Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Domácí počítačová síť

Jiří Macek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jiří Macek

Informatika

Název práce

Domácí počítačová síť

Název anglicky

Home area network

Cíle práce

Hlavním cílem bakalářské práce je porovnat možnosti tvorby domácí počítačové sítě v rozdílných prostředích a podmínkách, které mohou nastat v domácnostech. Uvést hlavní výhody a nevýhody použití síťových technologií v rámci daného prostředí. A v praktické části vytvoření návrhu domácí počítačové sítě.

Metodika

Bude provedena rešerše odborné literatury a publikovaných odborných článků. Dále bude vypracována analýza aktuálních síťových technologií pro tvorbu domácí počítačové sítě v rozdílných podmínkách, které mohou nastat. Nakonec bude s využitím teoretických poznatků vytvořen návrh domácí počítačové sítě v konkrétním případě.

Doporučený rozsah práce

40

Klíčová slova

Počítačová síť, Wi-Fi, Home area network, Domácí síť

Doporučené zdroje informací

Gary A. Donahue, Network Warrior, O'Reilly Media, 2007. ISBN 978-0-596-10151-0

HORÁK, J. – KERŠLÁGER, M. Počítačové sítě pro začínající správce. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.

ROSS, K W. – KUROSE, J F. *Počítačové sítě.* Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

Spurná I., Počítačové sítě – Praktická příručka správce sítě. Kralice na Hané: Computer Media, 2010. ISBN 978-80-7402-036-0.

Předběžný termín obhajoby

2016/17 LS – PEF

Vedoucí práce

Ing. Tomáš Vokoun

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 1. 11. 2016

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 9. 11. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 25. 12. 2016

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Domácí počítačová síť" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14. 3. 2017 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Tomáši Vokounovi za odborné vedení, pomoc a cenné rady při zpracovaní bakalářské práce.

Domácí počítačová síť

Souhrn

Tato bakalářská práce se zabývá problematikou tvorby počítačových sítí, především pak počítačových sítí v domácím prostředí. Postupně charakterizuje počítačové sítě od jednotlivých topologií, architektur až po standardy a zabezpečení sítí. Je zde představen referenční model ISO/OSI a dnes používaná architektura TCP/IP. Dále jsou zde uvedeny aktivní a pasivní prvky používané v počítačových sítích.

Praktická část se zabývá analýzou technologií pro vybudování domácí počítačové sítě v odlišných podmínkách. Jsou zde otestovány přenosové rychlosti technologií a útlum Wi-Fi signálu při průchodu skrz různé materiály. Poté jsou pomocí vícekriteriální analýzy variant vybrány vhodné hardwarové prvky pro konkrétní síť. Po zhotovení analýzy je realizován návrh domácí počítačové sítě. Je zde popsána konstrukce sítě, její konfigurace a závěrečné celkové otestování. Výstupem práce je navržení počítačové sítě použitelné ve většině domácností, s ohledem na nízké finanční náklady. Snahou je využití stávajících hardwarových prvků s nakoupením pouze nejnutnějších zařízení.

Klíčová slova: Počítačová síť, Wi-Fi, Útlum, Signál, Domácí síť, Analýza, ISO/OSI, TCP/IP, Hardware

Home area network

Summary

This bachelor thesis is about creations of computer network, especially computer network at home. Gradually characterizes computer networks from various topologies, architectures to standards and network security. There is description of the ISO/OSI reference model and today used TCP/IP architecture. Also, there are explained active and passive network components.

The practical part is engaged with analysis of technology for home area network in different conditions. Transmission speed of network technology and attenuation of Wi-Fi signal in different material are tested here. Then were chosen suitable network components for specific network by multiple-criteria decision analysis. After analysing is realized the network layout, including a description of network construction, configuration and final testing. Outcome of this work is design of computer network applicable in majority household, with consideration into financial expenses. Effort to use current hardware components and buy only necessary components.

Keywords: Computer network, Wi-Fi, Attenuation, Signal, Home area network, Analysis, ISO/OSI, TCP/IP, Hardware

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Bez počítačových sítí si již nedovedeme představit život. Od dob kdy se sítě využívaly pouze ve firmách nebo na univerzitách, uplynula již dlouhá doba a dnes existuje minimálně jednoduchá počítačová síť v každé domácnosti. Síť nám umožňuje jednodušší komunikaci uvnitř firem, nabízí možnost sdílení dat a tím zvyšuje naši produktivitu. V domácím prostředí nám zase zprostředkovává nejrůznější formou multimediální obsah a dokážeme díky ní chránit svá osobní data.

V praktické části je testován útlum Wi-Fi signálu v různých materiálech. A pomocí nabytých teoretických znalostí je navržena a vybudována domácí počítačová síť. Hlavním bodem při návrhu je otestování dostupných síťových technologií a zhodnocení nejlepší možné varianty pro konstrukci sítě v daném místě. Celá konstrukce sítě je tvořena především s ohledem na nízké finanční náklady.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem bakalářské práce je porovnat možnosti tvorby domácí počítačové sítě v rozdílných prostředích a podmínkách, které mohou nastat v domácnostech. Uvést hlavní výhody a nevýhody použití síťových technologií v rámci daného prostředí. A v praktické části vytvoření návrhu domácí počítačové sítě.

2.2 Metodika

Bude provedena rešerše odborné literatury a publikovaných odborných článků. Dále bude vypracována analýza aktuálních síťových technologií pro tvorbu domácí počítačové sítě v rozdílných podmínkách, které mohou nastat. Nakonec bude s využitím teoretických poznatků vytvořen návrh domácí počítačové sítě v konkrétním případě.

3 Teoretická východiska

3.1 Taxonomie počítačových sítí

Sítě lze dělit do mnoha různých skupin, tříd nebo typů. Dělí se podle různých kritérií, především dle vlastnictví na sítě veřejné a privátní. Podle způsobu použití na intranet a extranet, dle použitého přenosového média na drátové a bezdrátové sítě. A podle jejich dosahu na sítě personální, lokální, metropolitní a rozlehlé. (Peterka, 2005a)

Z pohledu dosahu jsou nejmenší personální lokální sítě označovány jako pLAN. Jejich dosah bývá velmi malý, maximálně několik metrů. Síť pLAN slouží potřebám jednotlivce a nejčastěji propojuje mobilní zařízení mezi sebou nebo připojuje periferie k zařízení. Náležitým příkladem je technologie Bluetooth. Zařízení Bluetooth pracují na rádiových vlnách, ve kterých jsou datové toky rozděleny do 75 různých frekvencí s dosahem přibližně 10 metrů. Přestože se jedná dosahem o malé sítě, jejich technologie mohou být velice vyspělé. Bluetooth podporuje automatickou konfiguraci, zabezpečení, ale i propagaci možností a služeb každého připojeného zařízení. Charakteristickými zařízeními využívající technologii Bluetooth jsou mobilní telefony, kamery, myši, klávesnice a sluchátka.

