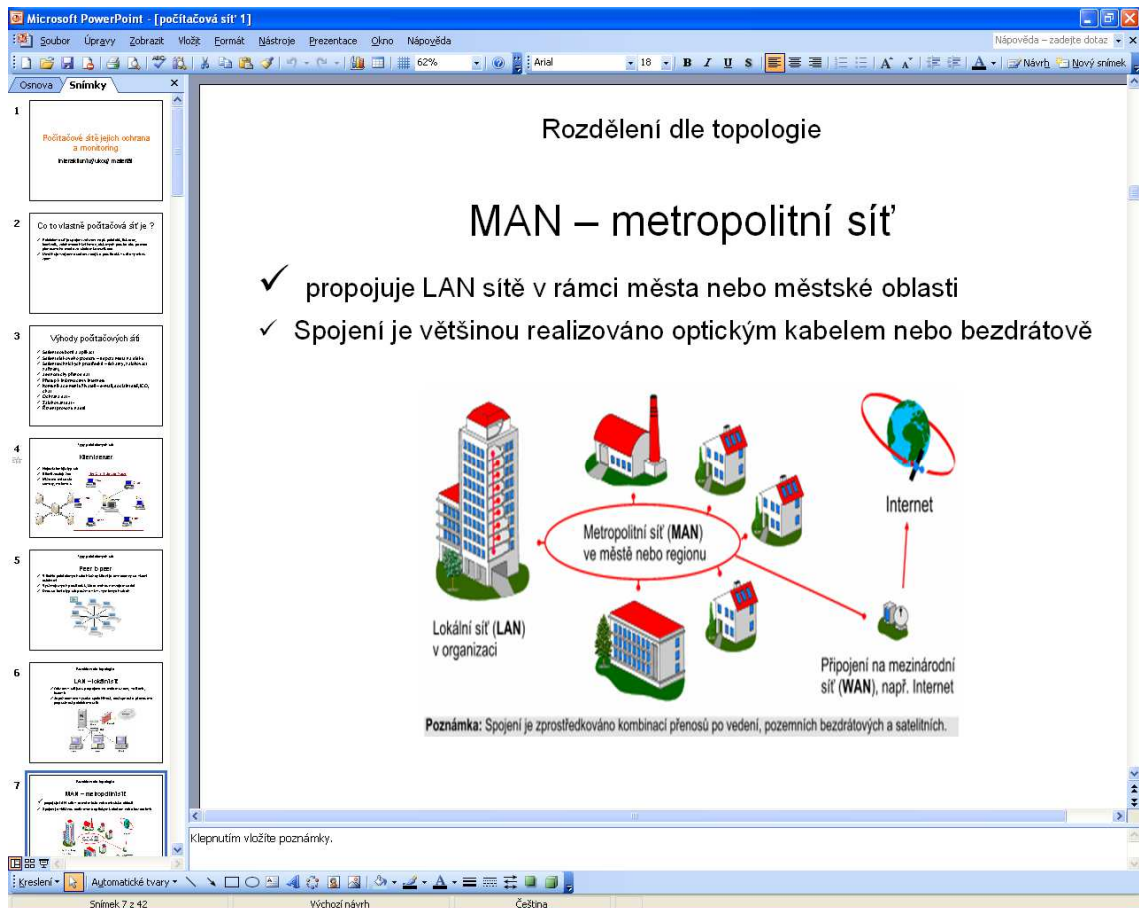
Pojem interaktivní prezentace znamená, že uživatel může danou prezentaci aktivně ovlivňovat, to znamená, že může spouštět například vložené applety a animace, hypertextové odkazy na obsah v Internetu nebo ukázky filmů apod. V poslední době ale tento výraz nabývá ještě dalšího významu. Interaktivní prezentace by měla být živá a zábavná. Vytvořit takovou prezentaci není vůbec jednoduché. Je nutné mít nejen zkušenosti s výukou, ale také prezentační a komunikační zkušenosti. V neposlední řadě je nutné ovládat některý druh prezentačního software, který nám umožní takovou interaktivní prezentaci vytvořit.

5.4 Prezentační software

Pro tvorbu interaktivního výukového materiálu je nutné vybrat vhodný software, ve kterém bude vytvořen. K dispozici je velké množství různých aplikací od placených až po free aplikace. Většina z nich prezentované informace rozdělují na snímky, které poté promítne posluchačům a prezentátor k nim přidá vlastní komentář. Snímky jsou obohaceny o videa, animace, hypertextové odkazy, zvuky atd. Prezentovat informace můžeme ale i jinými způsoby, ať už jsou to prezentace prostřednictvím videonávodů, flashových animací a také myšlenkových map. Uvádím zde přehled aplikací, které jsou neznámější a nejvíce používané běžnými uživateli.

5.4.1 MS PowerPoint

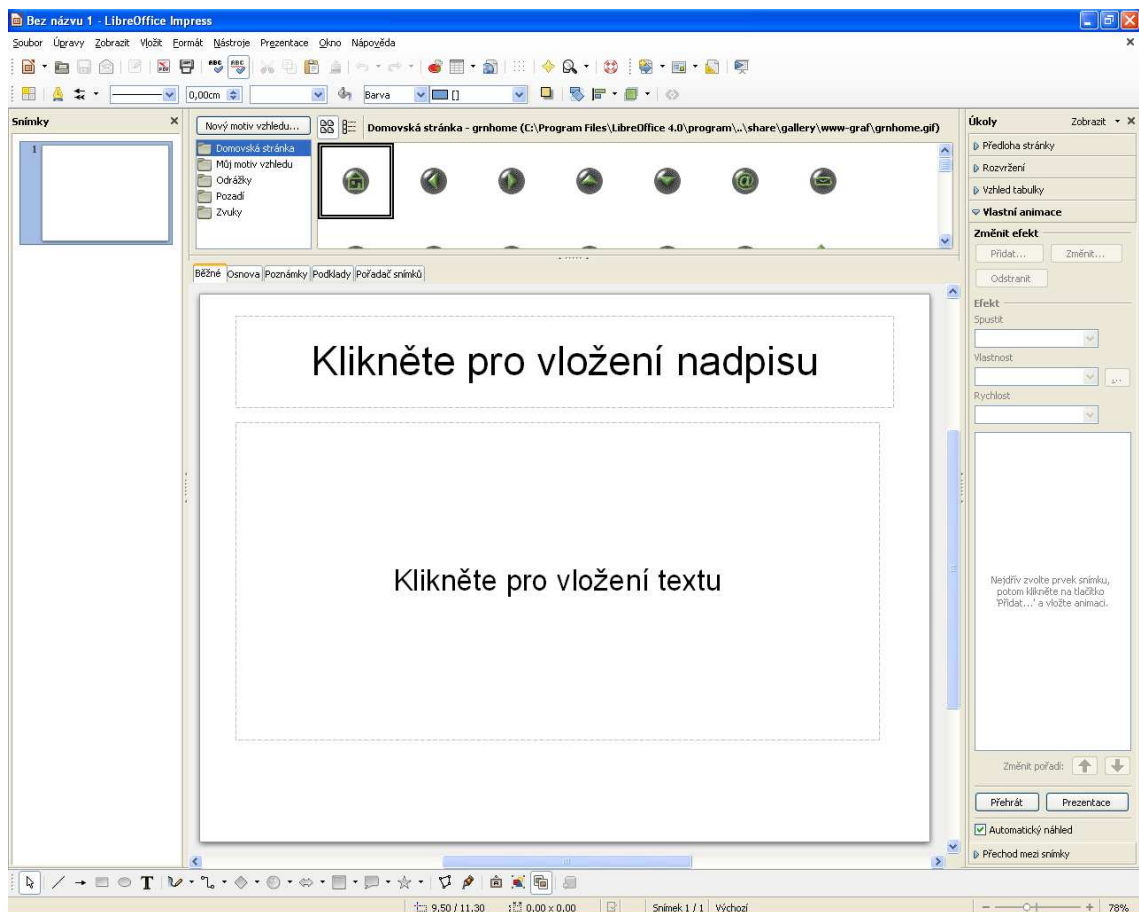
MS PowerPoint je součástí sady MS Office pro tvorbu grafických prezentací. Je to neznámější prezentační software uživatelů operačního systému MS Windows. Používá klasické prezentace založené na snímcích. Umožňuje tvorbu interaktivních prezentací.



