Univerzita Hradec Králové

Pedagogická fakulta

Katedra Informatiky Přírodovědecké fakulty

Bezpečná konfigurace školní počítačové sítě jako prostředek výchovy žáků

Diplomová práce

Autor:	Bc. Patrik Matejsek
Studijní program:	N7504 Učitelství pro střední školy
Studijní obor:	Učitelství pro střední školy – informatika
	Učitelství pro střední školy – základy techniky
Vedoucí práce:	PhDr. Michal Musílek, Ph.D.

Hradec Králové 2016

Univerzita Hradec Králové
Pedagogická fakulta

Zadání diplomové práce

Autor:	**Bc. Patrik Matejsek**
Studium:	P14P0422
Studijní program:	N7504 Učitelství pro střední školy
Studijní obor:	Učitelství pro střední školy - informatika, Učitelství pro střední školy - základy techniky
Název diplomové práce:	**Bezpečná konfigurace školní počítačové sítě jako prostředek výchovy žáků**
Název diplomové práce AJ:	Secure configuration of school computer network as an instrument of students education

Cíl, metody, literatura, předpoklady:

Cílem diplomové práce je specifikace vhodné podoby a konfigurace počítačové sítě v prostředí školy a školských zařízení, včetně opatření budující u žáků (studentů) správné bezpečnostní návyky. Převážnou část práce by měl tvořit zpracování technický návrh počítačové sítě, optimalizovaný pro daný typ zařízení. Jeho zpracování bude vycházet z analýzy specifik a potřeb a soustředí se na zabezpečení bezpečného a plynulého provozu sítě. Navržené řešení bude vyhodnoceno na základě kritérií uváděných v odborné literatuře. Kromě metalických prvků se ve školních infrastrukturách v současnosti používají také bezdrátové síťové prvky sítí, s nimiž jsou spojeny výhody, ale též problémy, zejména bezpečnostní, na které práce poukazuje. Součástí práce bude dotazníkové šetření aktuálního stavu počítačových sítí z hlediska použitého hardware, firmware a bezpečnostního nastavení ve vybraných středních školách.

Garantující pracoviště:	Katedra informatiky, Přírodovědecká fakulta
Vedoucí práce:	PhDr. Michal Musílek, Ph.D.
Oponent:	Ing. Jiří Jelínek, Ph.D.

Datum zadání závěrečné práce: 20.5.2015

Prohlášení

Prohlašuji, že jsem diplomovou práci vypracoval samostatně pod vedením PhDr. Michala Musílka, Ph.D. a uvedl jsem všechny použité prameny a literaturu. Prohlašuji, že diplomová práce je uložena v souladu s rektorským výnosem č. 1/2013 (Řád pro nakládání se školními a některými jinými autorskými díly na UHK).

V Hradci Králové dne 11. 7. 2016

…….

Poděkování

Na tomto místě bych rád poděkoval PhDr. Michalu Musílkovi, Ph.D. za vedení, cenné připomínky a odborné rady, kterými přispěl k vypracování této diplomové práce. Velké dík dále patří mým rodičům za podporu při studiu a zázemí.

Anotace

MATEJSEK, Patrik. *Bezpečná konfigurace školní počítačové sítě jako prostředek výchovy žáků*. Hradec Králové: Pedagogická fakulta Univerzity Hradec Králové, 2016. 106 s. Diplomová práce.

Diplomová práce se zaobírá problematikou konfigurace počítačové sítě ve školském prostředí. Celkově je práce rozdělena na tři hlavní části. První část práce obecně pojednává o teoretických poznatcích spojených s významem využívání počítačových sítí, jejich technologií a služeb. Dále je zmíněna problematika bezpečnosti počítačových sítí a znázorněny základní principy fungování bezdrátové sítě Wi-Fi, včetně způsobů jejího zabezpečení. Druhá část uzpůsobuje získané teoretické znalosti přímo potřebám modelového školního prostředí. Je představen základní model podoby školní sítě, na kterém je dále prezentováno několik návrhů pro zlepšení a zjednodušení její podoby s ohledem na dnešní trendy. Třetí část seznamuje s výsledky výzkumu dotazníkového šetření zaměřeného na aktuální stav vybraných školních síťových prostředích. Text kombinuje poznatky získané studiem odborné literatury a internetových zdrojů s praktickými zkušenostmi autora ve využívání těchto technologií.

Klíčová slova: počítačová síť, konfigurace, síťové služby, zabezpečení, bezdrátová síť, škola, směrovač, přepínač, přístupový bod, paket

Annotation

MATEJSEK, Patrik. *Secure configuration of school computer network as an instrument of students education*. Hradec Králové: Faculty of Education, University of Hradec Králové, 2016. 106 pp. Diploma Thesis.

The diploma thesis focuses on the issues of computer network configuration in education institutions. Overall, the diploma thesis is divided into three major parts. The first part generally describes the theoretical background of computer networks, the importance of their usage, the technology and the services related to them. The next area of focus is computer network security. The first part also describes the basic properties and functionality of wireless network Wi-Fi including its securing possibilities. In the second part, the researched theoretical knowledge base is accommodated specifically to fit the education-institutional model. Next, there is presented basic design of school network including several proposals for the improvement and facilitation of its appearance with respect to the current trends. The third part provides the results of the questionnaire inquiry which was designed to acquire the present state of selected education institutions' network conditions. The text is combination of the knowledge gained by studying of professional literature and internet sources with practical experience of the author in the usage of these technologies.

Keywords: computer network, configuration, network services, security, wireless network, school, router, switch, access point, packet

Obsah

Úvod

Studium problematiky počítačových sítí spadá v současnosti do nutnosti širokého obzoru vědomostí a jedná se o relativně složitý obor poznání. Toto speciální odvětví spadající do oblasti informačních a komunikačních technologií je jednou z nejdůležitějších technologií moderní výměny informací. S absencí oboru počítačových sítí bychom velmi složitě dosáhli současného informačního věku, neboť by Internet, bez kterého si většina nedokáže představit svůj denní život, ani neexistoval. V následujícím kapitolách se budeme zaobírat rozlohou menší oblastí počítačové sítě, ovšem stejně důležitou pro efektivní výměnu a zpracování informací.

Konkrétně se zaměříme na oblast lokální počítačové sítě uzpůsobené pro školní prostředí. Dané prostředí se obecně nikterak neliší od pravidel pro standardní korporátní sítě. Školy si však většinou nemohou dovolit investovat své provozní finanční prostředky do budování moderních sítí. Navíc z důvodu specializace daného oboru ani z větší části nedisponují potřebnými lidskými zdroji s požadovanými odbornými znalostmi, případně je nemohou adekvátně ohodnotit.

Cílem dané práce bude poukázat na důležité aspekty této problematiky a uzpůsobit je možnostem a potřebám daných institucí. Z tohoto důvodu bude cílem první části teoreticky vysvětlit veškeré důležité aspekty spojené s obecnými základy počítačových sítí a důležitosti jejich zabezpečení. Zaměříme se též na oblast bezdrátového způsobu šíření informací pomocí nelicencované technologie Wi-Fi. Druhá část se bude zaobírat počítačovou sítí v prostředí školy. Zde se již naplno zaměříme na aspekty návrhu konfigurace počítačové sítě, uzpůsobenou potřebám zmiňovaného typu statní instituce. Představíme si základní model typické školní počítačové sítě, kde cílem bude navrhnout změny zjednodušující práci v síti, zabezpečující její provoz a účinnější správu. Budou zmíněny též způsoby omezující nesprávný morální vývoj mládeže a tipy zaměřené na ochranu vlastního soukromí. Třetí a zároveň poslední část se bude zabývat zjištěním aktuálního stavu školních počítačových sítí podle předem definovaných hledisek. Cílem poslední části bude na základě dotazníkového šetření provést analýzu získaných dat od zástupců oslovených institucí.

1 Teoretická část

1.1 O počítačových sítích obecně

1.1.1 Význam počítačových sítí

V současné moderní informační a komunikační době může být až troufalé polemizovat nad myšlenkou vzniku počítačových sítí. Znalost historie nás však činí tím, čím jsme. Proto bychom se alespoň na chvíli měli zastavit nad počátky vzniku a významu jejího zavedení. Spojení více počítačů pro vzájemné předávání informací již dávno není výhradou velkých univerzitních či korporátních sítí. Stejně jako se před více než třiceti lety dostaly poprvé osobní počítače do našich domácností, taktéž již téměř nenalezneme domácnost, která by neměla vlastní síť.

Vraťme se však k myšlence vzniku takové počítačové sítě. Na začátku toho všeho stála přirozená potřeba lidí - komunikace. V době sálových počítačů bylo standardem centralizovat celé sestavy do jedné velké místnosti. Ke zpracování všech informací zde sloužil jeden nebo dva počítače. Počítačová síť vznikne, dojde-li ke vzájemnému propojení dvou nebo více počítačů. Brzy tak byl tento výpočetní model s centrálním systémem nahrazen modelem, ve kterém je výpočet realizován za pomoci jednodušších samostatných počítačů, které jsou však vzájemně propojeny. Nejedná se pouze o vzájemnou komunikaci, nicméně jednou z prvních služeb sítí byla právě elektronická komunikace mezi lidmi.

Za zmínku dále stojí například snadné přenášení dat a jejich ochrana či sdílení prostředků. Vezmeme si kupříkladu situaci, kdy máme k dispozici relativně výkonný počítač, fungující pouze lokálně, bez spolupráce a přístupu k síti. Pokud chceme dále sdílet soubory a prostředky, musíme nejprve vše potřebné zkopírovat na přenosné médium a dále přenést do jiného systému. Zkopírovaná data je pak možné například upravit nebo zpracovat v jiném systému a posléze znovu fyzicky dopravit zpět. Může to znamenat třeba i relativně triviální vytisknutí zpracovaných dat, ale tiskárna je umístěna na jiném pracovišti. Zamysleme se pouze nad časem, který jen touto nutnou činností ztratíme. A to jsme se ani dále hlouběji nezamysleli nad situací, co by se stalo,

kdyby došlo ke ztrátě daného přenosného média a jeho nalezení neoprávněnou osobou. Nebo fakt, že velikost souboru nám neumožňuje přenos z nedostatku kapacity.

Ovšem podobných příkladů bychom nalezli nespočet. Důvodů pro využívání služeb počítačové sítě tak máme hned několik a její nepoužití je v současnosti téměř nepředstavitelné ani v již výše zmiňovaných domácnostech. [2], [25]

1.1.2 Hlavní výhody počítačových sítí

I přes skutečnost, že se na každou jednu výhodu většinou váže minimálně jedna nevýhoda, si shrneme pár výhod při zavedení počítačových sítí. Začneme úsporou nákladů, kde v jednom oddělení máme více počítačů spojených v síti a skupinu pracovníků spolupracující na jednom projektu. Berme v daném příkladu pořizovací a provozní náklady tiskárny, kterou potřebují všichni spolupracovníci k výstupu. Místo toho, aby ke každému počítači byla připojena tiskárna a náklady se násobily, stačí nám jedna tiskárna připojená do počítačové sítě pro celé oddělení či patro. Počítačová síť nám dále umožňuje efektivní sdílení dat diskového prostoru, společného pro všechny pracovníky. Navíc, data se dají snadno kopírovat a přenášet jedním krokem bez použití prostředníka. Ochranu proti odcizení nebo ztrátě dat vyřešíme mnohem jednodušeji za využití centrálního úložiště dat, které může být navíc redundantní a mít přesně definovaná bezpečností pravidla. Zálohovací proces je díky tomuto řešení pravidelný a lépe řiditelný. Ze vzniklé centralizované zálohy je obnova dat rychlá a lehce dohledatelná. Při takovém řešení se navíc dá řídit celá síť, o dále neurčeném počtu počítačů, efektivně z centrálního místa. Obsluhuje ji osoba zabývající se správou informačních a komunikačních technologií. Pokud výše řečené výhody shrneme do bodů, počítačová síť nám převážně umožňuje:

- úsporu nákladů a času
- sdílení dat
- sdílení hardwarových prostředků (tiskárny, skenery, disky)
- zálohování a ochranu dat
- elektronickou komunikaci
- efektivní správu z centrálního místa

S příchodem moderních operačních systémů, chytrých zařízení a celosvětové sítě Internet se výhody vzájemného propojování počítačů dále prohlubují. Doba

moderního informačního věku je v plném proudu a je nutné se tomuto trendu naplno přizpůsobit. [2], [9]

1.1.3 Rozdělení počítačových sítí podle velikosti

Hovoříme-li o počítačové síti obecně, neřešíme většinou její rozdělení podle určité geografické oblasti. Rozdělení sítí podle velikosti je však jedním ze základních předpokladů pro určení charakteristik a podmínek pro jejich správné fungování. Obvykle vycházíme ze tří základních skupin: [2], [9], [11], [30]

- **Místní síť**, označena zkratkou LAN (Local Area Network): základní klasifikace kterékoliv počítačové sítě, omezení vychází na jedno lokální místo, konkrétně jedna budova nebo oddělení. Maximální geografická rozloha se uvádí do průměru 5 km.
- **Metropolitní síť**, označena zkratkou MAN (Metropolitan Area Network): zajišťuje spojení jednotlivých místních sítí mezi několika budovami ve velkém městě, zajišťuje přenos informací mezi vzdálenými pobočkami. Maximální geografická rozloha se uvádí do průměru 50 km a může být u nich využito odlišných prvků k šíření informací po síti.
- **Rozlehlá síť**, označena zkratkou WAN (Wide Area Network): neurčuje žádné geografické omezení, velký počet vzájemně propojených místních sítí po celém světě. Nejzákladnější rozlehlou sítí na světě je Internet.

Obr. 1 - Schéma rozdělení počítačových sítí podle velikosti

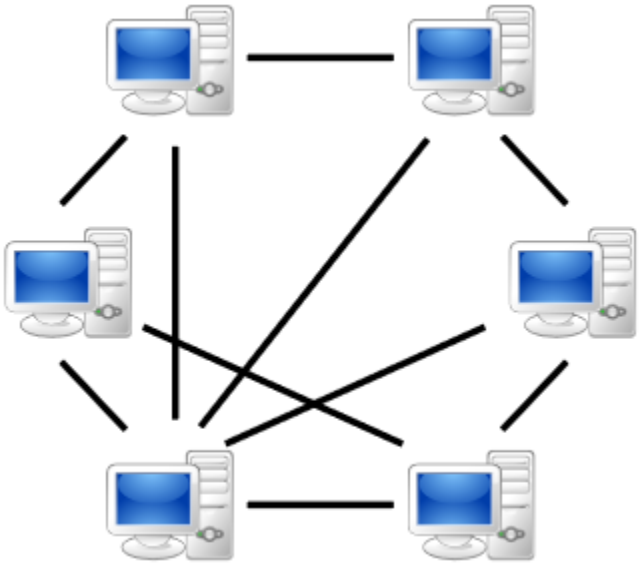
Zdroj: [7]

1.2 Kategorie počítačových sítí

Obecně rozlišujeme dva základní modely pro sdílení dat. Sdílení dat může probíhat na jedné totožné úrovni, kde jsou si všechna zařízení rovna, případně striktně rozdělena podle úrovní na služby. Takové sítě posléze označujeme jako kategorii: *peer-to-peer* nebo *sítě založené na serverech (client-to-server)*. Rozdělení do kategorií je z hlediska komunikace v síti důležité a obě kategorie nabízejí rozdílné schopnosti pro práci v síti.

1.2.1 Sítě peer-to-peer

Význam pojmu peer-to-peer je v češtině označován jako rovný s rovným. Pomocí tohoto spojení dosahujeme jednoduchého a přímého způsobu použití sítí. V této kategorii sítí neexistuje žádná centrální správa a komunikace probíhá na úrovni uživatelů. Ti si sami stanovují, jaké prostředky budou ze svého počítače sdílet ostatním. Dané sítě je možné provozovat na standartních klientských operačních systémech bez jakýchkoliv dalších doplňků či centrálních služeb. Výhodou provozování těchto sítí jsou tak nízké náklady a jednoduchost provozování. Bohužel se tento typ provozu projeví na zabezpečení sítě, které je z důvodu decentralizovaného řízení velice náročné. Každý uživatel může k otázce zabezpečení přistupovat rozdílně a centrální správa je velmi obtížně realizovatelná. Co se týče přehledu o datech, tedy na kterém počítači je co uloženo, jedná se o velice náročnou záležitost. Omezení tohoto typu sítí je závislé na konečné velikosti sítě. Obecně je možné poznamenat, že tento typ sítí lze doporučit pro propojení menšího počtu počítačů v malé firmě. Zpravidla je uváděnou hranicí síť o velikosti 10 klientských stanic a je možné je často zaznamenat též pod názvem *pracovní skupiny* (groups). Pro administrativní a veřejné budovy, kam se řadí například i školská zařízení, je tedy tento typ sítě nepoužitelný a je nutné zaměřit se na centrální řešení podoby sítě. [2], [9]

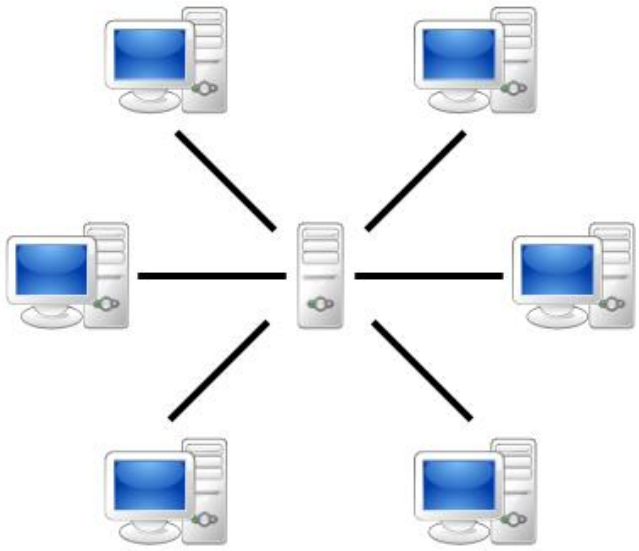


Obr. 2 - Vizualizace fungování sítí typu peer-to-peer

Zdroj: [18]

1.2.2 Sítě client-to-server

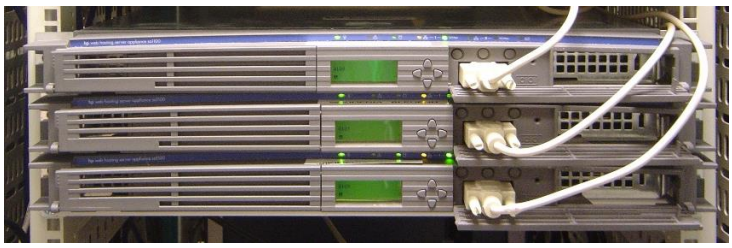
Provedení sítí typu client-to-server (klient – server) staví na centrální struktuře a pevném oddělení úloh klientských (uživatelských) zařízení a serverů. Ve výsledku se jedná o soustředění veškerých dat, služeb, údajů a poznámek na jeden bod v síti. Jeden bod se, s ohledem na zabezpečení, lépe chrání a spravuje, ačkoliv je nutné splnit určité doporučené náležitosti. Dané vyhrazené počítače se posléze nazývají jako servery (sluhové) a z důvodu množství požadavků jsou jejich hardwarové nároky vyšší než na běžná klientská zařízení. Server posléze reaguje na požadavky o zpracování ze strany klienta a zpracovaný výsledek posílá zpět nebo ukládá na své úložiště. Hardwarovými požadavky to však nekončí, neboť musejí být též splněny požadavky na specializovaný operační systém (síťový) a služby zpracovávající požadavky klientů. Propojení hardwaru a fyzické sítě je sice plně identické se sítěmi typu peer-to-peer, pouze jsou veškeré požadavky dotazovány proti serveru. Síťový operační systém a specializované služby například konkrétně organizují sdílení dat a princip jejich ukládaní řídí uživatelská práva a ověřují přístup, přidělují a překládají adresy nebo udržují aktuální zálohu. Výhodou daných sítí je vysoká bezpečnost dat, přehlednost a jednotné nastavování. Nevýhodou jsou vyšší pořizovací náklady a vyšší odborné znalosti správce (kvalifikovaného pracovníka).



Obr. 3 - Vizualizace fungování sítí typu client-to-server

Zdroj: [18]

Umístění serveru není přesně dané, ale doporučuje se jej, v rámci možností, umístit do samostatné, speciálně určené místnosti. Takovou místnost posléze nazýváme jako serverovnu nebo technickou místnost, kde se soustřeďují veškerá zařízení řídící provoz sítě. Je nutné pamatovat na fakt, že přes veškeré pořizovací náklady, jsou tím nejdůležitějším a nejdražším data. Technická místnost by měla mít vlastní zabezpečovací systém a možnost aktivního chlazení či odvodu odpadního tepla minimálně po dobu nadprůměrně teplých měsíců. S ohledem na velikost sítě (počet připojených počítačů a požadavků na zpracování) rozhodujeme, zdali nám pro provoz stačí pouze jeden server, nebo musíme použít větší množství a jednotlivé požadavky rozdělit, aby mohl být každý úkol nejefektivněji proveden. V případě většího množství serverů je doporučeno jejich umístění do standardizovaného rozvaděče (rack). Servery musejí fyzicky splňovat možnost umístění do rackové skříně a jsou zde umístěny pod sebou o rozdílné výšce (určeno speciální jednotkou *x*U, kde x = číslo 1 až 8). Velikost jednotky U (rack unit) se určuje v palcích, 1U se rovná velikosti 1,75“ (palců), což je 44,45 mm. [2], [9], [23]



Obr. 4 - Standardizované umístění serverů (velikost 3x 1U) v racku

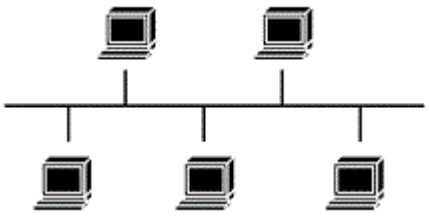
Zdroj: [6]

1.3 Topologie počítačových sítí

Topologie sítí nám slouží k určení způsobu propojení počítačů a dalších zařízení v konkrétním síťovém prostředí. Podle zvolené topologie určujeme jisté síťové standardy a podstatné výsledné vlastnosti sítě. Souvisí nejen s výslednou volbou fyzického přenosového média, ale též zobrazuje tok dat v síti mezi jednotlivými zařízeními. Podle daného záměru rozlišujeme fyzickou a logickou strukturu topologie. Fyzická struktura se zaměřuje na individuální rozložení síťových prvků a zvoleného přenosového média mezi prvky. Logická struktura značí tok dat v sítí z jednoho prvku ke druhému a nemusí nutně duplikovat fyzickou topologii. Znalost vlastní topologie usnadňuje přehled užívaných prvků a kabeláže v sítí, ale značí i trasu putování informací a může pomoci s její účinnější optimalizací a trasováním.

1.3.1 Sběrnicová topologie

Sběrnicová topologie se vyznačuje jedním hlavním přenosovým médiem po celé délce sítě (sběrnice). Stanice komunikující v síti se k danému médiu připojují pomocí odbočovacích prvků. Veškeré přenášené signály procházejí skrz celou délku sběrnice v obou směrech po jednotlivých stanicích do té chvíle, co dosáhnou cílové stanice. Na obou koncích sběrnice musí být umístěny elektrické rezistory (terminátory), které terminují možnost zpětného odrazu nedoručeného signálu a vzniku interferencí mezi nově vzniklými signály. Výhodou je snadná realizace, provoz a rozšíření. Topologie navíc nevyžaduje velké množství propojovací kabeláže, takže pořizovací náklady nejsou tak vysoké. Nevýhodou je samotné přenosové médium, kdy se v případě jeho poškození částečně nebo kompletně znemožní komunikace po celé šířce sítě. Navíc, délka kabelu hlavního média je omezena. V případě poruchy dochází k její obtížné lokalizaci. V současnosti se s danou topologií setkáme zřídka, ale svůj kus práce si odsloužila. Přenosovým médiem byl koaxiální kabel (tlustý i tenký). [2], [11], [17]

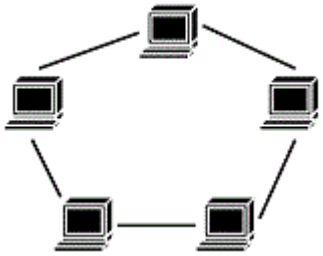


Obr. 5 - Sběrnicová topologie

Zdroj: [17]

1.3.2 Kruhová topologie

Kruhová topologie využívá faktu, že je vždy právě jedna stanice propojena s další dvojicí stanic na jedné i druhé straně. Tímto spojením dosáhneme hromadného propojení všech stanic do kruhu, místo jejich ukončení na obou stranách konce. Signál je cyklicky přenášen po jednotlivých zařízeních v síti. Tímto propojením dosáhneme menší efektivnosti, neboť zaslaná data ze zdroje k cíli musí nejprve postupně cestovat po všech aktivních zařízeních na trase. V takových sítích však není nutné řešit ochranu dat, jelikož na trase nevznikají kolize, protože signál cestuje cyklicky jedním směrem. Výhody jsou téměř shodné s předchozí topologií. Přenos dat je jednoduchý a není nutné velké řízení. V případě, že do sítě přidáme další uzel, šířka pásma (přenosová rychlost) se nemění. Nevýhodou, kromě menší efektivnosti, je v případě přerušení přenosového média porucha na celé síti. Potřebujeme-li přidat do sítě nový uzel (zařízení), musíme dočasně vypnout celou síť. Druh přenosového média je řešen speciálně a využívá se optických vláken nebo kroucené dvoulinky. Kromě toho je princip kruhové topologie ve většině případů řešen pouze logickou konstrukcí, zatímco fyzické propojení může být provedeno rozdílně (hvězdicová topologie), a to převážně z důvodu nulové kolize a minimálního zpoždění signálu na trase. [2], [9], [11], [17]



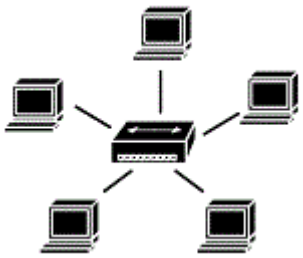
Obr. 6 - Kruhová topologie

Zdroj: [17]

1.3.3 Hvězdicová topologie

Hvězdicová topologie se stala základem pro budování soudobých sítí a v současnosti se jedná o nejpoužívanější způsob propojení zařízení v lokálních sítích. Využívá centrálního aktivního prvku (koncentrátor), z kterého je dále vedeno přenosové médium k právě jednomu zařízení. Každá stanice je tedy skrz daný prvek připojena vlastním kabelem a komunikace mezi zařízeními spravuje koncentrátor. Jako aktivní centrální prvek dnes využíváme přepínače (switch) nebo rozbočovače (hub). Hvězdicová topologie není v oblasti výpočetní techniky novinkou, pochází totiž

z prvopočátků připojování počítače k hlavnímu centrálnímu počítači (mainframe). Mezi výhody dané topologie řadíme nízké riziko náchylnosti k chybě. Přeruší-li se kabel mezi centrálním prvkem a jedním zařízením, zbytek sítě může bez větších obtíží dále pracovat, navíc je lehké danou závadu identifikovat. V porovnání se sběrnicovou topologií vyhrává vyšší výkonnost při srovnatelné přenosové rychlosti, neboť k jednomu kabelu se vždy řadí pouze jedno zařízení. Bohužel s využíváním dané topologie se nám zvýší pořizovací náklady z důvodu větší spotřeby kabeláže a nutnosti pořídit centrální aktivní prvek. Se současnou rostoucí poptávkou jsou však tyto ceny akceptovatelné na úkor podstatného zvýšení výkonu sítě. Síť přestává být funkční až v případě poruchy centrálního aktivního prvku, což řadíme jako nevýhodu, ale stačí posléze daný prvek jednoduše zaměnit za nový. Jako přenosové médium používáme kroucenou dvoulinku nebo optiku. [2], [9], [11], [17]

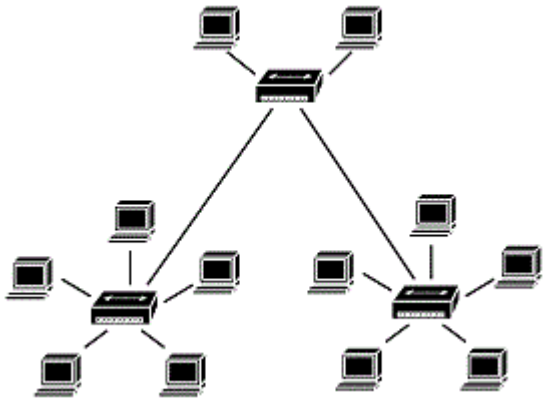


Obr. 7 - Hvězdicová topologie

Zdroj: [17]

1.3.4 Stromová topologie

Též označována jako hierarchická hvězdicová topologie. Stromová topologie vychází z hvězdicové topologie, kterou rozšiřuje o propojení více centrálních prvků mezi sebou. Využíváme ji v případech rozsáhlých počítačových sítí ve velkých budovách. Jednotlivé hvězdice zastupují například různá oddělení firem nebo patra. Ve školském prostředí ji využíváme v případech, kdy potřebujeme propojit více počítačových učeben mezi sebou. Výstup aktivních prvků z jedné i druhé učebny posléze končí v nadřazeném (kořenovém) aktivním prvku, který například zajišťuje připojení dále. Ve výsledku tak snižujeme potřebné množství kabelů pro provoz a zvyšujeme bezpečnost proti odposlouchávání síťové komunikace. Nevýhodou může být situace, kdy dojde k problému na kořenovém aktivním prvku. Přeruší se sice komunikace dále (Internet, vzdálená budova), ale počítače v jednotlivých učebnách spolu mohou mezi sebou nadále vyměňovat informace. [2], [11], [17]

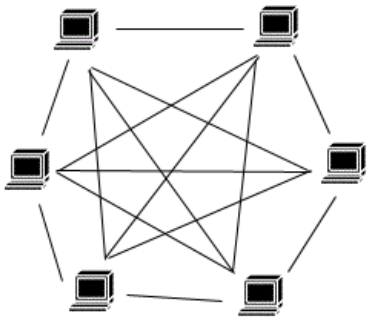


Obr. 8 - Stromová topologie

Zdroj: [17]

1.3.5 Smíšená topologie

Můžeme nalézt další názvosloví: topologie obecného grafu, smyčková, pletivová, Mesh topologie. Dochází k vícenásobnému propojování mezi uzly a vznikají redundantní (záložní) spojení. Využíváno u sítí, ve kterých je nutné zamezit jakýmkoliv výpadkům. Pokud výpadek na jedné straně nastane, signál se automaticky začne šířit jiným směrem, aby nakonec dorazil do určeného cíle. Danou topologii hojně využívají rozlehlé sítě jako je kupříkladu Internet nebo telekomunikační sítě. Výběr nejvhodnější trasy je řešen dynamicky samotnými aktivními prvky, které si udržují informace o sousedních aktivních prvcích. [2], [11], [17]



Obr. 9 - Smíšená topologie

Zdroj: [17]

1.3.6 Páteřní vedení

Vedení zajišťující rychlé propojení mezi jednotlivými segmenty sítě. Přesahující komunikace, nepatřící do daného segmentu, prochází dále právě pomocí tohoto vedení. Požadavkem je vysoká přenosová rychlost. Dále se můžete setkat s pojmy: páteř, páteřní spoj. [9]

1.4 Základní pojmy pro pochopení provozu na sítích

Abychom mohli v povídání o počítačových sítích pokračovat, je nutné se na chvíli zastavit u několika pojmů, které s nimi speciálně souvisí. Pomůže nám to v lepším pochopení principu práce a fungování počítačových sítí.