Lokální síť označována jako LAN (Local Area Network) je skupina propojených systémů, které se rozprostírají na určitém vymezeném prostoru. Může se jednat o pár počítačů propojených rozbočovačem nebo o rozsáhlejší sítě nacházející se v jedné místnosti, na jednom patře nebo po celé budově.

Jednotlivé sítě LAN od sebe dělí rozdílná adresace nebo přemosťující prvek. Jestliže mají dvě sítě LAN rozdílné rozsahy IP adres a je mezi ně vložen jeden nebo více přemosťujících prvků, například směrovačů, pak tyto dvě sítě považujeme za rozdílné. Oddělení LAN sítí je ještě více markantní, jestliže jsou přemosťující prvky od sebe fyzicky vzdáleny. Technologie umožňující přenos dat v síti LAN jsou nejčastěji Ethernet, Token Ring a FDDI. (Sosinsky, 2010)

Pro sítě rozprostírající se na velkém území je nejčastěji používán pojem WAN (Wide Area Network). WAN propojují jednotlivé lokální sítě, které od sebe mohou být geograficky velmi vzdálené a umožňují komunikaci mezi jednotlivými uživateli. Nejznámějším

příkladem takové sítě je Internet. Méně známé jsou sítě MAN (Metropolitan Area Network), které propojují lokální sítě nacházející se v geograficky blízké oblasti, která je větší než LAN a menší než WAN, většinou přibližně na území jednoho města. Další podobnou sítí je CAN (Campus Area Network), která se rozprostírá například v areálu univerzity nebo průmyslového areálu a spojuje fyzicky jednotlivé budovy. (Donahue, 2007) (Sosinsky, 2010) (Spurná, 2010)

3.2 Topologie sítí

Topologie udává způsob, jakým jsou v síti propojena jednotlivá zařízení. Toto zapojení ve výsledku podstatně ovlivňuje výsledné chování sítě. Na topologii může být nahlíženo z hlediska logického uspořádání nebo fyzického rozložení.

3.2.1 Logická topologie

Logická topologie udává způsob vysílání na síť. Jestliže zařízení na síti sdílí společné médium jedná se o *mnohonásobný přístup zařízení*. Pokud jsou výhradně spojeny dva počítače, jde o spojení *point-to-point (bod-bod)*. (Spurná, 2010)

Mnohonásobný přístup na sdílené médium

Existují dvě metody přístupu, stochastická metoda *Broadcast (vysílání)* a deterministická *Token passing („předávání peška“)*.

Broadcast – všechna zařízení v síti jsou si svým postavením rovna. Zařízení průběžně naslouchají, zdali na síti probíhá nějaký provoz. Pokud chce zařízení vysílat, učiní tak jakmile na síti nebude žádný provoz. Neexistuje zde žádná přednost ve vysílání, které zařízení začne vysílat jako první, uspěje. Nevýhodou je, že i přes tato opatření může docházet ke kolizím, protože v jeden okamžik, kdy na síti není žádný provoz může začít vysílat více počítačů. Po vzniku kolize počítače na chvíli přestanou vysílat a poté se o přenos pokusí znovu. (Horák, 2011) (Spurná, 2010)

Token passing – principem je kolující speciální paket (token), který určuje oprávnění vysílat. Počítač, u kterého je zrovna přítomen token může vysílat nebo token pouze předat dál, tím je zajištěn spravedlivý vysílací čas. Když pošle počítač do sítě data, jednotlivé uzly kontrolují, jestli jsou určená pro něj, pokud ne, posílá data na další uzel, dokud nedojdou do cíle. Většinou se zde používá kruhová fyzická topologie. (Horák, 2011)

Point-to-point

Počítače komunikují pouze přímo mezi sebou, a tudíž svojí komunikací nezasahují do zbytku sítě, obvykle zde nedochází ke kolizím. V bodové komunikaci mezi jednotlivými počítači může být více systémů, které tuto komunikaci řídí. Sítě typu point-to-point využívají často

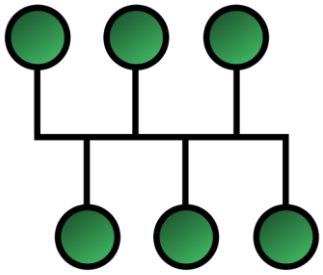
nadbytečné trasy, proto je nutné pro efektivní komunikaci v síti využít směrovače. (Sosinsky, 2010)

3.2.2 Fyzická topologie

Fyzická topologie charakterizuje síť z pohledu fyzického zapojení jednotlivých prvků, kterými mohou být uzly, koncová zařízení sítě nebo jejich spoje a propojení. Existuje mnoho jednotlivých podob topologie, ale mnohé sítě v praxi využívají kombinaci těchto typů topologií.

Sběrnicová topologie

Takovéto uspořádání bylo typické pro zapojení počítačů pomocí koaxiálního kabelu. Veškeré počítače jsou součástí jedné *kolizní domény*[1] a sdílejí průběžný kabel, vedený od stanice ke stanici. Výhodou takového zapojení je nízká cena kabeláže, na druhou stranu nevýhodou je velký počet spojů na průběžném kabelu, které způsobují časté poruchy. Zároveň jakékoli přerušení vedení znamená nefunkčnost celé sítě. (Horák, 2011) (Spurná, 2010)

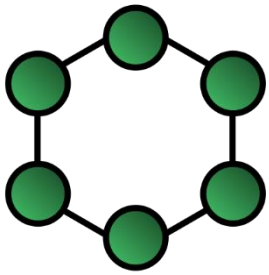


Obrázek 1 - Sběrnicová topologie

[1] Kolizní doména – část počítačové sítě, ve které je více zařízení připojeno na sdílené médium. Při vysílání více zařízení najednou dojde ke kolizi a znehodnocení dat.