Obr. 25 Ukázka pracovního rozhraní aplikace MS PowerPoint [autor]

5.4.2 Impress

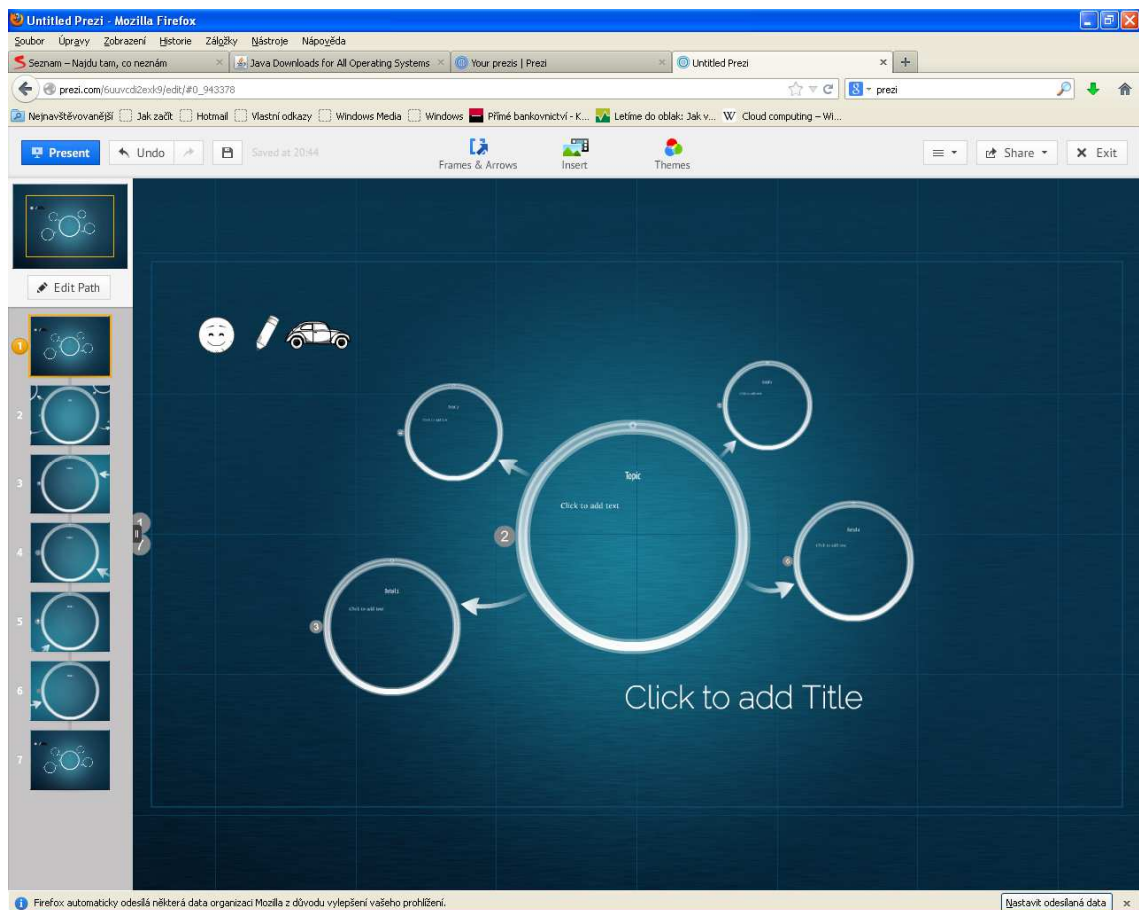
Impress je součástí free sady OpenOffice. Umožňuje vytvářet prezentace, ve kterých se vyskytují animace, obrázky, zvuky, grafika a text.



Obr. 26 Ukázka pracovního rozhraní aplikace Impress [autor]

5.4.3 Prezi

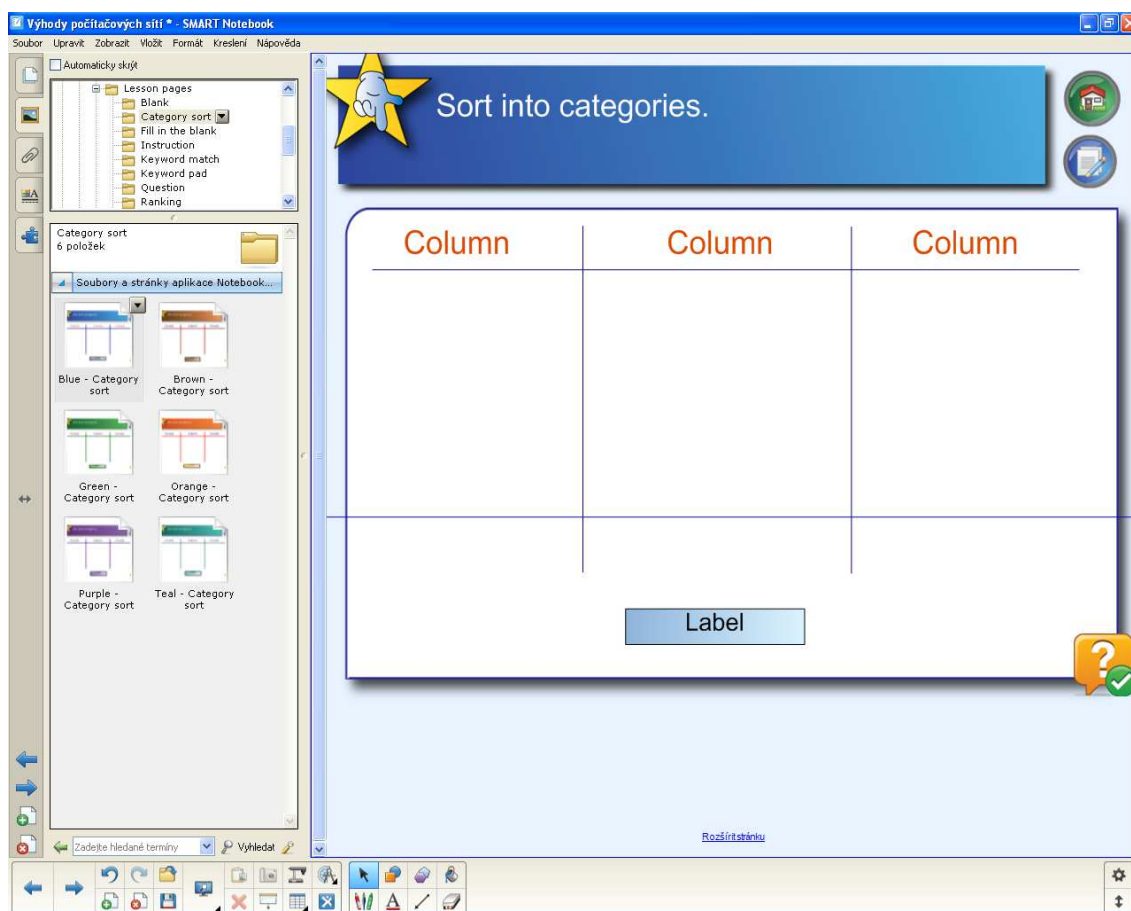
Klasický přístup používá rozdělení prezentace po snímcích. Tento software na to jde jinak. Používá zaostřování tzv. zooming na obsah. Díky tomu vytváří velmi atraktivní prezentace, které posluchače zaujmou.



Obr. 27 Ukázka pracovního rozhraní aplikace Prezi [autor]

5.4.4 Smart Notebook

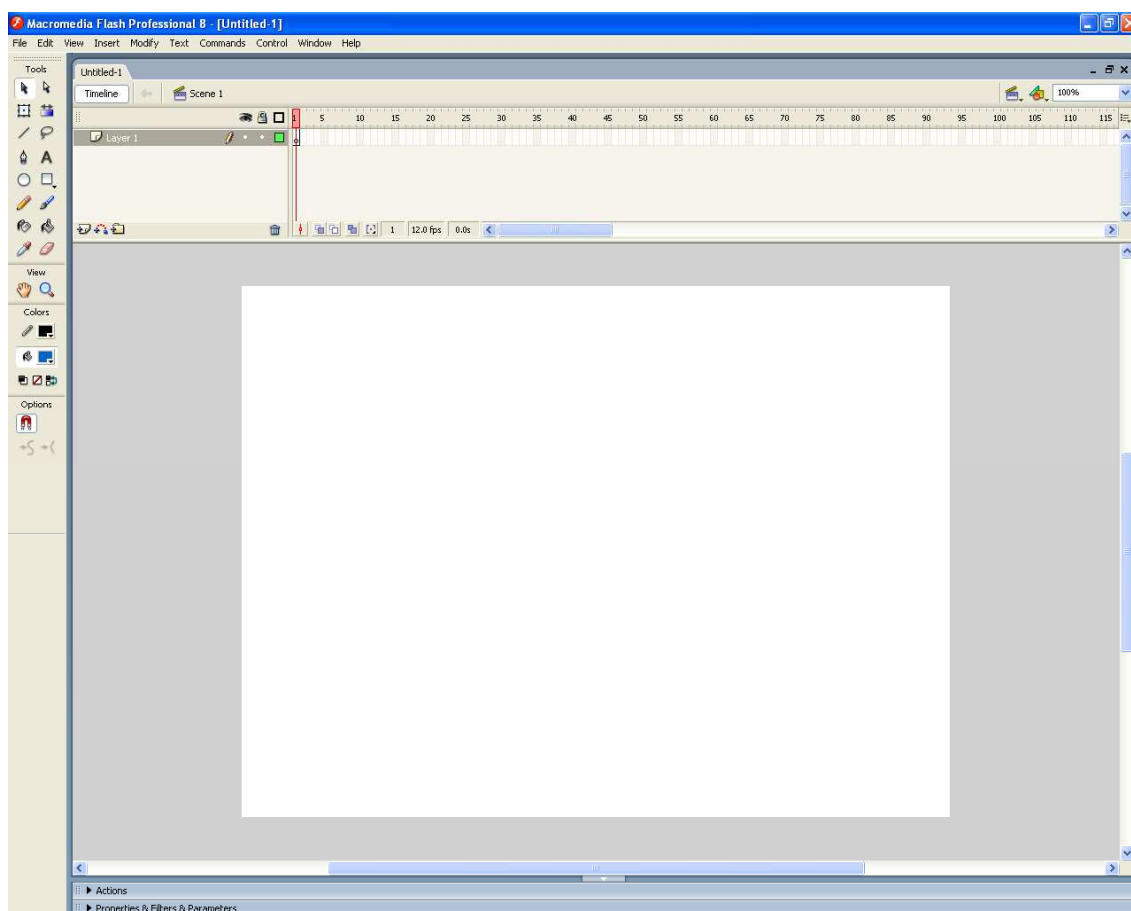
Software pro tvorbu prezentací pro interaktivní tabule. Obsahuje množství předdefinovaných šablon pro tvorbu výukových materiálů.



Obr. 28 Ukázka pracovního rozhraní aplikace Smart Notebook [autor]

5.4.5 Macromedia Flash 8

Tento software umožňuje vytvářet animované flashové prezentace.