1.4.1 Komunikace v počítačových sítích

Zaměříme-li se převážně na odvětví současných počítačových sítí, využíváme komunikačního modelu nespojových sítí. Dané sítě nepotřebují před samotnou výměnou dat nejprve navázat komunikaci mezi oběma komunikujícími stanicemi, jak se tomu využívá například v telefonních sítích. Data, která budeme dále přenášet, nejprve rozdělíme do menších částí, označovaných jako pakety (packety). Méně užívaným pojmem takto rozkouskovaných dat v češtině je balíček. Paket je odeslán do sítě a díky známé adrese cílové stanice dosáhne správného konečného místa. Pokud se na trase mezi komunikujícími stanicemi vyskytuje více uzlů, přítomné aktivní prvky danou adresu přečtou a odešlou paket správným směrem. Jednotlivé pakety putují po trase vlastní cestou a mohou do cíle dorazit ve špatném pořadí. Putování mezi více segmenty sítí zajišťují aktivní prvky, které mohou pakety filtrovat, usměrňovat, přepojovat a směrovat. Aby veškerá komunikace proběhla bez obtíží, je nutné zajistit totožná pravidla pro vzájemné porozumění komunikujících stran. K těmto účelům byly definovány přesná pravidla, pomocí kterých všechny prvky v sítí komunikují. Nazýváme je jako protokol a veškeré prvky v sítí, případně nějaká daná část sítě, jej musí používat. [2], [9]

1.4.2 Paket

Na začátku definice paketu (balíčku) můžeme začít s něčím, s čímž jsme se již všichni určitě setkali, tedy obyčejným poštovním balíčkem, zásilkou. Takový poštovní balíček má definovanou svoji velikost a umísťujeme sem cokoliv, co potřebujeme odeslat z místa A do místa B. V případě, že se nám daná věc do balíčku nevejde, musíme balíček zvětšit. Ovšem to však nelze provádět do nekonečna, takže je nutné zásilku rozdělit do více balíčků. Velikost balíčku v počítačových sítích je závislá na protokolu a data jsou podle vlastní velikosti zabalena do balíčků o předem určeném počtu a odeslány. Vrátíme-li se ještě zpět k teorii o poštovním balíčku, musíme se zaměřit na další kritéria, která je nutné splnit z důvodu úspěšného dosáhnutí cíle balíček. Kromě

samotného obsahu dále označujeme poštovní balíček adresou příjemce, adresou odesílatele a obecnou informací o obsahu, kupříkladu jestli je daný balíček křehké povahy. Takto standardizovaný balíček doneseme na poštu a ta podle obsažených informací provede transport balíčku na určené místo.

Paket v počítačových sítích je tedy množinou dat. Data jsou v informatice řešena na úrovni bitů. Množinu bitů, kterou je nutné přenést z jednoho zařízení na druhé, rozložíme na pakety, odešleme a posléze zpětně složíme do stejné podoby jako na začátku. Podoba paketu je závislá na protokolu, ale obecně je možné říci, že se skládá z několika částí, zabezpečující přesné dopravení dat na určené místo. Na začátku každého paketu je tzv. úvodní synchronizační úvodní skupina, která se skládá ze sekvence střídajících se jedniček a nul. Pokračuje informace, kam paket míří (cílová adresa) a odkud je vysílán (zdrojová adresa). Největší prostor paketu je vyhrazen množině bitů, tedy přenášených dat ukládaných do datového pole. Důležitost přenášených dat obsahuje struktura typu datového pole. Vše uzavírá pole kontrolního součtu (CRC), díky kterému ověřujeme správnost doručených dat a jejich shodnou podobu před odesláním. [3], [9]

Obr. 10 - Příklad podoby datového paketu

Zdroj: vlastní zpracování podle [9]

1.4.3 Rámec

V předchozí kapitole jsme se seznámili s paketem, ukázali si jeho strukturu a způsob jeho doporučení. Přesto se v literatuře setkáváme dále s pojmem rámec, který přímo navazuje na paket a upřesňuje detaily pro jeho správné doručení. Po rámci už následuje pouze samotné doručení skrz přenosové médium. Ve skutečnosti nám tak sítí putují až rámce, které si jednotlivé aktivní prvky předávají skrz vlastní fyzické adresy. Paket je z rámce vyjmut až těsně před jeho samotným rozbalením. Rámec, kromě fyzické cílové a zdrojové adresy jednotlivých uzlů, přidává také prvky zabezpečující ochranu proti případné ztrátě nebo interferenci dat. Před samotným odesláním dat totiž sítě využívají několika vrstev, kterými data musejí projít a v každé vrstvě jsou daná data doplněna o logický úkon, umožňující přenos informací mezi počítačovými systémy. Na význam jednotlivých vrstev se zaměříme dále. [3], [19]

1.4.4 Referenční model OSI

V počátcích počítačových sítí neexistoval jednotný univerzální systém, který by umožňoval komunikaci mezi prvky různých značek a platforem. Vznikali tak vlastní uzavřené a nekompatibilní systémy a jedinou možností bylo vystavět celou síť na jednom řešení. Při tehdejším počtu zařízení připojených do sítě to nebyl zase takový problém, ale představme si to v dnešním měřítku, v dnešním internetovém světě plném různými značkami a odlišnými typy zařízení. Z tohoto důvodu byl roku 1984 vyvinut organizací OSI referenční model OSI – Open Systems Interconnection. Můžeme se setkat též s označením modelu ISO/OSI. Model přesně definuje postup přemístění informace z aplikace v jednom počítači do druhého skrz síťové médium. Tímto způsobem byla vymezena struktura o celkově 7 vzájemně spolupracujících vrstvách. Informace postupuje od nejvyšší vrstvy (aplikační) po nejnižší (fyzická), kde je posléze transportována směrem k cíli, kde postupuje po vrstvách v opačném pořadí. Referenční model je modelem obecným, v němž jednotlivá vrstva reprezentuje skupinu souvisejících logických funkcí. Model tedy určuje souhrnnou funkci každé vrstvy a vzájemné chování mezi vyššími a nižšími vrstvami. „*Každá vrstva – logické seskupení úkolů – je dosti samostatná, takže úkoly definované ve vrstvě mohou být implementovány nezávisle. To umožňuje vývoj řešení s velkým množstvím funkcí, aniž by byly ovlivněny funkce jiných vrstev.*“ (Bigelow, 2004, s. 91)

Jak již bylo řečeno, model OSI definuje 7 vrstev, logických seskupení úkolů, které musí být splněny do okamžiku odeslání samotné informace do sítě. Dané vrstvy se dále rozdělují do dvou kategorií, na tzv. horní a dolní vrstvy. Horní vrstvy (5 – 7) přímo souvisí s aplikacemi a jejich implementace je obsažena pomocí softwarového řešení. Dolní vrstvy (1 – 4) zajišťují bezproblémový přenos informací v síti a jejich implementace souvisí více s hardwarovou úrovní nebo firmwarem. Zatímco u dolních vrstev se samotný fyzický přenos informace může lišit, horní vrstvy fungují ve většině případů stejně bez ohledu na platformu. Příkladem může být stav, kdy k přenosu informací u dolních vrstev využíváme kromě pevných sítí i bezdrátový přenos, ovšem aplikace z horní vrstvy (kupříkladu www, e-mail) funguje na obou typech připojení naprosto totožně. Daný model se stal základem pro každého výrobce síťových komponent či aplikací. Umožňuje pochopení principu fungování síťových prvků a patří k základní terminologii sítí. Nezbývá než si jednotlivé vrstvy alespoň v krátkosti představit pomocí tabulky níže.

Vrstva	Název vrstvy	Jednotky	Funkce vrstvy
7	**Aplikační**	data	Síťové procesy pro aplikaci, ověření uživatelů, vše závislé na aplikaci.
6	**Prezentační**	data	Reprezentace dat a šifrování. Řeší rozdíly v reprezentaci dat mezi aplikací a síťovým formátem - kóduje data pro přenos.
5	**Relační**	data	Komunikace jedné aplikace s druhou, posílání více dat po sobě. Udržuje celé spojení mezi dvěma počítači.
4	**Transportní**	segmenty	Zajišťuje kompletní přenos dat, kvalitu služby. Řeší spolehlivé odeslání všech dat ze zdroje do cíle pomocí segmentace a potvrzování.
3	**Síťová**	pakety	Směrování - určení cesty paketu, přenos dat z bodu do bodu, používá IP adresy. Komunikace mezi zdrojovým a cílovým zařízením pomocí IP adresy.
2	**Linková**	rámce	Fyzická adresace, detekce chyb, řízení toku a přístupu na médium. Komunikace mezi dvěma zařízeními v jedné podsíti (nebo na bránu) pomocí MAC adresy. Vytváří rámce (hlavička + data + zápatí).
1	**Fyzická**	bity	Fyzické parametry linky - média (kabely, rádio, světlo), signály a binární přenos. Řeší fyzické poslání dat (přenášeným bitům nepřiřazuje žádný význam).

Tabulka 1 - Vrstvy a funkce referenčního modelu ISO/OSI

Zdroj: vlastní zpracování podle [3]

Již při samotném vytváření daného modelu se však časem muselo ustoupit ze záměru striktně nahradit veškeré ostatní funkční modely právě modelem OSI. V praktickém využití sítí zvítězily jednodušší modely o méně vrstvách a daný model se odsunul do pozice modelu referenčního. V praxi zvítězil a stává se nejvíce užívaným model internetu (TCP/IP). Daný model byl standardizován dokonce dříve než model OSI, ale z již zmiňovaného referenčního modelu část jeho doporučení užívá. Model TCP/IP tolik nestandardizuje dolní vrstvy a počítá se s nasazením na již existující technologie, kterým ponechává dostatek prostoru pro dynamický vývoj. [2], [3], [9], [11]

1.4.5 Adresování zařízení v síti

Adresování zařízení v síti slouží k jedinečné identifikaci všech zařízení v síti. Každé zařízení v sítí má přidělenou svoji adresu, která je jedinečná, takže pro správné odlišení není možné, aby se v síti vyskytovaly dvě zařízení se společnou adresou. V současnosti je nepoužívanějším systémem adresování protokol IP, neboli Internet Protocol. Tento systém využívá logických adres na síťové vrstvě, označujících se jako adresy IP. „*Stejným způsobem, jakým používáme adresy v každodenním životě k označení určitých entit, označují síťové protokoly různé uzly v síti. Obecně vzato slouží adresy k označení určité budovy a PSČ se používá ke stanovení širokého, ale jasně daného regionu. Adresa IP se také skládá ze dvou částí: jedna označuje určitého hostitele a druhá síť, ve které se tento hostitel nachází.*“ (Bigelow, 2004, s. 103)

Struktura adresy IP

Původně navržené schéma pro adresy IP je složeno z 32 bitového čísla, kde je každý 1 Byte (8 bitů) oddělen pomocí tečky. Adresu je možné zapsat v základním dvojkovém tvaru po jednotlivých bitech, ovšem pro lepší pochopení ze strany uživatele se volí zápis v desítkové soustavě. Každý jeden Byte může nabývat hodnoty čísla 0 – 255 v desítkovém zápisu. Teoreticky můžeme nabývat hodnot 0.0.0.0 až 255.255.255.255, což v přepočtu představuje možnost použít více než 4 miliardy jedinečných adres. Samotná jedinečná IP adresa v sobě ukrývá kromě čísla konkrétního zařízení též číslo sítě, neboli segmentu, do kterého je zařízení přiřazeno. O tom, jak velká část adresy je věnována číslu síti a naopak číslu zařízení, rozhodují třídy adresy IP. Tříd IP adres je několik, ale nejvíce se užívají tři základní třídy adres označené A, B, C. Tabulka 2 ukazuje rozdělení bitů adresy podle zmiňovaných tříd, kde h = hostitel a s = síť.

Třída	Oblast čísel sítí	Počet bitů sítě	Oblast čísel zařízení	Počet bitů zařízení
A	0.h.h.h – 126.h.h.h	7	s.0.0.1 – s.255.255.254	24
B	128.0.h.h – 191.255.h.h	14	s.s.0.1 – s.s.255.254	16
C	192.0.0.h – 223.255.255.h	21	s.s.s.1 – s.s.s.254	8

Tabulka 2 - Rozdělení IP adres podle třídy

Zdroj: vlastní zpracování podle [2]

Určíme si kupříkladu IP adresu 192.168.14.100, kde díky prvnímu Bajtu vidíme, že spadá do oblasti sítí 192 – 223. Jedná se o adresu třídy C a adresám zařízení patří pouze poslední Bajt. V dané síti může být tedy maximálně 254 zařízení. [2], [19]

Použití podsítí

Předchozí zmiňovaná struktura rozdělení IP adres, které jsou definovány v každé třídě, se stala do budoucna velmi neefektivní. Pomocí podsítí dosáhneme možnosti vytvořit více než jednu síťovou adresu, případně rozšířit počet sítí v jedné společnosti. Podsítí označujeme samostatnou část počítačové sítě. Kolik adres se v dané podsíti používá, určuje tzv. maska sítě. Maska obsahuje strukturu adres sloužící ke stanovení, které bity z 32 bitové adresy patří adrese sítě. Navážeme-li na předchozí kapitolu a zvolíme již zmiňovanou IP adresu 192.168.14.100, patřící do třídy C, maska bude mít podobu 11111111.11111111.11111111.00000000 B. Ve výsledku to znamená, že jsou v masce nastaveny na jedničku bity, odpovídající části síťové adresy, zatímco nuly reprezentují bity hostitelské adresy. V dekadické soustavě vypadá zápis masky 255.255.255.0. Hodnotu podsítě je možné vyjádřit také pomocí prefixu. Jedná se o notaci vyjadřující počet jedniček zleva. Zápis pro daný příklad by byl 192.168.14.100/**24**. [2], [20]

Privátní IP adresy

Vzhledem k omezenému počtu jedinečných IP adres a nárůstu zařízení v síti bylo postupem času jasné, že současné řešení nemůže vydržet do nekonečna a nastane den, kdy adresy jednoduše dojdou. Jedním z řešení pro částečné omezení úbytku IP adres bylo vyhrazení privátních IP adres. Jedná se o třídy přesně vyhrazených IP adres, které lze využít opakovaně. Dané IP adresy jsou určeny pro použití v tzv. privátních sítích, konkrétně převážně v lokálních sítích LAN. Podmínkou pro jejich použití je užívat jich v sítích, které nejsou přímo dostupné z veřejné sítě. Zařízení, které má přidělenou takovou IP adresu, se na internetu signalizuje veřejnou IP adresou nejbližšího aktivního prvku, který mu obstarává přístup dále do sítě. Nejjednodušším řešením je využití služby NAT, o které se zmíníme dále v problematice zabezpečení sítí. Dané řešení se v současnosti využívá ve většině domácích i firemních sítích. O které IP adresy se konkrétně jedná, naznačuje tabulka 3. [3], [19]

Třída	Síť	Adresa sítě	Adresy hostů
A	10.0.0.0/8	10.0.0.0	10.0.0.1 - 10.255.255.254
B	172.16.0.0/12	172.16.0.0	172.16.0.1 - 172.31.255.254
C	192.168.0.0/16	192.168.0.0	192.168.0.1 - 192.168.255.254

Tabulka 3 - Vyhrazené privátní IP adresy

Zdroj: vlastní zpracování podle [3]

Nová generace IP adres

V polovině 90. let 20. století byl položen základ pro postupné vytvoření nového modelu, který by nahradil současný systém adres. Potřeba vytvoření nového protokolu internetu vznikla především z důvodu reakce na rychlé vyčerpání adres původního internet protokolu, označovaného jako IPv4. Nový systém se označuje jako IPv6 a kromě dostatečně bohatého adresního prostoru nabízí i některé nové vlastnosti. Oproti původní hodnotě 32 bitů adresy vzrostla adresa čtyřnásobně, tedy na délku 128 bitů. Pro lepší představu, na každého obyvatele planety připadá bezmála 30 tisíc síťových prefixů a každý prefix pojme 65 tisíc podsítí. Jednotlivá síť posléze dovede rozlišit miliardy miliard koncových zařízení, což vypovídá o dostatečně velké rezervě budoucích adres. Zápis nových adres probíhá výhradně v šestnáctkové soustavě, kde jsou jednotlivé dvojice Bajtů (čtveřice šestnáctkových číslic) odděleny dvojtečkami. Příklad podoby adresy zařízení IPv6: *2001:0db8:7654:3210:fedc:ba98:7654:3210*. Zápis je možné zkrátit vynecháním počáteční nuly nebo náhradou dvojtečkami v případě, kde se vyskytuje několik po sobě jdoucích nulových skupin. Zápis prefixu je totožný s IPv4, konkrétně *adresa/**délka***.

Následující trojice zápisů adresy IPv6 je tedy plně ekvivalentní:

ff01:0000:0000:0000:0000:0000:0000:0101
ff01:0:0:0:0:0:0:101
ff01::101

Význam použití protokolu IPv6 je v současnosti kladen na prostředí internetu. Jeho plné nasazení bylo dočasně zmraženo z důvodu nacházení dalších nových řešení též na bázi původního IPv4. Počátkem 21. století se navíc zdálo, že adresy IPv4 vydrží přinejmenším na dalších 20 let. Z tohoto důvodu byl zájem o nasazování nového protokolu spíše mizivý. Centrální zásoba adres IPv4 však byla v únoru roku 2011 vyčerpána a zájem o IPv6 se zvýšil. Nevýhodou je, že protokol IPv6 není zpětně kompatibilní s původní verzí. Tento fakt lze částečně vyřešit použitím konvertorů, ovšem ty nadále musí využívat adresu IPv4. Nebude to však již dlouho trvat a IPv6 se stane hlavním komunikačním protokolem budoucnosti. [3], [5]

1.5 Hardwarové prvky sítí

Hardwarem označujeme veškeré ústrojí, které jsme schopni fyzicky vidět a ohmatat jej. Mezi hardwarové prvky sítí řadíme veškerá zařízení a příslušenství, které dopomáhají k přenosu, zesílení, opakování, směrování či přečtení informace vyskytující se napříč síťového prostředí. Daný hardware ovlivňuje konečnou kvalitu, rychlost, odezvu, modularitu a globální výkon sítě. Prvky sítí dále rozdělujeme podle základních kritérií na pasivní prvky sítí a aktivní prvky sítí. Pomocí pasivních prvků dosahujeme spojení mezi aktivními prvky, přenášejí také signál z aktivních prvků, ale dále nijak neovlivňují tok signálu. Řadíme mezi ně například kabeláž, konektory, antény. Aktivní prvky se již podle názvu podílejí na způsobu šíření, zesílení nebo upravení signálu (informace). Patří mezi ně pojmy jako například rozbočovač, přepínač, směrovač, most nebo brána. Největší rozdíly mezi aktivními prvky jsou jejich rozdílné úrovně postavení práce lišící se úrovní vrstvy modelu ISO/OSI. [2], [9]

S mobilním věkem se též zvyšuje zastoupení prvků šířící informace pomocí bezdrátového signálu. Konkrétně v lokálních sítích (Wi-Fi) jejich síla pomalu začíná přesahovat. O této tématice se v krátkosti zmíníme v samostatné kapitole níže.

1.5.1 Kabely a konektory

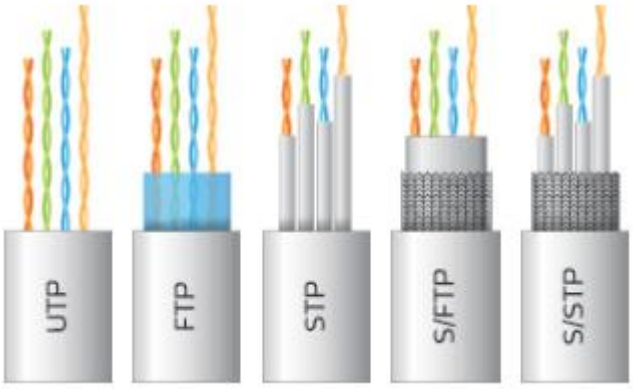
Od počátků prvních počítačových sítí již několik desetiletí uběhlo. Stejně jako se vyvíjel síťový standard a přenosové rychlosti se zvyšovaly, musely jej následovat též přenosová média. Jednou z nejdůležitějších vlastností síťových kabelů je totiž právě rychlost, s jakou mohou přenášet data. Data v počítačových sítích jsou šířena sériově (bity řazeny za sebou). Rychlost se vyjadřuje počtem bitů přenesených za jednotky času, konkrétně megabitech za sekundu (Mb/s). V následující kapitole se zaměříme převážně na, v současnosti nejpoužívanější, kabely a konektory.

Kroucená dvoulinka

Princip kroucené dvoulinky vychází původně z telefonního kabelu. Oproti původnímu telefonnímu kabelu však obsahuje vyšší počet vodičů. Konkrétní počet vodičů kroucené dvoulinky pro potřeby počítačových sítí je osm, což představuje čtveřici vzájemně kroucených párů. Kroucení představuje určitý stupeň ochrany proti působení rušení od sousedních páru vodičů, případně cizího elektromagnetického pole. Varianty kroucené dvoulinky jsou dnes nejrozšířenějším metalickým vodičem v sítích LAN.

Podle stupně vývoje a přenosové rychlosti dělíme kroucenou dvoulinku do kategorií. V praxi se nejpočetněji setkáme s kabely kategorie 5 nebo 5e (e = extended, rozšířené). Obě kategorie kabelů mají totožný počet párů vodičů, totožný typ konektorů, ale rozdílné přenosové rychlosti. Maximální přenosová rychlost pro kabely kategorie 5 je 100 Mb/s, kabely kategorie 5e dovolují přenos až 1000 Mb/s (1 Gb/s). Rozdíl představuje odlišná vnitřní konstrukce kabelu dovolující zvyšování šířky přenosového pásma. Šířku pásma si nejjednodušeji představíme na vodovodní trubce. Stačí použít vetší průměr trubky a za jednotku času nám oproti trubce užší proteče větší množství vody. Kategorie se dále vyvíjí a v současnosti se můžeme setkat s kabely kategorie 6, 6a a 7, kde se přenosové rychlost dostává na hranici 10 Gb/s. Pro dosažení normovaných přenosových rychlostí je nutné, aby ostatní kabelové a aktivní prvky odpovídaly kategorii kabelu.

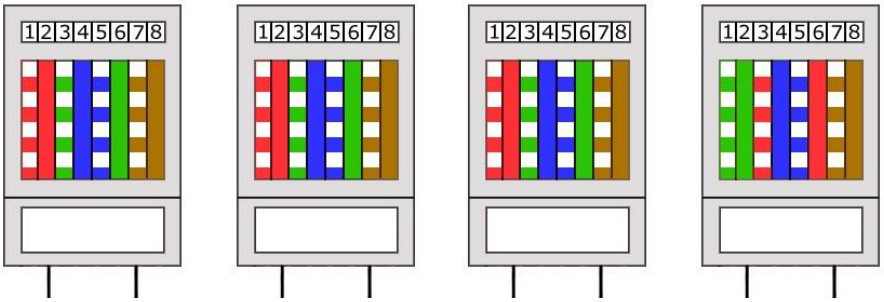
Podle stupně ochrany proti rušení rozlišujeme kroucenou dvoulinku jako nestíněnou – UTP a stíněnou – STP, FTP, S/FTP, S/STP. UTP obsahuje jednotlivé vzájemně kroucené páry, které jsou chráněny pomocí vnější plastické izolace. Cenově nejpřijatelnější a nejpoužívanější kabeláží sítí je LAN. V průmyslových prostředí s vysokým vnějším rušením je nutné nasadit variantu stínění spočívající v přídavném metalickém opletení. Stínění může být několikaúrovňové: stínění každého páru (STP), stínění pláště (FTP), současné stínění každého páru a pláště (S/STP). U stíněných kabelů je dále nutné použít konektory s kovovým opletením, aby došlo k uzemnění.



Obr. 11 - Druhy kroucené dvoulinky podle stupně ochrany

Zdroj: [22]

Nejpoužívanějším konektorem pro kroucenou dvoulinku je RJ-45. Oba dráty jednoho krouceného páru mají stejný barevný základ, ale vždy jeden z dvojice je navíc kombinovaný s bílou barvou. Barevné odlišení odpovídá normě a slouží k identickému zapojení na obou stranách kabelu. Užívanými barvami jednotlivých párů jsou oranžová, zelená, modrá, hnědá. Před osazením konektoru je nutné všechny páry částečně rozdělit a seřadit za sebou. Řazení vodičů odpovídá normě T1A/EIA 568-A nebo 568-B. Varianta B je alespoň u nás rozšířenější. Seřazení vodičů do konektoru může být na obou stranách totožné, rozdíl musí nastat v případě, že spolu propojujeme zařízení stejného typu (počítač-počítač). V daném případě musím použít tzv. křížený kabel, který má na jedné straně přehozené páry 1-2 a 3-6. Jinak řečeno, na obou koncích kabelu je nutné použít obě normy pro zapojení konektoru RJ-45. Po správném nasazení se konektor na kabel lisuje pomocí speciálních kleští. [2], [3], [9], [11]



Obr. 12 - Princip zapojení nekřížené / křížené kroucené dvoulinky

Zdroj: [33]

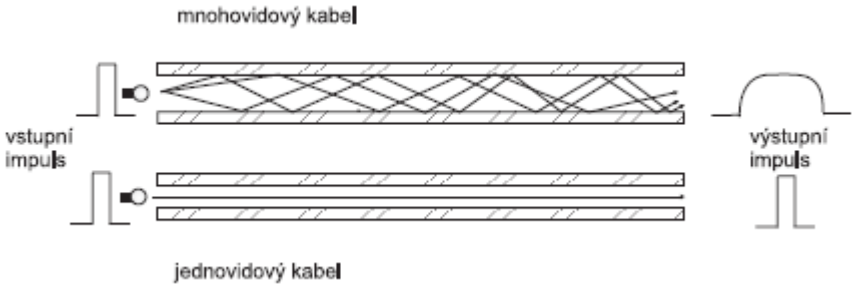
Optický kabel

Oproti předchozímu typu kabelu pracuje na naprosto odlišném principu. K šíření informací neslouží elektrické impulsy, ale světelné impulsy ve světelně vodivých vláknech. Výhodou optického kabelu je možnost přenášet signál rychleji a hlavně mnohem dále oproti ostatním druhům kabelů. Základním prvkem kabelu je optické vlákno, které je vždy umístěno v páru (několik párů). Vlákno je ve vrstvě sekundární ochrany, zabraňující mikro ohybům kabelu, které by tlumily průchod světelného paprsku. Posledním prvkem kabelu je konstrukční vrstva zvyšující pevnost kabelu a plastový vnější obal. Cena optického kabelu je výrazně vyšší a správná instalace vyžaduje drahé specializované nástroje, jejichž cena přesahuje stotisícové částky, a zkušenosti. Použití optických kabelů se většinou využívá spíše v páteřních vedeních a spojení síťových segmentů mezi budovami. V současnosti se dále mohou objevit u serverů a dovolují účinnější a rychlejší přenos.

Obr. 13 - Struktura optického kabelu

Zdroj: [9]

Podle způsobu vedení paprsku v optickém vlákně se rozlišují kabely mnohovidové a jednovidové. Mnohovidové kabely využívají odrazu světelného paprsku od pláště vlákna. Během přenosu dochází k rozložení světelného paprsku na více světelných částí. Na konci dochází k součtu doražených vidů a složení původní informace. Kabel má horší optické vlastnosti, ale nižší cenu a lépe se s ním pracuje. Jednovidové kabely mají minimální index lomu mezi jádrem a pláštěm optického vlákna. Kabelem díky tomu prochází jeden paprsek bez lomů a ohybů. Výsledkem je vyšší přenosová kapacita a možnost přenášet signál na dlouhé vzdálenosti bez nutnosti jeho obnovování. Cena oproti předchozímu provedení je však vyšší.



Obr. 14 - Způsoby vedení světelného paprsku v optickém vlákně

Zdroj: [9]

Kabel využívá dva typy konektorů: kulatý konektor (ST), hranatý konektor (SC). Z důvodu využívání odlišného média pro šíření signálu je nutné využívat převodníků. Ty zajišťují převod světelných impulsů na elektrické signály a naopak. Převodníky se dají pořídit samostatně, případně jsou přímo zabudovány v přepínačích nebo směrovačích. [2], [9], [27]

1.5.2 Aktivní prvky sítě

Kromě síťové karty počítače nebo jiného klientského zařízení nalezneme v počítačových sítích další aktivní prvky vložené do kabeláže (přenosového média). Dané prvky pomáhají aktivně s děním na síti a zajišťují úspěšnou komunikaci. Práce jednotlivých prvků přesně vychází z referenčního modelu OSI. Díky tomu jsme schopni v sítí rozlišit prvky podle jejich postavení a rozložit poměrně složité úkoly. Také aktivní prvky prošly za dobu své existence vývojem a rozšířily pole svého fungování, případně byly časem nahrazeny prvky inteligentnějšími, které méně zatěžují provoz na síti. V dané kapitole se pozastavíme převážně nad v současnosti nejužívanějšími prvky, ale pro porovnání se krátce zmíníme i o prvcích, které v současnosti budovaných sítích sice nenalezneme, ovšem v časově starších sítích je možné je stále zaznamenat. [2], [9], [10]

Opakovač (repeater)

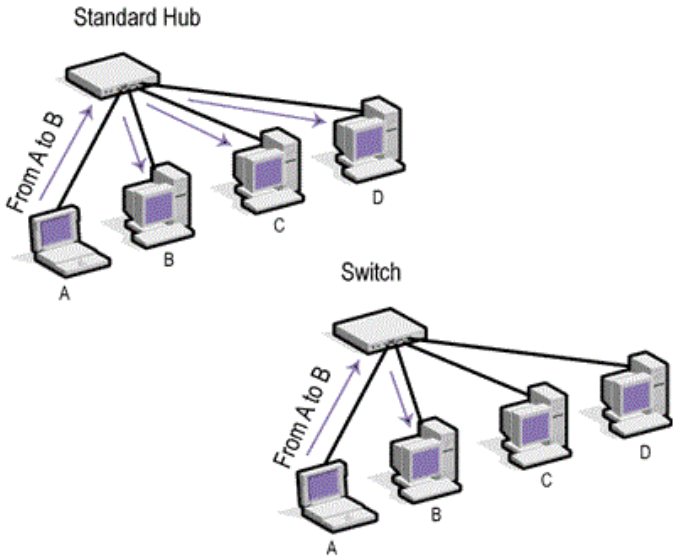
Tento konstrukčně jednoduchý prvek bylo možné hojně zaznamenat v sítích využívající koaxiální kabely, tedy sběrnicové topologie. V současných sítích je spíše výjimkou, ale je stále možné využít jeho daný potenciál. Vlivem vzdálenosti dochází k útlumu elektrického signálu, jeho degradaci a zkreslování. Činnost spočívá v zesílení signálu jím procházejícím, kdy dochází opakovanému navýšení jeho amplitudy. Opakovače je možné použít vždy k zesílení sítě stejného protokolu a rámce. Nejedná se o prvek inteligentní. Chybná data nebudou filtrována a nadměrný provoz sítě nebude nijak řízen. Z pohledu referenčního modelu OSI pracuje opakovač na nejnižší vrstvě, čili vrstvě fyzické. [2], [9], [10]

Rozbočovač (hub)

Rozbočovač bylo možné prvně zaznamenat v sítích využívajících hvězdicovou topologii. Jeho základním úkolem bylo jednotlivé propojení více koncových zařízení v síti. Dále v něm dochází k obnovení a znovu odeslání signálu, stejně jako v případě opakovače. Počet portů zůstává většinou sudého čísla a nejčastěji se v síti vyskytovaly rozbočovače o osmi, dvanácti, šestnácti nebo dvaceti čtyřech portech. Stejně jako opakovač pracuje rozbočovač na nejnižší vrstvě modelu OSI. Rozbočovač nerozlišuje jednotlivé pakety nebo rámce. Příchozí tok bitů jednoduše odešle po všech jeho portech. Zahlcuje tak síťový tok a rozšiřuje kolizní domény. V dnešní době je nahrazován přepínači, ale stále je možné je ve starších sítích zaznamenat. [2], [9], [10]

Přepínač (switch)

Nejpoužívanější normou definující práci současných sítí je varianta normy Ethernet, využívající přístupovou metodu zajišťující kontrolu přenosového média CSMA/CD. Přes svoji účinnost obsahuje tato metoda značnou nevýhodu v podobě postupného zahlcování provozu a zvyšování odezvy v případě strmého nárůstu počtu zařízení v síti. Díky využití přepínače můžeme tuto nevýhodu výrazně eliminovat. Přepínač totiž dokáže oddělit komunikující stanice od zbytku sítě vytvořením virtuálního okruhu mezi momentálně komunikujícími zařízeními. Máme-li na přepínači připojeno větší množství zařízení a komunikace probíhá pouze mezi dvojicí zařízení, nejsou díky virtuálnímu okruhu momentálně nekomunikující stanice zahlcovány cizími pakety, jako v případě rozbočovače. Nedochází ke zpomalování odezvy sítě a přenosová rychlost mezi koncovými zařízeními probíhá na maximu. Stejně jako v případě rozbočovače, počet portů odpovídá násobku sudých čísel. V současné době není problém setkat se s přepínačem obsahující i čtyřicet osm portů. Z pohledu referenčního modelu OSI pracuje přepínač na druhé vrstvě – linkové. Na této vrstvě se vyskytují rámce obsahující informace o fyzických adresách (MAC adresy) komunikujících zařízení. Přepínač s danými adresami pracuje a ukládá je do své interní paměti. Podle obsahu paměti dokáže filtrovat rámce a zajistit jeho rychlé přepnutí dále směrem ke správnému portu a zařízení za ním. Rámec je tak schopný nezatěžovat ostatní připojené zařízení, případně celé segmenty. Dále přepínač podporuje vytváření virtuálních lokálních sít. Přepínače hojně nahrazují práci rozbočovačů.