Kruhová topologie

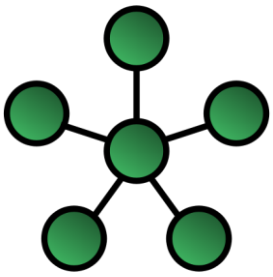
Zařízení jsou zde zapojena do souvislého kruhu, proto zde lze využít technologii Token passing. *Nevýhoda* je zde podobná jako u sběrnicové topologie, porucha na vedení nebo jednoho z uzlů zapříčiní selhání celé sítě. Například sítě IBM Token Ring využívají pro zabránění selhání zdvojení vedení. (Horák, 2011)



Obrázek 2 - Kruhová topologie

Hvězdicová topologie

Na rozdíl od předchozích zde existuje centrální prvek, hub (rozbočovač) nebo dnes nejčastěji switch (přepínač), do kterého jsou jednotlivé počítače zapojeny. *Výhodou* této topologie je její odolnost vůči poruchám a případná snadná lokalizace chyby. Jestliže selže vedení od jednoho počítače, není tím ohrožena funkčnost zbytku sítě. Jedná se dnes o nejpoužívanější topologii. (Horák, 2011)



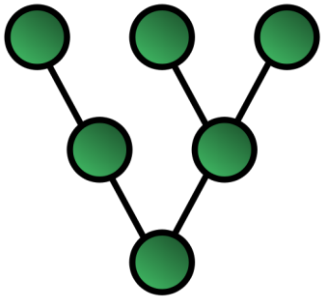
Obrázek 3 - Hvězdicová topologie

Topologie rozšířená hvězda

Jedná se o způsob zapojení, kdy několik sítí typu hvězda propojíme pomocí rozbočovače nebo přepínače, tím vznikne síť s topologií rozšířené hvězdy. Při použití rozbočovače je nutné dbát na rozumnou rozlehlost sítě, jinak zde může docházet ke zpožděným kolizím. S použitím přepínače toto nemůže nastat. (Spurná, 2010)

Hierarchická topologie

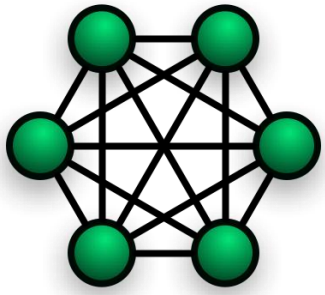
Hierarchické uspořádání je podobné topologii rozšířené hvězdy. Rozdíl je v existenci počítače, který je umístěn na vrcholu stromu, a který řídí provoz v síti. Počítače jsou stejně jako v topologii rozšířené hvězdy propojeny pomocí rozbočovačů a přepínačů. Hierarchická topologie musí zahrnovat alespoň 3 úrovně uzlů, jinak by se jednalo o topologii hvězdy. (Sosinsky, 2010) (Spurná, 2010)



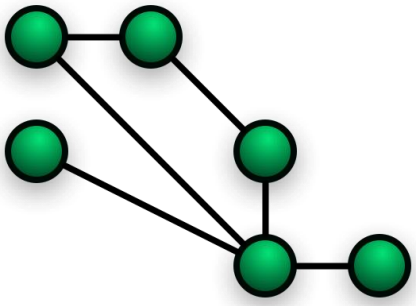
Obrázek 4 - Hierarchická topologie

Mesh topologie

Jedná se o dnes nejpoužívanější topologii, na které funguje i celý Internet. Mesh sítě hojně využívá Internet of Things[2] (Internet věcí), kdy na rozdíl od hvězdicové topologie nepotřebuje pro přístup do internetu směrovač. Existují dva druhy, úplná a částečná topologie mesh. Úplná vyžaduje spojení každého počítače s každým, a to je velmi nákladné řešení, proto se dnes využívá především neúplná topologie mesh, kde jsou některé linky vynechány. Toto decentralizované řešení má velkou výhodu, pokud selže jeden z uzlů ostatní stále mohou komunikovat, pouze bude tato komunikace probíhat přes jiné uzly. (Nizam, 2014) (Spurná, 2010)



Obrázek 5 - Úplná topologie mesh



Obrázek 6 - Částečná topologie mesh

[2] Internet of Things – propojení předmětů běžného využití mezi sebou za účelem jejich komunikace a kontroly. Ve většině případů realizováno pomocí bezdrátových technologií.

3.3 Síťová zařízení

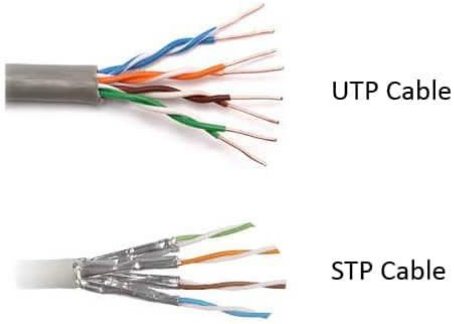
Pro vybudování sítě potřebujeme kromě počítačů obsahujících software podporující síťovou komunikaci také zařízení, kterými jednotlivé počítače propojíme. Jedná se především o přenosová média a aktivní síťové prvky.

3.3.1 Přenosová média

Existují tři hlavní druhy přenosu dat, pomocí elektrických signálů, světelných impulsů nebo pomocí bezdrátových technologií.

Prvním zástupcem přenosu pomocí elektrických signálů je nejvyužívanější *kroucená dvojlinka (twisted pair).* Skládá se ze 4 párů vodičů, kde každý pár je stočen dohromady, a nakonec jsou stočené i všechny páry. Toto kroucení má pozitivní vliv jak na rušení datového toku, tak i na vyzařování kabelu do svého okolí. Vodiče se nejčastěji vyrábí z mědi a mají impedanci 100 Ω. Maximální délka je 100 metrů a celý kabel se ukončuje konektorem typu RJ-45.

Využívají se dva typy, nestíněný označovaný jako UTP a stíněný STP. Stínění je provedeno pomocí obalení každého páru vodiče kovovou fólií a poté ještě všech vodičů dohromady. Tyto kabely jsou dražší a obtížněji se zakončují, je zde nutné správně uzemnit stínění v konektoru, jinak se kabel chová podobně jako anténa a rušení je naopak větší. (Spurná, 2010)



Obrázek 7 - Porovnání UTP a STP kabelu

Dalším médiem na bázi elektrických signálů je *koaxiální kabel*. Je tvořen dvěma vodiči, jedním měděným v jádru, okolo kterého je plastová izolace. Na této izolaci je síť tenkých drátků tvořící druhý vodič, který slouží primárně k elektromagnetickému odstínění vodiče v jádru kabelu. Používal se v sítích se sběrnicovou topologií, kde docházelo k častým kolizím


Obrázek 8 - Koaxiální kabel

dat, proto se dnes již v lokálních sítích nevyužívá. Impedance kabelu je 50 Ω a jeho maximální délka závisí na tloušťce použitého kabelu, 500 metrů (průměr 1 cm) nebo maximálně 185 metrů (průměr 0,35 cm). (Kostrhoun, 2001)