Obr. 29 Ukázka pracovního rozhraní aplikace Macromedia Flash 8 [autor]

5.5 Tvorba interaktivního výukového materiálu

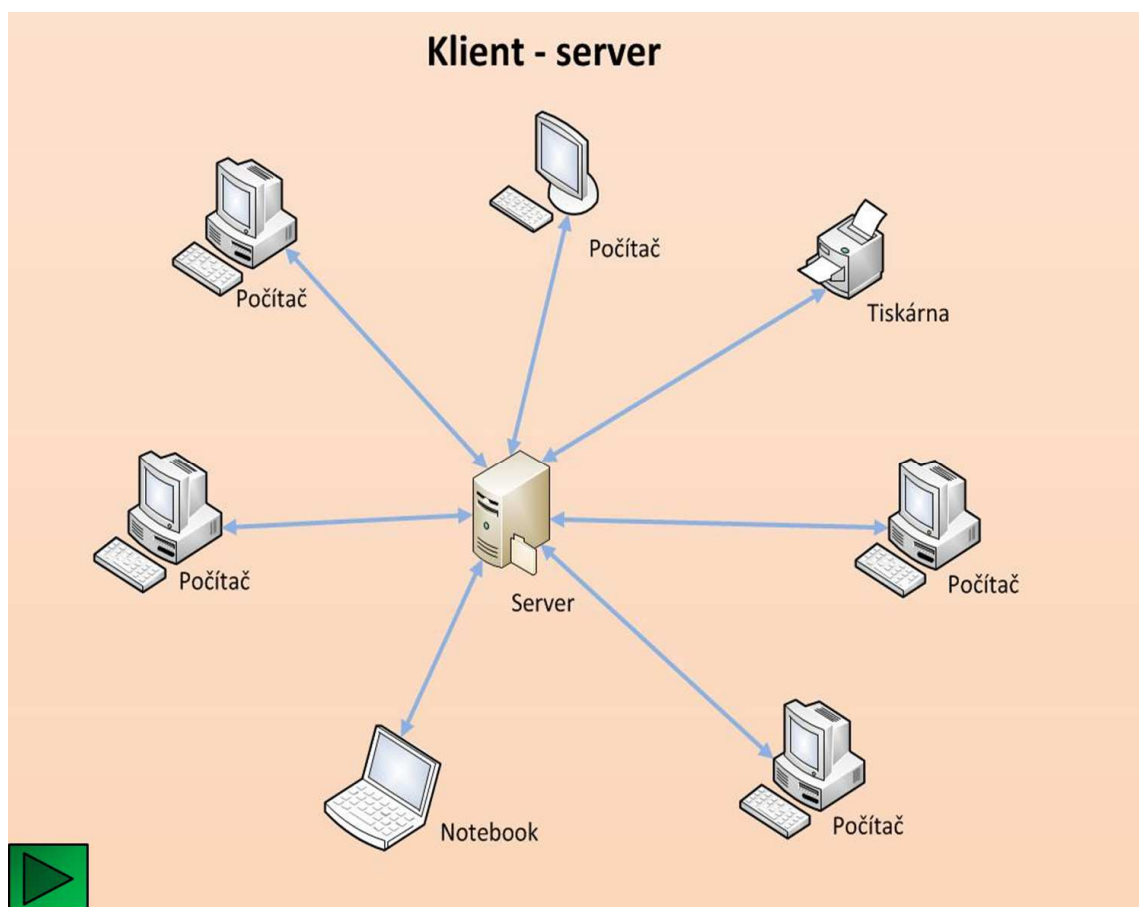
5.5.1 Výběr vhodného software

Výběr jsem prováděl tak, že jsem si nainstaloval jednotlivé aplikace a zkoušel jsem vytvořit krátkou interaktivní prezentaci s použitím všech prvků, které budu používat ve svém interaktivním výukovém materiálu. Hodnotil jsem jak prezentační stránku tak grafickou a také jednoduchost ovládání a snadnost vytvoření interaktivní prezentace. Nakonec jsem si k tvorbě interaktivní výukové prezentace vybral nástroj MS PowerPoint. Rozhodl jsem se pro tento nástroj z toho důvodu, že je schopen vytvořit kvalitní interaktivní prezentace, má jednoduché a intuitivní ovládání a s výslednou prezentací lze pracovat též ve spolupráci s interaktivní tabulí.

5.5.2 Interaktivní výukový materiál - scénáře

5.5.2.1 Komunikace Klient - server

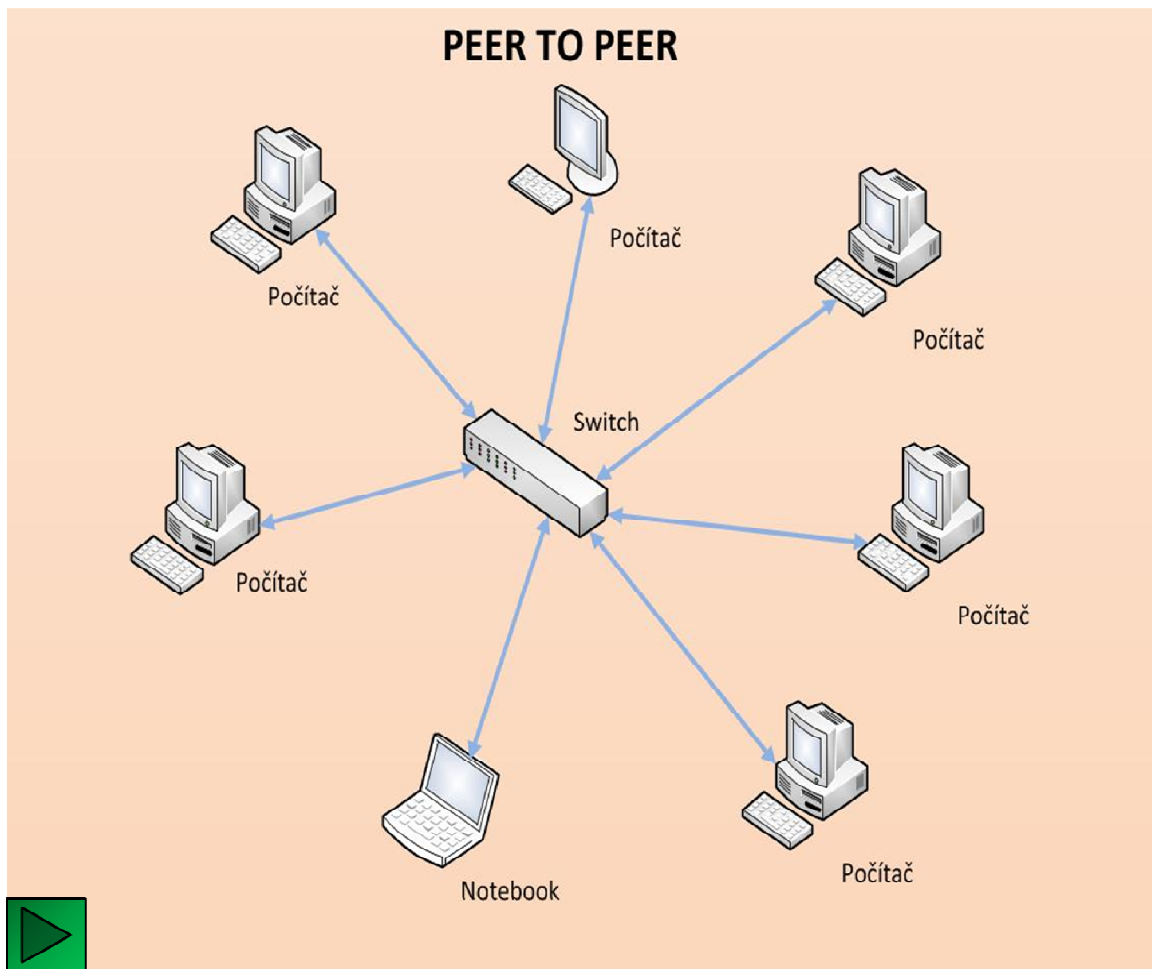
V této interaktivní prezentaci předvádím žákům princip komunikace v počítačové síti typu klient - server. Po kliknutí na spouštěcí tlačítko začíná komunikace a paket s požadavkem na data ze serveru se odesílá z klientského počítače na server. Server požadavek zpracuje a odešle datový paket s daty zpět na klientský počítač.