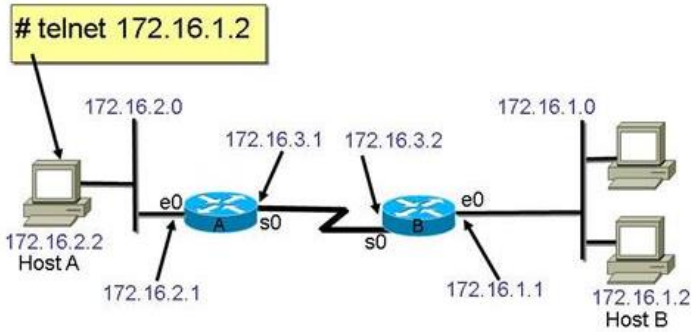
Obr. 15 - Rozdíl šíření signálu rozbočovače (hub) a přepínače (switch)

Zdroj: [14]

Ve spojitosti s přepínačem se můžeme dále setkat ještě s názvem most. Most může být odlišné zařízení v síti, má však podobné vlastnosti jako přepínač. Most je generačně starším zařízením a jeho hlavním úkolem je oddělování síťových segmentů. Oddělování segmentů je v mostech řešeno softwarově a u přepínačů hardwarově, díky čemuž pracují přepínače rychleji. Hlavním rozdílem je skutečnost, že most umožňuje propojení sítí o dvou rozdílných standardech. V současnosti se můžeme setkat například s pojmem bezdrátového mostu, což je v sítích Wi-Fi přístupový bod (AP). [2], [9], [10], [11]

Směrovač (router)

S aktivním využíváním směrovače se dostáváme do odvětví složitějších síťových prostředí. V těchto sítích již dochází k využívání více segmentů a podsítí. Pro tyto účely musíme použít sofistikovanější prvek, který nejen zná adresy každého segmentu, ale určuje nejvhodnější cestu pro odesílání dat a filtruje data na místních segmentech. Tento prvek označujeme jako směrovač a pracuje podle předpokladů třetí vrstvy modelu OSI – síťové. Pracuje tak přímo s pakety, od kterých získává více informací a zdokonaluje tak jejich přenos, případně správné směřování dále v síti. Směrovač se využívá v případech výměny informací mezi dvojicí zařízení na různých podsítích. Stanice, která zná logické adresy pouze ve své části segmentu sítě a dále nevidí, v případě potřeby komunikace se zařízením z odlišného segmentu odešle data přímo na směrovač. Směrovač podle cílové logické adresy paketu pozná, komu data patří. Pokud je cílové zařízení (jeho podsíť) dostupné přímo ze směrovače, informace jsou doručeny. Případně jsou data předána na zpracování dalšímu směrovači v cestě, který je zpracuje identicky. Tímto způsoben jsou data směřována až k samotné cílové IP adrese. Pakety jsou tak efektivně směřovány a dopravovány skrz rozsáhlé sítě, i přes skutečnost, že se počítače nevidí a mají tedy rozdílné adresy sítě.



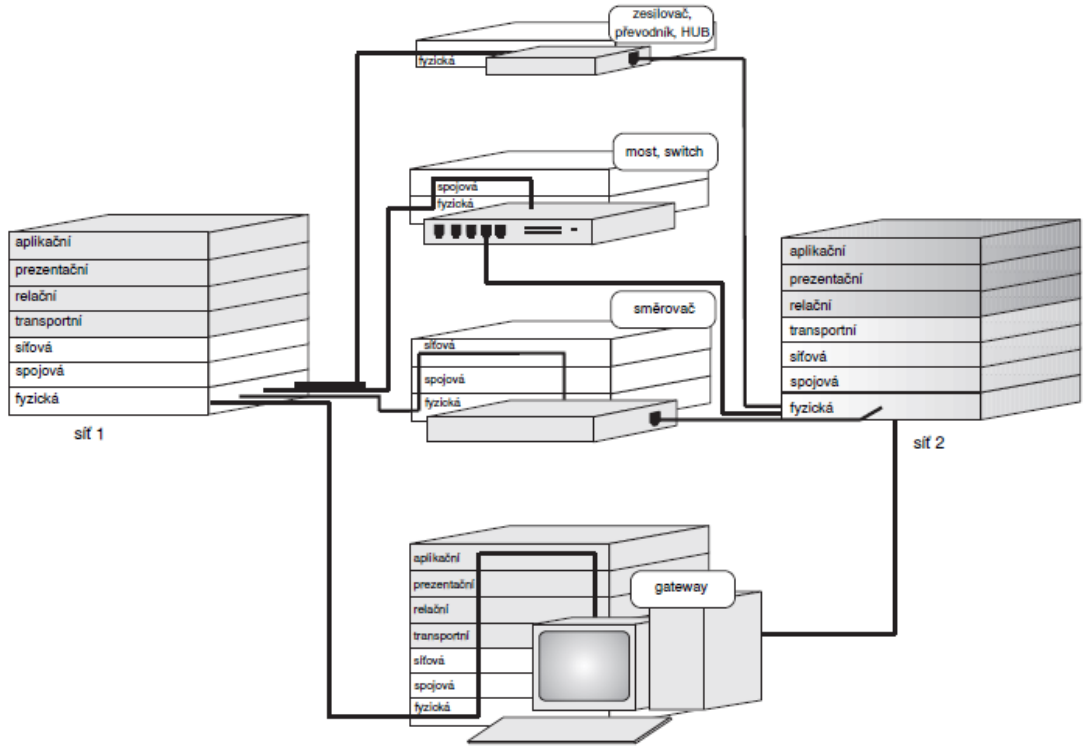
Obr. 16 - Příklad směrování přenosu z hostitelské stanice A na stanici B

Zdroj: [8]

Směrování může být řízeno pomocí dvou základních protokolů: staticky a dynamicky. Statické směrování je vždy závislé na ručním zadání možných cest paketů přímo ze strany administrátora. Výsledná směrovací tabulka je pevně daná a směrování paketů probíhá vždy stejnou cestu. Tento typ směrování je použitelný v menších sítích o několika segmentech a směrovačích. V případě rozsáhlé sítě musíme optimálně sledovat nejkratší trasy paketů pro co nejmenší odezvu. K daným účelům slouží dynamická volba optimální cesty, která je užívána například na straně internetu. Směrovač je schopný automaticky volit nejoptimálnější trasu paketu a přizpůsobovat se měnícím se podmínkám sítě. Takové směrování je vysoce náročné na konfiguraci. Je však vysoce efektivní v případě výpadku sítě a využití záložních tras pro úspěšné dopravení paketu do požadovaného cíle. [2], [10]

Brána (gateway)

Funkcí brány je možnost připojení radikálně odlišných sítí. Díky jejímu fungování na nejvyšší aplikační vrstvě dochází k efektivnímu přetváření paketů a převádění dat z jednoho typu sítě do jiného typu sítě. Zařízení z obou sítí tedy rozumí datům toho druhého. Z větší části jsou brány účelně úkolově specifické a vyhrazené pro určitý typ přenosu. [2], [9], [10]



Obr. 17 - Spojení dvou sítí pomocí jednotlivých aktivních prvků s ohledem na OSI

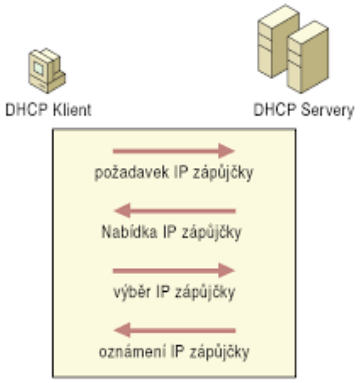
Zdroj: [9]

1.6 Síťové služby

V současných počítačových sítích je k dispozici řada služeb, které nejen obstarávají správný průběh komunikace, ale také ulehčují práci správcům a pomáhají uživatelům. V dané kapitole si krátce představíme minimální základ služeb, které by neměly chybět v žádné velké i malé organizaci. Některé z nich již všichni hojně využíváme ve svých domácnostech a pomáhají nám s prací na síti. Konkrétně se služby zaměřují na vhodnou identifikaci počítačů a jiných zařízení v síti, pomáhají nalézt objekty a slouží k přizpůsobení prostředí celosvětové sítě Internet. [2]

1.6.1 Služba pro dynamické přidělování adres

Službu, respektive protokol, je možné zaznamenat pod názvem DHCP (Dynamic Host Configuration Protocol). Cílem je zjednodušit správu konfigurace logických adres zařízení připojených k síti TCP/IP. Adresy IP a s nimi související data jsou centrálně řízena serverem, který po připojení do sítě automaticky přiřazuje zařízením adresy. Nakonfigurovaný DHCP server obsahuje databázi dostupných adres. Kromě samotné IP adresy služba dále automaticky přiděluje adresy brány, serverů doménových jmen nebo například název výchozí domény. Aby byla služba provozuschopná, musí být kromě správně nakonfigurovaného serveru nastaveno u jednotlivých klientů automatické přidělování IP adres. IP adresa je přiřazena ihned po první inicializaci klienta v síti. Přiřazená IP adresa je časově omezena. „*Tento proces se označuje jako zápůjčka. Zápůjčky mohou být čas od času obnoveny, což zajišťuje relaci bez přerušování. Zápůjčky jsou obnovovány po uplynutí zhruba poloviny jejich délky. Je-li obnovení úspěšné, zůstává adres IP přiřazena klientovi. Pokud není úspěšné, vrátí se adresa IP do fondu adres pro jiného uživatele.*“ (Bigelow, 2004, s. 167) [2], [26]



Obr. 18 - Postup inicializace přiřazení dynamické IP adresy

Zdroj: [12]

1.6.2 Služba pro přidělování názvů

O adresování pomocí jedinečných logických adres jsme si již řekli. Pomocí těchto adres jsou zařízení schopna zjistit, kde je odkazované zařízení umístěno a zahájit komunikaci. Vzhledem ke skutečnosti, že musíme práci v síti povýšit též na úroveň uživatelskou, možná obecněji lépe řečeno na úroveň lidskou, využíváme služeb pro přidělování názvů. Trik spočívá v jednoduchém nahrazení číselného souboru jedinečné logické adresy za lépe zapamatovatelný název – jméno. Kupříkladu vyskytuje se v naší síti zařízení s IP adresou 192.168.11.54, přidáme k němu pomocí dané služby lépe zapamatovatelný název pro člověka, tedy „U2-PC01“. Budeme-li se posléze na daný počítač odvolávat, je možné napsat pouze jeho název. Název je přeložen službou pro přidělování názvů na jeho logickou adresu, aby jej mohlo zdrojové zařízení identifikovat. Nejznámější službou pro tyto účely je v současnosti služba DNS (Domain Name System). Původně se DNS využívala pro potřeby sítě Internet, ovšem nasazuje se již běžně i v místních sítích LAN. Ve spojení s internetem je nejjednodušším příkladem přístup k webovým serverům. Zadáme-li do našeho webového prohlížeče název **www.seznam.cz**, DNS server jej přeloží na veřejnou IP adresu **77.75.79.39**. Kdybychom do svého prohlížeče zadali tuto veřejnou IP, dostali bychom se na totožné místo. Otázkou je, co se lépe pamatuje, že? [2]

Obr. 19 - Vyhledání jedinečné logické adresy pomocí názvu přes službu DNS

Zdroj: [26]

1.6.3 Adresářové služby

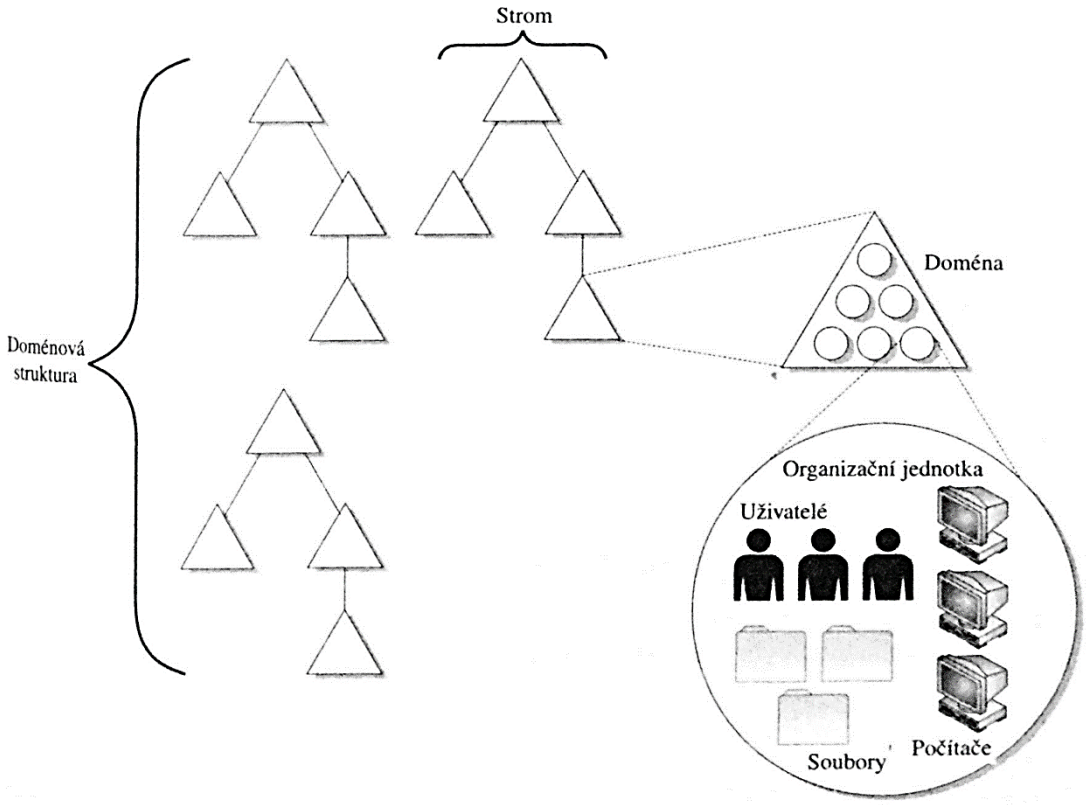
Na úvod si vybavíme situaci, kdy máme člověka, o kterém potřebujeme například zjistit jeho telefonní číslo nebo místo bydliště. V takovém případě je nejzákladnějším dokumentem telefonní seznam, zlaté stránky nebo vlastní kontakty. Jedná se o strukturovaný dokument obsahující alespoň základní informace, které potřebujeme znát ke splnění našeho cíle. Nyní celou teorii přenesme do oblasti počítačových sítí, kde potřebujeme identifikovat nějaký typ objektu v síti. Objektem může být

uživatelský profil, skupina uživatelů, počítače, tiskárny, složky a soubory. Adresářová služba se od příkladu na začátku příliš neliší. Jedná se o centrálně distribuovaný adresář, který je uložený na serveru a obsahuje veškeré potřebné informace o objektech v dané síti. Celek využívající adresářové služby též nazýváme jako **doména.** Doména dále kromě výše zmíněného obsahuje například informace o právech jednotlivých skupin uživatelů, zabezpečení, centrální správu hesel, způsoby ověřování nebo možnost automatického odesílání aktualizací softwaru. Adresář je centrální, usnadňuje správu množství objektů a uživatelům dává možnost přistupovat ke všem objektům domény jednotnými přihlašovacími údaji. V současnosti nejvyužívanější adresářovou službou je služba Active Directory od společnosti Microsoft, o které si dále napíšeme více detailů. Je nutné poznamenat, že základ je stejný pro ostatní adresářové služby jiných společností. [2], [9]

Databáze Active Directory

Potřebujeme-li centrálně spravovat větší organizaci, je databáze Active Directory (AD) tou správnou volbou. Jedná se o databázi celé sítě organizace spravující seznamy dat, týkající se různých atributů (vlastností) objektů daného systému. Celou databázi je možné rozdělit do dvou struktur, na strukturu logickou a fyzickou. [2], [9]

Logická struktura konkrétně neřeší skutečné umístění síťových prvků v prostoru. Vše vychází ze základního prvku, nazývaného jako **objekt**. Objekt je množina vlastností zastupující daný síťový prostředek například v podobě uživatelského účtu, skupiny, počítače nebo sdílené složky. Jednotlivé objekty je možné dále seskupovat do kontejnerů. Kontejner je vyšším objektem databáze, do kterého se ukládají objekty i další kontejnery. Nejnižším stupněm kontejneru se nazývá **organizační jednotka**, představující administrativní skupinu organizace – oddělení, ročník, třída. Uspořádáme-li libovolně více objektů a organizačních jednotek dohromady, vznikne doména, tedy základní jednotka celé logické struktury Acive Directory. Objekty a jednotky můžeme v doméně vnořovat do sebe nebo stavět na stejnou úroveň. V jedné organizaci většinou využíváme jedné domény. Databáze Active Directory ovšem umožňuje možnost obhospodařování několika doménami, jejichž vnitřní struktura je rozdílná. Jedna doména si udržuje informace pouze o svých vlastních objektech a do objektů jiné domény nemá přístup. Přístup můžeme částečně zaručit, sestavíme-li **strom** a vytvoříme topologii logicky podobnou topologii hvězda. [2], [9]



Obr. 20 - Struktura adresářové služby databáze Active Directory

Zdroj: [2]

Fyzická struktura se zaměřuje na fyzické vlastnosti prostoru, kde je databáze uložena. Údaje o objektech domény se většinou ukládají na vyhrazený server, který posléze nazýváme jako **řadič domény**. Řadič domény můžeme nakonfigurovat na operačním systému Microsoft Windows Server, což je specializovaný síťový operační systém pro potřeby serverových služeb. Máme-li více serverů sloužících jako řadič domény, můžeme využít prvku redundance. Řadiče domény jsou v případě výpadku vzájemně zastupitelné a změna na jednom řadiči je automaticky migrována na zbytek řadičů. Umístění řadičů domény se může geograficky lišit. Pokud však jsou součástí jedné domény (databáze AD), spolupracují spolu v jedné síti. Minimální sestava pro provoz dané adresářové služby je jeden řadič domény a klientské stanice organizace zařazené do společné domény spravující řadičem domény. Kromě stanic je možné do domény zařadit další server bez funkce řadiče domény. Takový server se nazývá serverem členským a bude poskytovat jiné služby klientům v doméně. Databáze AD plně využívá služeb názvových serverů DNS a dynamicky aktualizuje logické adresy všech členských zařízení domény. Instalace DNS serveru se službou Active Directory je tedy podmínkou. [2], [3], [9]

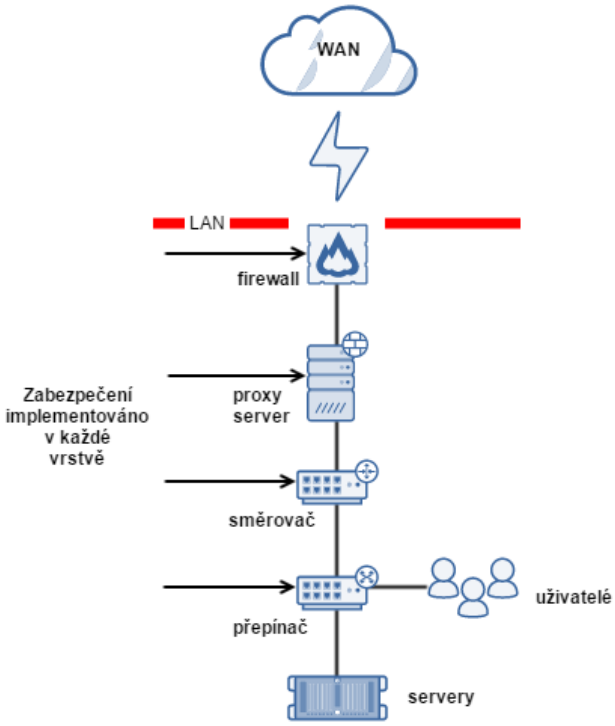
1.7 Bezpečnost počítačových sítí a její zásady

O bezpečnosti počítačových sítí bylo vydáno na několik desítek knih, jejichž průměrná délka přesahuje 450 stran. Obecně se jedná o vysoce závažné téma, které v některých případech dokonce zajišťuje existenci některých společností. Denně na celém světě proběhne tisíce v počátku převážně nevinných útoků, které se časem můžou obrátit v závažný problém. Útoky se již netýkají pouze velkých organizací, ale s rozmachem sítě Internet jsou zasažitelné též malé podniky a dokonce jednotliví uživatelé. Právě tyto objekty totiž zabezpečení stále podceňují a nemluvíme zde pouze o bezpečnosti hesla typu „*12345*“. V následující kapitole se převážně pozastavíme nad přehledem bezpečnostních technologií a představíme si alespoň ty nejzákladnější prvky, zlepšující bezpečnost naší vnitřní sítě.

1.7.1 Základní principy zabezpečení

Vrstvená bezpečnost

Není možné se při zamýšlení nad bezpečností sítě opírat pouze o jedno obranné místo. Je správné rozdělit zabezpečení na více vrstev. Vhodný návrh vychází ze zabezpečení implementované konzistentně ve všech aktivních prvcích sítě.



Obr. 21 - Vrstvená bezpečnost sítě

Zdroj: vlastní zpracování podle [28]

Řízení přístupu

Za provoz sítě odpovídá správce, který může dále určit, kdo nebo co bude mít přístup do sítě. Doporučuje se zásada politiky nejmenších oprávnění. Tato politika při veškerých rozhodnutích o přístupu vychází ze situace: „*veškerou komunikaci nejprve zablokovat a posléze výslovně povolit pouze to, co daný objekt potřebuje ke své práci*“. Touto politikou jsme alespoň částečně schopni zakázat veškerá zadní vrátka pro prolomení přístupu do sítě. Tento režim chování se převážně objevuje u prvků, které nazýváme jako Firewall. Dále je nutné předem definovat skupiny oprávnění a rozhodovat o míře důvěry jednotlivých objektů v síti. Obecně řečeno, skupina učitelů by měla v síti vlastnit vyšší práva než skupina studentů a možnost tak využívat více prostředků sítě či přístupů.

Uvědomění uživatelů

Zaručit školení uživatelů a posílení jejich uvědomění v otázkách bezpečnosti. V jistém směru se to dá ošetřit s využitím zásad adresářových služeb, kde můžeme definovat platnost uživatelských hesel, jejich minimální délku nebo nemožnost opakování předchozího hesla. Dále je nutné podpořit paměť uživatelů, aby se hesla do systémů nevyskytovaly na papírku hned vedle klávesnice. Zaručí se tak mírně dalším nepříjemnostem.

Monitorování

Každé kvalitní zabezpečení je nutné zpětně kontrolovat či sledovat. Každá organizace by měla tyto jednotlivé systémy průběžně monitorovat a ověřovat jejich bezpečnost či odolnost vůči útokům. Jedná se převážně o speciální detekční systémy a logování provozu.

Aktualizace systému

Pravidelně aktualizovaný systém nám zaručí aktuálnost veškerého kódu obsahující bezpečností záplaty, řešící chyby systému během jeho životnosti. Nejvhodnějším řešením je nastavení automatických aktualizací ve spojení s centrální databází aktualizací přímo uvnitř naší lokální sítě. Zamezí se dlouhodobému přehlížení neaktuálního softwaru. Navíc ve spojení s databází aktualizací zefektivníme využitelnost sítě a zamezíme zahlcování linky do internetu.

[2], [3], [28], [31]

1.7.2 Filtrování paketů

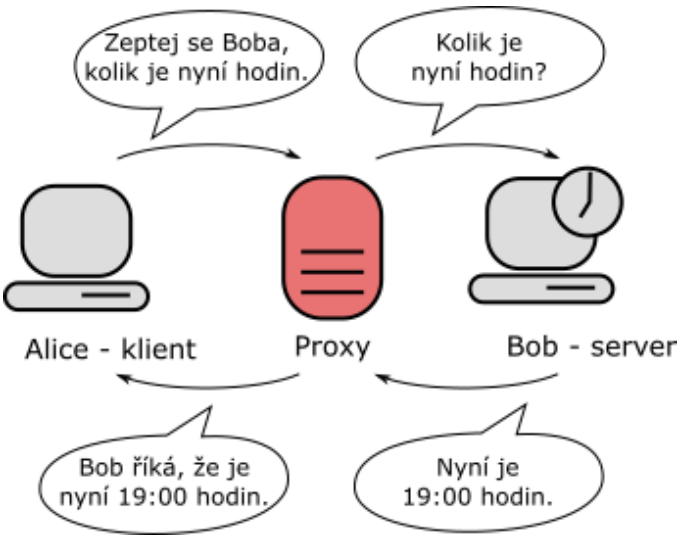
Již podle názvu můžeme soudit, v jaké vrstvě referenčního modelu OSI daný způsob zabezpečení operuje. Jedná se o jeden z nejstarších a zároveň nejběžnějších typů dostupných technologií pro inspekci paketů na síťové vrstvě. Filtrování paketů tím pádem může používat většina směrovačů pracujících na dané vrstvě. Využívá se v kombinaci s ostatními technologiemi firewall a tvoří často první obrannou linii. Princip spočívá v prvotní kontrole obsahu paketu zaměřující se na zdrojovou a cílovou IP adresu. Dále je možné kontrolovat například číslo portu pro stanovení rozšířenějších pravidel. Podle výsledku aplikace určitého pravidla se stanoví, jestli je možné paket propustit skrz směrovač dále, anebo dojde k jeho zahození a následné ztrátě. Kontrola probíhá zvlášť na každém paketu. Rozhodování o paketu probíhá velice rychle z důvodu prověřování pouze základních atributů. Z tohoto důvodu je nevýhodou nemožnost zachycení zlomyslnějšího kódu ukrývajícího se ve vyšších vrstvách komunikace. [28], [31]

1.7.3 Stavová inspekce paketů

Využívá pokročilejší metodu inspekce paketů pracujících v transportní vrstvě. Nejpoužívanějšími prvky dané vrstvy jsou tzv. **firewally**, které sledují přenos a stav spojení protokolů TCP. Zatupuje většinou druhou obrannou linii v síti. Konkrétně se daná technologie orientuje na spojení a sleduje jeho stav. Pro fungování je nutné nadefinovat určitá pravidla, podle kterých následně probíhá kontrola. V případě, že kontrolovaný paket dané pravidlo povoluje, doplní se do tabulky stavů nová položka. Do okamžiku, kdy je položka v seznamu aktivní, procházejí pakety stejné komunikační relace bez podrobnější inspekce, neboť se shodují s definovanou položkou. Touto metodou docílíme celkového urychlení činnosti. Jednotlivá pravidla se přitom ukládají do sestupného seznamu. Při inspekci procházejícího paketu se postupuje od vrchu směrem dolů až do chvíle, kdy jeho obsah odpovídá definovaným restrikcím. Pravidlo, které paket odmítá nebo zahazuje, má vždy přednost před pravidlem, které jej naopak povoluje. Na tento fakt je nutné si dát pozor v případech, kdy část paketů povolujeme a zbytek zakazujeme. V takovém případě nejprve nadefinujeme povolení pro určité porty a následně umístíme pravidlo pro zákaz zbylých portů. [15], [28]

1.7.4 Ochrana na úrovni aplikační

Firewally využívající stavovou inspekci paketů jsou v podstatě rozšířenou variantou běžných paketových filtrů. I přes svoji spolehlivost však nedokáží kontrolovat pakety na vyšších vrstvách referenčního modelu OSI. Můžeme se tak běžně setkat s útoky vůči serverům, které obyčejný Firewall nedokáže zachytit. Abychom zajistili téměř úplnou ochranu naší sítě, měli bychom využít služeb ochrany v nejvyšší referenční vrstvě – aplikační. Zařízení na této úrovni označujeme jako **proxy server**, někdy také jako *aplikační brána*. Pro zajištění dané úrovně ochrany musí proxy reálně vstoupit do probíhající komunikace v roli prostředníka a aktivně kontrolovat každé spojení. V případě, že tak proxy označí vybrané spojení za povolené, otevře směrem k cílovému zařízení druhé spojení od sebe sama jménem původního hostitele. Při probíhající inspekci je oddělena datová část každého procházejícího paketu a dojde ke kontrole obsahu. Po kontrole dochází znovu k sestavení paketu a odeslání. Ve výsledku tak veškerá komunikace mezi klientem a serverem probíhá skrz proxy. Při počáteční inicializaci je ze strany klienta navázáno potřebné spojení s proxy, které se dále podle požadavku spojí s cílovým serverem. V další fázi již proxy odesílá serveru veškeré požadavky přijaté od klienta a zpátky mu předává zpracované požadavky od serveru. Díky proxy jsme schopni zachytit požadavek již na začátku a využít jeho potenciál k odfiltrování nevhodného obsahu. Můžeme například zaručit nemožnost prohlížení stránek s nevhodným obsahem uvnitř knihoven nebo školních počítačových učeben. Jedná se o vysoce mocný nástroj, ovšem jeho konfigurace je již mírně složitější k pochopení. [17], [28]

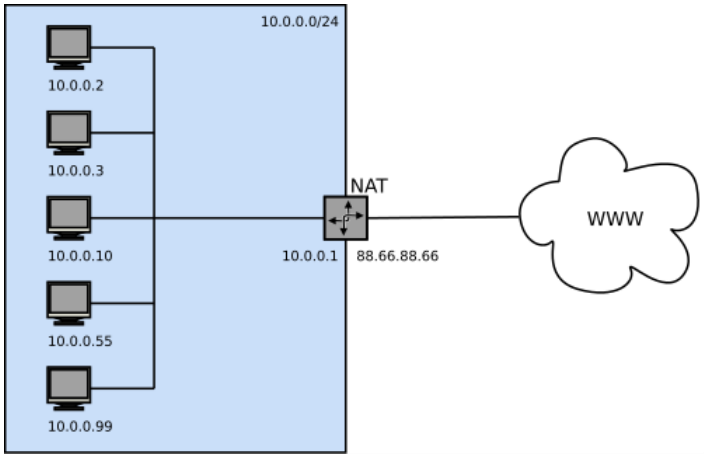


Obr. 22 - Princip fungování proxy serveru

Zdroj: upraveno podle [21]

1.7.5 Překlad síťových adres

Překladový mechanismus, označovaný v literatuře jako NAT, slouží organizacím k vyřešení otázky nedostatku veřejných IP adres verze 4 ve svých lokálních sítích připojených k internetu. Mechanismus NAT vznikl právě z důvodu omezení úbytku veřejných IP adres. V současné době není k dispozici dostatek veřejných IP adres, abychom je byli schopni přiřadit všem zařízením v síti. Všechna zařízení v síti však potřebují pro výměnu dat svoji jedinečnou IP adresu. Abychom splnili tyto podmínky a zároveň neplýtvali drahocennými veřejnými adresami, využijeme právě daného mechanismu. NAT nám umožňuje fyzicky oddělit internetovou část sítě, kde se vyskytují veřejné adresy, a lokální část sítě, kde využijeme jednu ze tří tříd privátních adres. Díky tomuto mechanismu mohou zařízení v lokální síti komunikovat a potřebují-li přistoupit k Internetu, uvádí se do provozu překlad adres. Překlad adres, neboli jejich převod, je realizován vždy na posledním hraničním aktivním prvku lokální sítě, který odesílá pakety dále do veřejné sítě. Dané zařízení (směrovač, firewall) přeloží lokální privátní adresu, kterých může být i několik stovek, na adresu veřejnou, která může být již pouze jedna. Veškerá zařízení za NAT pak ve veřejné síti vystupují touto jednou veřejnou IP adresou a jsou za ní též tzv. schovaní, což zvyšuje bezpečnost. Cílové zařízení v Internetu totiž vidí požadavek z jedné veřejné IP adresy, za kterou však může být schováno nespočetné množství zařízení. NAT tak případnému útočníkovi ztěžuje mapování topologie cílové sítě, neboť jeho požadavek dorazí nejdále k hraničnímu prvku (jeho veřejné IP). Nevýhodou daného řešení může být případ, kdy se uživatel vnitřní sítě autentizuje pro přístup k určitému chráněnému zdroji vně sítě. Přístup k tomuto zdroji totiž okamžitě získá i zbytek vnitřní sítě. [28]



Obr. 23 - Vizualizace překladu privátních adres na veřejnou adresu skrze NAT

Zdroj: [24]

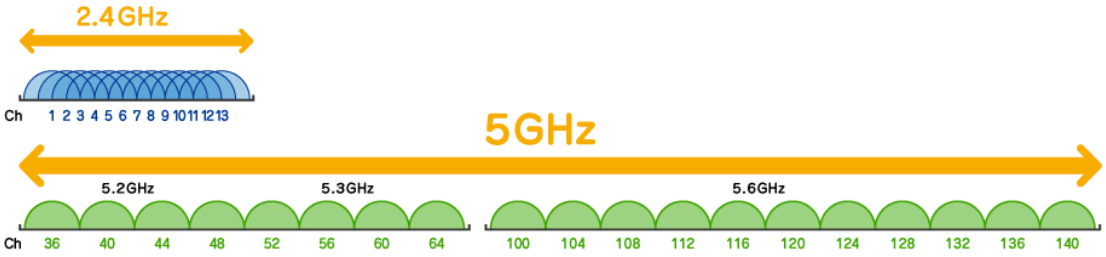
1.8 V krátkosti o Wi-Fi

V současnosti bude na světě relativně těžké nalézt člověka, který by nevěděl, co se pod danou zkratkou o čtyřech písmenek skrývá. Wi-Fi (Wireless Fidelity) je technologií definující bezdrátový přenos signálu v oblasti bezdrátových lokálních sítí (WLAN). Jako přenosového média se zde využívá vzduchu, konkrétně elektromagnetického vlnění v oblasti mikrovln. Konkrétně se jedná o frekvence v rozsahu 2,4 GHz a 5 GHz. Tato technologie je označována jako standard IEEE 802.11 a definuje pravidla přenosu informací na fyzické a části linkové vrstvy referenčního modelu OSI. Vzhledem k tomu, že se pro přenos využívá elektromagnetických vln, jsou právě tyto dvě vrstvy mírně odlišné od sítí pevných. Následující vrstvy modelu OSI jsou pak již plně totožné. Ve skutečnosti to znamená, že pokud budu zařízení z bezdrátové sítě komunikovat se zařízením z pevné sítě na linkové vrstvě, budeme potřebovat aktivní prvek označovaný jako přístupový bod – AP. Daný prvek nám zajistí přemostění bezdrátového signálu do sítí pevných a dále jsou již data přenášena podle standardu pevných sítí. Směrovače na vrstvě síťové (3. vrstva) již nerozlišují, zdali paket vznikl v síti bezdrátové nebo pevné. Z tohoto důvodu spolu mohou existovat v jedné podsíti oba způsoby šíření informací v síti pospolu a využívá se množství potenciálu Wi-Fi. Jedním z nich je mobilita, kdy uživatel není limitován pevným stanovištěm, ale může k síti přistupovat v rámci dostupného signálu Wi-Fi. S mobilitou však vzniká problém zabezpečení přenosu, neboť v dostupnosti signálu je síť přístupná komukoliv. V dané kapitole si představíme pár základních poznatků pro využívání a zabezpečení Wi-Fi v organizacích. Bezdrátové lokální sítě se neustále vyvíjejí a jejich rychlost v současnosti přesahuje hranici 3 Gb/s.