Nejrychlejším spojem jsou *optická vlákna*, ty k přenosu využívají světelné impulsy. V optickém vlnovodu se světelné paprsky částečně odrážejí na rozhraní dvou prostředí s rozdílnou optickou hustotou a část jich projde do druhého prostředí, tímto únikem vznikají ztráty. Na principu odrazů funguje přenos v optickém vlákně. Oproti výše uvedeným jsou optické kabely velmi drahé a využívají se především pro páteřní sítě. (Plexo, 2008)

3.3.2 **Aktivní prvky**

Hub

Dříve se jednalo o pasivní prvek, který pouze spojoval jednotlivé zařízení dohromady. Dnes je již hub považován za aktivní prvek, protože zároveň plní funkci zesilovače. Rozbočovač posílá veškerý přijatý signál, který zároveň zesílí, na všechna svá připojená zařízení. Počítače připojené k rozbočovači tvoří tzv. kolizní doménu. Operuje na první vrstvě ISO/OSI modelu. (Spurná, 2010)

Bridge

Rozděluje dva nebo více segmentů sítě. Na rozdíl od rozbočovače posílá data pouze do segmentu, ve kterém se nachází cílový počítač. Rozhoduje se podle MAC adres připojených zařízení. Jestliže je cíl ve stejném segmentu sítě jako zdroj, bridge nepropustí komunikaci do ostatních segmentů sítě. Převážně se uplatňuje na sběrnicové topologii a pracuje na druhé vrstvě ISO/OSI modelu. (Horák, 2011)

Switch

Přepínač vytváří lokální síť a rozděluje ji na oddělené kolizní domény. Řídí provoz na síti pomocí MAC adres a je schopen vytvořit virtuální okruh mezi dvěma počítači tak, aby svojí komunikací nezasahovali do zbytku sítě. V dnešní době díky své ceně již většinou nahradil hub a bridge. Pracuje na druhé vrstvě ISO/OSI modelu.

Router

Jde o nejinteligentnější aktivní prvek z výše uvedených. Spojuje více sítí dohromady a podle nastavené metriky ukládá informace o připojených zařízeních v sítích a cestách k nim do tzv. směrovací tabulky. Poté dle této tabulky směruje pakety nejlepší možnou cestou k cíli. (Cisco, 2017) (Spurná, 2010)

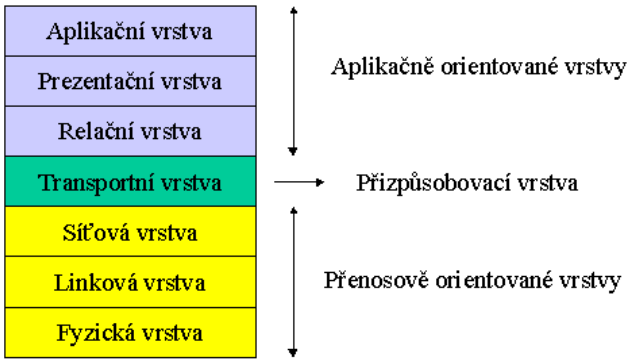
3.4 Referenční model ISO/OSI

Na počátku počítačových sítí začaly vznikat síťové architektury, které dávají představu kolik má existovat vrstev a k čemu by měly sloužit. Nejdříve existovaly pouze proprietární řešení, například architektury SNA (System Network Architecture) od firmy IBM nebo DECNET od Digital Equipment Corporation. Průběhem času bylo potřeba vytvořit všeobecnější architekturu, která by byla dostatečně otevřená a nestarala by se o ní pouze jedna firma.

Organizace ISO (International Organization for Standardization) nejdříve vytvářela architekturu otevřených systémů (Open Systems Interconnection Architecture), ve které byla charakterizována jak samotná síť, tak i jednotlivé uzly včetně jejich fungování. Takto rozsáhlá architektura se organizaci ISO nepovedla vytvořit, a nakonec připravila místo celé architektury pouze referenční model, který obsahuje sedm vrstev a uvádí jejich účel. Název se tedy změnil na Open Systems Interconnection, dnes označován zkratkou ISO/OSI. (Peterka, 2005b)

3.4.1 Vrstvy modelu ISO/OSI

- Aplikační vrstva
- Prezentační vrstva
- Relační vrstva
- Transportní vrstva
- Síťová vrstva
- Linková vrstva
- Fyzická vrstva



Obrázek 9 - Model ISO/OSI

Aplikační vrstva

Tato vrstva umožňuje uživatelům přistupovat k síťovým službám. Například využívat vzdálený přístup k souborům, počítačům a tiskárnám nebo zasílat elektronické zprávy. V aplikační vrstvě se vždy nachází pouze část aplikace, kterou je třeba standardizovat. U výše zmiňovaného e-mailu se jedná o mechanismy pro přenos jednotlivých zpráv. Uživatelské rozhraní e-mailového klienta již není třeba standardizovat, tudíž nenáleží do aplikační vrstvy, ale nachází se odděleně. (Peterka, 2005b)

Prezentační vrstva

Stará se o správnou interpretaci dat mezi zdrojovým a cílovým zařízením. Data mohou být kódována různým způsobem, proto by cílové zařízení nemuselo zaslané zprávě rozumět stejně jako zařízení zdrojové. O sjednocení kódování (formy) dat se stará právě tato vrstva ISO/OSI modelu. Zároveň data šifruje tak, aby jejich obsah nebyl čitelný pro žádné zařízení po cestě mezi zdrojem a cílem. (Spurná, 2010)

Relační vrstva

Synchronizuje a navazuje přenos mezi relačními vrstvami obou stran přenosu. Zajišťuje ověření uživatelů a zabezpečení přístupu k zařízení. Často splývá s vrstvou prezentační. (Horák, 2011)

Transportní vrstva

Jedná se o tzv. přizpůsobující vrstvu. Spojuje tři nejvyšší aplikačně orientované a tři nejnižší přenosově orientované vrstvy. Je zodpovědná při odesílání za konverzi zprávy na segmenty a poté při příjmu za opětovné spojení segmentů do zprávy. Umožňuje také pomocí údajů o zdrojovém a cílovém portu současný běh více datových přenosů najednou. Port identifikuje aplikaci (proces), které jsou data určena. Díky tomu je možné zároveň zobrazovat internetové stránky, posílat e-mail a mnoho dalšího. (Spurná, 2010) (Peterka, 2005b)

Síťová vrstva

Přenáší pakety mezi dvěma uzly, mezi jimiž neexistuje přímé spojení. Uchovává údaje o cílové a zdrojové síťové adrese. Pomocí těchto adres zajišťuje výběr trasy spojení, tento výběr se nazývá routing (směrování). Pracují zde směrovače.