Obr. 30 Ukázka komunikace v síti klient - server [autor]

5.5.2.2 Komunikace peer to peer

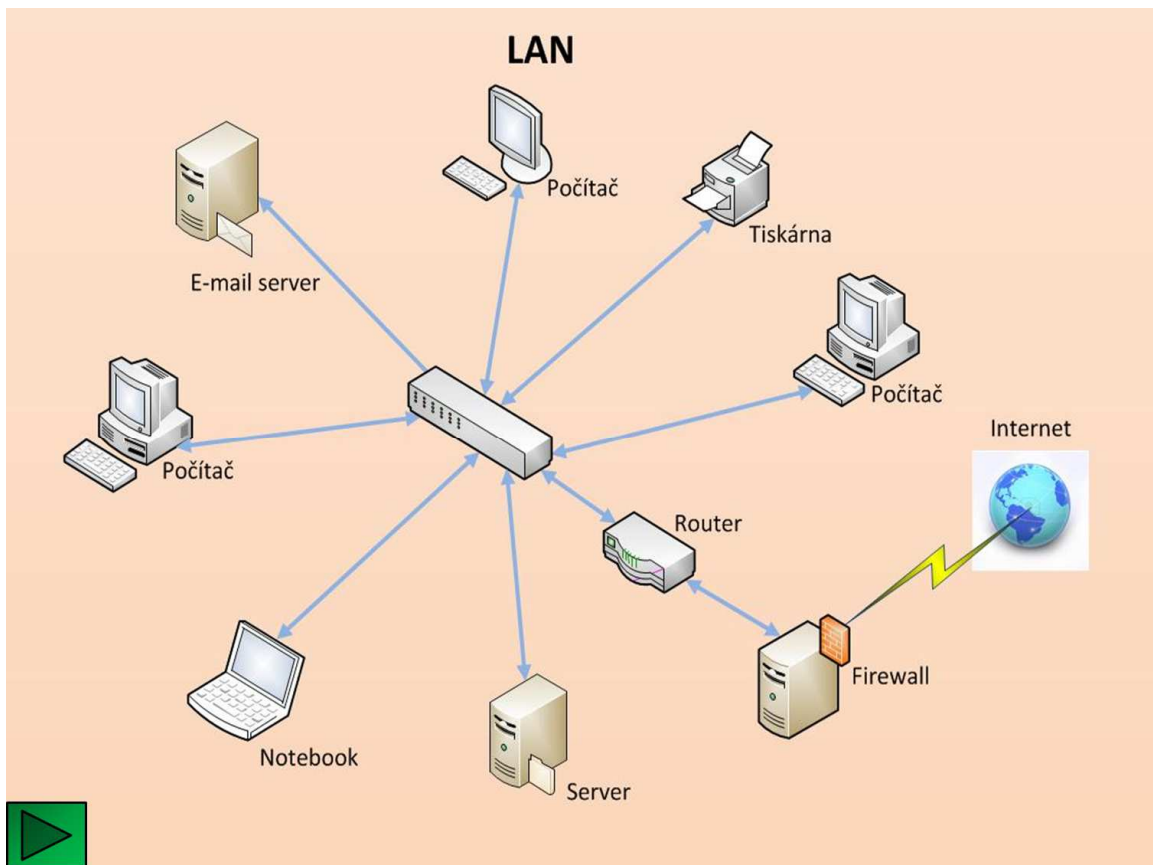
V této interaktivní prezentaci předvádím žákům princip komunikace v počítačové síti typu peer to peer. Po kliknutí na spouštěcí tlačítko začíná komunikace a datový paket s požadavkem na data z počítače se odesílá na jiný počítač v síti. Počítač požadavek zpracuje a datový paket s daty se vrací zpět na počítač, který požadavek vznesl.



Obr. 31 Ukázka komunikace v síti peer to peer [autor]

5.5.2.3 Komunikace v LAN síti

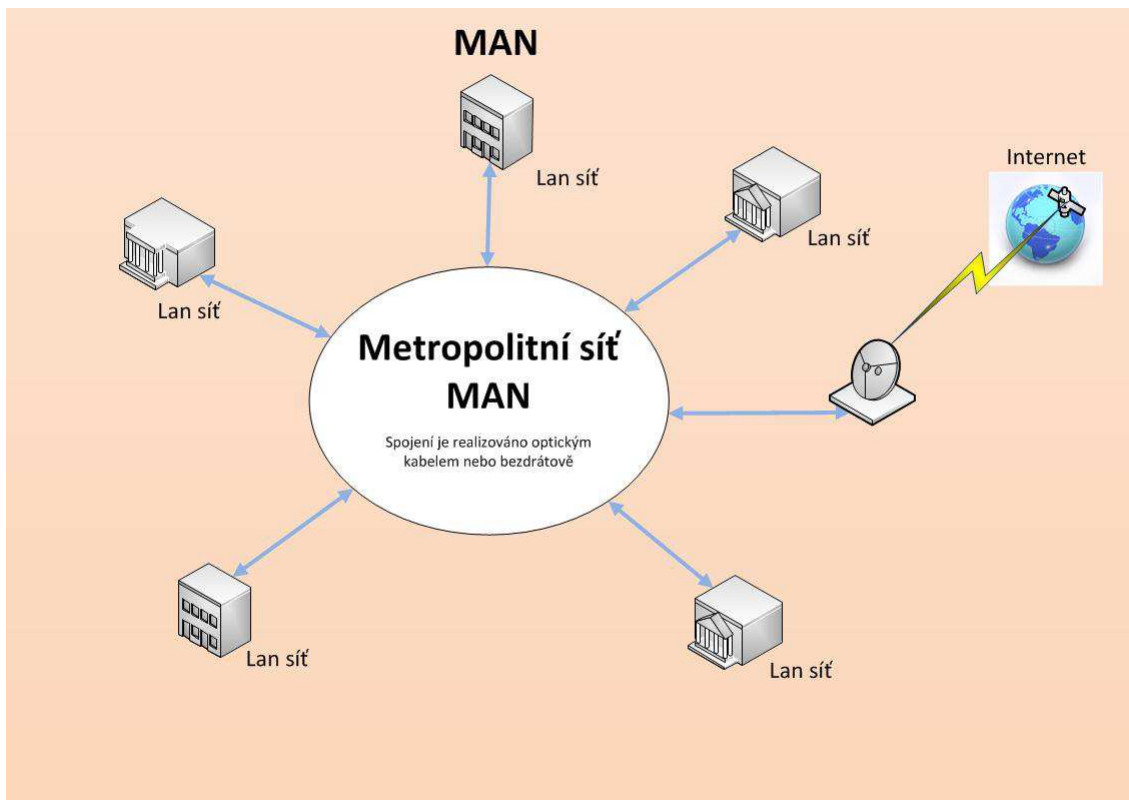
V této interaktivní prezentaci předvádím žákům princip komunikace v počítačové síti LAN. Datový paket je poslán příjemci v LAN síti.



Obr. 32 Ukázka komunikace v síti LAN [autor]

5.5.2.4 Komunikace v MAN síti

V této interaktivní prezentaci předvádím žákům princip komunikace v počítačové síti MAN. Datový paket je poslán příjemci v jiné budově začleněné v MAN síti.



Obr. 33 Ukázka komunikace v síti MAN [autor]

5.5.2.5 Komunikace ve WAN síti

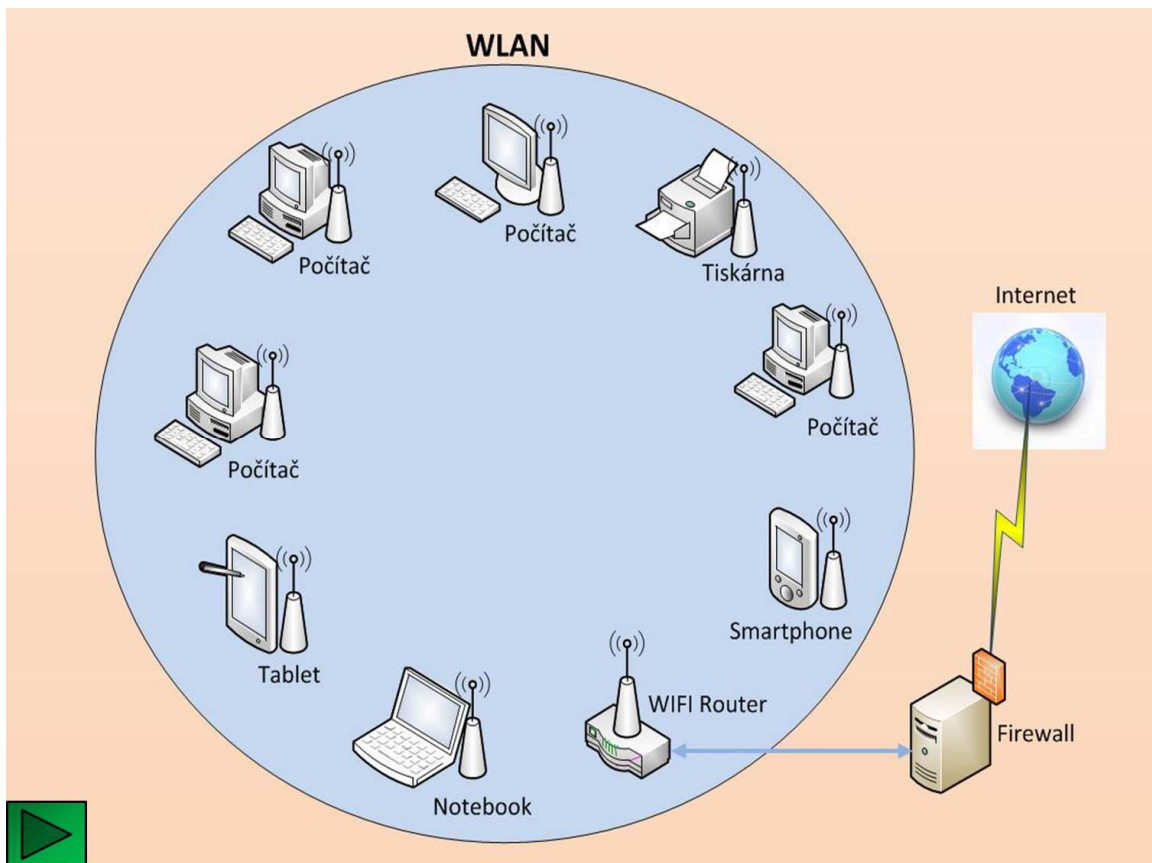
V této interaktivní prezentaci předvádím žákům princip komunikace v počítačové síti WAN. Datový paket je poslán příjemci na jiném kontinentě, který je začleněn ve WAN síti.