1.8.1 Frekvenční pásmo

Jak již bylo řečeno, standard 802.11 definuje šíření vln v mikrovlnném pásmu. Konkrétně se pro šíření signálu využívá nelicencovaných pásem rozprostřeného spektra. Za využívání pásma se tak neplatí žádný právní poplatek a může jej užívat kdokoliv s patřičným vybavením. Nevýhodou je vysoká úroveň rušení, tzv. interference, neboť je šířka pásma předem definovaná a nelze rozšiřovat. Standartní měrná jednotka pro frekvenční pásmo se udává v hertz (Hz). Hertz definuje

počet cyklů za vteřinu. Frekvence jeden hertz tedy představuje jeden cyklus za vteřinu. V oblasti sítí Wi-Fi jsou data přenášena v rozsahu frekvence 2,4 GHz a 5 GHz. Původně byl standard 802.11 definován na frekvenci 2,4 GHz, později bylo pro modifikaci definováno pásmo 5 GHz. Obě pásma se liší svými vlastnostmi a nejsou zpětně kompatibilní. Frekvence 2,4 GHz zůstává nadále nejpoužívanějším frekvenčním rozsahem v sítích WLAN. Konkrétní rozsah začíná na 2,4 GHz a končí na 2,4835 GHz, šířka jednoho kanálu je 20 MHz (původně 22 MHz). Nevýhodou je vysoká interference z důvodu překrývání jednotlivých pásem. Ve výsledku můžeme v současnosti ze 13 pásem dané frekvence zvolit pouze 4 pásma, které se vzájemně nepřekrývají, konkrétně kanál 1, 5, 9 a 13. U frekvence 5 GHz je situace o něco lepší. Jednotlivé kanály s šířkou 20 MHz se již nepřekrývají, ale následují za sebou. Každý kanál je tak jedinečný a vzniká možnost výběru méně rušeného kanálu. Co se týká rušení, je však na tom v současnosti 5 GHz pásmo, alespoň ve venkovních prostorech, stejně jako pásmo 2,4 GHz. [4], [29]



Obr. 24 - Rozdíl šířky frekvenčního pásma 2,4 GHz a 5 GHz

Zdroj: [1]

1.8.2 Faktory ovlivňující bezdrátový přenos

Přírodní a další vlivy mohou zcela zrušit šíření bezdrátového signálu, případně zkrátit vzdálenost dosahu. Při plánování a návrhu bezdrátových sítích je vhodné znát působení prostředí na elektromagnetické vlnění. Toto vlnění lze chápat stejně jako šíření světelných či zvukových vln prostorem. Znamená to tedy, že i když není tento druh záření pro člověka viditelný, platí na něj stejná fyzikální pravidla.

Útlum

Útlum je přímo závislý na vzdálenosti a jeho vliv je možné vysvětlit na jednoduchém příkladu. Můžeme si představit hladinu rybníka, do kterého pustíme kámen. V místě pádu vznikne efekt v podobě vln, které jsou šířeny do všech směrů a jsou větší tím, čím jsou blíže ke zdroji. Vlny dále od zdroje se roztahují a postupně zmenšují do

chvíle, než se ztratí. V případě bezdrátových vln je situace obdobná. Vyzařovaný signál postupuje od svého zdroje a vlivem vzdálenosti se postupně ztenčuje. Útlum vymezuje dosah pomocí určování energetických ztrát v souvislosti se vzdáleností. Zařízení vyskytující se blíže k vysílači získají koncentrovanější signál, který se vzdáleností mění a zmenšuje se též maximální přenosová rychlost dat.

Absorpce

Amplituda neboli síla záření signálu ze zdroje je vlivem pohlcování snižována a zmenšuje se tak vzdálenost, na kterou je signál schopný putovat. Příčinou pohlcování jsou zdi, lidská těla, koberce nebo například dřevo. V místě, kde dochází k pohlcování signálu, vznikne teplo a vlna se zastaví. Tohoto vlivu využívá mikrovlnná trouba, kdy dochází k pohlcování mikrovlnných vln na straně jídla. V bezdrátových sítích je tento vliv negativní a může rapidně přispět k zhoršení kvality signálu a zmenšit vzdálenost dosahu. Ve většině případech nejsme schopni toto ovlivnit. Je však možné se pokusit alespoň umístit aktivní prvek lépe do prostoru.

Odraz

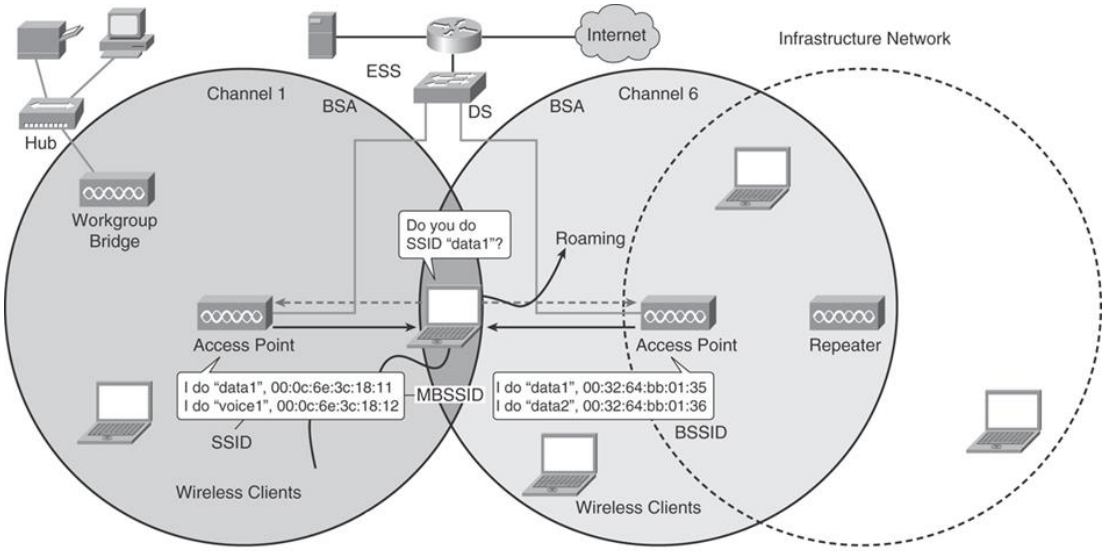
Již jsme si představili skutečnost, že elektromagnetické vlnění se šíří v prostoru shodně jako kupříkladu světelné vlnění. Představme si tak situaci, kdy namíříme světelný zdroj proti zrcadlu, a světlo se odrazí pod určitým úhlem na protější zeď. Tento efekt zdroje interference se nemusí objevovat pouze u zrcadel. Podobné odrazové vlastnosti může mít například obrazovka monitoru nebo obraz rámovaný ve skle. Vlivem odrazu může nastat efekt vícecestnosti, kdy nastane situace rozmnožení stejných částí signálu vícekrát a zbytečné zahlcování linky.

[4]

1.8.3 Přístupový bod – AP

Přístupovým bodem nazýváme takový aktivní prvek, který slouží jako zdroj vysílaného signálu a klienti se pomocí něj připojují do sítě. Veškerá komunikace mezi jednotlivými klientskými zařízeními probíhá vždy prostřednictvím přístupového bodu. Ve většině případů používají přístupové body pro šíření signálu všesměrové antény. Signál je tak rovnoměrně šířen do všech směrů (úhel 360°). Daná bezdrátová topologie se označuje jako *infrastrukturální síť*. Přístupový bod šíří jedinečný název sítě označovaný jako SSID, který musí mít veškeré stanice totožné. Pomocí SSID stanice

ví, do jaké sítě patří a veškeré požadavky jsou předávány přímo na přístupový bod. Topologie infrastrukturální sítě patří do oblasti tzv. základní oblasti služeb (zkratka BSS) a definuje vždy jeden přístupový bod s jedním SSID na celou síť. Ve větších organizacích však většinou jeden přístupový bod nestačí. Nejen z důvodu omezené kapacity pro připojené klienty, ale hlavně z důvodu omezené oblasti šíření signálu. V takových případech využíváme topologii rozšířené oblasti služeb (zkratka ESS). Skládá se vždy minimálně ze dvou přístupových bodů BSS spojených dohromady v jedné podsíti. Všechny přístupové body používají k identifikaci totožné SSID. Klient je tedy schopný mobilně cestovat skrz jednotlivé AP bez toho, aby musel měnit logickou adresu nebo znovu provádět autentifikaci. [4], [32]



Obr. 25 - Rozšířená oblast služeb (ESS) se dvěma AP

Zdroj: [4]

1.8.4 Zabezpečení bezdrátových sítí

Bezdrátové sítě využívají k šíření informací elektromagnetické vlnění šířené vzduchem. Je relativně zřejmé, že z důvodu možného odposlechu kdekoliv v rámci dosahu signálu, nemohou být tyto sítě natolik bezpečné jako sítě pevné. Existuje několik metod zabezpečení bezdrátových sítí. Před samotným využíváním bezdrátových sítí je nutné zvážit tu variantu zabezpečení, která se do podmínek naší sítě hodí nejvíce. Odpověď vždy většinou závisí na uživatelích, tedy nakolik potřebujeme skrývat obsah uživatelského provozu. Wi-Fi připojení můžeme nabídnout hostům a na zabezpečení tolik nepohlížet. V případě organizace je však více než vhodné se o možnosti šifrování provozu zajímat a využít je. [4]

Primitivní způsoby pro zabezpečení

Zde řadíme metody *skryté SSID* a *filtrování podle MAC adresy*. Dovoluji si nazvat tyto možnosti zabezpečení za primitivní. Sice fungují a ztěžují případnému útočníkovi práci, ale s dnešními technikami jsou lehce prolomitelné. Technika skrytého SSID zamezuje veřejné vysílání jedinečného identifikátoru sítě z AP. SSID je na AP sice nastaveno, ale není možné jej standardními technikami vyhledat a připojit se. Možnost připojit mají pouze ti klienti, který tento jedinečný identifikátor znají a pevně jej nastaví na svých zařízeních. Při výměně rámců mezi klientem a AP je pomocí speciálního SW možné při sledování sítě název SSID zachytit a následně provést bezproblémovou autentizaci. Při filtrování pomocí MAC adresy se na AP definují fyzické adresy aktivních prvků klientských zařízení, jejichž připojení je povoleno. Objeví-li se požadavek na připojení od zařízení s povolenou fyzickou adresou, je tedy povolen. Při sledování sítě je možné fyzickou adresu odchytit a snadno zfalšovat. Po změně MAC útočníka je možné bez problému přistoupit k obsahu sítě. [4]

Autentizace předem sdíleným klíčem (WEP)

Daný způsob ověřování je založen na použití tajného statického klíče WEP. Identita jednotlivých uživatelů není zjišťována, ověřuje se pouze příslušný klíč. Klíč je shodně nastaven na straně klienta i přístupového bodu a je používán k vygenerování pseudonáhodné číselné řady k zašifrování dat. V současnosti je tento způsob ověřování považován za překonaný. Z důvodu stále stejného statického klíče je možné ze strany útočníka zachytit text výzvy a posléze i zašifrovanou odpověď. Vzhledem ke skutečnosti, že prvotní text výzvy není šifrovaný, dokáže útočník jednoduše odvodit statický klíč WEP. Klíč WEP se navíc používá pouze při šifrování textu výzvy a slouží pouze pro účely autentizace. Zabezpečení WEP neukrývá ani nešifruje žádná data uživatele posléze, co dojde k připojení na přístupový bod. [2], [4]

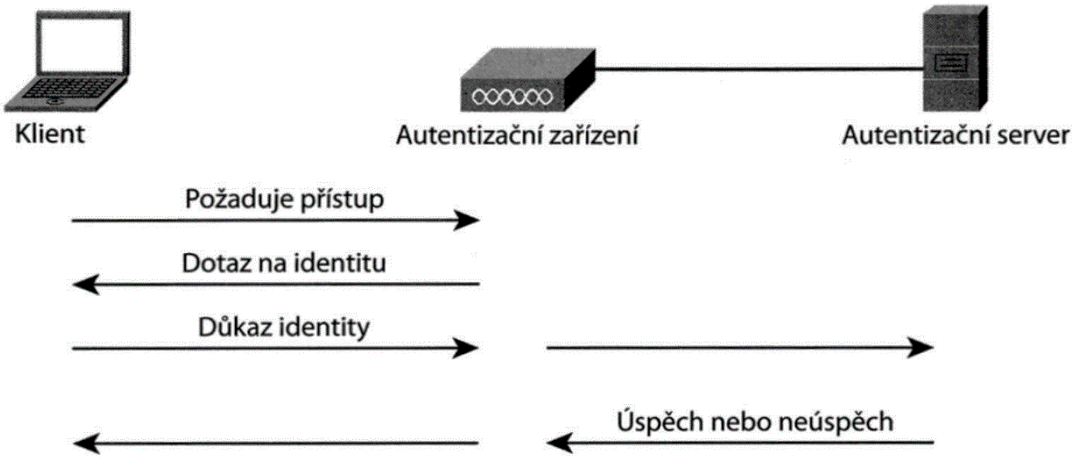
Šifrovaná autentizace pomocí WPA/WPA2

Zabezpečení WPA (Wi-Fi Protected Access) vzniklo jako reakce na lehce prolomitelné zabezpečení WEP. Daný standard uvedla roku 2003 Wi-Fi aliance. Zabezpečení WPA automaticky mění hodnotu šifrovacího klíče. Představuje tak zlepšení oproti statickému řešení zabezpečení WEP. Díky tomu jsou klíče odolnější oproti útoku hrubou silou. Standard WPA umožňuje zvolit mezi dvojicí autentizačních režimů: **osobní** a **podnikový**. Osobní režim operuje s předem sdílenými klíči a jedná

se o řešení doporučované k šifrování prostředí domácích sítí. Podnikový režim vyžaduje navíc autentizační server. Při autentizaci klíčů se používá speciální protokol RADIUS. V současnosti se můžeme dále setkat s modernizovaným standardem WPA2. Daný standard zastupuje druhou verzi původního standardu WPA. Daný standard využívá silnějšího šifrování a dynamické klíče využívají ukládání do mezipaměti. Ve výsledku je celý proces připojení rychlejší. V současnosti se jedná o nejvyužívanější metodu šifrování komunikace na bezdrátových sítích. [4]

Standard 802.1x

Daný standard centralizovaného ověřování je znám již z pevných sítí. Při centralizované autentizaci je ověřována identita uživatele pomocí odlišných způsobů. Ve většině případů se jedná o ověřování využívající uživatelského jména a hesla osoby, která je součástí organizace. Uživatelům není prozrazen veřejný klíč, ale každý využívá k připojení do bezdrátové sítě vlastní údaje. Tyto údaje může mít s využitím adresářových služeb totožné, jako má například pro přístup do domény AD. Údaje jsou předány skrz přístupový bod na autentizační server. Autentizační server je většinou externím serverem využívající protokol RADIUS. Daného zabezpečení se využívá ve větších institucích, kde každý uživatel vlastní jedinečné přihlašovací údaje a klíč nemusí být veřejně sdílen a používá se pouze pro šifrování komunikace. [4]



Obr. 26 - Centralizované ověřování uživatele standardu 802.1x

Zdroj: [4]

2 Praktická část

Po nezbytné obecné části týkající se základů počítačové sítě a jejích služeb se dostáváme k jejímu praktickému využití. Počítačové sítě a služby s nimi spojené nalezneme v nespočetném množství institucí, podniků, organizací a též domácností. Veškeré výše zmíněné teoretické základy platí pro všechny stejnou měrou. Pouze se jejich fungování uzpůsobí velikosti, důležitosti, dostupnosti a bezpečnosti konečné sítě. Před samotnou realizací převážně korporátních sítí probíhá ze strany společnosti nebo specializované firmy celková analýza a technický návrh topologie sítě. Tento proces je však ve většině případů možný za předpokladu budování sítě v nových prostorách nebo kompletní výměny stávajícího řešení. Samotná analýza se řadí mezi relativně drahé záležitosti. My se zaměříme na prostředí sítí v budově školského zařízení. Konkrétně se zamyslíme nad stavem sítě ve školách vyššího sekundárního stupně. Větší procento těchto škol má ze statusu příspěvkové organizace omezené finanční možnosti, které může využít k modernizace síťového zázemí. Většina škol tak vychází z určitého historického základu podoby počítačové sítě, který dále rozšiřuje. Přesně daný stav školy si v následujících řádcích namodelujeme a pokusíme se alespoň částečně popsat postup jejího přiblížení současným trendům.

2.1 Obecná analýza potřeb školské instituce

Na úvod se sluší začít s trochou matematiky. Odhadem se v průměrné české škole vyskytuje denně na 500 osob. Kdybychom každou danou osobu měli z hlediska počítačové sítě považovat za potencionálního klienta sítě, dostáváme se do oblastí středních až velkých lokálních sítí. Tato skutečnost platí za předpokladu, bude-li každý uživatel schopný využívat prostředky sítě. Škola ve většině případů sice takovým množstvím klientských zařízení nedisponuje. Otázkou je stav, kdy škola nabídne možnost připojení vlastních klientských zařízení například pomocí bezdrátové sítě. Současný rozmach chytrých zařízení nás posléze může na takové číslo dostat. Na začátku bychom měli vycházet z doporučení vázaných se na pravidla pro velké sítě. Ucelená literatura neexistuje, jsou však známa jistá doporučení pro usnadnění správy takto rozsáhlých sítí. Z těchto doporučení budeme dále vycházet. Musíme se zaměřit nejen na vlastní topologii a návrh sítě, ale doporučit i služby, které nám v její správě pomohou.

Celý dokument bude modelově stavět na určitém počátečním stavu školní počítačové sítě a návrhu změn pro zajištění účinnějšího fungování spojeného s mravní výchovou převážné většiny klientů. Nesmíme totiž zapomenout, že se jedná o veřejnou instituci, pro kterou platí také jisté mravní zásady a i ty dále vystihneme. Stav počítačových sítí se na jednotlivých školách značně liší, takže nalézt společný model nebude lehké. Budeme-li stavět na síti podobné velikosti, většinou si již s jednou podsítí nevystačíme. Oddělení podsítí budeme řešit pomocí směrovače, případně přepínače pracujícím na 3. vrstvě modelu OSI. Abychom ušetřili finance na jednotlivé aktivní prvky, zvolíme logické dělení podsítí pomocí virtuálních logických sítí (VLAN). Dané řešení přináší výhodu možnosti realizace podsítí na jednom fyzickém zařízení. Pro správu jednotlivých uživatelských účtů je vhodné v takovém počtu zvolit centrální správu pomocí adresářových služeb. Z důvodu většinového smluvního závazku mezi jednotlivými zřizovateli SŠ se softwarovou firmou Microsoft, se nabízí využít jejich služeb a správu realizovat skrze doménu Active Directory. Klientské zařízení (počítače) budou též ve většině případů obsahovat operační systém Microsoft Windows. Bude tedy možné nastavovat zásady pro jednotlivé skupiny uživatelů. Umožní nám to ovlivňovat chování systému v případě, že jej ovládá žák nebo učitel, případně jiný nepedagogický pracovník školy. Moderní škola by měla zajistit také možnost přístupu k bezdrátovému připojení a využití sítě Internet. Jako topologii pro danou oblast sítě budeme muset zvolit větší množství přístupových bodů, abychom zajistiteli co nejúčinnější pokrytí. Dále budeme muset zvolit vhodný způsob jejího zabezpečení. Samotné provedení sítě bude záležet na výchozím bodě. Přes omezené finance není většinou možné vystavět novou síť, ale přizpůsobit se aktuálnímu stavu. Proto bude vhodné definovat potenciál současného řešení a navrhnout stupně její případné modernizace. Rád bych veškeré tyto aspekty dále podrobněji popsal a zaměřil se na ty, které vidím jako důležité. Využijeme k tomu příklad dále zmiňované modelové situace.

2.2 Síť modelové středoškolské instituce

2.2.1 Představení instituce

Model lokální počítačové sítě se týká odborné střední školy na malém městě. Do školy denně dochází 300 studentů ve třech čtyřletých studijních oborech. Dále je ve škole trvale zaměstnáno 40 zaměstnanců, z nich 36 má téměř denní kontakt se síťovým zařízením. Škola se skládá z hlavní budovy o třech funkčních patrech a přízemí, přístavby s patrem, přízemím a tělocvičnou. Jeden z oborů se přímo týká výuky informačních a komunikačních technologií. Škola má tak veškeré potřebné vybavení spojené s počítačovými učebnami a laboratořemi odborného výcviku. Přesný počet počítačových učeben je roven číslu čtyři. Škola nezaměstnává samostatnou pozici správce sítě. O provoz sítě se stará učitel ICT s příplatkem za správu a náročnější úpravy jsou předávány třetí straně.

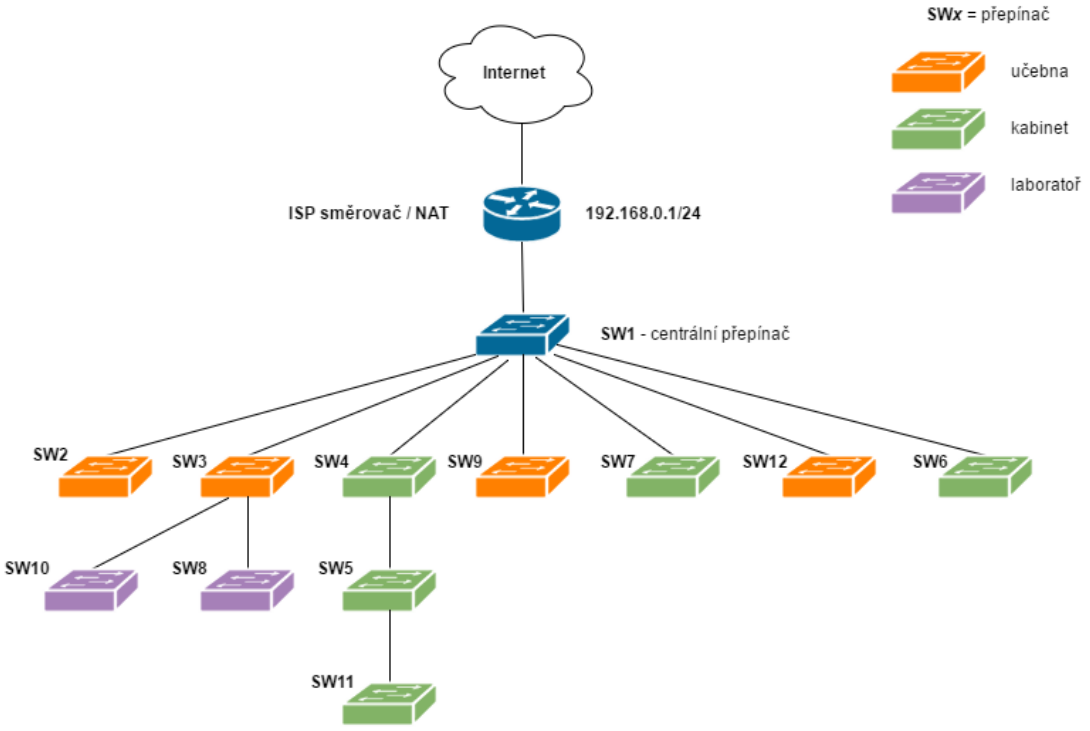
2.2.2 Popis stávajícího stavu

Budování počítačové sítě probíhalo postupně v několika fázích. Původně škola využívala topologii sběrnice s využitím koaxiálních kabelů. V současnosti již plně využívá topologii rozšířené hvězdy postavenou na kroucené dvoulince. Topologii je možné přirovnat k síti rozsáhlé. Konkrétně jsou fyzicky k síti připojeny čtyři počítačové učebny, osm kabinetů a trojice laboratoří odborného výcviku. Síť a aktivní prvky jsou převážně sto megabitové (100 Mb/s).

Infrastruktura

Jako přenosové médium se využívá kroucené dvoulinky v kategorii 5 a 5e. Centrálním prvkem zde vystupuje 24 portový přepínač umístěný v kabinetu učitele obstarávající správu sítě. Zde je síť pomocí jednotlivých portů přepínače dále větvena do podoby rozšířené topologie. Daný kabinet je umístěn v zadní části přístavby. Převážná část páteřních spojů je vedena v plastových lištách. Kromě hlavního přepínače se v síti vyskytuje dalších 12 přepínačů. Ty jsou systematicky rozmístěny pro potřeby počítačových učeben, laboratoří a jednotlivých kabinetů. Každá učebna má vlastní 24 portový přepínač, z kterého jsou dále napojena klientská zařízení. Toto řešení je shodné též s jednotlivými laboratořemi. Mírně chaotické je zapojení kabinetů, kde v určitých místnostech neplatí individuální přepínač na kabinet. Znamená to, že z jednoho kabinetu lze napojit zařízení umístěné v jiné místnosti. K centrálnímu

přepínači je dále připojen souborový server umožňující sdílení složek a souborů. Jako další server je veden databázový systém školní agendy umístěný v kanceláři zástupce ředitele. Podsíť je řešena prefixem /24, dovolující definovat celkem 254 jedinečných logických adres pro klientská zařízení. Škola tak na celou síť využívá právě jedné podsítě, mezi kterou není nutné směrovat. Směrovač s funkcí NAT je využívám pouze pro přístup do sítě Internet. Tento směrovač však je plně pod správou poskytovatele bezdrátového připojení a škola k jeho konfiguraci nemá potřebná práva. V současnosti ve škole neexistuje centrální řešení pro přístup k bezdrátové síti.



Obr. 27 - Větvení síťové infrastruktury modelové školy

Zdroj: autor

Síťové služby

Škola využívá dostupné prostředky sítě relativně minimálně. I přes většinové připojení všech klientských zařízení do sítě, je většina požadavků na služby řešena lokálně. Nejvíce využívanou službou je možnost přístupu k internetu a sdílení souborů skrze síťové disky. K daným účelům je využíváno síťového operačního systému Novell NetWare. „*Operační systém NetWare využívá aplikací síťového serveru i síťových klientů. Klientská aplikace je určena ke spouštění na různých klientských operačních systémech. S nainstalovaným systémem NetWare Client může pracovní stanice zcela využívat souborových a tiskových služeb a zabezpečení.*“ (Bigelow, 2004, s. 139)

Veškeré počítače v síti musejí mít ke svému hostitelskému operačnímu systému naistalován klientský program umožňující komunikaci se souborovým serverem Novell. Sdílení souborů je pak chráněno přes uživatelské jméno a heslo, které je nutné zadat před samotným přihlášením do sítě. Pohledem na další služby, škola nevyužívá vlastní DHCP ani DNS server. Veškerá konfigurace je řešena individuálně pomocí statické IP adresy. Používání názvů není kvůli absenci DNS možný. Z důvodu centrálního úložiště dat se však nejedná o takový problém, přesto to již v současnosti není tolik obvyklé.

Dále škola využívá centrálního systému školní agendy Bakaláři. Tento systém je nainstalován na počítači zástupce ředitele a využívá databázi SQL. Přístup pro rodiče je řešen modulem skrz Webové rozhraní. Na daném počítači tak běží služba *Internet Information Services* (IIS) sloužící jako webový server a škola si pronajímá jednu vlastní veřejnou IP adresu. Díky tomu je zaručen přístup k webovému rozhraní agendy i mimo lokální síť školy.

Servery a klientská zařízení

Škola využívá jeden vyhrazený server pro obsluhu klientů. Jako operační systém na něm běží síťový NetWare od společnosti Novell. Jeho napojení je provedeno přímo na centrální směrovač. Využívá se jako centrální úložiště sdílených školních dokumentů a prací jednotlivých studentů. Velikost osobní složky pro studenta činí 125 MB, učitelé mají k dispozici 1 GB vlastního prostoru. Disk je dostupný pouze po předchozím přihlášení přes Novell klienta. Zálohování není řešeno automaticky a pravidelně, ale manuálně v určitých etapách školního roku (po začátku školního roku, před rodičovskými schůzkami, pololetí).

Hardwarová konfigurace serveru:

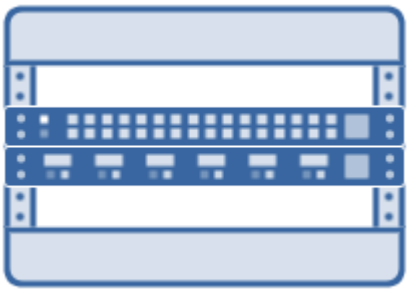
- CPU – Intel Xeon E5205 (2 jádra, 1.86 GHz, 6 MB L2 Cache)
- MB – Fujitsu Siemens D2509
- RAM – 4 GB DDR2, 666 MHz
- HDD – 2x 500 GB (RAID 1 – zrcadlení)
- NIC – Broadcom BCM5708C, přenosová rychlost 1 Gbps

Škola má v síti připojeno celkem 110 pevných počítačů. Jednotlivé parametry se liší. Nejvýkonnější sestavy se nacházejí v počítačových učebnách, kde je vždy hardwarová

konfigurace totožná pro veškeré počítače. Průměrově nejběžnější architekturou procesoru je Intel Core i3 s operační pamětí velikosti 4 GB a pevným diskem 500 GB. Škola využívá plně software a operační systém od společnosti Microsoft. Přihlašování klientů probíhá lokálně.

Provedení počítačové učebny

Ve všech čtyřech počítačových učebnách se nachází celkem 17 počítačů. Jeden počítač slouží pro potřeby vyučujícího a zbylých 16 využívají studenti. Model všech učeben je stejný. Obsahuje vždy 4 řady stolků se čtyřmi studentskými počítači a poslední oddělený stolek vzadu pro počítač vyučujícího. V každé učebně je umístěn jeden 24 portový směrovač a ke každému počítači vede jeden UTP kabel. Původně měla škola dvě učebny výpočetní techniky, z kterých se zachovalo i původní síťové vybavení. Jsou označeny jako VYT1 a VYT2 a obsahují každý 24 portový přepínač o přenosové rychlosti 100 Mb/s a UTP kabeláž Cat 5. Daná kategorie 5 (cat 5) je standardizována pro rychlost 100 Mb/s. Později byly postupně vybudovány další dvě učebny označované jako VYT3 a VYT4. Tyto učebny již obsahují přepínače s podporou gigabitového Ethernetu a odpovídající UTP kabeláž Cat 5e pro gigabitové přenosy (1 Gb/s). Směrovače jsou umístěny v nástěnné rackové skříni o velikosti 6 až 9 jednotek (6U, 9U). Kabely od jednotlivých počítačů nekončí přímo ve směrovači, ale směřují nejprve do tzv. patch panelu. Patch panel je řada zásuvek konektorů RJ-45 uzpůsobená pro umístění do rozvaděče. Umísťuje se většinou spolu se směrovačem a propojení probíhá skrze krátké patch UTP kabely (délka 0.25 až 1 m). Rozmístění v daném rozvaděči naznačuje Obr. 28. Přihlašování k jednotlivým počítačům je řešeno lokálně skrz univerzální účet pro studenta a učitele.