Mezi nejjednodušší algoritmy směrování patří *záplavové směrování*. Každý uzel, který se zúčastní přenosu pošle paket dál na všechny sousední uzly, kromě toho, ze kterého paket přijal. Tímto vzniká velké množství duplicitních paketů, které je nakonec třeba eliminovat, ale máme jistotu, že se takto rozesílané pakety dostanou do svého cíle. Existují i sofistikovanější algoritmy, které hledají cestu k cíli pomocí znalosti celé topologie sítě. V síťové vrstvě by tak měly jednotlivé uzly znát kromě svých přímých sousedů celou síť, ve které se nacházejí. (Peterka, 2005b)

Linková vrstva

Uskutečňuje přenos rámců v lokálních sítích. Obsahuje údaje o cílové a zdrojové fyzické adrese v aktuální lokální síti kde se rámec nachází. Pokud jsou data posílána do jiné lokální sítě, na hraničním zařízení (většinou směrovač) jsou údaje o fyzických adresách vyměněny za nové. Na rozdíl od síťové vrstvy zná každý uzel pouze své přímé sousedy. Pracují zde přepínače, mosty a síťové karty. (Spurná, 2010) (Peterka, 2005b)

Fyzická vrstva

Jejím úkolem je fyzicky přenášet data. Činí tak po jednotlivých bitech, zabývá se jakým signálem jsou jednotlivé bity reprezentovány, jaké jsou použity konektory, jak je řešená synchronizace a jaká přenosová rychlost se používá. Není zde zřejmá interpretace jednotlivých bitů, ani které bity patří k sobě, toto mají za úkol vyšší vrstvy, kterým poskytuje pouze dvě služby, a to příjem a odeslání bitu. (Peterka, 2005b)

3.5 Architektura a protokoly rodiny TCP/IP

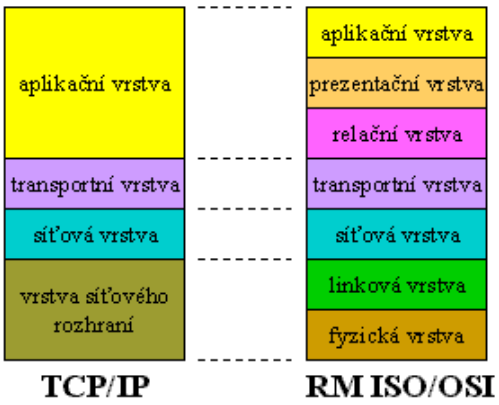
Referenční model ISO/OSI se nikdy do obecného využití nedostal a to především, protože vznikal zčásti odděleně od reality. Model obsahoval velké množství funkcí a vlastností, ale nikdo nevěděl, jak takto rozsáhlý standard zavést do praxe. Než se model stihl upravit do podoby, která by již šla standardizovat, začala se využívat nová architektura nazývaná jako *rodina protokolů TCP/IP*.

Za vznikem architektury TCP/IP stojí především rozšíření sítě ARPANET[3] na univerzity a posléze mezi veřejnost. Síť ARPANET z počátku využívala především protokol NCP (Network Control Protocol), ten se ale nehodil pro běžné používání sítě veřejností, a tak akademická sféra zapojená do výzkumné sítě ARPANET dostala od resortu obrany USA za úkol vyvinout sadu protokolů, které by bylo možné standardizovat. Dnes se používá ve většině počítačových sítí včetně celého Internetu. (Peterka, 2005c) (Donahue, 2007)

Architektura TCP/IP je rozdělena na 4 vrstvy na rozdíl od modelu ISO/OSI, který je dělený na vrstev sedm. Ale pouze 3 nejvyšší vrstvy jsou standardizované protokoly TCP/IP. Nejnižší vrstva starající se o fyzický přenos dat přebírá normy z jiných technologií. Většinou se jedná o Ethernet, Wi-Fi, Token Ring nebo xDSL. (Microsoft, 2003)

3.5.1 Vrstvy modelu TCP/IP

- Aplikační vrstva
- Transportní vrstva
- Síťová vrstva
- Vrstva síťového rozhraní



Obrázek 10 - Porovnání TCP/IP s ISO/OSI

[3] ARPANET – neboli Advanced Research Projects Agency NETwork byla armádní a výzkumná počítačová síť, která je považována za předchůdce dnešního Internetu.

Aplikační vrstva

Stejně jako u modelu ISO/OSI i zde se nachází vždy pouze část aplikace, která je třeba standardizovat. Protokoly síťové vrstvy zajišťují komunikaci mezi aplikacemi a zbytkem sítě. Definují pravidla síťové komunikace a specifikují podobu a formát dat. Pro identifikaci cílové aplikace se používají tzv. porty z transportní vrstvy. (Spurná, 2010)

Protokol DNS

Každé síťové zařízení je identifikované pomocí IP adresy a zároveň má většina přiřazené i jméno. Tato služba zajišťuje překlad jmenných názvů jednotlivých zařízení na odpovídající síťové adresy. DNS se nejčastěji používá pro přístup uživatelů na webové stránky. Je totiž jednodušší zapamatovat si jméno www.google.cz než síťovou adresu 172.217.1.3.

Jednotlivé konverze jsou uloženy v cache paměti DNS serverů, které tyto seznamy aktualizují a předávají si je mezi sebou. Jestliže počítač nezná síťovou adresu, ale pouze jmennou, dotáže se DNS serveru a ten mu vrátí adresu síťovou. Pokud DNS server konverzi nezná, zašle požadavek na další DNS server a poté si ji již uloží do cache paměti. Stejně tak činí počítač, a tudíž se již příště nemusí dotazovat DNS serveru. (Spurná, 2010)

DNS obvykle přistupuje na port číslo 53.

Protokol HTTP

Zajišťuje přenos dat z webového serveru ke klientovi. Uživatel zadá webovou adresu, která se následně přeloží pomocí DNS na IP adresu a naváže se spojení s cílovým serverem. Server vrátí zpět požadovaná data, většinou ve formátu HTML kódu a ty se uživateli zobrazí v prohlížeči.

Základní protokol HTTP není nijak šifrovaný, tudíž veškerá přenášená data lze zachytit. Dnes se však ve většině případů využívá šifrovaná verze HTTPS, která přenášená data zabezpečuje prostřednictvím protokolu TLS[4] (Transport Layer Security). To nám zaručuje

[4] TLS – Transport Layer Security je kryptografický protokol, poskytující možnost zabezpečené komunikace pro webové služby.

příjem nepozměněných dat od serveru a poskytuje šifrování dat posílaných od uživatele na server. (Google, 2017)

HTTP obvykle přistupuje na port číslo 80 a HTTPS na port 443.