Obr. 34 Ukázka komunikace v síti WAN [autor]

5.5.2.6 Komunikace v WLAN síti

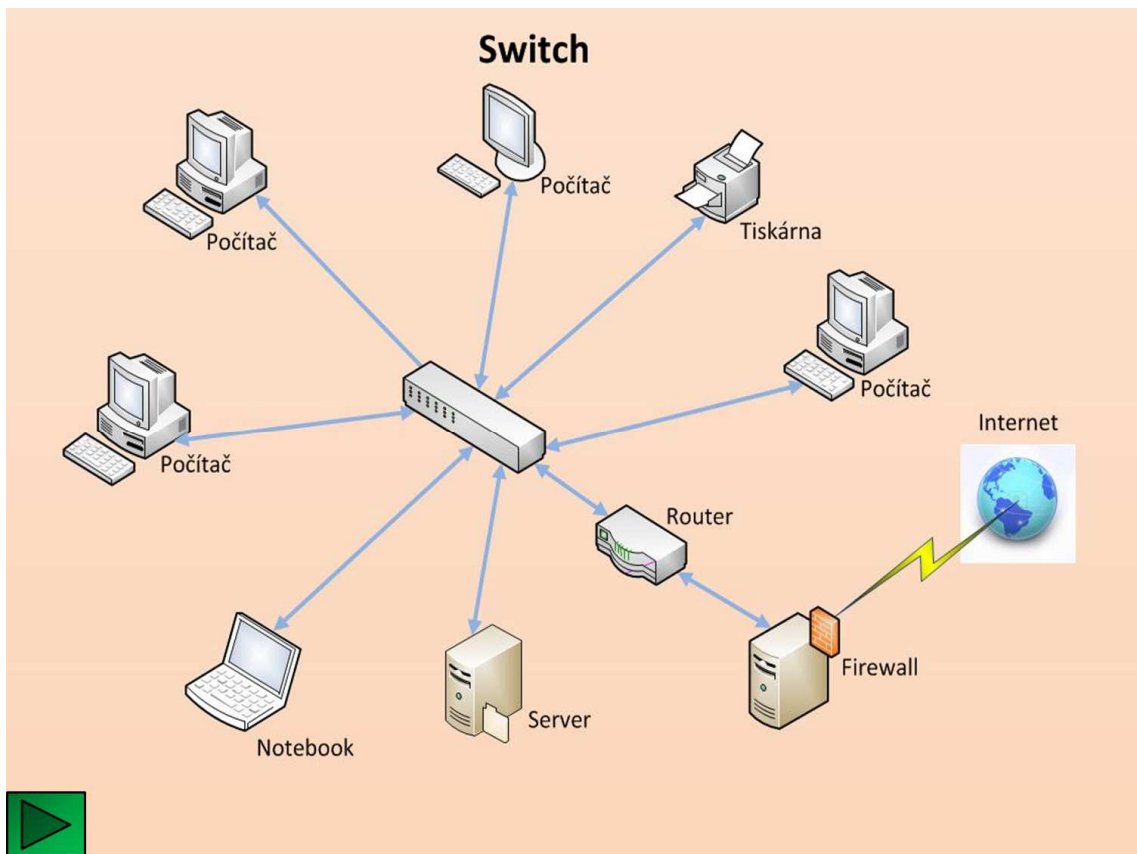
V této interaktivní prezentaci předvádím žákům princip komunikace v počítačové síti WLAN. Datový paket je převeden na radiový signál a ten je odvyšlán cílovému počítači. Na cílovém počítači je radiový signál převeden zpět na data.



Obr. 35 Ukázka komunikace v síti WLAN [autor]

5.5.2.7 Switch – přepínání komunikační cesty

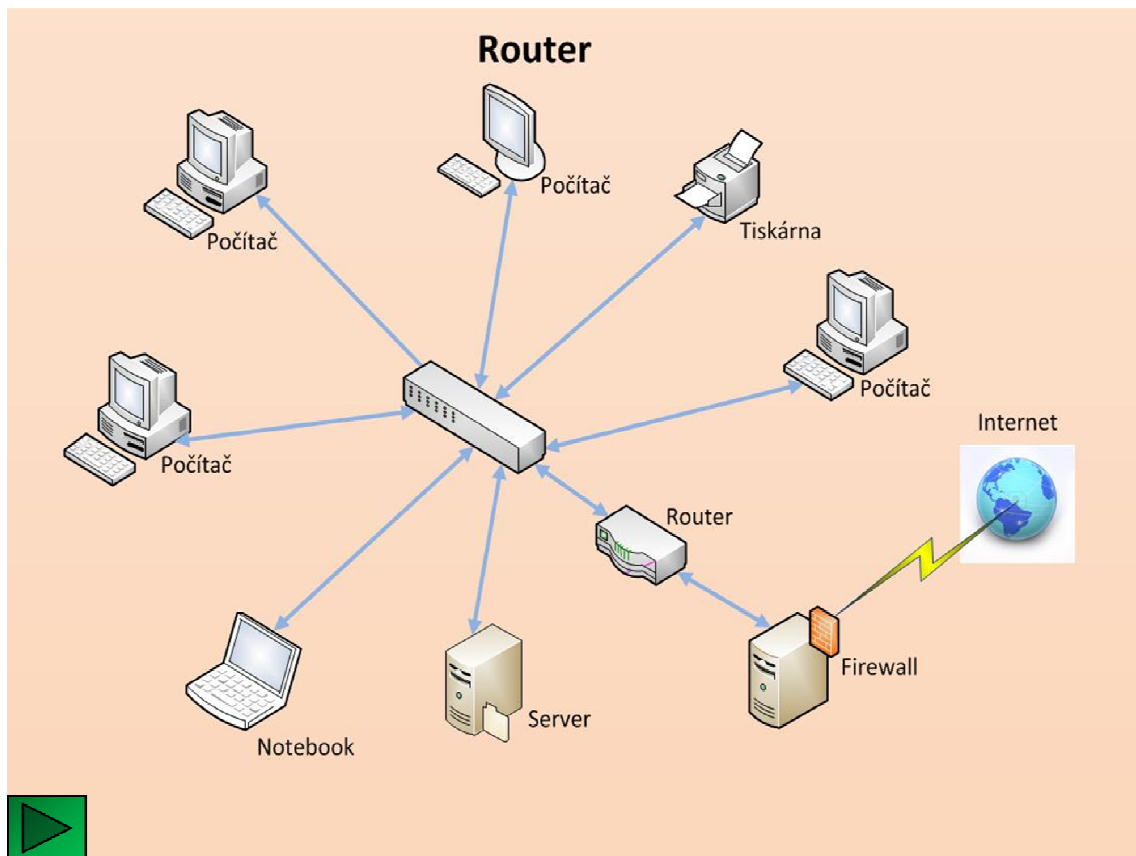
Žáci zde mohou vidět práci aktivního prvku v počítačové síti. Interaktivní prezentace ukazuje, jak datový paket po jeho aktivaci odchází do switchu a ten ho zasílá určenému adresátovi.



Obr. 36 Ukázka funkce switche v LAN síti [autor]

5.5.2.8 Router – směrování paketů

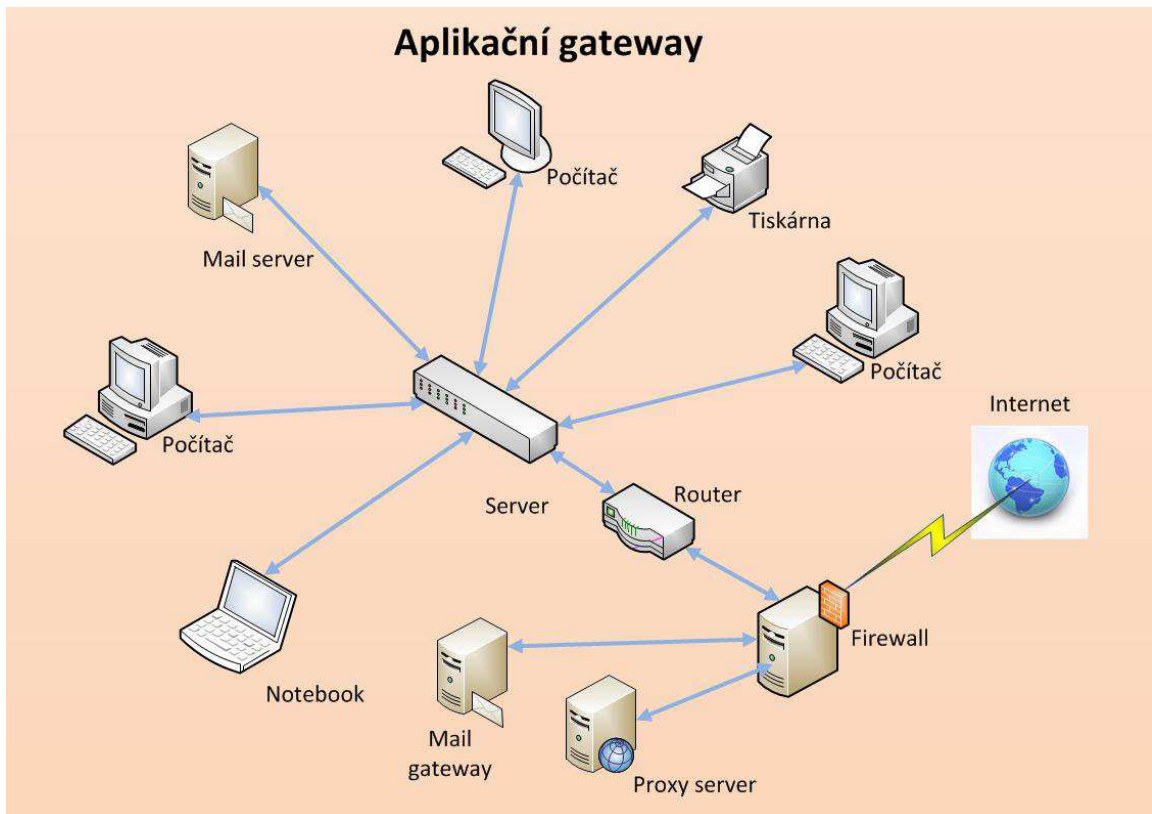
Zde ukazují směrování datového paketu příjemci pomocí aktivního prvku, který se nazývá router. Po aktivaci datový paket odchází na router, který jej odešle adresátovi v jiné počítačové síti. Adresa příjemce je uvedena v datovém paketu jako IP adresa počítače v dané počítačové síti.