Obr. 28 - Podoba rozvaděče síťové technologie (racku) v učebnách VYT

Zdroj: autor

Připojení do internetu

Škola pro připojení k internetu využívá vyhrazenou bezdrátovou linku v pásmu 5 GHz. Rychlost linky je stanovena na 8 Mb/s pro stahování (download) a 5 Mb/s pro nahrávání (upload). Objem přenesených dat je neomezený. Záložní linka není k dispozici.

2.2.3 Hodnocení účelnosti

Pohledem na současný stav sítě u modelového školního prostředí je nutné konstatovat, že současný stav sítě nepatří mezi kritické. Škola svépomocí dosáhla přechodu ze zastaralé sběrnicové topologie na topologii hvězda s využitím kroucené dvoulinky. Tento stav měl sice postupný vývoj, ale je možné jej považovat za dostatečný a funkční. Navíc se u většiny páteřních tras objevuje kabeláž UTP se standardizovanou kategorií 5e pro gigabitový přenos. Do budoucna tak postačí výměna zbylých 100 Mb aktivních prvků pro plné využívání již standardního gigabitového Ethernetu. Tento stav neplatí pro nejstarší učebny výpočetní techniky, kde je veškerá kabeláž, včetně páteřního propojení s centrálním přepínačem, řešena kabely UTP kategorie 5. Zde bude v případě výměny současných počítačových sestav nutné počítat s kompletní výměnou síťové kabeláže novější generace spolu s přepínačem.

Podsíť s 254 jedinečnými IP adresami je pro současný stav školní sítě dostatečná. Škola má zájem o vybudování a poskytování přístupu k bezdrátovému připojení pro zaměstnance a studenty. Zde již bude tedy nutné začít řešit i vrstvení na podsítě a pořízení školního směrovače. Poskytovatel internetu totiž neumožní přístup k úpravě jejich zařízení. Současný centrální přepínač je konfigurovatelný a umožňuje vytvářet virtuální lokální sítě (VLAN). Tuto vlastnost dále využijeme k rozdělení školní sítě na logické celky a jejich směrování.

Výhrady mohou vzniknout u síťových služeb. Současný síťový operační systém Novell byl školou pořízen někdy na konci roku 2004. Jedná se o velice zastaralé řešení s relativně složitou správou. Zde budu navrhovat jeho komplexní odstavení a zavedení správy skrz efektivnější adresářové služby. Z důvodu výhodného kontraktu se softwarovým gigantem Microsoft, bude vhodné využít jeho služeb a využít nového serveru pod operačním systémem Windows Server. Potenciál daného serveru bude možné dále využít pro účinnější správu uživatelských účtů, centrální konfiguraci a řízení přístupu.

2.3 Návrhy pro zlepšení síťové podoby

Po přečtení předchozí kapitoly jsme získali informace o aktuálním stavu síťového prostředí modelové školy. V následující kapitole představíme několik návrhů pro její modernizaci a přípravu současným trendům.

2.3.1 Výměna síťové kabeláže VYT1 a VYT2

Učebny označované jako VYT1 a VYT2 jsou počítačovými učebnami, které škola vybudovala během let 2004 až 2005. Přes již relativně zastaralé hardwarové vybavení se škola rozhodla pro modernizaci a pořídila nové stroje. Dané počítače již obsahují síťové karty (NIC) umožňující teoretický přenos až 1 Gb/s. Současná síť je pomocí kabeláže a směrovače standardizována pro přenos 100 Mb/s. Pro srovnání, maximální rychlost přenosu z pevného disku na daném standardu činí přibližně 12 MB/s. U gigabitu je daná rychlost desetinásobná a dostáváme se k možnosti přenosu i 125 MB/s. Vše samozřejmě záleží též na ostatních komponentech, ovšem u standardního pevného disku jsme schopni na gigabitu dosáhnout rychlosti přenosu po síti až 90 MB/s. Při práci se sdílením a síťovými disky jsme schopni dosáhnout několikanásobného zrychlení odezvy sítě a jejího přenosu. Samozřejmostí je nutnost mít na celé trase aktivní prvky s gigabitovými porty, tedy *NIC1 – směrovač – NIC2*.

V určitých případech by postačila výměna směrovačů v každé učebně. Bohužel obě zmiňované učebny jsou vybudovány na kabeláži a zásuvkách kategorie 5 (Cat 5). V jiných situacích je daná kategorie kabeláže pro gigabit dostačující, ovšem z pohledu standardizace není daný stav akceptovatelný a mohly by vznikat chyby přenosu. Abychom mohli plně využívat možností gigabitového přenosu, potřebujeme minimálně rozšířenou kategorii 5, označovanou jako kategorie 5e (Cat 5e). Kategorie 5e je v současnosti nejlevnější variantou využívání gigabitových přenosů na kroucené dvoulince. V současnosti jsou již lépe cenově dostupné též kabely novějších generací, kde za zmínku stojí kabeláž kategorie 6 (Cat 6). Oproti kategorii 5e má rozšířenou šířku pásma a přes pokles pořizovací ceny se stává stabilnějším a vhodnějším kandidátem pro gigabitové přenosy. Rozhodne-li se pro danou novější kategorii, získáme navíc možnost budoucího využití pomalu standardizovaného deseti gigabitu (10 Gb/s). Kategorie 6 je schopna využívat deseti gigabitový přenos do vzdálenosti 55 m. Pořizovací cena je v současnosti ovšem stále vysoká, čas ukáže.

Co bude nutné vyměnit

Z důvodu absence podpory gigabitového přenosu současné kabeláže se doslova jedná o kompletní výměnu a nový návrh síťové podoby. Současná podoba učeben je doslova totožná, pouze jsou zrcadlově převráceny. Ve výsledku bude dostačující navrhnout řešení pro jednu učebnu.

Pojďme se podívat, z jakých prvků se aktuálně síť učebny skládá:

- 1x nástěnný rozvaděč (rack) o velikosti 6U
- 1x 100 Mbps 24 portový aktivní prvek – směrovač
- 1x patch panel s 24 zásuvkami RJ-45 kategorie 5
- 17x zásuvka RJ-45 u jednotlivého počítače
- UTP kabel Cat5 potřebné délky a počtu
- páteřní kabel UTP mezi centrálním přepínačem a přepínačem učebny

Z výše uvedeného seznamu bude prakticky nutné vyměnit vše kromě nástěnného rozvaděče, který slouží k ochraně a uložení síťových komponentů. Jednotlivé UTP kabely jsou k počítačům vedeny skrze podlahové lišty k individuálním řadám stolů. Dané řešení vedení pomocí plastových lišt bude zachováno, neboť není možné investovat do kompletních stavebních úprav učebny.

Navrhované prvky

Sluší se začít tím nejdůležitějším – směrovačem. Na trhu existuje spousty značek a rozdílných kvalit. Jistotu zaznamenáme v prvcích od firmy Cisco, ovšem musíme také počítat s vyšší cenou. Mezi více profesionální produkty patří dále řešení od firmy HP (Hewlett Packard), které nabízí výkonově podobné sestavy s nižší cenou a jednodušší správou. Znamená to, že se zaměříme na konfigurovatelné přepínače, které většinou pomocí webové správy umožňují konfiguraci VLAN a jiných služeb. Daným potřebám perfektně odpovídá přepínač **HP 1820 24G (J9980A)**. Jedná se o plně gigabitový přepínač pracující na vrstvě 2 a obsahující 24 portů pro UTP konektor RJ-45. Dále obsahuje 2 porty SFP dovolující případné připojení optického kabelu. Konfigurace probíhá pomocí webového rozhraní, přepínač je však schopný fungovat bez nutnosti konfigurace ihned po zapojení.

Navrhuji nahradit UTP kabeláž rovnou za Cat6 namísto Cat5e. Cenově se to již o tolik neliší a škola bude připravena do budoucnosti.

Pro propojení jednotlivých zařízení a ochraně její kabeláže bude potřeba pořídit též ostatní pasivní prvky se standardizací Cat6. Pro potřeby patch panelu volím 24 portový **Patch panel LYNX Cat 6**. V daném panelu budou končit veškeré UTP kabely vedoucí od počítačů. V případě potřeby je možnost připojení i stínění, není však podmínkou.

Druhou stranu kabelu nezapojíme přímo do počítače, ale provedeme nejprve umístění do zásuvky. Zamezíme tím zbytečnému namáhání nebo zničení kabelu. Nesmíme tedy zapomenout na 17x **UTP 1xRJ45 zásuvku CAT6 na omítku**. Daná datová zásuvka bude umístěna pod stolem každého počítače. K propojení počítače nám již posléze bude stačit krátkého UTP kabelu, označovaného jako patch kabel.

UTP kabeláž se prodává v ceně po metru. Existuje možnost zakoupit tzv. box či cívku, obsahující většinou 305 m kabelu, což je pro potřeby jedné učebny dostačující. Vzhledem ke skutečnosti, že budou kabely vedeny v lištách a chráněny proti vnějším vlivům, postačí koupit jej v provedení *drát*. Cenově vychází oproti licně levněji. Vzhledem ke skutečnosti, že budujeme síť na několik let dopředu, je vhodné zvolit kvalitního výrobce kabelu, například **Belden UTP kabel 7965E, Cat6, 305 m**. Zakoupený box využijeme pro tažení všech tras, tedy nejen mezi počítačem a směrovačem (konkrétně zásuvkou počítače a patch panelem), ale též pro krátké patch kabely i páteřní linky. Poslední položkou na seznamu jsou samotné konektory RJ-45. Většinou se prodávají po balení 100 ks. Konektory, jakožto pasivní prvky, musí také podporovat Cat6 a umožňovat osazení na kabely typu *drát*.

Způsob vedení kabeláže

Vedení kabeláže bude totožné se současným stavem. Pouze se nahradí zastaralé prvky. Ochrana kabeláže v plastových lištách. Ochrana aktivních prvků pomocí uzamykatelného rozvaděče. Způsob vedení kabeláže je naznačen v příloze A na konci dokumentu.

Způsob zapojení portů přepínače

Navrhovaný přepínač obsahuje celkem 24 portů pro UTP kabel označené jako port 1 až port 24. Logicky je vhodné zapojit a očíslovat jednotlivé počítače od portu 1 dále. První počítač bude umístěn v první řadě nalevo, číslo bude s každým počítačem po pravici narůstat. Poslední port přepínače (port 24) bude vyhrazen pro páteřní linku. Volné porty zůstávají nezapojeny, případně jako záloha při rozbití aktivního portu.

Následující tabulka jednoduše zaznamenává zapojení jednotlivých portů přepínače. Zelená barva čísla znamená odlišný druh konektoru. V daném případě se jedná o dvojici SFP portů, které však zůstanou nevyužity. Je vhodné podobným způsobem provádět dokumentaci pro pozdější opravy a diagnostiky problémů.

24P_SWITCH – SW2 (VT1)

port	1	2	3	4	5	6	7	8
cíl	**PC01**	**PC02**	**PC03**	**PC04**	**PC05**	**PC06**	**PC07**	**PC08**
port	9	10	11	12	13	14	15	16
cíl	**PC09**	**PC10**	**PC11**	**PC12**	**PC13**	**PC14**	**PC15**	**PC16**
port	17	18	19	20	21	22	23	24
cíl	**PC17**	**-**	**-**	**-**	**-**	**-**	**-**	**SW1/5**
port	25	26						
cíl	-	-						

Tabulka 4 - Popis zapojení jednotlivých portů přepínače učebny VYT1

Náklady na vybudování

1x přepínač HP 1820 24G	4 672 Kč
1x Patch panel LYNX Cat 6	1 239 Kč
1x UTP kabel Belden 7965E, Cat6, drát, 305m cívka	4 352 Kč
1x konektor RJ45-8p8c,50µm Au, drát, CAT6, 100ks	561 Kč
17x zásuvka UTP RJ45 CAT6 na omítku	1 986 Kč
Celkem s DPH	**12 810 Kč**

Celkové výdaje za materiál pro výměnu současné kabeláže činí 12 810 Kč. Nejedná se ve výsledku o tolik závažnou částku. Výsledkem vznikne síť připravená pro plný gigabitový přenos s vidinou možného budoucího rozšíření. Otázkou je, zdali je škola schopna vybudování dané sítě svépomocí. V případě zakázky může odhadem částka za přestavbu vyšplhat i ke 20 000 Kč. Daná firma však za provoz plně odpovídá a udává záruku. V případě naší modelové školy se jedná o výstavbu svépomocí, neboť škola má již zkušenosti z předchozí výstavby. Navíc se jedná o odbornou školu a může tak zapojit své studenty do praxe pro rozšíření jejich obzorů.

2.3.2 Výhody adresářové služby Active Directory

Již v teoretické části jsme si prozradili klady adresářových služeb spojené s centrální síťovou správou. V následujícím textu bychom se konkrétně měli krátce pozastavit nad výhodami využívání adresářové služby Active Directory (AD) ve školním prostředí a uvést tipy pro její následnou konfiguraci. Omezená kapacita dané literatury nedovoluje se přímo zaobírat samotnou instalací. Na internetu však existuje nespočetné množství návodů pro její instalaci. Služba Active Directory je dostupná

v operačním systému Windows Server od verze 2003 do současnosti. Dále tak budeme předpokládat, že se škole podařilo úspěšně nainstalovat a nakonfigurovat danou službu. Naším cílem bude plně nahradit síťový operační systém Novell a jeho služby. S instalací služby AD je nutné nainstalovat též názvový server (DNS) pro řízení názvů domény. Pro název domény doporučuji použít totožnou oficiální internetovou doménu školy. Vezmeme si kupříkladu Univerzitu Hradec Králové, která provozuje vlastní webovou prezentaci pod doménou *http://uhk.cz* a doména služby AD má totožný název *uhk.cz*. Pod definovanou doménu posléze zařadíme veškeré počítače v síti.

Jednou z výhod adresářových služeb je možnost ověřování uživatelských jmen centrálně skrz síťové prostředí. Škola se do současnosti tolik nezaobírala možnostmi síťového ověřování uživatelů do operačního systému a vše řešila lokálně. V případě celé učebny to znamenalo, obejít každý počítač zvlášť a definovat jeho účty. Nakonfigurované účty navíc byly značně obecné a potencionálně nebezpečné. Obsahovaly jednotné přihlašování, například *student* a totožné heslo známé pro veškeré studenty školy.

S použitím dané adresářové služby jsme schopni pro každého studenta nadefinovat jedinečný přihlašovací účet, který může využívat po celou dobu studia. Účet bude veden jeho jménem i heslem a bude za něj též zodpovědný. Pro návyky správné bezpečnostní politiky je vhodné uživatelům nadefinovat pravidla bezpečného hesla. Znamená to určit například minimální počet znaků hesla, jeho složitost (velká a malá písmena, číslovky, další znaky) či dobu jeho platnosti. Studenty i zaměstnance školy to nejen naučí tréninku vlastní paměti, ale upozorní na důležitost péče o vlastní soukromí. V případě nějaké škody jsme navíc schopni relativně rychle identifikovat posledního aktivního uživatele, který se již nebude skrývat za obecným jménem *student*.

Struktura uživatelského jména

Nejvhodnější podobou uživatelského jména je využití příjmení a křestního jména uživatele. Z příjmení si vezmeme prvních pět znaků, je-li příjmení kratší, užije se celé příjmení a již se nedoplňuje žádnými znaky. Dále si vypůjčíme první dva znaky křestního jména a posléze přidáme číslici zaručující jedinečnost uživatelského jména.

Uživatel jménem **Novoměstský Františ**ek má podobu uživatelského jména: ***novomfr1***. V případě výskytu stejné skladby jména, by měl další uživatel *novomfr**2***.

Cestovní profil

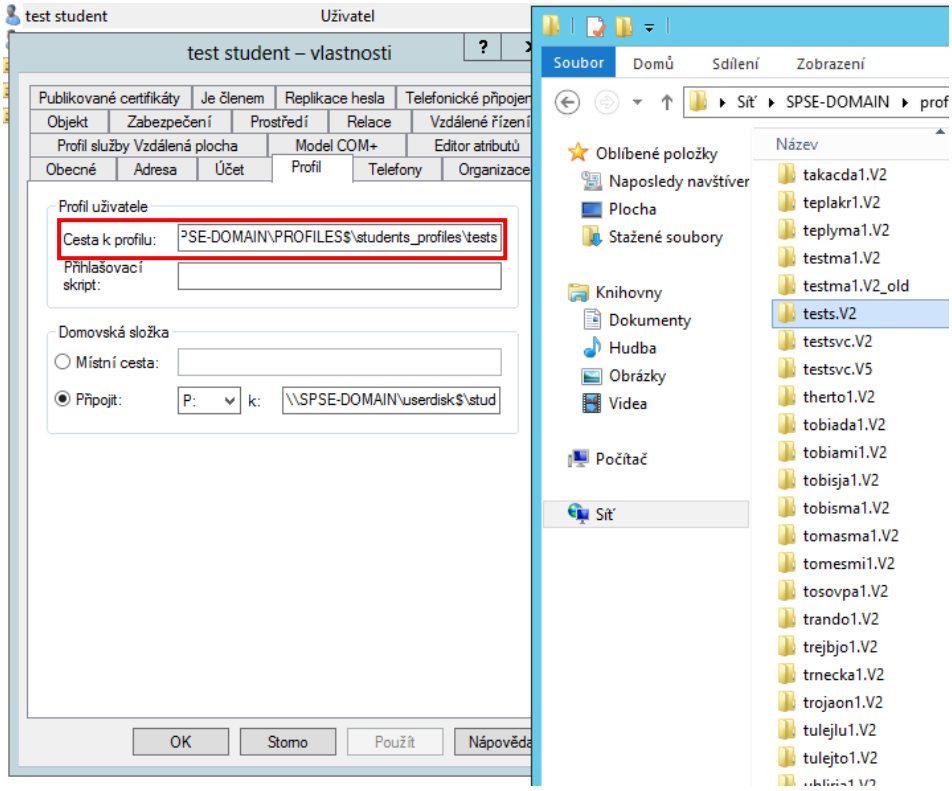
Cestovním profilem je speciální typ síťového uživatelského účtu v doméně AD u operačních systémů Windows. Tento typ profilu se hodí do takových síťových prostředí, kde uživatelé využívají více počítačů v síti pro svoji práci. Je tak ideální též pro školská prostředí, kdy se student může vyskytovat v různých počítačových učebnách. Bez cestovního profilu by veškeré jeho nastavení a soubory zůstávaly pouze na jednom lokálním počítači. Kdyby se pod svými údaji přihlásil na počítač jiný, přihlášení by díky centrální správě sice proběhlo, ale na daném počítači by se vytvořil znovu čistý profil bez dat. Cestovní profil se naopak po práci a odhlášení z počítače ukládá místo do lokálního úložiště na síťové úložiště serveru. Při přihlášení na jiný počítač je tento profil ze serveru stažen do lokálního počítače a po odhlášení je znovu na serveru přepsán na novější data. S uživatelem tak sítí cestuje nastavení jeho plochy, dokumenty, záložky, kontakty nebo rozmístění ikon. Pracovní plocha každého počítače vypadá shodně a uživateli nezáleží na fyzickém místě práce.

Konfigurace cestovního profilu

Konfigurace cestovní profilu je z pohledu správy relativně jednoduchou záležitostí. Správa doménových profilů AD probíhá v nástroji *Uživatelé a počítače služby Active Directory*. Po vytvoření nového uživatelského účtu klikneme pravým tlačítkem na **Vlastnosti**. Otevře se nové okno pro konfiguraci účtu. Cestovní profil konfigurujeme pod záložkou **Profil**, kde zadáme síťovou cestu pro profil. Tímto systému řekneme, že se jedná o cestovní profil s ukládáním na server. Předtím je nutné vytvořit sdílenou složku v síti. Nejlépe na serveru, kde provozujeme službu AD, případně na souborovém serveru. Příklad síťové cesty systému Windows:

```
\\SPSE-DOMAIN\PROFILES$\students_profiles\%username%
```

SPSE-DOMAIN představuje doménový název zařízení, kde bude profil ukládán. DNS server jej podle dynamicky generované tabulky domény přeloží na číselnou IP adresu. *PROFILES$* udává vlastní sdílenou složku, značka dolaru představuje označení skryté složky (v průzkumníku souborů není viditelná). Proměnná *%username%* se po potvrzení nastavení automaticky přepíše na pravé uživatelské jméno. Cestovní profil se v dané složce vytvoří automaticky při prvním přihlášení uživatele do domény. V dané cestě nalezneme složku s názvem uživatele s příponou.



Obr. 29 - Podoba konfigurace cestovního profilu

Zdroj: autor

Správa zásad skupiny

Jedná se o nástroj umožňující definovat skupinové restrikce a nastavení totožná pro každé zařízení a uživatele v doméně. Zásady je možné přímo směřovat pouze na skupinu uživatelů nebo počítačů. Po nainstalování AD již je automaticky nakonfigurováno pár zásad pro počítače i uživatele v síti. Pomocí zásad můžeme například přiřadit omezená práva pro studentské účty, zamezit instalaci a připojení vyměnitelných médií, zajistit mapování síťových jednotek, definovat pravidla uživatelského hesla nebo zamezit připojení k internetu. Nástroj je dostupný po nainstalování služby Active Directory. Konfigurace je přehledná a umožňuje další rozšířená nastavení. Pro síťové prostředí by se například mohlo hodit omezení celkové velikosti cestovních profilů nebo definování cest pro ukládání dokumentů, obrázků, videí, položek plochy či stažených souborů uživatele.

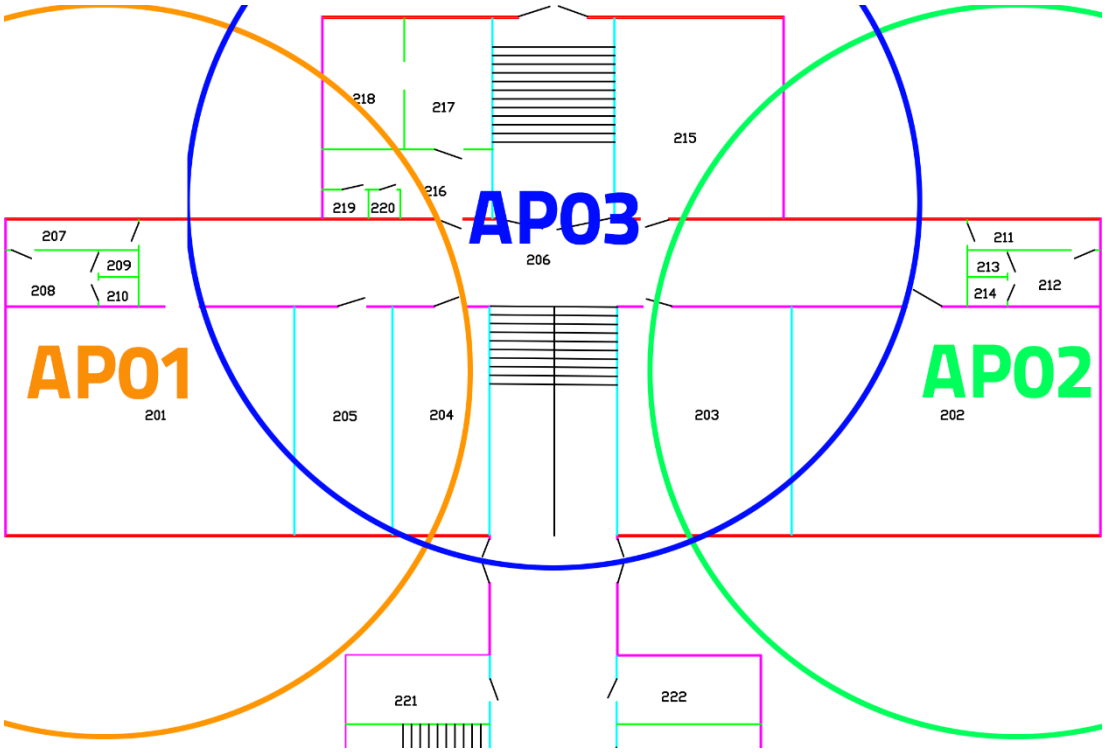
2.3.3 Návrh bezdrátové školní sítě

Pro udržení tempa se současným vývojem počítačových sítí je absence bezdrátové sítě relativně troufalým řešením. Na příkladu modelové školy provede návrh realizace bezdrátové sítě a příklady pro její vhodnou konfiguraci.

Základní úvaha

Pro rozšíření školní sítě o WLAN (bezdrátová lokální síť) bude nejdůležitějším aktivním prvkem přístupový bod (AP). Vzhledem ke skutečnosti, že síť bude využívána v rámci vnitřních prostor a nebude tolik rušena vnějšími vlivy, se jako nejvhodnější řešení nabízí využít stále nejrozšířenějšího pásma 2,4 GHz. Frekvence 5 GHz je z technického hlediska dokonalejším řešením, bohužel však stále existuje malé množství klientských zařízení, které s ním dokáží pracovat. Jako standard nám do daných prostor bohatě postačí *802.11g*. Daný standard umožňuje rychlost přenosu 54 Mb/s a vzhledem ke skutečnosti, že z většiny bude bezdrátová síť využívána pro přístup k internetu, je rychlost dostatečná. Oproti novějšímu standardu *802.11n* využívá výchozí šířku pásma (20 MHz) a není tak tolik náchylná k interferencím. Standard 802.11n může sice také využívat výchozí šířky pásma, přenosová rychlost je však přibližně srovnatelná s předchozím standardem. Pro rychlejší přenosové rychlosti okolo 150 Mb/s, které standard 802.11n umožňuje, již musíme využívat šířku pásma 40 MHz, čímž však vzniká vyšší procento vzájemné interference na pásmu 2,4 GHz.

Přístupové body pro vnitřní prostory obsahují všesměrovou anténu. Ta je s přihlédnutím různých faktorů ovlivňující bezdrátový přenos schopna pokrytí prostoru dvou standardních učeben. Všesměrové antény jsou uzpůsobeny k ideálnímu šíření signálu tzv. *„po patře“*. Ve výsledku nevyzařují signál do dokonalého tvaru koule, ale připomíná tvar koblihy. S přihlédnutím na dané vlastnosti a faktory vychází, že pro bezproblémové pokrytí všech funkčních části budovy školy nám nevystačí jeden přístupový bod. Síť bude složena pomocí několika přístupových bodů plnící vlastnosti topologie rozšířené oblasti služeb (ESS). V hlavní budově se bude nacházet celkem devět AP, strategicky rozmístěných po třech AP na patře. Ve zbylých částech komplexu umístíme dalších 8 AP. Celkem se o pokrytí bude podílet 17 AP. Škola se rozkládá na ploše 2 570 m^2, každé AP tak bude schopno pokrýt 150 m^2.



Obr. 30 - Teoretické rozmístění AP na jednom patře hlavní budovy

Zdroj: autor

Potřebné komponenty

Budování bezdrátové sítě spadá pod výstavbu kompletně nové oblasti sítě. Je to stejné jako vybudování a zasíťování nové učebny výpočetní techniky. Pouze s tím rozdílem, že dané komponenty budou fyzicky rozmístěny po celém objektu, ovšem logicky budou spadat do oblasti jedné podsítě. Pro přístupový bod se nabízí volit ověřeného výrobce profesionálních síťových technologií *Cisco*. Pořizovací cena takového bodu však přesahuje i 5 000 Kč. Na trhu tak existuje několik dalších výrobců, kteří si za dobu svého kvalitního fungování vysloužili zájem ze strany spotřebitelů a jejich cenová politika staví na méně movité zákazníky. Jedním z králů nelicencovaných bezdrátových technologií je i lotyšská firma *Mikrotik*. Jejich výrobky převážně využívají poskytovatelé bezdrátového připojení k šíření svých technologií. Daná firma před nedávnem představila vnitřně uzpůsobené AP přesně definované pro naše účely. Označuje se jako **MikroTik cAP-2n AP** a pracuje v pásmu 2,4 GHz využívající standardu 802.11b/g/n. Napájení AP probíhá skrze PoE (Power over Ethernet), což je standard šíření napětí skrz páry UTP kabelu přímo do konektoru RJ-45. Abychom nemuseli ke každému AP táhnout napětí z vlastního adaptéru, využíváme POE panel. Daný panel je podobný patch panelu a obsahuje dvě řady zásuvek RJ-45. Do horní

řady konektorů RJ-45 se připojují porty bez napájení (např. směrovač). Do spodní řady konektorů RJ-45 se připojují zařízení využívající napájení po síťovém kabelu. Pro dané účely volíme **WaveRF 24-portový pasivní POE panel – stíněný**. Panel je pasivní, je nutné jej napájet pomocí externího stejnosměrného zdroje. Pro naše účely se nejlépe hodí **Průmyslový napájecí zdroj POWER** s hodnotami napětí 12V a proudu 6A, což plně dostačuje pro napájení všech AP.

Jednotlivé přístupové body propojíme pomocí přepínače. K těmto účelům je nejlepší variantou přepínač **MikroTik Cloud Router Switch CRS125** obsahující 24 portů pro gigabitový přenos a konzoli pro umístění do síťového rozvaděče. Díky tomu, že se jedná o totožného výrobce, je možná centrální správa všech AP z daného zařízení.

Nesmíme zapomenout zakončit všechny trasy kabelů od jednotlivých AP do patch panelu. Pro dané účely nám plně postačí standardizace pro UTP kategorie 5e. Zvolíme základní 24 portový **Patch panel UTP cat.5e 24p 1U Black**.

Pro ochranu daných prvků zvolíme nástěnný rack, kde zakončíme veškerou technologii bezdrátové sítě. Volíme **Nástěnný rozvaděč Lexi-NET 9U** o rozměrech 600/450 mm.

Na závěr nesmíme opomenout na ostatní nutné příslušenství, jako je UTP kabel Cat5e pro spojení jednotlivých AP, síťové konektory, síťové zásuvky a další nutné příslušenství. V našem případě je nutné zakoupit plastové lišty pro ochranu kabelů.

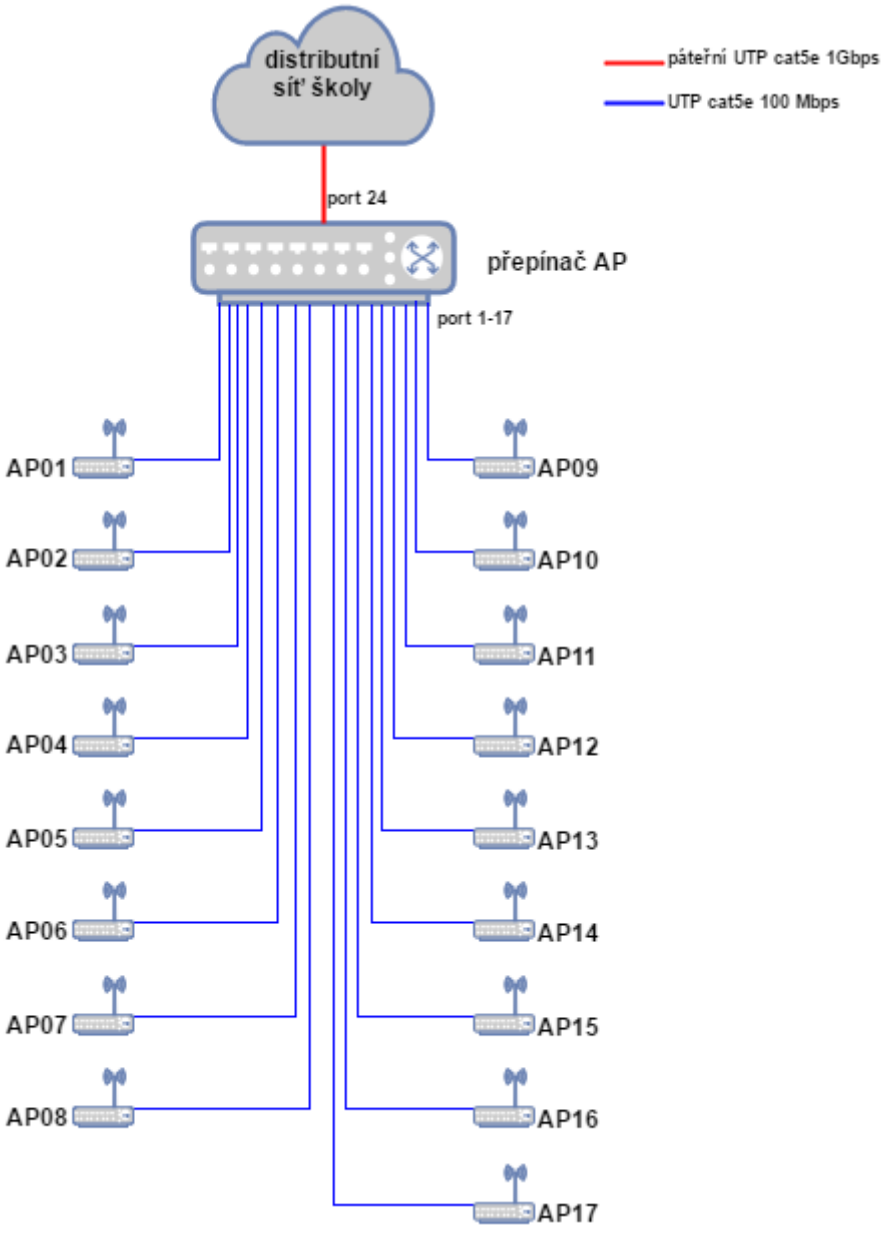
Náklady na vybudování

17x MikroTik cAP-2n AP/Hotspot 2,4 GHz, 802.11n - vnitřní	19 023 Kč
1x MikroTik Cloud Router Switch CRS125	4 376 Kč
1x WaveRF 24-portový pasivní POE panel - stíněný	1 203 Kč
1x POWER Průmyslový napájecí zdroj 12 V, 6 A	661 Kč
1x Patch panel UTP cat.5e 24p 1U Black	431 Kč
1x Nástěnný rozvaděč Lexi-NET 9U 600/450	2 670 Kč
2x SOLARIX, balení 305 m, UTP kabel Cat5E, drát, PVC	3 568 Kč
1x Konektor RJ45-8p8c,50µm Au, drát, nesklád, CAT5e, 100ks	318 Kč
17x zásuvka UTP RJ45 CAT6 na omítku	1 986 Kč
Další náklady za příslušenství	3 000 Kč
Celkem s DPH	**37 226 Kč**

Znovu se jedná o částku vynaloženou za samotné pořízení jednotlivých prvků. Tabulka sice počítá s dodatečnou částkou za příslušenství, ovšem finální částka se vždy může lišit s ohledem na rozmístění a náročnosti vybudování sítě.