Protokol DHCP

Pomocí DHCP serveru mohou připojená zařízení získávat automaticky síťová nastavení, například IP adresu, masku podsítě, síťovou adresu brány nebo adresy DNS serverů. Pokud má zařízení nastaveno získávání IP adresy pomocí DHCP, tak po připojení do sítě kontaktuje DHCP server a ten mu přidělí volnou IP adresu z nastaveného rozsahu. (Kurose, 2014)

Klient u DHCP komunikuje na portu 68 a server naslouchá na portu 67.

Protokoly POP, SMTP a IMAP

Tyto protokoly využívá ke své práci elektronická pošta. *Protokol POP* slouží ke stažení e-mailu ze serveru ke klientovi. Naopak *protokol SMTP* se stará o odeslání e-mailu od klienta. V dnešní době se nejvíce využívá *protokol IMAP,* přes který je možné pracovat s e-maily na straně serveru bez potřeby všechny e-maily stahovat do počítače. (Kurose, 2014)

Protokol POP k připojení klienta využívá většinou port 110, SMTP server poslouchá na portu číslo 25 a IMAP server obvykle naslouchá na portu 143. (Spurná, 2010)

Transportní vrstva

Transportní vrstva v architektuře TCP/IP je svojí funkčností shodná s tou v modelu ISO/OSI. Je zodpovědná za rozdělení zprávy na segmenty (TCP) nebo datagramy (UDP) a následné složení zprávy do původní podoby. Využívá k tomu dva přenosové protokoly, spojově orientovaný a spolehlivý *TCP* a nespojový a nespolehlivý *UDP*.

Protokol TCP

Jde o hlavní protokol transportní vrstvy. Jedná se o spojově orientovaný a spolehlivý protokol, proto pro přenos nejdříve vytvoří mezi klientem a serverem oboustranné spojení, tím je zajištěno spolehlivé doručení dat. (Spurná, 2010)

Spojení je inicializováno metodou „three-way-handshake“, volně přeloženo jako „třícestné podání ruky“. Klient nejdříve zašle serveru synchronizační segment, server poté odpoví, že na žádost o přenos přistupuje. Jako poslední krok musí klient zaslat zpět potvrzující zprávu. Následně začíná klient odesílat očíslované segmenty a server potvrzuje příchozí data, případně klient znovu odesílá ze strany serveru nepotvrzená data. (Microsoft, 2003)

Využívá se například k přenosu webových stránek nebo e-mailů, kde jsou nepřípustné ztráty segmentů, díky kterým by docházelo ke zkreslení obsahu.

Protokol UDP

Na rozdíl od protokolu TCP funguje protokol UDP nespojově a je označován za nespolehlivý. Při přenosu datagramů může nastat situace, kdy některé z nich putují sítí delší nebo pomalejší trasou než jiné a do cíle tak dorazí v jiném pořadí, než je klient odeslal. Tímto dochází ke zkreslení výsledného obsahu, které protokol TCP řeší číslováním segmentů, podle něhož je schopen data předat v nezměněné podobě. Naopak protokol UDP seřazuje v cíli datagramy podle pořadí, ve kterém přišly.

Protokol UDP funguje nespojově, tudíž před přenosem dat nevytváří spojení mezi účastníky přenosu, ale data odesílá ihned, když aplikace požaduje přenos. Cílové zařízení také pomocí protokolu UDP nezasílá zdroji zprávy o doručení dat. (Horák, 2011)

Využívá se především v situacích, kdy je hlavní rychlost přenosu a nevadí určité ztráty datagramů. Jedná se například o přenos hlasu pomocí technologie VoIP[5], video streaming nebo ho využívá technologie DNS.

Síťová vrstva

Podobně jako vrstva transportní je i síťová vrstva svojí funkcí shodná s tou v modelu ISO/OSI. Jejím hlavním úkolem je přenos dat mezi uzly pomocí adresování. Dále zajišťuje zapouzdření dat přejatých z transportní vrstvy do IP paketu.

[5] Voice over Internet Protocol – Technologie umožňující přenos hlasu v počítačových sítích pomocí paketů v rodině protokolů TCP/IP.

IP protokol

Protokol IP doručuje pakety co nejrychleji bez zbytečné kontroly a zahlcování sítě, proto je označován za nespolehlivý. O kontrolu dat se stará protokol z vyšší transportní vrstvy, nejčastěji TCP.

Dnes nejpoužívanějším je protokol IP verze 4, zkráceně IPv4. Využívá 32 bitové síťové adresy nejčastěji zapisované v dekadickém tvaru, tomuto vyhovuje například adresa 10.0.0.32. Pro oddělení adresy sítě a identifikace počítače se používá tzv. maska. Na místě síťové adresy se v masce nachází v binárním zápisu samé jedničky. (Spurná, 2010)

Pro použití adresace v lokálních sítích jsou vyhrazeny 3 třídy IP adres se standardními síťovými maskami. (Horák, 2011)

- Třída A: 10.0.0.0–10.255.255.255 (maska: 255.0.0.0)
- Třída B: 172.16.0.0–172.31.255.255 (maska: 255.255.0.0)
- Třída C: 192.168.0.0–192.168.255.255 (maska: 255.255.255.0)

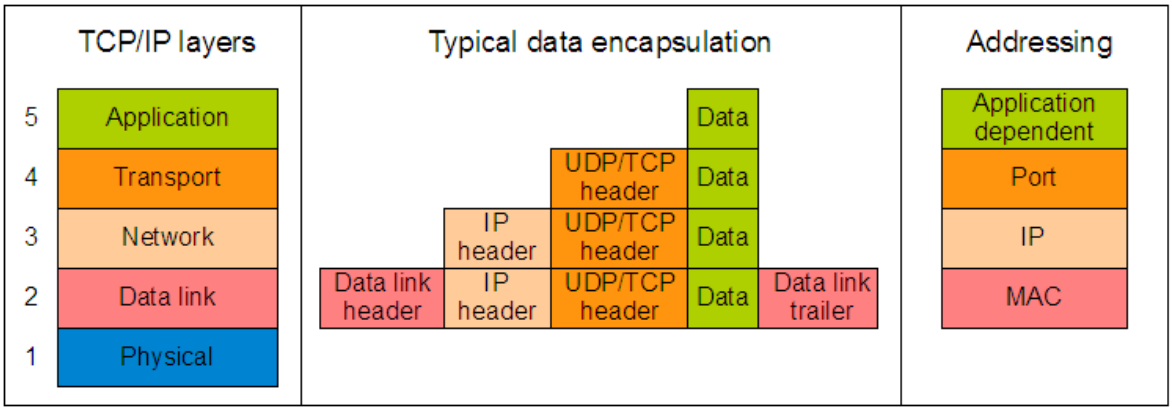
Nejpoužívanější protokol IPv4 využívající 32 bitové adresy (4 294 967 296 unikátních IP adres) dnes již nedostačuje. Potýkáme se s nedostatkem unikátních adres, a proto se začíná používat nová verze protokolu nazývaná jako IPv6. Adresní prostor tohoto nového protokolu je v rozsahu 128 bitů. Pro adresaci lokálních sítí se však stále používá protokol IPv4.