Obr. 37 Ukázka funkce routeru [autor]

5.5.2.9 Gateway - komunikace aplikační brány

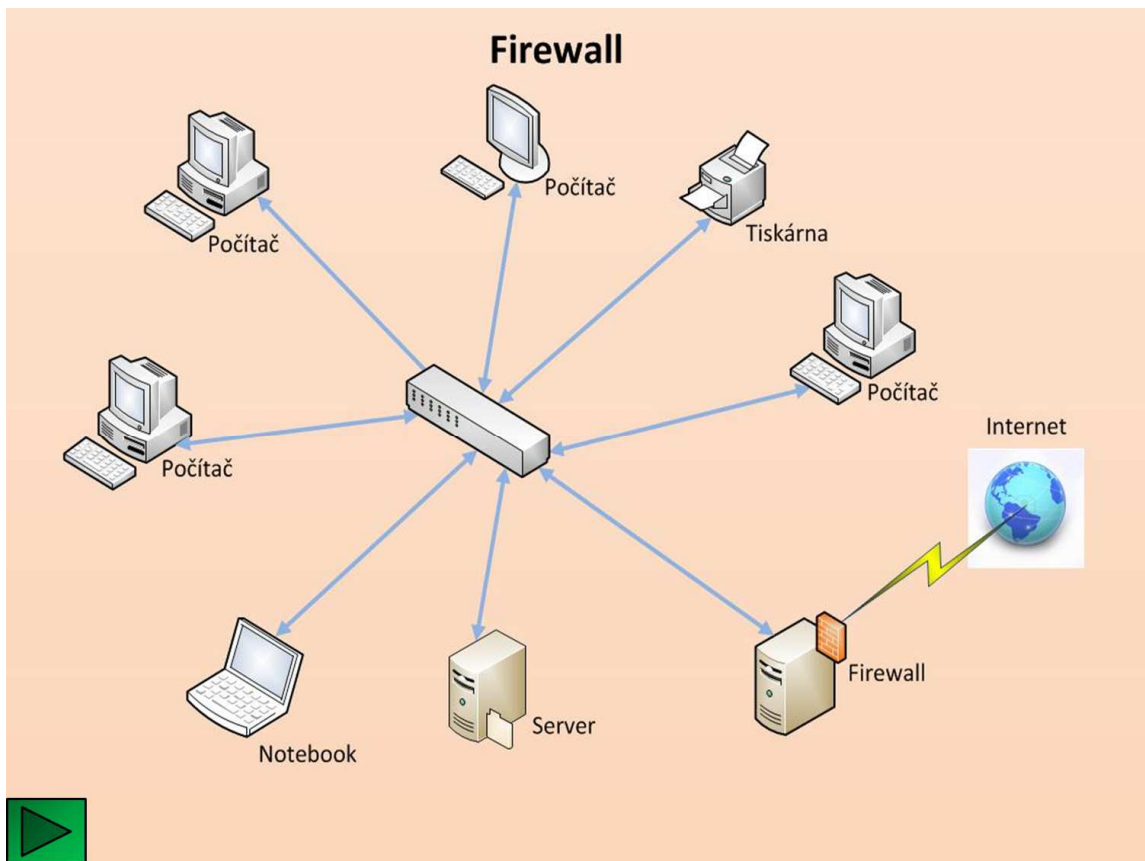
V této interaktivní prezentaci předvádím žákům princip komunikace v počítačové síti přes aplikační gateway. V tomto případě jde o mail gateway. E-mail je poslán na mail server, který jej odesílá na mail gateway a ta zajistí odeslání e-mailu příjemci. Mail gateway zajišťuje i příjem e-mail zpráv.



Obr. 38 Ukázka funkce mail Gateway [autor]

5.5.2.10 Firewall – filtrování paketů

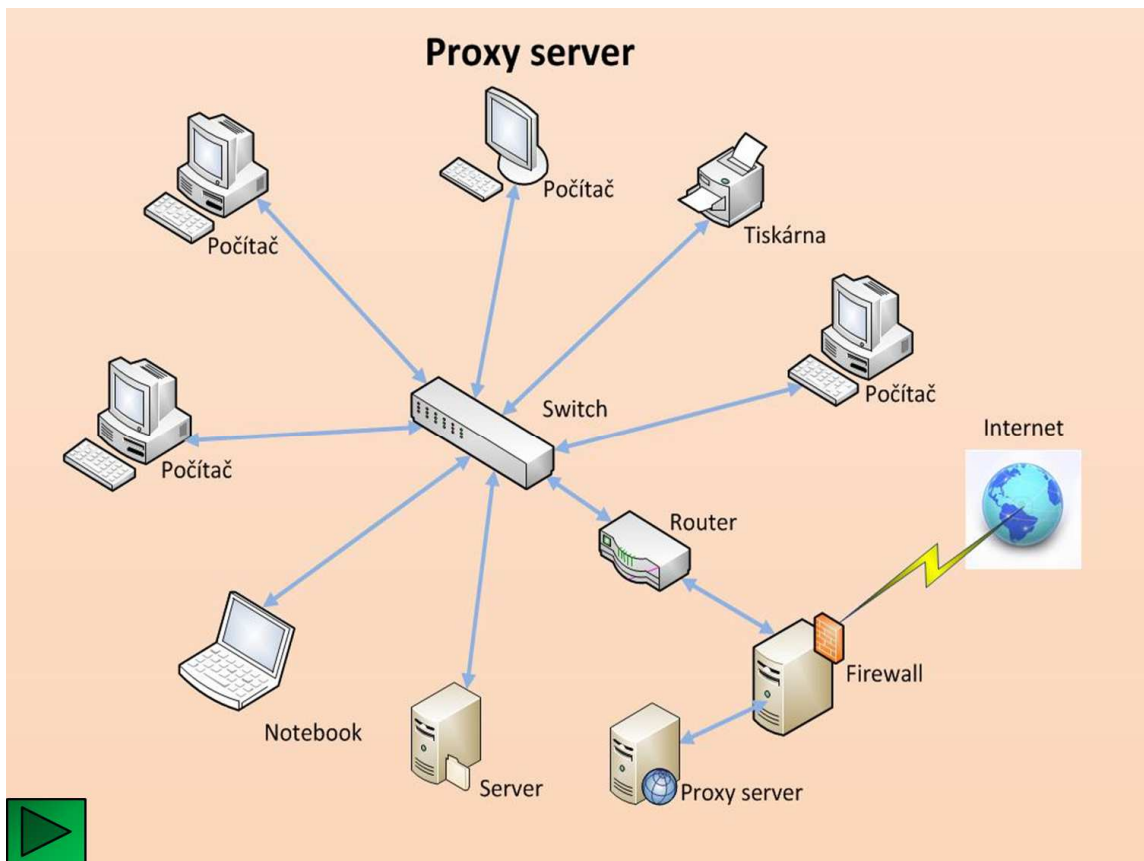
V této interaktivní prezentaci ukazují žákům funkci firewallu v počítačové síti. Datový paket je prověřen po příchodu na firewall, zda má povolení ke vstupu do počítačové sítě. V případě že nemá, tak mu firewall neumožní vstoupit do počítačové sítě.



Obr. 39 Ukázka funkce firewallu [autor]

5.5.2.11 Proxy server - předávání paketů do veřejné sítě

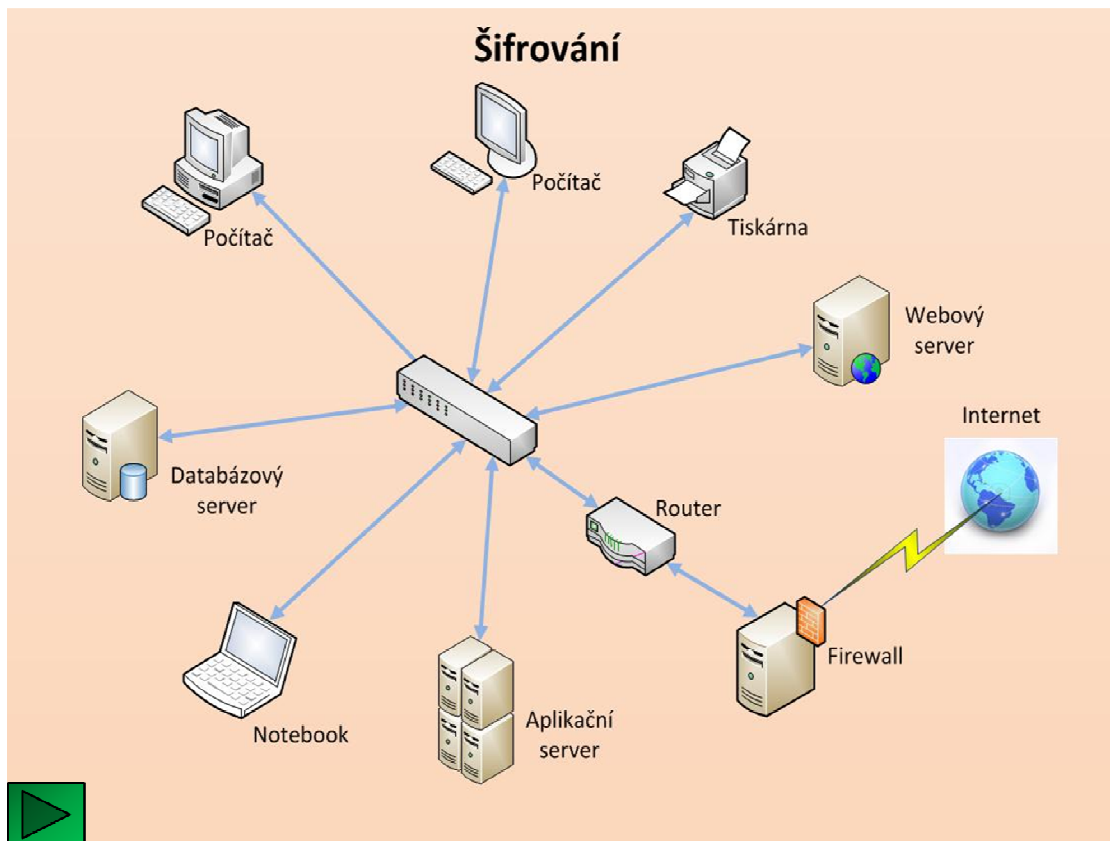
V této interaktivní prezentaci předvádím žákům jak proxy sever zajišťuje předávání datových paketů od jednotlivých počítačů z privátní počítačové sítě do veřejné sítě a naopak. Datový paket se odešle z počítače na proxy server a ten jej předá do veřejné počítačové sítě.