Topologie zapojení

Zapojení jednotlivých prvků vychází z předem definované úvahy při nákupu potřebných komponentů. Jedná se o relativně jednoduchý způsob propojení do hvězdy. Jednotlivé přístupové body jsou zapojeny do portu 1 až 17 obsluhujícího přepínače. Dále je přepínač propojen pomocí páteřního kabelu do původní distribuční sítě školy. Na přesný způsob zapojení páteřní sítě se již daná kapitola nezaměřuje. V příkladu na modelovou školu by se však jednalo o propojení s centrálním směrovačem školy (SW1) viz obr. 27.



Obr. 31 - Topologie zapojení přístupových bodů

Zdroj: autor

Fyzické umístění přístupových bodů

Fyzické umístění jednotlivých přístupových bodů podléhá vzájemnému vykrytí mezi prvky. Jedná se o relativně náročný pracovní úkon. Samotné rozmístění přístupových bodů je relativně snadné. Zakoupené prvky obsahují vše potřebné pro jejich umístění na podélnou nebo příčnou zeď. Horší situací je tažení přenosového média k jednotlivým AP. Veškerá kabeláž vychází z racku umístěného v kanceláři zástupce. Školní komplex byl postupně budovaný mezi lety 1948-1970, kdy počítačové sítě byly pouze v plenkách. Budova nemá potřebné technické zázemí ani průtahy jednotlivých zdí. Škola tak na tyto úkony najala specializovanou technickou firmu, která provedla tažení kabeláže mezi jednotlivými přístupovými body. Tažení probíhá znovu pomocí plastových lišt z patch panelu v racku do zásuvky umístěné nedaleko AP.

Obr. 32 - Navrhovaný způsob fyzického zapojení AP

Zdroj: autor

Doporučená konfigurace bezdrátové sítě

Při konfiguraci bezdrátové sítě se budeme řídit pravidly definovanými pro topologie bezdrátových sítí ESS (rozšířená oblast služeb). Pro zajištění roamingu je nutné, aby veškeré přístupové body vysílaly totožný jedinečný identifikátor SSID. Pomocí něj bude docházet k připojování klientů bez ohledu na právě fyzicky připojované AP. Název SSID by měl vypovídat o významu využití sítě. Vhodným názvem by tak mohlo být: *WIFI_SKOLA, SKOLNI_WIFI, WIFI_STUDENT*, či kupříkladu *SKOLA_WLAN*. Dané SSID je nutné nastavit pro každé AP zvlášť. Dále je nutné zajistit, aby se připojeným klientům automaticky přidělila jedinečná logická adresa z předem definovaného rozsahu adres. Pro tyto účely využijeme služeb virtuální lokální síť (VLAN), o kterém se dále zmíním v následující kapitole. VLAN nám navíc umožní oddělit technickou podsíť a podsíť pro klienty. Technickou podsíť využijeme pro konfiguraci přístupových bodů (konfigurace prvků probíhá pomocí IP adres) a naopak podsíť pro klienty již bude čistě sloužit připojeným klientům.

Doporučené zabezpečení bezdrátové sítě

Pro síť daných rozměrů se rozhodně nabízí využít jedinečného ověřování pomocí standardu 802.11x skrz server RADIUS. RADIUS server je možné přímo propojit s databází Active Directory a využívat ověřování skrz doménové účty studentů a zaměstnanců. Díky tomuto řešení se jednotliví uživatelé hlásí pod totožnými vlastními údaji jako například při přihlašování do operačního systému počítače v doméně. Nehrozí tak prozrazení jednotného hesla při jiném způsobu šifrování. Navíc je možné využít definice skupin. Rozdělením skupin například na studenty a zaměstnance můžeme definovat jistá pravidla pro přístup do sítě. Nejzákladnějším pravidlem může být například omezení přístupu uživatelů ze skupiny *student* pouze po dobu vyučování od pondělí do pátku v čase 6:00 až 17:00. Mimo stanovený čas bude pokus o ověření ze strany studentů eliminován. Úvodní konfigurace je sice mírně náročnější, ale díky instalaci RADIUS serveru přímo na doménový řadič Windows Serveru je synchronizace relativně jednoduchá a rychlá. Možné návody řešení je možné nalézt pomocí vyhledávače na internetu. Zabezpečení využívá typu šifrování WPA-podnikové nebo WPA2-podnikové.

Filtrování požadavků

Z důvodu zajištění bezpečnosti a využívání školní bezdrátové sítě převážně pro studijní účely je vhodné navíc chránit přístup bezdrátové sítě do nebo z Internetu bránou firewall. Ta zajišťuje bezpečnost interní sítě, umožňuje logování provozu a filtruje nežádoucí provoz.

Vlastní navrhovaný seznam internetových služeb a protokolů, které je možné využívat z bezdrátové sítě školy:

- **HTTP** 80 (TCP)
- **HTTP** 8080 (TCP)
- **HTTPS** 443 (TCP)
- **FTP** 21 (TCP)
- **SSH** 22 (TCP)
- **Telnet** 23 (TCP)
- **DNS** 53 (TCP/UDP)
- **ICMP** (ping)
- **IMAP** 143 (TCP)
- **IMAPS** 993 (TCP)
- **POP3** 110 (TCP)
- **POP3S** 995 (TCP)
- **SMTP** 25 (TCP)
- **SMTPS** 465 (TCP)
- **SMTPS** 587 (TCP)
- **NNTP** 119 (TCP)
- **NNTPS** 563 (TCP)
- **RSYNC** 873 (TCP/UDP)
- **SVN** 3690 (TCP/UDP)
- **RTSP** 554 (TCP/UDP)
- **RTMP** 1935 (TCP)
- **L2TP** 1701 (UDP)
- **PPTP** 1723 (TCP/UDP)
- **OpenVPN** 1194 (TCP/UDP)
- **H.323** (TCP/1720,1503, UDP/1719)
- **SIP** (TCP/1863, UDP/5060)

Seznam obsahuje názvy jednotlivých služeb s číslem a druhem portů transportní vrstvy. K daným účelům postačí definice pravidel skrz stavovou inspekci paketů. Zamezíme tím například možnosti hraní online her využívající speciálních portů a využívání bezdrátové sítě čistě pro potřeby práce s informacemi.

2.3.4 Rozdělení podsítí na logické celky

Modelová škola v současnosti využívá jedné podsítě s prefixem /24, dovolující přiřadit 254 jedinečných logických adres pro hosty. Konkrétně se jedná o podsíť *192.168.0.0*/24 (třída C privátních IP adres). Pro hosty je možné využít IP adresy *192.168.0.1* až *192.168.0.254*. S rozšiřujícími službami hrozí, že daný počet IP adres nebude brzy dostatečný, zvlášť pokud zapojíme do dané podsítě i klienty bezdrátové sítě. Tento stav je možné vyřešit konfigurací nové podsítě, například *192.168.1.0*/24 a získat tak dalších 254 adres. Ke každé nové podsítí je však nutné přidat i nový směrovač, který umožňuje směrování paketů mezi jednotlivými podsítěmi. Případně pro každou podsíť tahat jedno fyzické přenosové médium. Existuje však jednodušší varianta řešení podsítí - pomocí virtuálních lokálních sítí (VLAN). Na celou rozsáhlou síť většinou postačí jeden směrovač zajišťující jejich směrování. Logicky můžeme oddělovat části připojené na jednom přepínači umožňující jejich konfiguraci. Znamená to, že část portů přepínače můžeme připojit do jednoho logického celku a jiné zase do druhého odděleného logického celku. Konfigurace VLAN je řešena na 2. vrstvě referenčního modelu OSI pomocí konfigurovatelných přepínačů. Abychom však mohli logické celky směrovat mezi sebou, potřebujeme zmiňovaný směrovač nebo přepínač s funkcí L3 (směrováním). Škola vlastní konkrétně trojici konfigurovatelných přepínačů (SW1, SW3 a SW4). Bohužel však nemá prvek, který by případné logické celky směroval, neboť nemá k dispozici vlastní směrovač. Nicméně by škola ráda využívala dané technologie a rozhodla se zainvestovat koupí vlastního směrovače, který může dále využít i na řízení dalších síťových služeb.

Potřebné komponenty

Hlavní záležitostí v daném případě bude nutnost pořídit pro potřeby školy relativně výkonný směrovač. Směrovače určené do domácností jsou z pohledu výkonu nepoužitelné. S ohledem na velikost sítě je nutné porozhlédnout se po firemních (profesionálních) řešeních. Trh s profesionální síťovou technikou je rozsáhlý. Navíc je možné pro potřeby směrování vyhradit výkonnější počítač architektury x86 (PC) s operačním systémem Linux. Dané řešení je ale relativně složité na správu a je nutné mít již určité zkušenosti. Ohledně vyhrazeného síťového řešení se znovu nabízí firma *Cisco* a jejich mocný operační systém užívaný na přepínačích a směrovačích IOS. Správa většinou probíhá v pomocí příkazové řádky a pro jeho správu je též nutné mít již jisté vlastní zkušenosti. Navíc firemní řešení Cisco jsou relativně drahá na pořízení.

Znovu je tak vhodné zastavit se u řešení lotyšské firmy *Mikrotik*. Jejich nabídka obsahuje zařízení spadající pod sérii *Cloud Series Devices*. Jedná se o výkonnou řadu přepínačů a směrovačů založenou na operačním systému RouterOS. Tento specializovaný operační systém původem vychází z Linuxu a je možné jej spravovat skrz grafické i webové rozhraní. Pro zajištění budoucího rozvoje sítě navrhuji zvolit jeden z nejvýkonnějších směrovačů dané série, konkrétně **Mikrotik CCR1036** s 12x Gbit porty a 4 GB operační paměti. Vzhledem k více verzím daného produktu je přesné označení směrovače **Mikrotik CCR1036-12G-4S**. Směrovač obsahuje výkonný procesor uzpůsobený pro síťový provoz s 36 individuálními jádry a pracovní frekvencí 1,2 GHz. Daný směrovač je plně gigabitový a umožňuje celkově zpracovat až 8 miliónů paketů za sekundu s propustností až 16 Gb/s. Jedná se o velice výkonné řešení, které zajistí, že síť nebude zpomalována z důvodu nedostatečné hardwarové kapacity, a to i do budoucna. Navíc díky značně konfigurovatelnému operačnímu systému směrovače je možné směrovač dále využít jako Firewall, DHCP server nebo NAT.

Náklady na pořízení

1x směrovač Mikrotik CCR1036-12G-4S	22 593 Kč
Celkem s DPH	**22 593 Kč**

Vyšší pořizovací cena je dána výkonem aktivního prvku a široké možnosti jeho využití. Pomocí jednoho zařízení můžeme navíc provozovat více síťových služeb i přes splnění základního požadavku na směrování. Hlavní funkcí směrovače bude směrování mezi jednotlivými logickými celky, ale díky možnosti ostatních služeb je možné definovat například dynamické přiřazování IP adres pro jednotlivé logické podsítě. Firma Mikrotik nabízí i levnější řešení ze stejné série směrovačů, kdy ceny začínají na částce necelých 10 000 Kč. I v tomto případě se jedná o dostatečně výkonné řešení, ačkoliv způsobuje menší použitelnost do budoucna.

Logické rozdělení sítě

Již bylo naznačeno, že podsítě budeme řešit logicky pomocí přidání čísla VLAN (tagu) do rámce. Všechny přepínače mají defaultně nastavený výchozí VLAN číslo 1 (VLAN1). U konfigurovatelných přepínačů je možné přidat jiné číslo VLAN, čímž logicky vznikne jiná oblast, neboť jsou rámce vycházející z takto upraveného portu značeny odlišným číslem VLAN. Na jednom fyzickém portu přepínače je možné

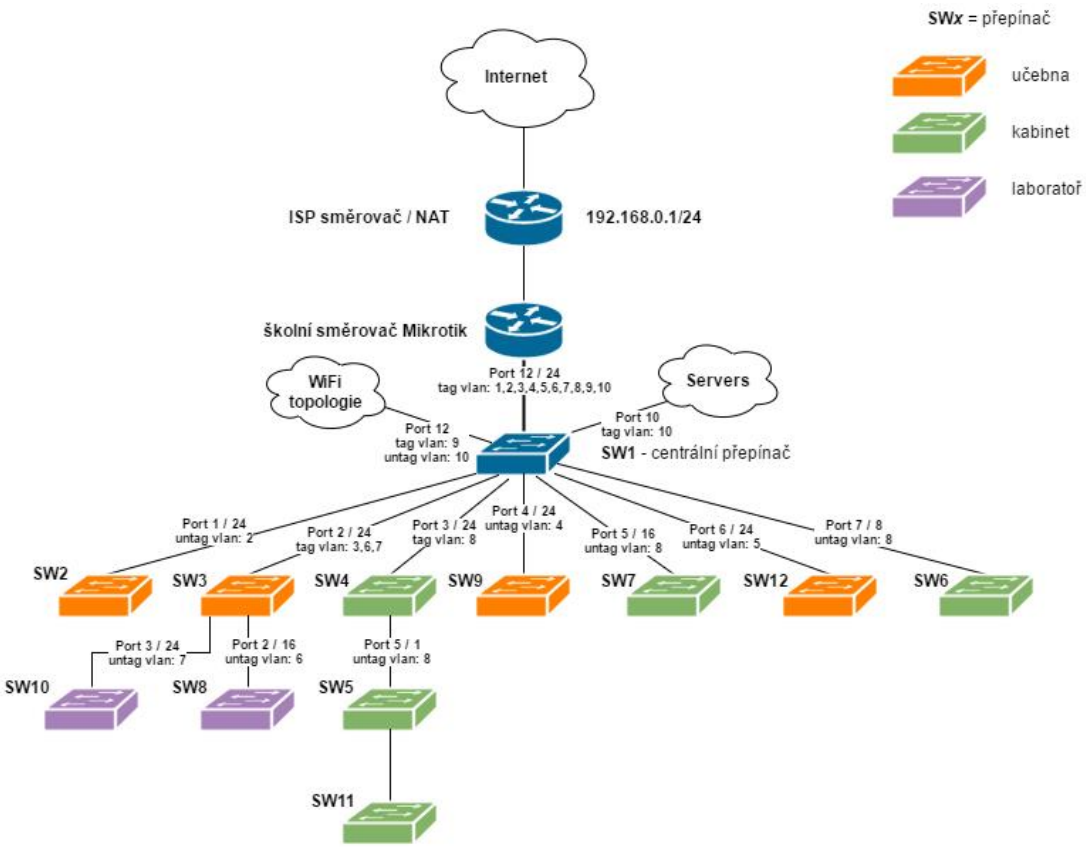
definovat vícero logických sítí a dosáhnout tak odděleného provozu na jediném přenosovém médiu. Na dané vrstvě navíc není možné, aby spolu dva logicky oddělené celky mohly komunikovat. Toto je možné definovat až na vrstvě síťové, kde se také přiřazují logické adresy (IP adresy) jednotlivých zařízení v daných celcích. Před samotnou konfigurací je nutné zamyslet se nad logickým rozdělením celé sítě. Provedeme-li rekapitulaci stavu sítě modelové školy podle obr. 27, přijdeme na následující podobu. Škola má celkem čtyři počítačové učebny, takže pro každou učebny se vytvoří samostatný logický celek. Dále zde máme dvě odlišné laboratoře praktické výuky, kdy každá učebna využívá své speciální zařízení a příslušenství. Znamená to přidání dalších dvou VLAN pro jednu laboratoř. Poslední známou částí jsou kabinety, kde jsou umístěny počítače pro tvorbu výukových materiálů, síťové tiskárny a scannery. Této oblasti je vhodné přiřadit také vlastní logickou podsíť. Postupem času nám však vznikly další oblasti sítě, jako je technologické zázemí pro servery a aktivní prvky sítě nebo podsíť pro klienty bezdrátové sítě. Logické rozdělení naznačí následující tabulka.

ID	Popis
VLAN1	*defaultní VLAN (nelze změnit)*
VLAN2	učebna výpočetní techniky 1 (VYT1)
VLAN3	učebna výpočetní techniky 2 (VYT2)
VLAN4	učebna výpočetní techniky 3 (VYT3)
VLAN5	učebna výpočetní techniky 4 (VYT4)
VLAN6	laboratoř Cisco
VLAN7	laboratoř mikroprocesorové techniky
VLAN8	kabinety + kanceláře
VLAN9	bezdrátová síť
VLAN10	servery + technologická část sítě

Tabulka 5 - Logické rozdělení školní sítě podle oblastí

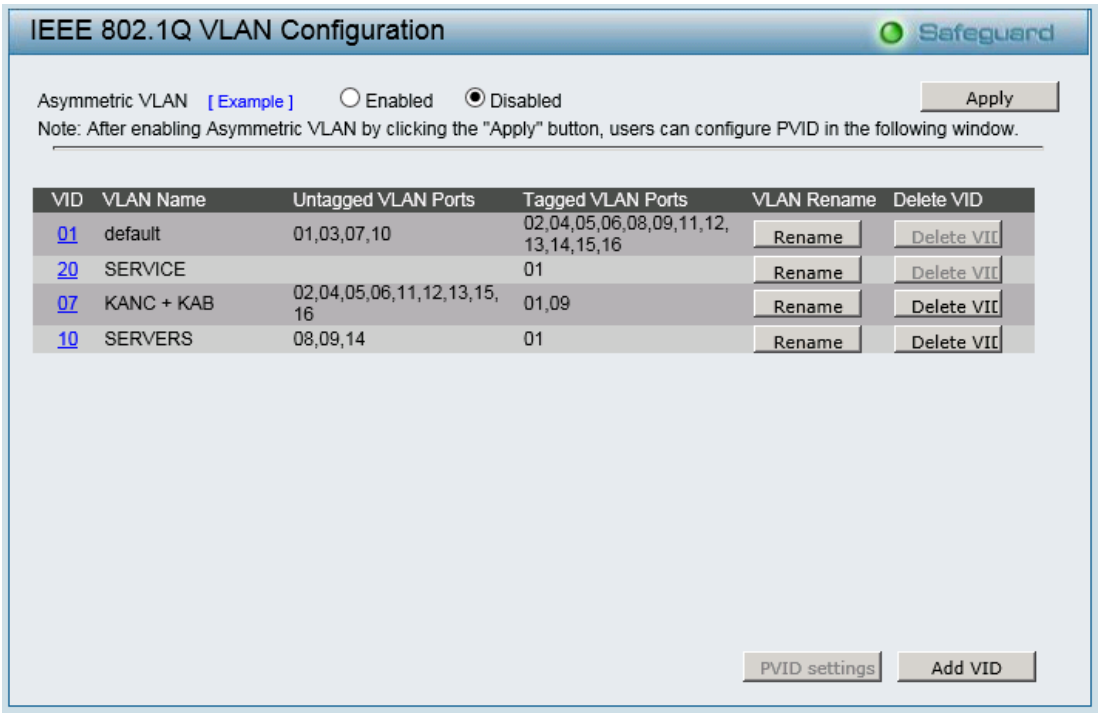
Zdroj: autor

Nepočítáme-li výchozí VLAN1, celou podsíť jsme rozdělili na devět logických celků, které můžeme dále rozdělit na jednotlivé podsítě a zamezit tak případnému nedostatku IP adres. Rozdělení bude realizováno primárně na konfigurovatelném centrálním přepínači, zatímco bude pro jednotlivé zapojené porty definováno číslo VLAN. Výjimka se týká pouze portů k přepínačům SW3 a SW4. Tyto přepínače mají z důvodu dále se nacházejících aktivních prvků též možnost konfigurace VLAN. Na těchto portech tak nebude napřímo nastaveno číslo VLAN (untag), ale pouze označena čísla VLAN, které mohou portem procházet (tag). Více naznačují následující obrázky.



Obr. 33 - Topologie logického rozdělení sítě modelové školy

Zdroj: autor



Obr. 34 - Ilustrační obrázek znázorňující konfiguraci VLAN

Zdroj: autor

Nastavení překladu adres pro přístup k internetu

Původní rozsah podsítě modelové školy byl definován ze strany poskytovatele internetových služeb a měl již zmiňovanou podobu **192.168.0.0/24**. Daný rozsah je nastaven na ISP směrovači umožňující přístup do sítě Internet. Znamená to, že ISP směrovač zná pouze zařízení z dané podsítě a v případě vytvoření nových podsítí s odlišným rozsahem by na zařízení nereagoval. Nové podsítě by tak neměly přístup do internetu. Škola bohužel nemá přístup k danému směrovači, ale díky pořízení vlastního směrovače může využít jeho potenciálu při využití služby pro překlad adres (NAT). Ve výsledku postačí umístit školní směrovač mezi centrální přepínač (SW1) a ISP směrovač, jak již znázorňuje obr. 33. Port, který je přímo propojený na ISP přepínač, bude mít IP adresu z výše uvedeného rozsahu, například **192.168.0.2/24**. Posléze postačí konfigurovat NAT tak, aby veškeré požadavky z vnitřní sítě do internetu překládal na tuto IP adresu a ve vnitřní síti již může být jakákoliv jiná třída privátních IP adres. Požadavky putující za oblast vnitřní sítě školy vystupují pod IP adresou školního směrovače, která spadá do podsítě konfigurované na prvku směrujícím dále do světa.

Rozsah IP adres pro jednotlivé logické podsítě

Po úspěšném rozdělení sítě na logické celky je nutné definovat pro jednotlivé VLAN vlastní rozsahy IP adres pro zajištění správné komunikace mezi zařízeními. Konfigurace rozsahů bude probíhat na pořízeném školním směrovači. Rozsahy IP adres se definují přímo na vytvořenou virtuální lokální síť. Na úvod je nutné se rozhodnout, jakou třídu adres zvolíme pro nově definované podsítě. Škola původně využívala podsíť patřící pod třídu C. Nyní je vhodné, ovšem ne nutné, zvolit odlišnou třídu privátních IP adres. Rozhodnutí padlo na třídu B s rozsahem umožňující přiřadit až 1 048 576 jedinečných adres. Základní rozsah adres dané třídy je 172.16.0.0 – 172.31.255.255 s prefixem 172.16.0.0/**12**. Z daného rozsahu je možné vytvořit menší podsítě obsahující méně bitů pro hosty. Kupříkladu se standardním prefixem /**24** dovolujícím přiřadit 254 jedinečných adres (posledních 8 bitů pro hosty). Danou hodnotu prefixu zvolíme pro všechny VLAN, neboť 254 IP adres do každého logického celku je dostatečná rezerva. Zvlášť, když škola donedávna takto velkou podsíť užívala na celou svoji síť. Problém by mohl nastat pouze v případě klientů bezdrátové sítě. Ve škole se denně vyskytuje více než 300 osob a počet adres pro hosta je tak nutné dimenzovat na toto číslo osob. Znamená to, že místo standardních 8 bitů

pro hosta, přidáme jeden bit navíc. U rozsahů s prefixem **/23** jsme schopni využít až 510 adres pro hosty, což už je dostatečný počet pro obsluhu všech klientů. Pro lepší orientaci bude třetí Byte síťového rozsahu odpovídat číslu VLAN. Definice rozsahu pro VLAN**7** bude mít podobu 172.16.**7**.0/24. Tento systém není možné dodržet u rozsahu pro bezdrátovou síť, neboť by z důvodu vyššího počtu adres pro hosty přesahoval rozsah i do IP adres definovaných pro VLAN10. Pro bezdrátovou síť (VLAN9) definujeme rozsah 172.16.**90**.0/23. Konkrétní rozsahy jednotlivých logických podsítí naznačuje následující tabulka.

ID	Popis	Rozsah	Adresy hostů
VLAN1	*defaultní VLAN*	-	-
VLAN2	učebna VYT1	172.16.2.0/24	172.16.2.1 - 172.16.2.254
VLAN3	učebna VYT2	172.16.3.0/24	172.16.3.1 - 172.16.3.254
VLAN4	učebna VYT3	172.16.4.0/24	172.16.4.1 - 172.16.4.254
VLAN5	učebna VYT4	172.16.5.0/24	172.16.5.1 - 172.16.5.254
VLAN6	laboratoř Cisco	172.16.6.0/24	172.16.6.1 - 172.16.6.254
VLAN7	laboratoř MPT	172.16.7.0/24	172.16.7.1 - 172.16.7.254
VLAN8	kabinety	172.16.8.0/24	172.16.8.1 - 172.16.8.254
VLAN9	bezdrátová síť	172.16.90.0/23	172.16.90.1 - 172.16.91.254
VLAN10	servery	172.16.10.0/24	172.16.10.1 - 172.16.10.254

Tabulka 6 - Definice rozsahů jednotlivých logických podsítí

Zdroj: autor

2.3.5 Rychlý způsob blokování nevhodného obsahu

Na internetu je možné nalézt nepřečetné množství informací a odvětví. Bohužel zde však nalezneme i taková odvětví, která nemají ve veřejném prostředí školní instituce co pohledávat. Bavíme se zde o odvětvích zabývajících se násilným, pornografickým, rasistickým a jiným nevhodným obsahem. Tyto materiály mohou nesprávně působit na morální vývoj mládeže a mělo by být vynaloženo úsilí pro jejich maximální omezení. Většina škol řeší tuto problematiku výslovným zákazem ve školním nebo provozním řádu. Otázkou zůstává, zdali i úspěšně. V odvětví počítačových sítí existuje několik účinných způsobů, jak alespoň částečně zamezit možnosti jejich zobrazení. Liší se složitostí své konfigurace a správy. Z důvodu omezených lidských zdrojů bychom měli definovat takové řešení, které je jednoduché pro svoji správu a nabízí levné východisko pro zabezpečení problému. Denně přibyde na internetu několik tisíc nových stránek. Musíme nalézt takové řešení, které je schopné co nejúčinněji zamezit přístupu k novým stránkám a neobtěžovat nutností denní aktualizace databáze.

Blokování skrz veřejný názvový server

Nejúčinnějším řešením pro dané účely by byla konfigurace vlastního Proxy serveru. Ve výsledku se však jedná o relativně náročnou operaci, ke které je nutné mít již získaný určitý stupeň vědomostí. Existuje rychlé východisko v podobě využití specializovaného názvového serveru (DNS) pro možnost téměř okamžitého zablokování nevhodného obsahu. Filtrování probíhá na úrovni překladů názvu domén. Dorazí-li na takový server požadavek na překlad domény, která je vedena v černé listině, adresa není přeložena a přístup je blokován. Výhodou je, že ze strany školy stačí pouze nakonfigurovat primární a sekundární adresu daného názvového serveru na svém školním směrovači a blokování začíná být aktivní. Aktuálnost databáze černé listiny adres spravuje přímo provozovatel názvového serveru. Existuje několik provozovatelů zmiňovaných serverů, mezi nimiž nalezneme řešení, která jsou nabízena zcela zdarma, a to buď po registraci či dokonce přímo, bez nutnosti se registrovat. Nejvhodnějším kandidátem ze serverů s nutností bezplatné registrace je portál *http://www.opendns.com/* spadající pod společnost Cisco. Po registraci je možné zaškrtnout přímo celá odvětví, která chcete zakázat, případně pouze individuální domény. Pro nejrychlejší blokaci bez nutnosti registrace doporučuji službu na adrese *https://dns.norton.com/configureRouter.html*, která je provozována ze strany společnosti Norton. Na dané adrese si můžeme vybrat ze třech tříd úrovně blokace:

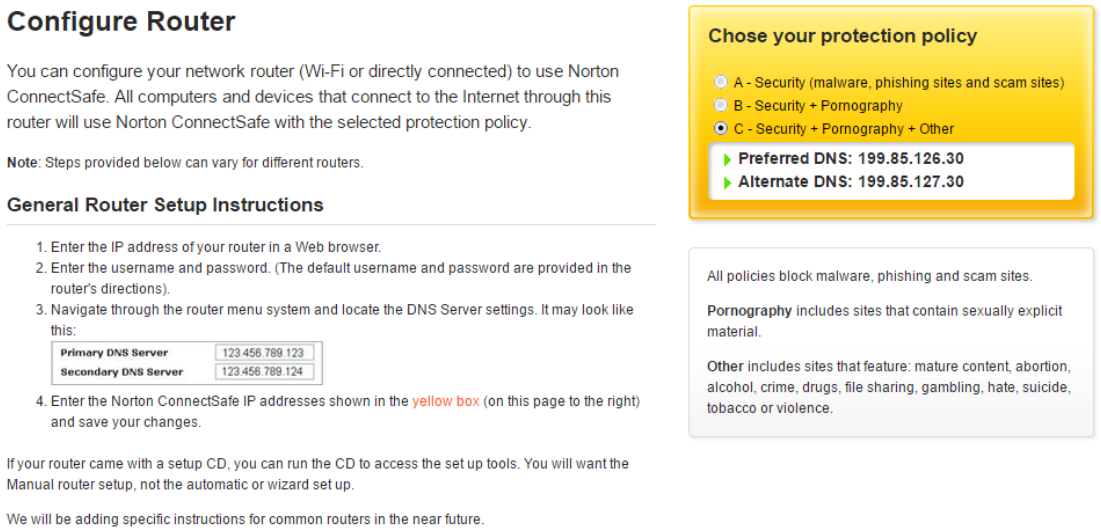
A. Třída **Security** – blokace stránek obsahující malware, podvodné a reklamní stránky (adresy DNS serverů: 199.85.126.10, 199.85.127.10).
B. Třída **Security + Pornography** – kromě výše zmíněného dochází k blokaci stránek se sexuálním a pornografickým kontextem (adresy DNS serverů: 199.85.126.20, 199.85.127.20).
C. Třída **Security + Pornography + Non-Family Friendly** – politika účinná k ochraně proti kontextu zabírajícím se drogám, alkoholismu, hazardním hrám, nenávisti, násilí, sebevraždám či tabáku (adresy DNS serverů: 199.85.126.30, 199.85.127.30).

Abychom 100% zaručili nemožnost vlastní úpravy těchto DNS serverů ze strany klientů, je nutné na školním směrovači nastavit nové pravidlo NAT pro požadovanou podsíť, kde chceme obsah blokovat (doporučuji nastavit pro všechny podsítě):

```
chain=dstnat action=dst-nat to-addresses=199.85.126.30 to-
ports=53 protocol=udp src-address=172.16.2.0/24 dst-port=53
```

Daný příklad nastavení je určen pro síťový systém RouterOS, jehož pořízení bylo doporučováno v předchozí kapitole.

Pravidlo vymezuje, aby veškeré odesílané požadavky na portu 53 (DNS) byly přesměrovány na adresu DNS serveru **199.85.126.30**, což je jeden ze serverů ze třídy C ochrany společnosti Norton. Tyto žádosti budou zpracovány v případě, že je požadavek odesílán z podsítě s rozsahem **172.16.2.0/24**. Zmiňovaný rozsah jsme v minulé kapitole přiřadili logické podsítí pro učebnu *výpočetní techniky 1* (VYT1). Aby bylo pravidlo aktivní i na jiných podsítích, je nutné jej definovat znovu s pozměněnou zdrojovou adresou rozsahu (src-address).