Zapouzdření dat

Při odesílání dat se nejdříve provádí tzv. zapouzdření dat. Na obrázku č. 9 je vyobrazena struktura zapouzdření dat v architektuře TCP/IP.

Ve chvíli kdy aplikace žádá odeslání dat, předá tyto data nižší transportní vrstvě, která k datům přidá podle použitého protokolu (TCP nebo UDP) hlavičku, obsahující zdrojový a cílový port. Poté je segment předán do síťové vrstvy, kde je přidána IP hlavička, ve které se nachází údaje o adresaci, tímto je vytvořen paket, který se předává níže do vrstvy síťového rozhraní. Zde se přidávají informace o zdrojové a cílové fyzické adrese a vzniká zapouzdřený rámec, který se ve formě bitů posílá na fyzickou síť.

Ve chvíli kdy rámec narazí v síti na uzel, je rámec rozbalen v opačném pořadí, až do té míry, na kterou úroveň se dané zařízení potřebuje dostat. Například směrovač rámec rozbalí na úroveň síťové vrstvy, aby byl schopen přečíst IP adresu a podle ní rámec dále adresovat. Ve chvíli přijmu dat cílovým zařízením se provádí rozbalování dat od nejnižší vrstvy až po konkrétní data. (Bouška, 2007) (Spurná, 2010)



Obrázek 11 - Zapouzdření dat v TCP/IP

3.6 Standardy sítí

S vývojem počítačových sítí se postupem času uváděly v platnost různé normy, které se kryly s využitím sítí v reálném světě. Většina takových standardů vzešla ze spolupráce předních výrobců, například skupiny DIX (DEC, Intel, Xerox), ovšem například technologie Token Ring pocházela pouze od IBM. O standardizaci se stará organizace IEEE (Institute of Electrical and Electronics Engineers), podle této organizace se jednotlivé normy i označují.

Normy se snaží přijímat v co nejobecnější podobě, aby byla umožněna spolupráce co nejvíce produktů od různých výrobců. V průběhu posledních bezmála 40 let vznikl souhrn 15 standardů, tento počet však není konečný, s novými technologiemi přichází i nové standardy. (Sosinsky, 2010) (Horák, 2011)

Pro lokální počítačové sítě jsou nejdůležitější dva standardy a to IEEE 802.3 pro ethernet a IEEE 802.11 pro bezdrátové sítě.

3.6.1 Standardy Ethernetu – IEEE 802.3

Ethernet je nejvyužívanější technologií pro budování lokálních počítačových sítí. Definuje přenos rámců na fyzické a linkové vrstvě ISO/OSI modelu pomocí přístupové metody CSMA/CD[6]. První verzi Ethernetu, která byla vzorem pro standard IEEE 802.3 byla vytvořena skupinou DIX. Rychlost této verze byla max. 10 Mb/s. Nejrozšířenějším přenosovým médiem pro ethernet se stala kroucená dvojlinka. (Sosinsky, 2010)

Ethernet se dělí dle rychlostí na:

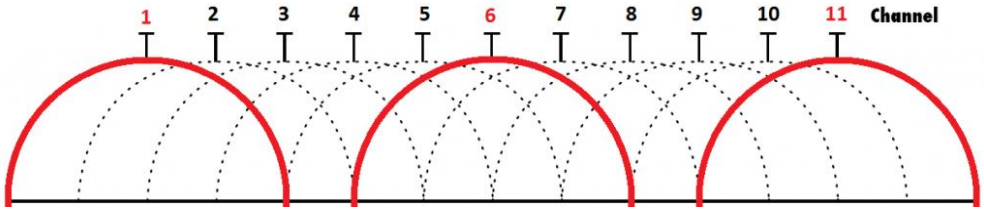
- Ethernet – rychlost max. 10 Mb/s, provozován na kabelech UTP kategorie 3 (cat3)
- Fast Ethernet – rychlost max. 100 Mb/s, provozován na kabelech UTP cat5
- Gigabit Ethernet – rychlost max. 1 Gbit/s, provozován na kabelech UTP cat5e
- 10 Gigabitový Ethernet – rychlost max. 10 Gbit/s, lze provozovat na UTP cat6, ale pouze do 55 metrů délky. Pro plných 100 metrů je třeba UTP cat6a. (Solarix, 2016)

[6] Carrier Sense Multiple Acces with Collision Detection – Přístupová metoda, která reguluje přístup jednotlivých uzlů ke společně sdílenému přenosovému médiu. Zahrnuje detekci kolizí.

3.6.2 **Standardy bezdrátových sítí – IEEE 802.11**

Bezdrátové sítě se dnes využívají v každé firmě, ale i domácnosti. Každý člověk má aspoň jedno zařízení, které se připojuje k síti LAN IEEE 802.11, která je známá spíše jako Wi-Fi. O přenos rádiového signálu se v tomto standardu používá několik druhů modulací se stejným protokolem. Jedná se zejména o 802.11a, b, g, n a ac.

Tyto sítě většinou využívají pro přenos rádiové frekvence v pásmech 2,4 GHz nebo 5 GHz. Tyto pásma se dále dělí na kanály, na které se poté daná Wi-Fi síť připojuje. Pásmo 2,4 GHz má ve skutečnosti rozptyl 2,4–2,485 GHz. Těchto 85 MHz je rozděleno do 11 kanálů po 20 MHz, které se částečně překrývají. Maximální počet sítí, které se nebudou překrývat je roven 3, toto lze zajistit připojením na kanál č.1, 6 a 11.



Obrázek 12 - Kanály pásma 2,4 GHz

Obdobně je to u pásma 5 GHz, kde se ale nachází 19 kanálů a je možné připojit až 19 nepřekrývajících se sítí, díky 20 MHz kroku a nepřekrývajícím se kanálům. (Kurose, 2014)

IEEE 802.11a

Nejstarší norma pro bezdrátové sítě, využívající pásmo 5 GHz. Její teoretická maximální rychlost je 54 Mbit/s. Díky pásmu 5 GHz měl tento standard vysokou rychlost, na druhou stranu o to menší dosah. Také je zde méně zařízení, které by mohli přenos rušit. Celý standard pracuje s modulační metodou OFDM[7] na fyzické vrstvě.