Obr. 40 Ukázka funkce proxy serveru [autor]

5.5.2.12 Šifrovaná komunikace

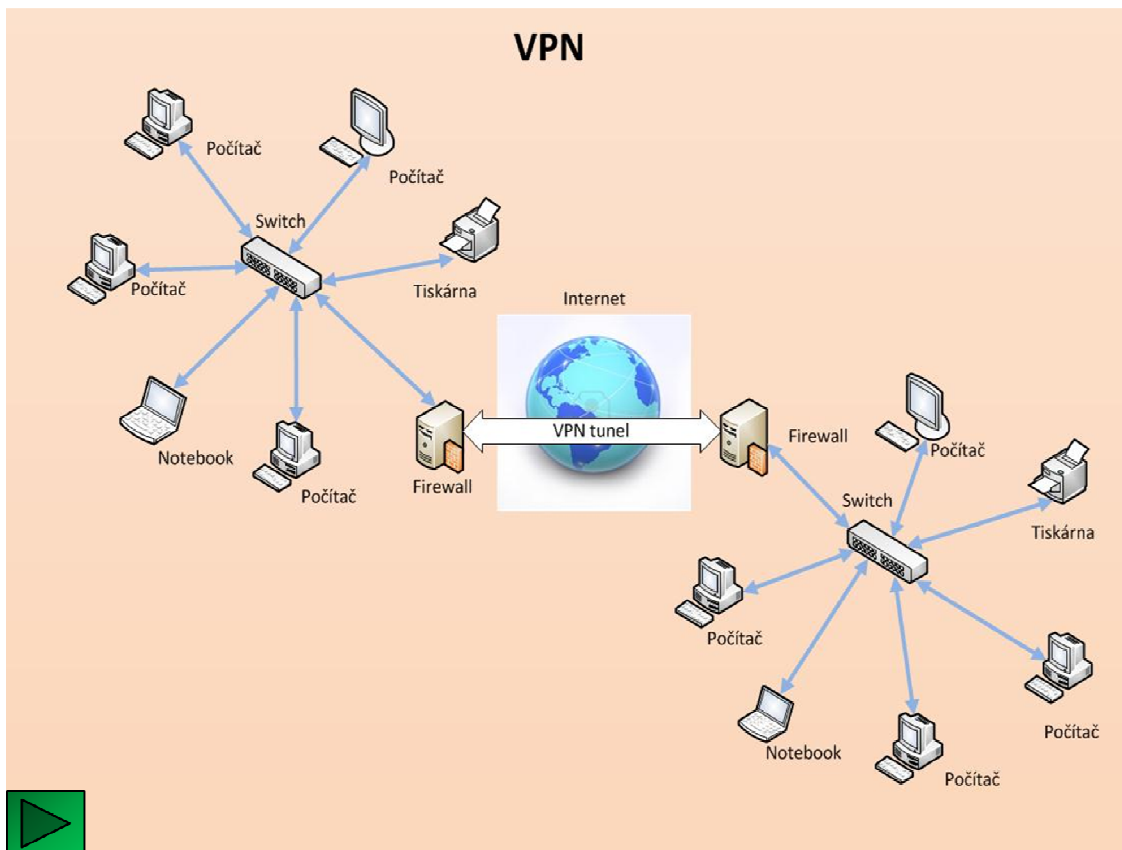
V této interaktivní prezentaci ukazují, jak probíhá zašifrovaná komunikace v počítačové síti. Datový paket se zašifruje a odešle se příjemci. Příjemce datový paket dešifruje a zpracuje.



Obr. 41 Ukázka principu šifrování [autor]

5.5.2.13 VPN

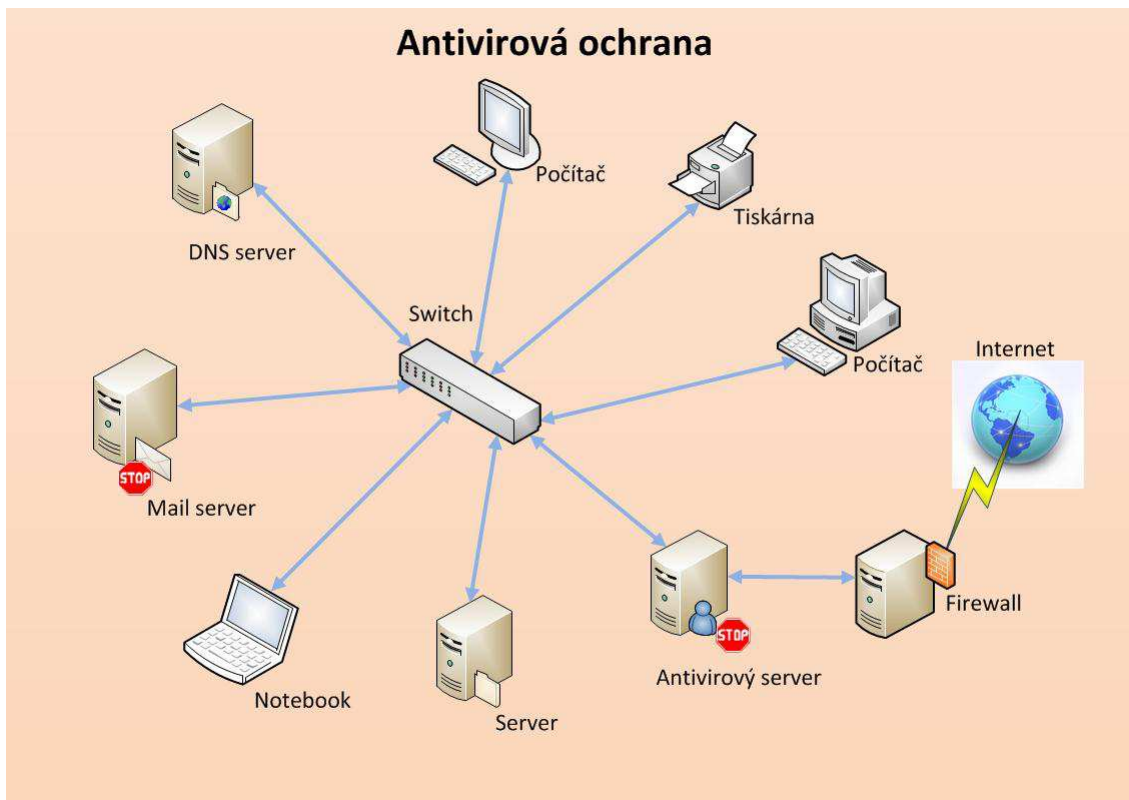
V této interaktivní prezentaci předvádím žákům princip komunikace přes zašifrovaný VPN tunel. Datový paket je poslán příjemci v jiné LAN počítačové síti přes Internet pomocí tohoto VPN tunelu.



Obr. 42 Ukázka principu VPN tunelu [autor]

5.5.2.14 Antivirová ochrana

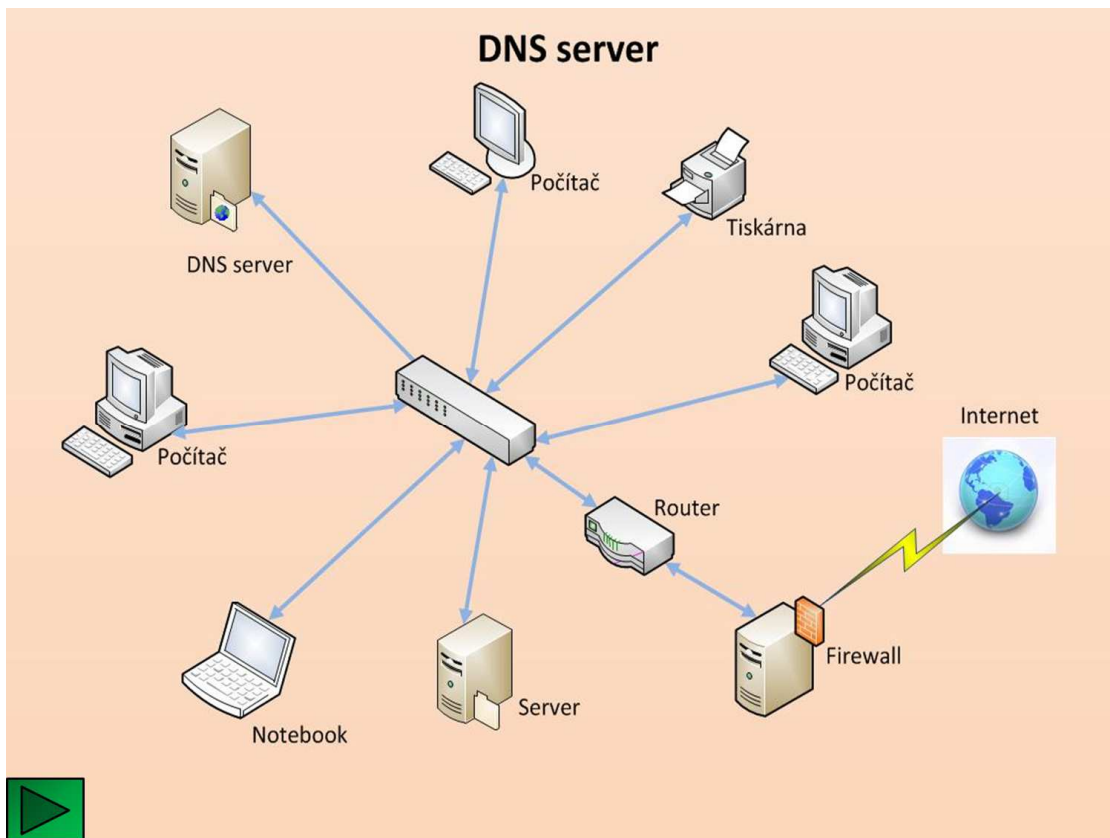
V této interaktivní prezentaci předvádím žákům, jak funguje antivirová ochrana v počítačové síti. E-mail zpráva z vnější sítě přichází na antivirový server, který ji zkontroluje. Pokud neobsahuje virus, je propuštěna do vnitřní počítačové sítě a při uložení na poštovním serveru je prověřena antivirovým programem. Odtud si ji vyzvedne adresát.