Obr. 35 - Ukázka informací o službě pro blokování obsahu skrz DNS

Zdroj: [16]

Obr. 36 - Výpis zprávy při pokusu navštívit stránky s blokovaným obsahem

Zdroj: autor

2.3.6 Zabezpečení webového rozhraní systému Bakaláři

Věřím, že Bakaláře, aneb program pro vedení a správu školní administrativy, nemusím dlouze představovat. Daný systém využívá ke své administrativě nadpoloviční většina českých základních a středních škol. Jedná se o výkonný nástroj s dlouholetým vývojem a přizpůsobením se potřebám škol. Díky jednotnému systému a databázi je možné dokonale využít všech možností práce s agendou. Od seznamu jednotlivých studentů, tříd, zápisů známek, tvorby rozvrhů, po například zobrazení výchovných opatření. Pro lepší spojení rodičů a veřejnosti se školou slouží modul webového rozhraní, který si školy mohou podle návodu na oficiálních stránkách samy nakonfigurovat. Přihlašování do rozhraní je řešeno jedinečným jménem a heslem. Po zadání správných údajů jsou uživateli zobrazena relativně citlivá data o požadovaném žákovi (studentovi). Zde vzniká jisté bezpečností riziko, neboť většina škol provozuje dané rozhraní skrz standardní nezabezpečený protokol HTTP. Hrozí možné odposlechnutí komunikace mezi serverem a klientem třetí stranou, tedy možnost úniku citlivých údajů. V následujících několika odstavcích si ukážeme postup pro zabezpečení webového rozhraní pomocí zabezpečeného protokolu HTTPS skrz jedinečný ověřený certifikát. Případné třetí straně tak alespoň minimálně ztížíme možnost dalšího odposlechu. Text předpokládá již dokončenou základní instalaci webové aplikace pod webovou službou IIS od Microsoftu.

Získání ověřeného certifikátu

Abychom mohli provozovat zabezpečený protokol HTTPS, musíme si nejprve nechat vystavit ověřený SSL certifikát. Je možné si sice vystavit a podepsat vlastní certifikát, ale webové prohlížeče před samotným zobrazením stránky vypisují chybu certifikátu a upozorňují návštěvníka o možném nebezpečí. Pro zamezení daného upozornění, je nutné si nechat certifikát vystavit od ověřeného vydavatele certifikátů. Vystavení takového SSL certifikátu je většinou za roční poplatek a navíc existuje více jejich druhů a jsou cenově ohodnoceny podle úrovně zabezpečení. Pro dané účely bohatě poslouží certifikát s ověřením na úrovni domény, který je nejlevnější. V současnosti existuje dokonce pár certifikačních autorit, které danou úroveň certifikátu vydají zdarma po registraci. Nejznámější je komunitní certifikační autorita *CAcert.org*. Cena za placený certifikát pak začíná na 139 Kč za rok. Největší výběr certifikátů je možné získat na adrese *http://www.ssls.cz/*. Pro vydání samotného certifikátu je nutné si nejprve vygenerovat tzv. CSR žádost pro následné vystavení

SSL certifikátu. Zde vyplníte základní informace o doméně, pod kterou webové rozhraní provozujete (například *baka.spsskola.cz*) a základní údaje o škole. Žádost je možné si vystavit přímo ve službě IIS pod záložkou *Certifikáty serveru*, případně rychleji pomocí webového prohlížeče, kupříkladu *https://www.ssls.cz/csr/*. Vygenerovanou žádost i s primárním klíčem předáte vybrané certifikační autoritě, která na jejich základu vystaví ověřený SSL certifikát.

Import certifikátu do webové služby

Standardně je většina SSL certifikátů vystavena ve formátu PEM (přípona .crt či .cer). Pro plnou kompatibilitu s webovou službou IIS je nutné takový certifikát exportovat do formátu PKCS#7 (přípona .p7b). Postup pro export je následující:

1. Klikněte dole na tlačítko Start a vyhledejte program *certmgr.msc*.
2. Klikněte pravým tlačítkem myši na složku *Osobní* > Všechny úkoly > Importovat a postupujte podle instrukcí pro nahrání PEM certifikátu.
3. Klikněte na importovaný certifikát pravým tlačítkem myši > Všechny úkoly > Exportovat.
4. Klikněte na tlačítko *Další* > vyberte formát certifikátu P7B a dokončete průvodce.

Podařilo-li se nám bezpečně vyexportovat certifikát v podporovaném formátu, otevřeme program pro správu webové informační služby a pokračujeme podle následujících kroků:

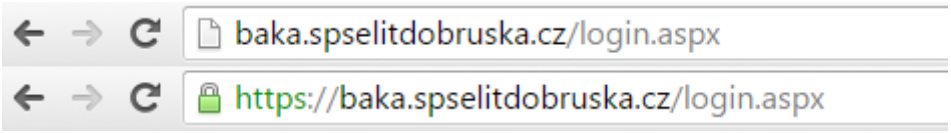
1. V levém části správce vybereme název počítače, pod kterým služba běží.
2. V prostřední části správce se v sekci IIS nachází ikona s názvem *Certifikáty serveru*, do ní se dostanete dvojitým kliknutím.
3. V pravé části správce vybereme název akce *Dokončit žádost o certifikát*.
4. Po zadání názvu a cesty k exportovanému P7B certifikátu, dojde k jeho importování do služby IIS.

Konfigurace zabezpečeného webového protokolu

Pro konfiguraci zabezpečeného protokolu HTTPS se vrátit k programu pro správu webové informační služby (IIS) a postupovat pomocí následujících kroků:

1. V levém části správce rozklikneme složku *Weby*.
2. Pravým tlačítkem myši klikneme na virtuální web, obsahují aplikaci webového portálu a vybereme možnost *Upravit vazby…*.
3. V otevřeném okně by se měla pouze zobrazit vazba nezabezpečeného protokolu http s portem 80, klikneme tak na tlačítko *Přidat…*.
4. V položce *Typ* nastavíme **https**, položku *IP adresa* necháme na výchozí hodnotě a *Port* nastavíme na standardní **443**.
5. Pod položkou *Certifikát SSL* vybereme námi importovaný ověřený certifikát a nastavení potvrdíme tlačítkem *OK*.

V daném okamžiku je možné zobrazit webový portál skrz zabezpečený protokol HTTPS a vytvořit tak zabezpečené spojení mezi klientem a serverem. Postačí k příkladové doméně *baka.spsskola.cz* přidat řetězec **https://***baka.spsskola.cz*. V adresním řádku prohlížeče se zobrazí ikonka visacího zámku. Rozdíl informování o typu protokolu ve webovém prohlížeči ilustrativně dokládá následující obrázek.



Obr. 37 - Nezabezpečený a zabezpečený protokol v prohlížeči Chrome

Zdroj: autor

Automatické přesměrování na zabezpečený protokol

I přes správně nakonfigurovaný zabezpečený protokol HTTPS nemáme jistotu, že všichni uživatelé budou k webovému rozhraní přistupovat se zadaným řetězcem **https://**. Webový portál je totiž stále aktivní též pod nezabezpečeným protokolem, který má před zabezpečeným přednost. Řešením může být jeho úplné zakázání, jenže u nezkušených uživatelů by se stránky hlásily jako nefunkční. Lepším řešením je konfigurace automatického přesměrování veškerých požadavků na zabezpečený protokol HTTPS. Ve výsledku to znamená, že pokud uživatel podá požadavek pod nezabezpečeným HTTP, bude automaticky přesměrován na zabezpečený HTTPS. Abychom mohli dané přesměrování v programu pro správu webové informační služby nakonfigurovat, je potřeba doinstalovat speciální modul pro IIS. Název modulu zní **URL Rewrite** a je ke stažení z *http://www.iis.net/downloads/microsoft/url-rewrite*.

Po úspěšné instalaci se nám v prostřední části správce pod sekcí IIS zobrazí nová ikonka s názvem URL Rewrite. Daný modul je pouze v angličtině, následující postup bude tak obsahovat anglické názvosloví.

1. V nabídce daného modulu klikneme v pravé části správce na *Add Rule(s)…*.
2. V novém okně zvolíme v sekci **Inbound rules** možnost *Blank rule*.
3. Individuálně pojmenujeme nové pravidlo, například *HTTPS redirect*.
4. V oblasti **Match URL** nastavíme:
    a. **Requested URL:** Matches the Pattern
    b. **Using:** Regular Exprresions
    c. **Pattern:** .*
    d. zaškrtneme volbu **Ignore case**.
5. V oblasti **Conditions** přidáme nové pravidlo volbou *ADD…* a nastavíme:
    a. **Conditions input:** {HTTPS}
    b. **Check if input string:** Matches the Pattern
    c. **Pattern:** off
    d. zaškrtneme volbu **Ignore case**.
6. V oblasti **Action** nastavíme:
    a. **Action types:** Redirect
    b. **Redirect URL:** https://{HTTP_HOST}/{R:0}
    c. **Redirect type:** Found (302)
    d. zaškrtneme volbu **Append query string**.
7. V pravé části klikneme na volbu *Použít*

Od tohoto okamžiku je automatické přesměrování aktivní. Veškeré požadavky na webový server jsou přesměrovány pod zabezpečený protokol HTTPS. Není možné, aby kdokoliv přistupoval pod nezabezpečeným protokolem a ohrozil možnost úniku citlivých údajů včetně přihlašovacího jména a hesla.

3 Výzkumná část

Výzkum si klade za cíl zjistit aktuální situaci počítačových sítí na středních školách z hlediska použitého hardwaru, firmwaru a bezpečnostního nastavení. Šetření je konkrétně cíleno na prostředí středních škol z Královéhradeckého a Pardubického kraje. Zpracované výsledky mají zobrazovat reálnou situaci sítí veřejného sektoru. Šetření nebylo cíleno na školy podle vybraného zaměření, ale byly požádány veškeré školy nabízející vzdělání v daných krajích. Podle současného RVP patří informatická gramotnost k jedné z nejdůležitějších vzdělávacích disciplín. Školy by tak měly být schopny poskytnout alespoň základní znalosti z tohoto oboru a vlastnit patřičné vybavení využívající síťové připojení.

3.1 Základní informace

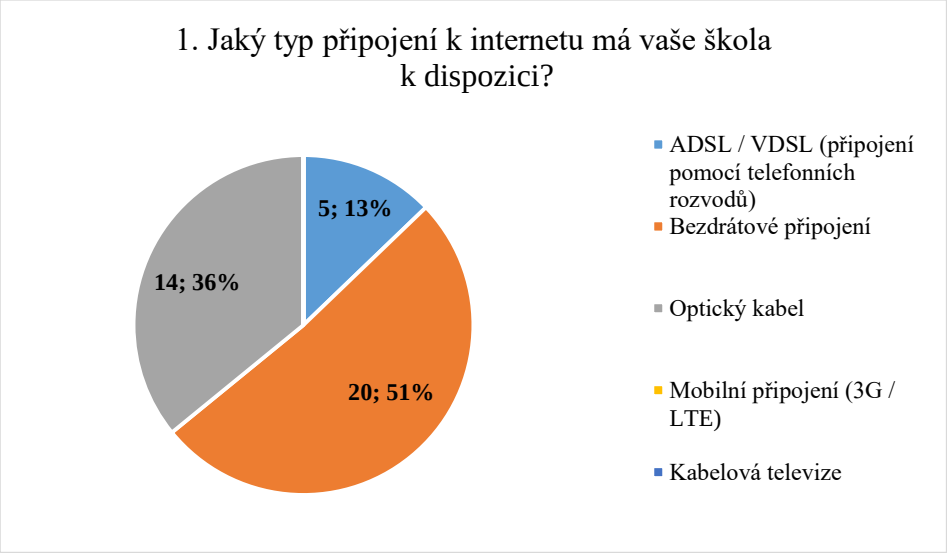
Data pro výzkum byla získána formou internetového dotazníkového šetření. Jedná se o jednu z kvantitativních metod způsobem psaného řízeného rozhovoru. Vzhledem k počtu původně oslovených respondentů (vedení škol) vychází dotazník jako nejméně časově náročnou formou výzkumu například oproti rozhovoru. Při konstrukci dotazníku je nutné si promyslet a přesně definovat hlavní cíl dotazníkového průzkumu a podle něj logicky a stylisticky správně připravit konkrétní dotazy. Podoba otázek v dotazníku může být formou otázek uzavřených, otevřených a škálovatelných. Metody používané v teorii a praxi a tedy i dotazníky musí být vědecké, objektivní, standardní, spolehlivé, platné (validní), kvantitativně i kvalitativně interpretovatelné a úsporné. Jenom tak mohou přinášet nové poznatky a verifikovat je. [13]

Dotazníkové šetření probíhalo během měsíce března roku 2016. Pomocí aplikace *Formuláře Google Drive* bylo sestaveno 12 strukturovaných otázek, jejichž obsah je možné posoudit v následující kapitole. Celkově byly osloveny veškeré střední školy (veřejné, soukromé, církevní) umístěné na území Královéhradeckého a Pardubického kraje. Ze 138 respondentů se k odpovědi ochotně odhodlalo 39 škol. Oslovení probíhalo elektronickou formou skrz mailovou zprávu na oficiální kontaktní e-mail školy. Veškeré dokumenty spojené s tvorbou dotazníku, konkrétně jeho přesné znění, průvodní dopis a seznam zúčastněných škol je možné získat v příloze. Dotazník je možné si též prohlédnout online na adrese: *http://goo.gl/forms/4X0KE6SPoc*.

3.2 Analýza výzkumu

1. Jaký typ připojení k internetu má vaše škola k dispozici?

Nejčetnější odpovědí otázky týkající se typu připojení k internetu bylo bezdrátové připojení. Využívá ho více než polovina (51%) dotazovaných institucí. Optického kabelu využívá 36% škol a připojení pomocí telefonních rozvodů má k dispozici 13% dotazovaných. Zbylá řešení možného připojení k internetu (mobilní připojení a kabelová televize) zůstaly bez odpovědi. Výsledek potvrzuje neoficiální průzkumy využívaných typů připojení v České republice, se kterými jsem se při čtení setkal. Česká republika patří mezi velmoci využívající bezdrátové připojení. Kvalitnější připojení totiž není možné (optický kabel), neboť jsou jím zasíťované pouze větší městské celky.

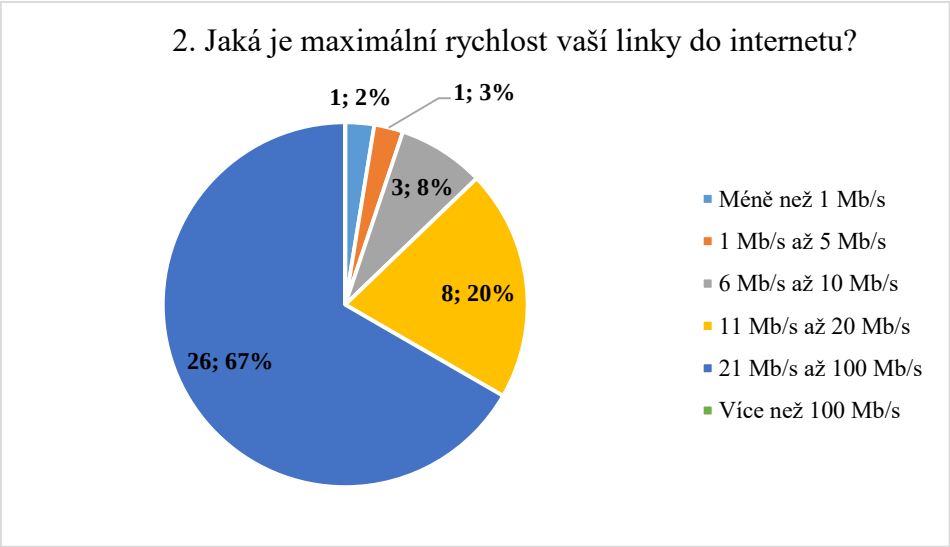


Graf 1 - Typ připojení k internetu

Zdroj: autor

2. Jaká je maximální rychlost vaší linky do internetu?

Co se týče rychlosti připojení, celkem 67% středoškolských institucí má přístup k internetu rychlému 21 Mb/s až 100 Mb/s. Výsledky dále ukazují, že rychlejší linku než právě zmíněnou, nemá ani jedna z vybraných škol východočeského regionu. Dalších 20% škol může využívat rychlosti mezi 11 Mb/s až 20 Mb/s. Pomalejší linku, o rychlosti 6 Mb/s až 10 Mb/s, vlastní 8% institucí. O zmínku pomalejší připojení (1 Mb/s až 5 Mb/s) využívají 3% škol a nejpomalejší internet mají 2% středních škol. V tomto případě se jedná o rychlost menší než 1 Mb/s. Průzkum ukazuje význam rychlosti linky do internetu ve spojení s nejnovějšími trendy internetové doby. Přes relativně vysoké rozmezí rychlosti je možné říci, že připojení do internetu s rychlostí vyšší než 21 Mb/s, se dá považovat za dostatečné pro velikost a potřeby instituce o velikosti školy. Průzkumy uvádějí průměrná rychlost linky do internetu v České republice na hodnotě pohybující se okolo 14 Mb/s. Rychlost menší než 1 Mb/s je tedy již silně podprůměrné a nedostatečné dnešnímu trendu využívání internetových služeb.



Graf 2 - Maximální rychlost linky do internetu

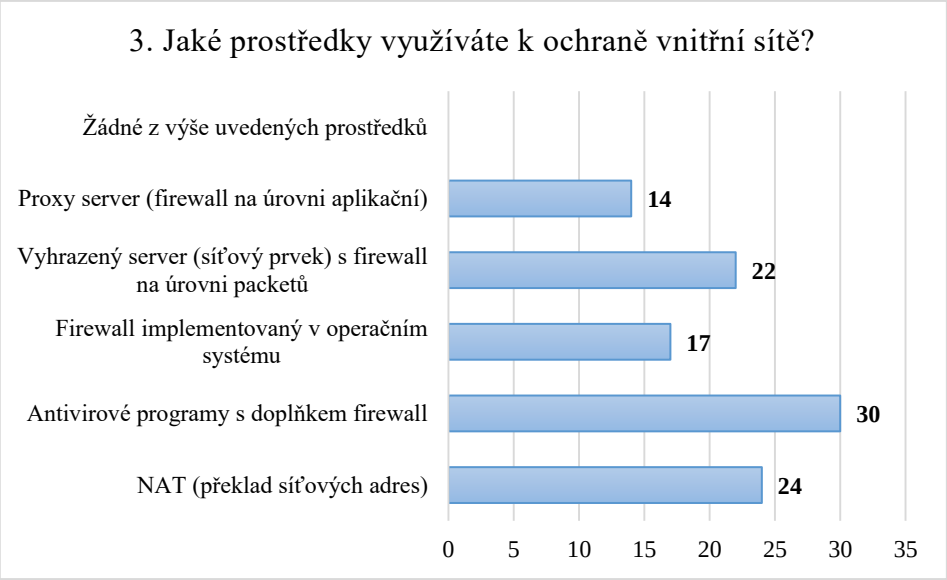
Zdroj: autor

3. Jaké prostředky využíváte k ochraně vnitřní sítě?

Další otázka řeší prostředky užívané k ochraně vnitřní sítě. V případě této otázky bylo možné vybrat více než jednu odpověď, což znamená, že ochrana vnitřní sítě je prováděna za pomocí kombinace níže uvedených prostředků.

Z uvedených odpovědí vyplývá, že nejběžnějším ochranným prostředkem vnitřní sítě je antivirový program s doplňkem firewall, který využívá 30 z 39 institucí.

To odpovídá přibližně 77% celkového počtu. Druhým nejvíce užívaným prostředkem je NAT, jež využívá 62% středních škol. V tomto případě je daný výsledek mírně sporný. NAT neboli překlad adres by měly v současnosti využívat všechny oslovené instituce využívající protokol IPv4. Výsledek může být zkreslen z důvodu menší odborné znalosti daného prostředku ze strany respondentů. Další možností může být fakt, že některé školy nevyužívají vlastní směrovač a veškeré záležitosti týkající se správy internetového připojení nechávají plně na straně poskytovatele internetu. Dalšími prvky jsou vyhrazený server (síťový prvek) s firewall na úrovni packetů (56%), firewall implementovaných v operačním systému (44%) a proxy server (firewall na úrovni aplikační) - (36%). Což odpovídá složitosti konfigurace ochrany na aplikační úrovni.



Graf 3 - Prostředky ochrany vnitřní sítě

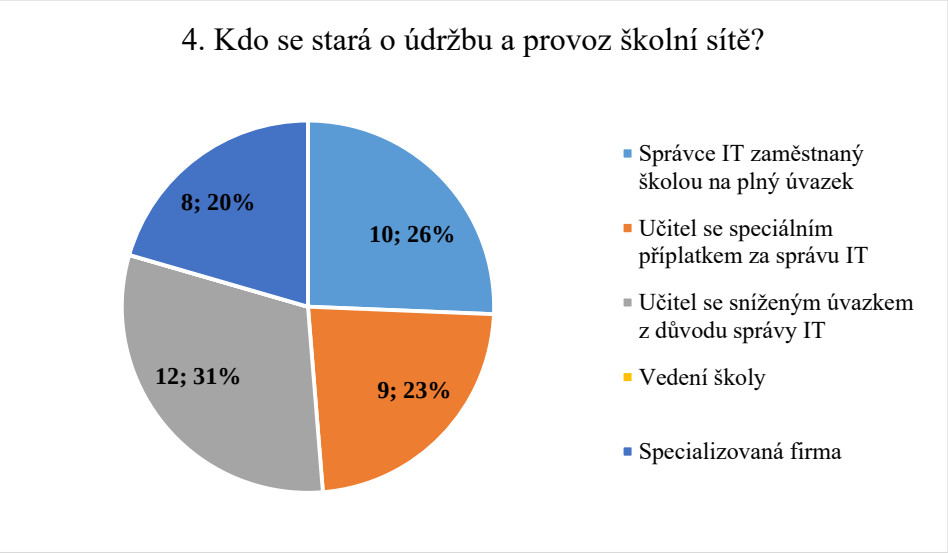
Zdroj: autor

Seznam ochranných prostředků dle četnosti užití:

1. Antivirové programy s doplňkem firewall - 77%
2. NAT (překlad síťových adres) – 62%
3. Vyhrazený server (síťový prvek) s firewall na úrovni packetů – 56%
4. Firewall implementovaných v operačním systému – 44%
5. Proxy server (firewall na úrovni aplikační) – 36%

4. Kdo se stará o údržbu a provoz školní sítě?

Bavíme-li se o údržbě a provozu školní sítě, naskytne se nám několik možností, jak jej řešit. V rámci našich respondentů se nejčastěji o školní síť stará učitel se sníženým úvazkem (31%). Dalších 26% představuje najatého správce IT, který je zaměstnán školou na plný úvazek. Třetí možností je učitel se speciálním příplatkem za správu IT, kterého nalezneme ve 23% středoškolských institucích. Posledních 20% středních škol využívá služeb specializované firmy. Školy většinou postrádají finance na platy svých zaměstnanců a vlastní správce IT je spíše luxusem. O síťové prostředky se posléze stará učitel se zaměření na ICT, který může své teoretické poznatky dále využít v praxi. Otázkou je, zdali je daný učitel schopen plně zabezpečit veškeré aspekty týkající se správy sítě. Dalším řešením jsou tak specializované firmy, které školám zajišťují kompletní správu a škola je pak může platit z jiných finančních rezerv. V daném řešení postrádám vlastní ztotožnění se se stavem sítě. Naopak učitelé se věnují své práci.

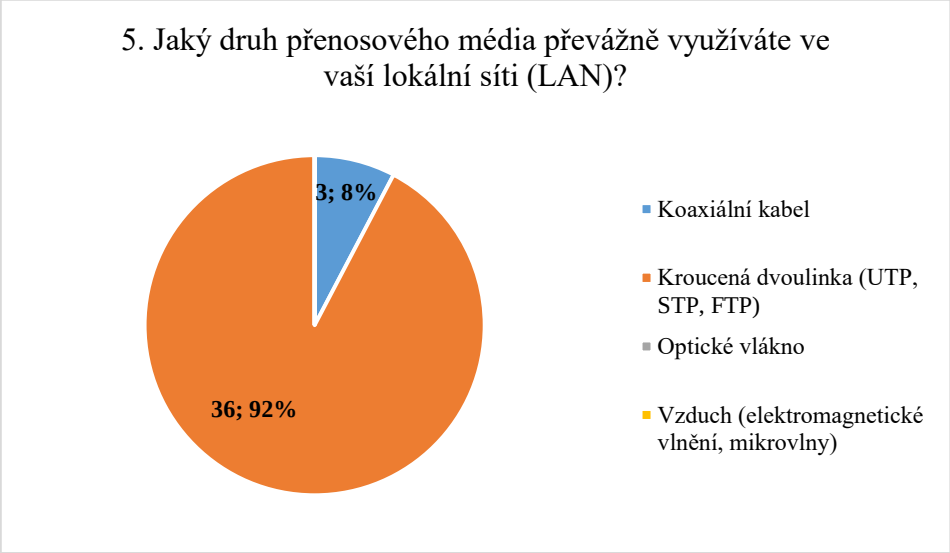


Graf 4 - Osoba zodpovědná za údržbu a provoz sítě

Zdroj: autor

5. Jaký druh přenosového média převážně využíváte v lokální síti (LAN)?

Otázka týkající se druhu přenosového média nám poskytla následující odpovědi. Naprostá většina (92%) vybraných středních škol využívá k přenosu kroucenou dvoulinku. Zbylých 8% stále využívá koaxiální kabel. Ani jedna z dotazovaných institucí nevyužívá optické vlákno či vzduch. Tento výsledek naplno odpovídá současným trendům sítí. Kroucená dvoulinka umožňuje v poměru cena / kvalita nejvyšší využitelnost a plně dostačuje pro potřeby všech institucí. Koaxiální kabel je v současnosti již přežitkem minulosti a nedostačuje moderní podobě síti. Přesto se ukazuje, že někde má stále své místo a je otázkou, co může být důvodem jeho údržby.



Graf 5 - Druhy přenosového média

Zdroj: autor

6. Jakou teoretickou přenosovou rychlost má většina prvků ve vaší lokální síti?

Nejčastější přenosovou rychlostí většiny prvků lokální sítě je 1 Gb/s, kterou se pyšní 64% dotazovaných škol. V současnosti se jedná o standardní rychlost, kde cena aktivních prvků již je velice nízká. Dalších 33% využívá rychlost dosahující 100 Mb/s a nadále jsou však dostačující. Takovým školám většinou postačí výměna za rychlejší aktivní prvky a není nutná úprava kabeláže. Zbylá 3% se musí spokojit s 10 Mb/s. Což odpovídá původnímu standardu Ethernet řešeného na koaxiálním kabelu. Poslední možnost – rychlost 10 Gb/s – nedosahuje hardware ani jedné středoškolské instituce. Tyto aktivní prvky jsou nadále několika násobně dražší a musí být ve většině případů nahrazena též kabeláž (UTP cat. 6+, případně optika). Daná rychlost se doporučuje spíše pro vysoce zahlcované páteřní linky a servery. Pro běžné klienty je spíše nadbytečným přepychem.

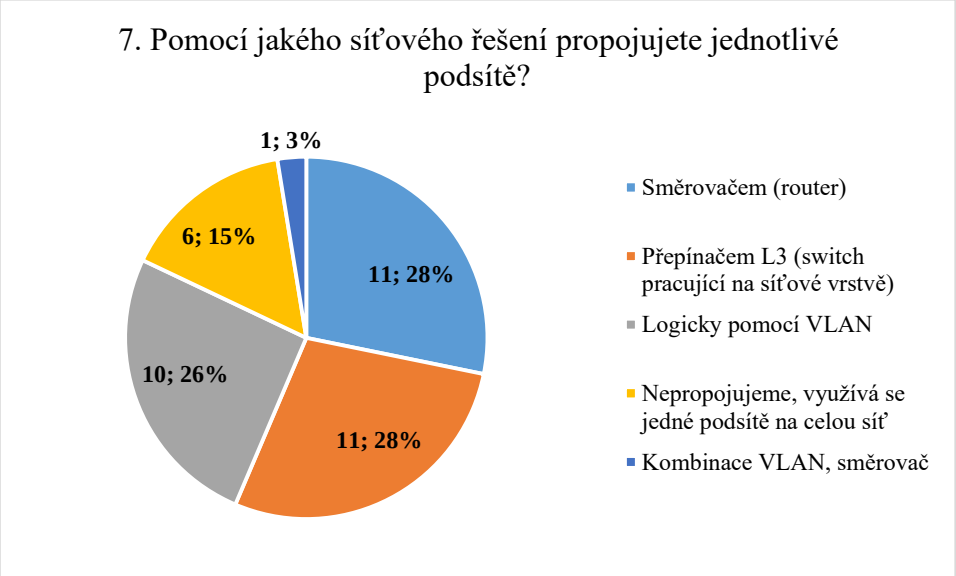
Graf 6 - Přenosová rychlost většiny aktivních prvků

Zdroj: autor

7. Pomocí jakého síťového řešení propojujete jednotlivé podsítě?

Problematika síťového řešení dotazovaných subjektů je řešena obvykle směrovačem (routerem) – 28% nebo L3 přepínačem (28%). Další možností je logické propojování podsítí pomocí VLAN, jež jako odpověď označilo 26% dotazovaných. Celkem 15% středních škol podsítě nepropojuje, jelikož využívají jednu podsíť na celou síť a konečně 3% škol využívají kombinace VLAN a směrovače. V tomto případě vše záleží na historickém budování podoby sítě. Směrovače a přepínače pracující na síťové vrstvě, přinášejí standardní a ověřené řešení. Oba aktivní prvky jsou si principem

shodné, L3 přepínače však dosahují rychlejší směrovací schopnosti a odezvy. Mírným zjednodušením může dále být využití virtuálních lokálních sítí (VLAN). Díky nim jsme schopni ušetřit na aktivních prvcích, neboť jsou pakety označovány pouze logicky. Oproti standardnímu řešení nám tak po jednom fyzickém médiu může putovat více logicky označených podsítí, což při fyzickém oddělení není možné. Na jednu podsíť zde odpovídá právě jeden fyzický aktivní prvek a jedno přenosové médium. Využíváním jedné podsítě jsou dané instituce závislé na omezeném počtu logických klientských adres. Většinou se jedná o číslo 254 adres pro klienty, do kterého se škola musí vejít. Dané řešení je většinou řešeno na školách méně zaměřených na ICT, neboť nevyužívají tolik aktivních zařízení a je to jednoduché na správu.



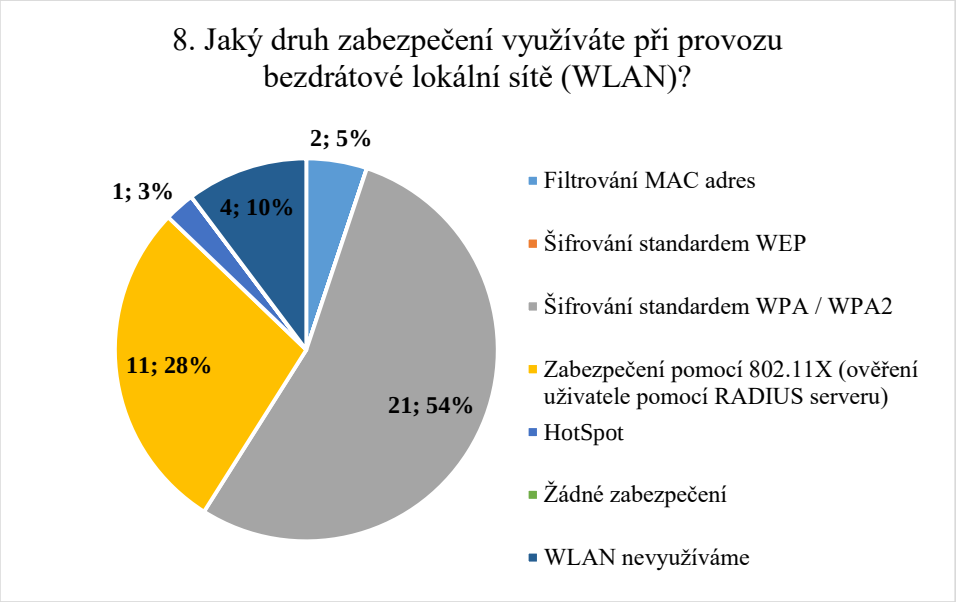
Graf 7 - Realizace podsítí

Zdroj: autor

8. Jaký druh zabezpečení využíváte při provozu bezdrátové lokální sítě (WLAN)?

Více než polovina (54%) vybraných institucí užívá k zabezpečování bezdrátové lokální sítě šifrování standardem WPA/WPA2. K dalším z více užívaných druhů zabezpečení patří nepochybně i zabezpečení skrze ověření uživatele pomocí RADIUS serveru. Toho využívá 28% vybraných středních škol. Celých 10% vůbec WLAN nevyužívá. Dalšími, ne tak četně užívanými, druhy jsou filtrování MAC adres (5%) a HotSpot (3%). Zastaralé šifrování WEP a otevřená autentizace (žádné zabezpečení) se v průzkumu neobjevila. Školy jsou tak s problémem zabezpečení bezdrátových sítích seznámení na dobré úrovni. Menším problémem může být zneužití filtrace MAC

adres. Případný útočník však musí mít již jisté teoretické zkušenosti. Ve většině případů převažují spíše čistě uživatelé.

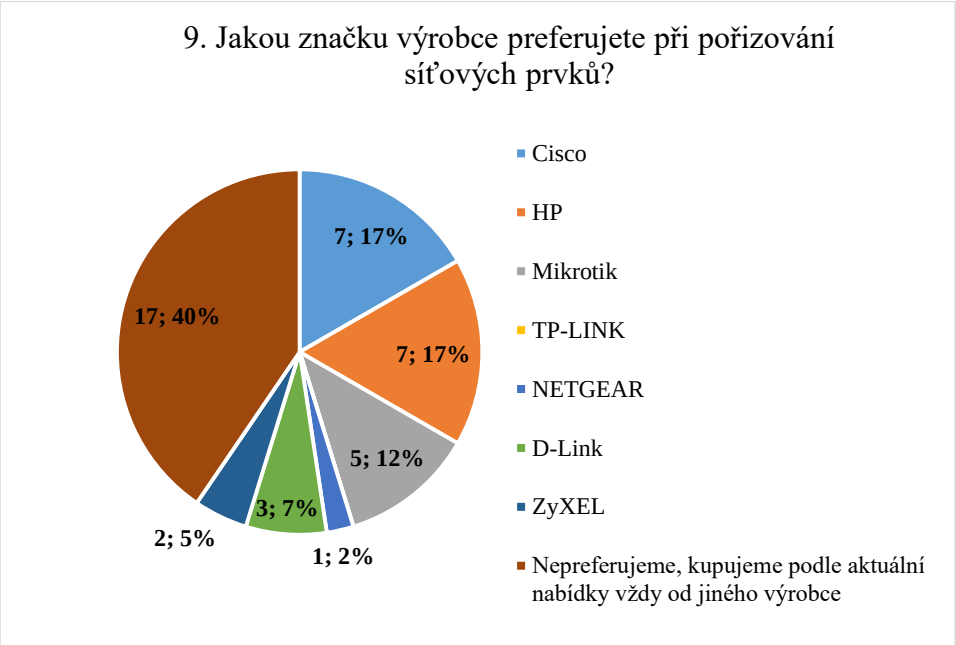


Graf 8 - Druhy zabezpečení bezdrátové sítě

Zdroj: autor

9. Jakou značku výrobce preferujete při pořizování síťových prvků?

Podle dat zjištěných v průzkumu je zřejmé, že nejoblíbenější výrobci síťových prvků jsou Cisco a HP. Obě značky volí 17% respondentů. Potvrzuje to jejich postavení v oblasti aktivních prvků, kde většinou obsazují první místa týkající se kvality a spolehlivosti. Nicméně 40% institucí nepreferuje žádného výrobce, neboť nákupy uskutečňuje podle aktuální nabídky a trendů, pokaždé od jiného výrobce. Toto nejednotné řešení komplikuje případnému správci práci. Každý firmware prvku se konfiguruje odlišně a správce se s tím musí vypořádat. Dalšími značkami, jež vybrané školy nakupují, jsou Mikrotik (12%), D-Link (7%), ZyXEL (5%) nebo NETGEAR (2%). Jedná se o osvědčené společnosti a minimálně Mikrotik umožňuje kvalitní rozšíření síťových služeb. V daném směru není tolik složité zvolit špatně a školy po většinou na aktivních prvcích nešetří.

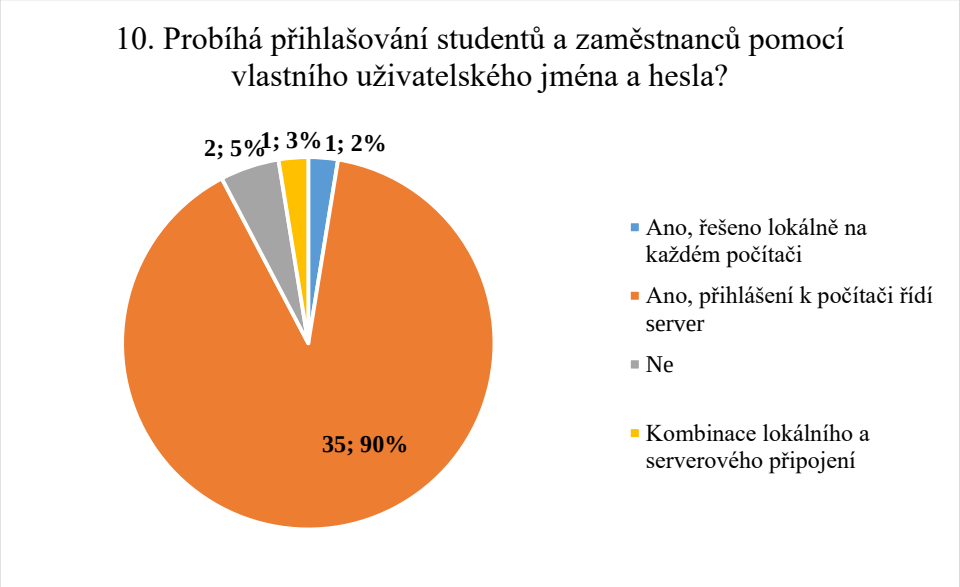


Graf 9 - Značky výrobců síťových prvků

Zdroj: autor

10. Probíhá přihlašování studentů a zaměstnanců pomocí vlastního uživatelského jména a hesla?

Kromě 5% případů se studenti přihlašují pomocí vlastního jména a hesla. Z 90% se jedná o přihlášení řízené serverem. Zbytek případů je řešen buď lokálně na každém počítači (2%), anebo kombinací lokálního a serverového připojení (3%). Adresářové služby za využití přihlašovacího serveru jsou nejjednodušší metodou správy uživatelů. Nedivím se, že většina škol využívá tohoto vysoce modulárního řešení.

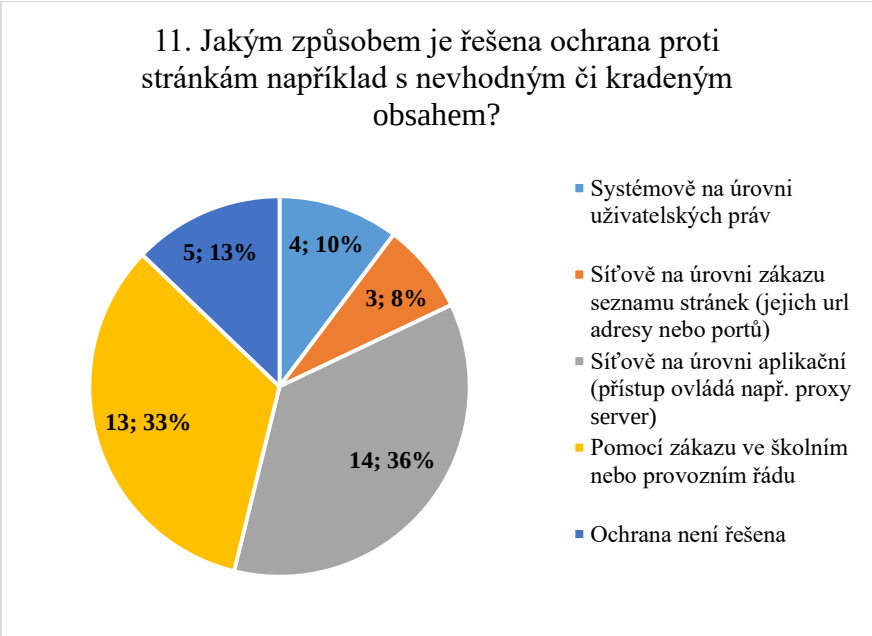


Graf 10 - Podoba přihlašování uživatelů do sítě

Zdroj: autor

11. Jakým způsobem je řešena ochrana proti stránkám například s nevhodným či kradeným obsahem?

Otázka ochrany proti stránkám s nevhodným či kradeným obsahem je řešena v 36% síťově na úrovni aplikační. Jedná se o maximální možnou ochranu, která je téměř 100%. Zákazem ve školním nebo provozním řádu dociluje ochrany 33% institucí. Bohužel dané řešení většinou nic neřeší. Méně častou alternativou je systémové řešení na úrovni uživatelských práv (10%), nebo síťové řešení na úrovni zákazu seznamu stránek (8%). Ochranu vůči nevhodnému obsahu neřeší 13% dotazovaných škol. Otázkou je, zdali je toto správné rozhodnutí.

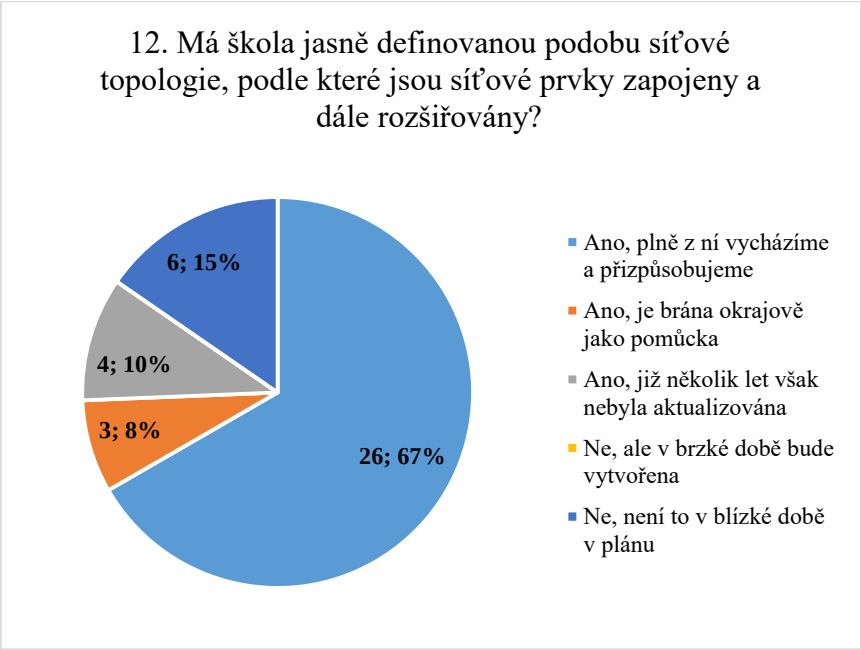


Graf 11 - Způsob ochrany proti nevhodným stránkám

Zdroj: autor

12. Má škola jasně definovanou podobu síťové topologie, podle které jsou síťové prvky zapojeny a dále rozšiřovány?

Většina dotazovaných subjektů má definovanou síťovou topologii. Přináší to tak usnadnění správy. Konkrétně se jedná o 67% škol, které z topologie plně vychází a přizpůsobuje se jí. Dalších 10% má topologii definovanou, avšak zastaralou, jelikož ji několik let neaktualizovalo. Některé školy (8%) berou topologii okrajově jako učební pomůcku. Zbylých 15% odpovídá institucím, které topologii definovanou nemají, a ani v blízké době mít neplánují.



Graf 12 - Využívání topologie sítě

Zdroj: autor

Závěr

Hlavním cílem práce bylo specifikovat vhodnou podobu a konfiguraci počítačové sítě v prostředí školy a ve školských zařízeních. Na modelu školní počítačové sítě jsme si představili několik způsobů úpravy a rozšíření její konfigurace, předtím však bylo nutné se seznámit s určitými teoretickými poznatky. Práce je tak rozdělena na úvodní obecně zaměřenou teoretickou část, za kterou navazuje již modelově pojatá praktická část. Součástí obsahu práce mělo být dotazníkové šetření, jehož výsledek je prezentován v poslední části práce. Dohromady se práce skládá ze tří hlavních částí, které jsou dále strukturovány do jednotlivých kapitol a podkapitol. S přihlédnutím hledisek didaktických zásad práce zmiňuje bezpečností zásady spojené s provozem počítačové sítě ve školách a vymezuje způsoby ošetření proti nesprávnému morálnímu vývoji žáků a studentů.

V úvodu teoretické části se pozastavuji nad myšlenkou významu vzniku počítačových sítí a jejich přínosem pro moderní práci s informacemi. Teoretická část dále pokračuje obecnými poznatky týkajícími se fungování počítačové sítě. Zmiňuji se zde převážně o významu topologií a vysvětlení základních pojmů spojených s provozem sítě. Velký prostor je dán též hardwaru užívaného pro činnost sítě, neboť je dál použit při sestavování doporučení pro provoz. Poslední dvě témata jsou zaměřena na bezpečnost a provoz bezdrátové počítačové sítě. Vysvětluji základní definice jednotlivých technologií, jejich princip fungování a význam. Celý význam kapitoly slouží převážně k lepšímu chápání a orientování se v praktické části textu.

Praktická část se zaměřuje přímo na vymodelovaný stav prostředí počítačové sítě. Z důvodu mé pětileté zkušenosti se správou a údržbou školní počítačové sítě jsem si dovolil vymodelovat určitý počáteční stav sítě, na kterém dále představují návrhy na její zlepšení. Část obsahuje celkem šestici tipů pro přizpůsobení zmiňované sítě moderním směrům a vhodnou mravní výchovu mládeže. Najdeme zde například možnosti modernizace síťového prostředí učebny výpočetní techniky, návrh pro vybudování školní bezdrátové sítě nebo jednoduchý způsob omezování nevhodného obsahu webových stránek. Vybrané kapitoly obsahují podněty na nákup konkrétního příslušenství i s výpisem nákladů na pořízení. Z důvodu praktických zkušeností se správou, je vše okomentováno vlastním způsobem chápání, splňující veškeré technické fungování a principy.

Poslední výzkumná část se zabývá otázkou šetření aktuálního stavu počítačové sítě ve vybraných středních školách. Analýza dotazníkového šetření je řešena výpisem výsledků jednotlivých otázek, včetně okomentování a grafického zobrazení grafů.

Osobně se domnívám, že se mi stanovených cílů práce podařilo dosáhnout. Teoretická část jednoduše vysvětluje veškeré důležité aspekty spojené s obecnými základy počítačových sítí a způsoby jejich zabezpečení. Praktická část na získaných poznatcích definuje příklady konfigurace sítě v určeném prostředí. U analýzy dat dochází k reprezentaci jejich výsledků a okomentování z pohledu určitých obecných zásad principů počítačových síti.

Seznam použité literatury

[1] *Aterm Station Wi-Fi 5 GHz* [online]. 2013 [cit. 2016-06-10]. Dostupné z: https://121ware.com/product/atermstation/special/tv_mode/03.html

[2] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Brno: Computer Press, 2004. ISBN 80-251-0178-9.

[3] BOUŠKA, Petr. *SAMURAJ-cz* [online]. 2005- [cit. 2016-05-31]. Dostupné z: http://www.samuraj-cz.com

[4] CARROLL, Brandon. *Bezdrátové sítě Cisco: autorizovaný výukový průvodce*. Brno: Computer Press, 2011. Samostudium. ISBN 978-80-251-2884-8.

[5] *Co je IPv6* [online]. 2012 [cit. 2016-06-01]. Dostupné z: https://www.ipv6.cz/Co_je_IPv6

[6] *Data center. In: Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2016-05-31]. Dostupné z: https://en.wikipedia.org/wiki/Data_center

[7] FOŘT, Petr. *Jak se plete počítačová síť - základy sítí* [online]. 2004 [cit. 2016-04-20]. Dostupné z: http://pctuning.tyden.cz/software/jak-zkrotit-internet/4111-jak_se_plete_pocitacova_sit-zaklady_siti

[8] *Free Cisco CCNA Exam Certification Guide* [online]. 2000 [cit. 2016-06-01]. Dostupné z: https://www.certificationkits.com/cisco-certification/cisco-ccna-640-802-exam-certification-guide/

[9] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 3., aktualiz. vyd. Brno: Computer Press, 2006. Bestseller (Computer Press). ISBN 80-251-0892-9.

[10] HORÁK, Michal. *Aktivní prvky sítí – princip switche, hubu* [online]. 2009 [cit. 2016-06-01]. Dostupné z: http://www.buben.piranhacz.cz/aktivni-prvky-siti-princip-switche-hubu/

[11] JELÍNEK, Jiří. *Počítačové sítě: Metodická příručka*. Hradec Králové, 2014.

[12] KLEMENT, Milan. *Technologie počítačových sítí: DHCP* [online]. Olomouc, 2011 [cit. 2016-06-11]. Dostupné z: http://www.kteiv.upol.cz/uploads/soubory/klement/web1/TPS_2014/prednasky/p%C5%99ed%2011.pdf

[13] KOHOUTEK, Rudolf. *Dotazník jako průzkumná metoda* [online]. 2010 [cit. 2016-06-24]. Dostupné z: http://rudolfkohoutek.blog.cz/1002/dotaznik-jako-pruzkumna-metoda

[14] *Networking basics* [online]. 2010 [cit. 2016-06-01]. Dostupné z: http://www.networking-basics.net

[15] NORTHCUTT, Stephen. *Bezpečnost sítí: velká kniha*. Brno: CP Books, 2005. Security (CP Books). ISBN 80-251-0697-7.

[16] *Norton ConnectSafe – Configure Router* [online]. 2016 [cit. 2016-06-25]. Dostupné z: https://dns.norton.com/configureRouter.html

[17] PALATINUS, Lukáš. *Topologie sítí* [online]. 2014 [cit. 2016-04-20]. Dostupné z: http://blog.banan.cz/Internet/Topologie-siti

[18] *Peer-to-peer. In: Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2016-05-30]. Dostupné z: https://en.wikipedia.org/wiki/Peer-to-peer

[19] PETERKA, Jiří. *Archiv článků a přednášek Jiřího Peterky* [online]. 1996 [cit. 2016-06-01]. Dostupné z: http://www.earchiv.cz/i_slov2.php3

[20] *Podsíť. In: Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2016-06-01]. Dostupné z: https://cs.wikipedia.org/wiki/Pods%C3%AD%C5%A5

[21] *Proxy server. In: Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2016-06-10]. Dostupné z: https://en.wikipedia.org/wiki/Proxy_server

[22] *Quelle différence entre les cables* [online]. 2013 [cit. 2016-06-01]. Dostupné z: https://www.alliancelec.fr/blog/quelle-difference-entre-les-cables-prises-rj45-utp-ftp-stp-cat5-cat6-n12

[23] *Rack unit. In: Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2016-05-31]. Dostupné z: https://en.wikipedia.org/wiki/Rack_unit

[24] SCHARM, Martin. *Connecting through a NAT - the non-trivial direction* [online]. 2011 [cit. 2016-06-10]. Dostupné z: https://binfalse.de/2011/06/30/connecting-through-a-nat-the-not-trivial-direction/

[25] SMYSITELOVÁ, Lucie. *Historie rozlehlých počítačových sítí* [online]. 1999 [cit. 2016-04-20]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/xsmysit.html

[26] *Správa hlavních síťových služeb* [online]. 2006 [cit. 2016-06-01]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc786019%28v=ws.10%29.aspx

[27] ŠERÝ, Rostislav. *Optické sítě* [online]. 2006 [cit. 2016-06-01]. Dostupné z: http://programujte.com/clanek/2006120301-opticke-site/

[28] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0417-6.

[29] TRČÁLEK, Antonín. *Všechno, co byste měli vědět o Wi-Fi* [online]. 2012 [cit. 2016-06-10]. Dostupné z: http://www.zive.cz/clanky/vsechno-co-byste-meli-vedet-o-wi-fi/omezena-pasma-a-standardy-anteny/sc-3-a-162796-ch-80485/default.aspx

[30] VELTE, Toby J. a Anthony T. VELTE. *Síťové technologie Cisco: velký průvodce*. Brno: Computer Press, 2003. Administrace (Computer Press). ISBN 80-722-6857-0.

[31] WENSTROM, Michael J. *Zabezpečení sítí Cisco: autorizovaný samostudijní výukový kurz*. Vyd. 1. Brno: Computer Press, 2003. Cisco systems. ISBN 80-722-6952-6.

[32] *Wi-Fi sítě - vše co jste kdy chtěli vědět* [online]. 2008 [cit. 2016-06-10]. Dostupné z: http://pctuning.tyden.cz/hardware/site-a-internet/11138-wi-fi_site-vse_co_jste_kdy_chteli_vedet_12

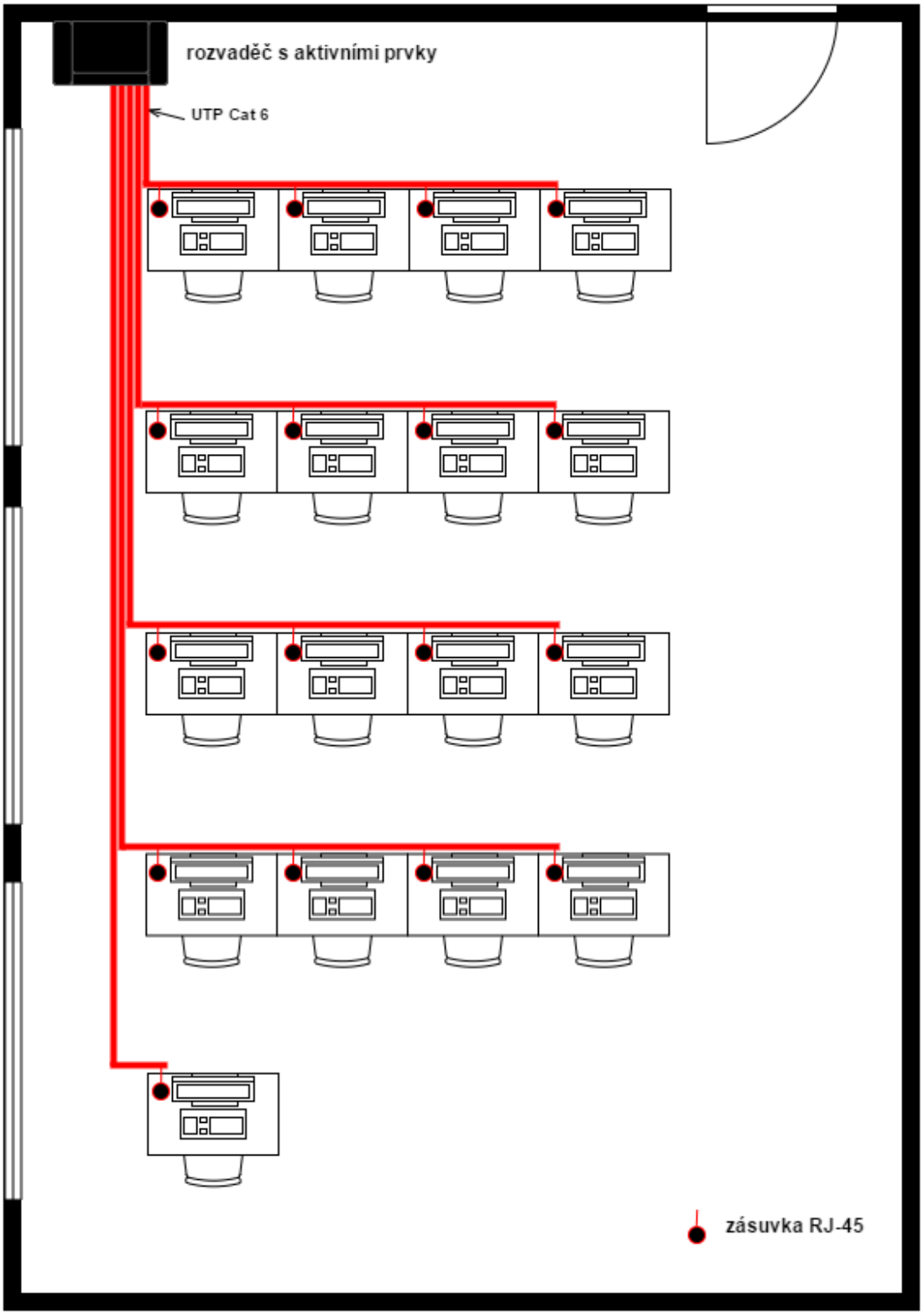
[33] *Zapojení internetového kabelu (RJ45)* [online]. 2015 [cit. 2016-06-01]. Dostupné z: http://zapojenikabelu.cz/rj45.html

Seznam obrázků

Seznam tabulek

Seznam příloh

Příloha A – Způsob vedení kabeláže učebny výpočetní techniky



Příloha B – Seznam škol uvedených do dotazníku podle pořadí vypracování

1. SPŠel•it Dobruška
2. Střední průmyslová škola, Trutnov, Školní 101
3. Soukromá střední škola podnikatelská - ALTMAN, s.r.o.
4. OA Trutnov
5. Gymnázium Dobruška
6. Gymnázium Broumov
7. SOŠ
8. SPŠ Hronov
9. Gymnázium a Střední odborná škola pedagogická, Nová Paka
10. Gymnázium F. M. Pelcla, Rychnov nad Kněžnou
11. Gymnázium Vrchlabí
12. Gymnázium Boženy Němcové, Hradec Králové
13. SPŠ kamenická a sochařská Hořice
14. SZŠ Pardubice
15. SOŠ a SOU Lanškroun
16. VOŠS a SŠS Vysoké Mýto
17. Gymnázium Josefa Ressela, Chrudim
18. Letohradské soukromé gymnázium o.p.s.
19. Gymnázium Dvůr Králové nad Labem
20. Gymnázium, Pardubice, Mozartova 449
21. gozhorice.cz
22. SOŠ a SOU obchodu a služeb Chrudim
23. SŠ obchodní a služeb SČMSD, Polička, s.r.o.
24. Střední škola služeb, obchodu a gastronomie Hradec Králové
25. VSŠ a VOŠ MO v Moravské Třebové
26. SP
27. VOŠ stavební a SPŠ stavební arch. Jana Letzela, Náchod
28. Masarykova obchodní akademie Jičín
29. VOŠZ a SZŠ Trutnov
30. Česká lesnická akademie Trutnov - střední škola a vyšší odborná škola
31. GYMNÁZIUM
32. SPŠ, SOŠ a SOU Nové Město nad Metují
33. Gymnázium, Pardubice, Dašická 1083
34. SPŠKS Hořice
35. SŠGS Nová Paka
36. Gymnázium Jaroslava Žáka, Jaroměř
37. Střední škola zahradnická Kopidlno
38. Obchodní akademie T. G. Masaryka Kostelec nad Orlicí
39. SPŠ, SOŠ a SOU Hradec Králové

Příloha C – Obsah průvodního dopisu zaslaného na mailovou adresu jednotlivých škol

zasláno dne 10. března 2016

Vážená instituce, vážené vedení,

dovolte mi se na úvod krátce představit, jmenuji se Patrik Matejsek a jsem studentem 5. ročníku pedagogické fakulty UHK. Jakožto student posledního ročníku magisterského studia mi k úspěšnému absolvování kromě státních závěrečných zkoušek zbývá zpracování diplomové práce. Tato diplomová práce má název: Bezpečná konfigurace školní počítačové sítě jako prostředek výchovy žáků a jejím cílem je specifikace vhodné podoby a konfigurace počítačové sítě v prostředí školy a školských zařízení, včetně opatření budující u žáků (studentů) správné bezpečnostní návyky.

Výzkumnou oblastí z mé strany bude zpracování strukturovaného dotazníku zaměřeného na aktuální podobu školních počítačových sítí na středních školách. S dovolením bych vás tímto rád požádal, zdali byste si našli dvě minuty a zapojili se jako školská instituce do daného průzkumu, který probíhá online formou. Bylo by vhodné, kdyby se vyplňování dotazníku zhostila osoba, která se přímo podílí na fungování školní počítačové sítě, případně samo vedení školy. Získaná data budou použita v již zmiňované diplomové práci a nebude s nimi nijak dále nakládáno. Bude-li z vaší strany zájem, jsem ochotný se s výsledky průzkumu na požádání z vaší strany podělit.

Do průzkumu se zapojíte kliknutím na odkaz online dotazníku s url: http://goo.gl/forms/4X0KE6SPoc

Za vaši ochotu a čas jsem moc zavázán, děkuji za vaši pomoc.

Přeji hezký zbytek dne.

Bc. Patrik Matejsek

Příloha D – Obsah online dotazníku výzkumné části

Dotazník: Aktuální stav počítačových sítí na SŠ

*Povinné pole

Otázky k šetření:

1. Jaký typ připojení k internetu má vaše škola k dispozici? *

- ○ ADSL / VDSL (připojení pomocí telefonních rozvodů)
- ○ Bezdrátové připojení
- ○ Optický kabel
- ○ Mobilní připojení (3G / LTE)
- ○ Kabelová televize
- ○ Jiné: _____

2. Jaká je maximální rychlost vaší linky do internetu? *

- ○ Méně než 1 Mb/s
- ○ 1 Mb/s až 5 Mb/s
- ○ 6 Mb/s až 10 Mb/s
- ○ 11 Mb/s až 20 Mb/s
- ○ 21 Mb/s až 100 Mb/s
- ○ Více než 100 Mb/s

3. Jaké prostředky využíváte k ochraně vnitřní sítě? *

- ☐ NAT (překlad síťových adres)
- ☐ Antivirové programy s doplňkem firewall
- ☐ Firewall implementovaný v operačním systému
- ☐ Vyhrazený server (síťový prvek) s firewall na úrovni packetů
- ☐ Proxy server (firewall na úrovni aplikační)
- ☐ Žádné z výše uvedených prostředků

4. Kdo se stará o údržbu a provoz školní sítě? *

- ◯ Správce IT zaměstnaný školou na plný úvazek
- ◯ Učitel se speciálním příplatkem za správu IT
- ◯ Učitel se sníženým úvazkem z důvodu správy IT
- ◯ Vedení školy
- ◯ Specializovaná firma

5. Jaký druh přenosového média převážně využíváte ve vaší lokální síti (LAN)? *

- ◯ Koaxiální kabel
- ◯ Kroucená dvoulinka (UTP, STP, FTP)
- ◯ Optické vlákno
- ◯ Vzduch (elektromagnetické vlnění, mikrovlny)

6. Jakou teoretickou přenosovou rychlost má většina prvků ve vaší lokální síti? *

- ◯ 10 Mb/s
- ◯ 100 Mb/s
- ◯ 1 Gb/s
- ◯ 10 Gb/s

7. Pomocí jakého síťového řešení propojujete jednotlivé podsítě? *

- ◯ Směrovačem (router)
- ◯ Přepínačem L3 (switch pracující na síťové vrstvě)
- ◯ Logicky pomocí VLAN
- ◯ Nepropojujeme, využívá se jedné podsítě na celou síť
- ◯ Jiné: _____

8. Jaký druh zabezpečení využíváte při provozu bezdrátové lokální sítě (WLAN)? *

- ◯ Filtrování MAC adres
- ◯ Šifrování standardem WEP
- ◯ Šifrování standardem WPA / WPA2
- ◯ Zabezpečení pomocí 802.11X (ověření uživatele pomocí RADIUS serveru)
- ◯ HotSpot
- ◯ Žádné zabezpečení
- ◯ WLAN nevyužíváme

9. Jakou značku výrobce preferujete při pořizování síťových prvků? *

- ◯ Cisco
- ◯ HP
- ◯ Mikrotik
- ◯ TP-LINK
- ◯ NETGEAR
- ◯ D-Link
- ◯ ZyXEL
- ◯ Nepreferujeme, kupujeme podle aktuální nabídky vždy od jiného výrobce
- ◯ Jiné: _____

10. Probíhá přihlašování studentů a zaměstnanců pomocí vlastního uživatelského jména a hesla? *

- ◯ Ano, řešeno lokálně na každém počítači
- ◯ Ano, přihlášení k počítači řídí server
- ◯ Ne
- ◯ Jiné: _____

11. Jakým způsobem je řešena ochrana proti stránkám například s nevhodným či kradeným obsahem? *

- ◯ Systémově na úrovni uživatelských práv
- ◯ Síťově na úrovni zákazu seznamu stránek (jejich url adresy nebo portů)
- ◯ Síťově na úrovni aplikační (přístup ovládá např. proxy server)
- ◯ Pomocí zákazu ve školním nebo provozním řádu
- ◯ Ochrana není řešena
- ◯ Jiné: _____

12. Má škola jasně definovanou podobu síťové topologie, podle které jsou síťové prvky zapojeny a dále rozšiřovány? *

- ◯ Ano, plně z ní vycházíme a přizpůsobujeme
- ◯ Ano, je brána okrajově jako pomůcka
- ◯ Ano, již několik let však nebyla aktualizována
- ◯ Ne, ale v brzké době bude vytvořena
- ◯ Ne, není to v blízké době v plánu
- ◯ Jiné: _____

Prosím, uveďte název vaší střední školy: *

Vaše odpověď