Obr. 43 Ukázka principu antivirové ochrany [autor]

5.5.2.15 DNS server – překlad jména na IP adresu

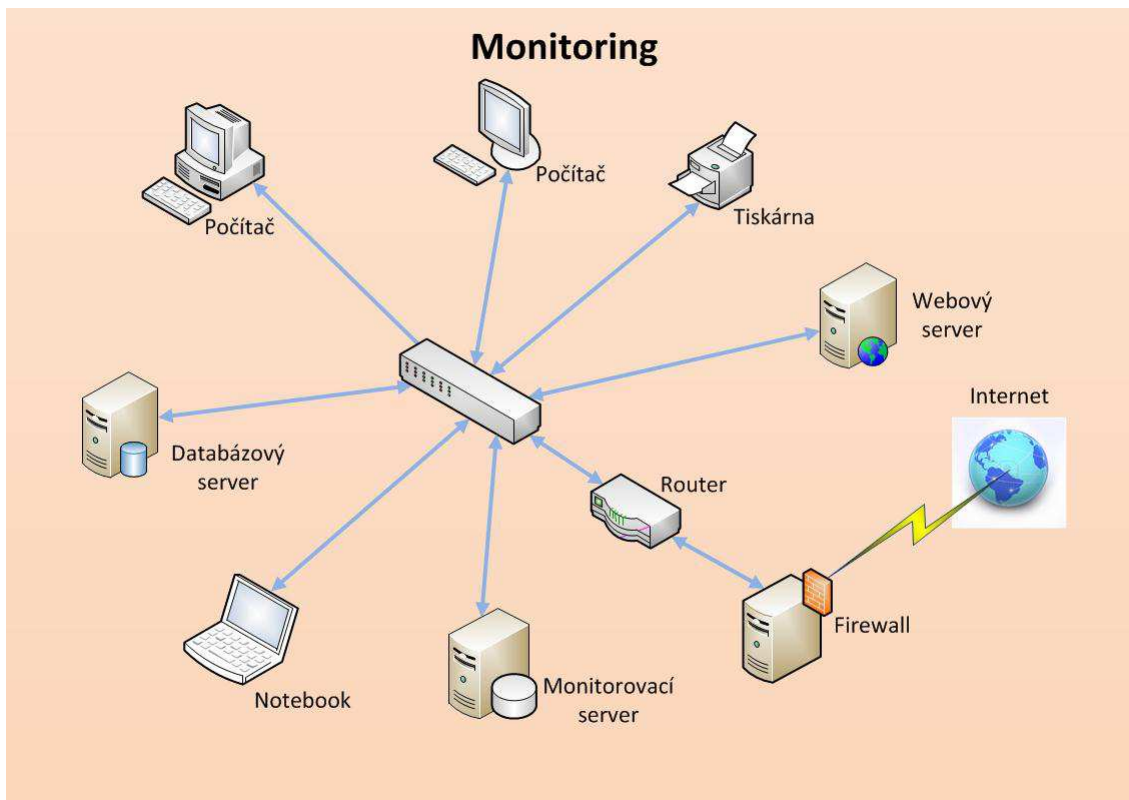
V této interaktivní prezentaci ukazují jak DNS server překládá jméno na IP adresu. Na počítači v internetovém prohlížeči uživatel zadá URL adresu, na kterou se chce připojit. Počítač odešle dotaz na DNS server, kde žádá o sdělení IP adresy přiřazené k dotazovanému jménu. Po té začíná komunikovat s daným serverem na základě jeho jednoznačné identifikace IP adresou v dané počítačové síti.



Obr. 44 Ukázka funkce DNS serveru [autor]

5.5.2.16 Monitoring počítačové sítě

V této interaktivní prezentaci žákům ukazují, jak je možné monitorovat počítačovou síť. Monitorovací server odešle dotazy na zařízení v síti, zjistí potřebné informace a uloží je do své databáze.



Obr. 45 Ukázka principu monitorování počítačové sítě [autor]

6 ZÁVĚR

V této diplomové práci byl vytvořen interaktivní výukový materiál pro žáky základní školy. První teoretická část se věnuje základním znalostem o zařízeních, ze kterých se počítačová síť skládá, jejich funkci a principu komunikace v těchto sítích. Ve druhé části byl vytvořen interaktivní výukový materiál, který názorným způsobem poskytne žákům základní přehled o principu fungování počítačových sítí. K realizaci byly použity knihy o problematice počítačových sítí a také velké množství elektronických materiálů, které je možné najít na Internetu. Byla vytvořena sada obrázků, na kterých je předveden pomocí animace princip komunikace v počítačové síti, její ochrana před napadením potenciálním útočníkem a její monitoring. Tyto materiály byly vytvořeny přístupnou formou pro žáky základní školy, tak, aby byly přiměřené jejich znalostem o počítačích a zároveň je seznámily s principem práce počítačových sítí, se kterými se setkávají v běžném životě.

Použitá literatura:

- [1] HEJNA, Ladislav. *Lokální počítačové sítě*. 1. vyd. Praha: Grada, 1994, 139 s. ISBN 80-856-2399-4.
- [2] STREBE, Matthew a Charles PERKINS. *Firewally a proxy-servery*. Vyd. 1. Brno: Computer Press, 2003, xxi, 450 s. ISBN 80-722-6983-6.
- [3] KÖHRE, Thomas. *Stavíme si bezdrátovou síť WI-FI*. Vyd. 1. Brno: Computer Press, 2004, 295 s. ISBN 80-251-0391-9.
- [4] HABRAKEN, Joe. *Počítačové sítě: průvodce úplného začátečníka*. 1. vyd. Praha: Grada, 2006, 492 s. ISBN 80-247-1422-1.
- [5] ODOM, Wendell. *Počítačové sítě bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005, 383 s. ISBN 80-251-0538-5.
- [6] DOBDA, Luboš. *Ochrana dat v informačních systémech*. 1. vyd. Praha: Grada Publishing, 1998, 286 s. ISBN 80-716-9479-7.
- [7] Derfler F.J. Feed L. *Jak pracují sítě* ZD Press 1994
- [8] SCHATT, Stan. *Počítačové sítě LAN OD A do Z*. [1. vyd.]. Překlad Tomáš Rutrle. Praha: Grada, c1994, 378 s. ISBN 80-856-2376-5.
- [9] <http://www.svetsiti.cz/>
- [10] <http://www.linuxsoft.cz/>
- [11] http://cs.wikipedia.org/wiki/Hlavn%C3%AD_strana
- [12] http://sdeleni.idnes.cz/foto.aspx?r=tec_sdeleni&foto1=AHR3bf9f2_kabel_s_volnou_sekundarni_ochranou.jpg
- [13] <http://www.linuxsoft.cz/img/zabbix/map.png>
- [14] http://commons.wikimedia.org/wiki/File:UTP_cable.jpg
- [15] http://dealer.penta.cz/kabel-solarix-stp-kabel-cat-6a-drat-500m-lsoh-civka_ie5969551.jpg
- [16] http://www.phil.muni.cz/wcit/home/Pictures/kabel_utp_rj45.jpg
- [17] http://extrahardware.cnews.cz/galerie/pictures/clanky/epc/2012/07cervenec/minitest-sitovych-karet/minitest-sitovych-karet_02.jpg
- [18] <http://www.dsl.cz/jak-na-to/2-zaciname/201-jak-pripojit-pc-k-internetu>
- [19] <http://home.zcu.cz/~klenhova/druhyUSB.html>
- [20] <http://www.hasco.cz/reference/strukturka.htm>

- [21] http://www.wifi-shop.cz/airlive-poe-fsh2442g-switch-24x-poe-10-100-4x-1000-mbps-port-switch-2x-sfp-combo-management-19-rack_d3334.html
- [22] <http://cs.wikipedia.org/wiki/Soubor:ERS-8600.JPG>
- [23] http://www.luxus.cz/obchod_pic/tl-wr841nd-01.jpg
- [24] <http://www.linuxsoft.cz/img/zabbix/dashboard.png>
- [25] <http://www.novell.com/coolsolutions/feature/16723.html>
- [26] http://pctuning.tyden.cz/ilustrace3/simandl/optika_obrazky/LC_connecto_r.jpg