[7] Orthogonal Frequency Division Multiplexing – technika multiplexování pomocí frekvenčního dělení kanálu. Využívá několik navzájem se překrývajících pomocných nosných vln a tím dosahuje vysokých rychlostí.

IEEE 802.11b

Na rozdíl od 802.11a má tento standard větší přenosovou vzdálenost, a to díky použitému pásmu 2,4 GHz. Bohužel tímto klesla maximální rychlost na pouhých 11 Mbit/s. Je zde též možnost rušení od věcí každodenního použití, jako například od mikrovlnné trouby, která také využívá pásmo 2,4 GHz. Používá se zde modulace DSSS[8].

IEEE 802.11g

Standard s označením 802.11g rozšiřuje přechozí IEEE 802.11b, pracuje na stejné frekvenci 2,4 GHz a je proto zpětně kompatibilní. Teoretická maximální rychlost se zvýšila na 54 Mbit/s, reálná rychlost přenosu dat se pohybuje v rozmezí přibližně 25-30 Mbit/s, vše samozřejmě závisí na prostředí a rušení. (Mitchell, 2016)

IEEE 802.11n

Pracuje s frekvencí 2,4 i 5 GHz a využívá modulaci OFDM s technologií MIMO. *„Technologie MIMO pracuje na bázi vysílání několika signálů různými cestami, prostřednictvím více antén. Teoreticky je tak možné přidáváním antén stále propustnost zvyšovat, prakticky se ale pro vnitřní prostředí a menší dosah používají 2 až 4 antény.“* (Horák, 2011)

Díky této technologii dosahují Wi-Fi sítě 802.11n teoretických rychlostí až 600 Mbit/s, reálně však maximálně 200 Mbit/s.

IEEE 802.11ac

Nejnovější a prozatím nejrychlejší standard bezdrátových sítí, ustanoven v roce 2014. Operuje pouze na frekvenci 5 GHz a pro zvýšení rychlosti má oproti 802.11n rozšířeny komunikační kanály ze 40 MHz až na 160 MHz. Také dokáže pracovat s až 8 cestami oproti 4 u předchozího standardu. Jde o první Wi-Fi standard pro gigabitový přenos. Teoretická rychlost při použití všech 8 dostupných cest se blíží 7 Gbit/s. (Cisco, 2015)

[8] Direct Sequence Spread Spectrum – technologie přímého rozprostřeného spektra. Zavádí se umělá nadbytečnost bitů, tímto je signál více rozprostřen a je méně náchylný k rušení.

3.7 Zabezpečení sítě

Při počtu používaných bezdrátových zařízení, ať už se jedná o mobilní telefony, notebooky, tablety nebo v dnešní době oblíbené různé chytré spotřebiče je domácí počítačovou síť nutno pokrýt také bezdrátovým signálem. Oproti metalické síti je u bezdrátové snazší napadnutí přenosu dat a jejich případné zneužití. Je tedy nutné dostatečně zabezpečovat všechny bezdrátové sítě, ty domácí nevyjímaje.

Tím nejzákladnějším zabezpečením je zajisté změna výchozího hesla pro přístup do konfigurace bezdrátového aktivního prvku sítě. V domácích podmínkách se povětšinou jedná o Wi-Fi modem od poskytovatele internetu, případně Wi-Fi routery a přístupové body. Dalším krokem by mělo být nastavení dostatečně silného hesla pro přihlášení k síti Wi-Fi. Takové heslo poté šifruje přístup do naší bezdrátové sítě. Existuje několik protokolů zabezpečení, již zastaralý WEP a modernější WPA a WPA2.

WEP

Tento protokol byl zaveden roku 1999, a doslovně znamená soukromí ekvivalentní kabelovému přenosu (Wired Equivalent Privacy). To se však již roku 2001 vyvrátilo, a to díky prolomení zabezpečení WEP. Zabezpečení je provedeno pomocí 40 nebo 104 bitových klíčů a algoritmu proudového šifrování dat. Hlavním bezpečnostním rizikem je zde použití nezašifrovaného přenosu klíčů a jejich neměnná podoba. I přesto, že je v dnešní době tento protokol považován za velice nebezpečný a nevhodný k použití, je podporován mnohými zařízeními. (Scarpati, 2017)

WPA

Protokol nového bezpečnostního standardu 802.11x, je zde opraveno několik chyb z protokolu WEP. Klíče již nejsou neměnné, ale jsou generovány mechanismem TKIP[9] po určitém čase nebo přenesených paketech nové. Používají se 128 bitové klíče s 48 bitovým inicializačním vektorem. I přes toto vylepšení je protokol při použití TKIP považován za prolomitelný. (Sosinsky, 2010)

[9] Protokol dočasné integrity klíčů.

WPA2

Nejnovější protokol, který je od roku 2004 součástí bezpečnostního standardu 802.11i. Uplatňuje se zde nový šifrovací algoritmus AES[10], který generuje 256 bitové klíče a používá blokovou šifru na rozdíl od proudové u svých předchůdců. Kombinace WPA2 s AES je dnes nejbezpečnější standard, který by se v případě podpory ze strany zařízení měl bez výhrad využívat.

[10] Advanced Encryption Standard – pokročilý šifrovací standard.

4 Vlastní práce

Vlastní práce se zabývá analýzou technologií v rozdílných podmínkách. Především měřením útlumu Wi-Fi signálu v různých materiálech. Poté je zde vypracován návrh a konfigurace sítě, včetně finálního otestování v konkrétní domácnosti.

4.1 Analýza technologií v různých podmínkách

Počítačovou síť v domácnostech lze vytvořit pomocí mnoha technologií. Prostřednictvím strukturované kabeláže, moderním způsobem po stávajících silnoproudých rozvodech nebo pomocí bezdrátové sítě. Poslední jmenované je asi nejpoužívanější řešení ve většině domácností, především z důvodu jednoduché instalace bez nutnosti rozvádět kabelovou síť.

Použití pouze metalické sítě dnes již ve většině případů není vzhledem k počtu mobilních zařízení možné. Nejlepší je kombinace páteřní metalické sítě a bezdrátové sítě Wi-Fi. Metalickou síť lze vybudovat pomocí kroucené dvojlinky standardu Ethernet nebo využít stávající silnoproudý rozvod, přes který umožňují data přenášet tzv. PowerLine adaptéry.

4.1.1 PowerLine adaptéry

Jedná se o moderní způsob přenosu dat. Maximální teoretická rychlost přenosu se velice liší model od modelu, pohybuje se od 200 Mbit/s až do 1 Gbit/s. Teoretický dosah takového řešení je udáván max. 300-400 metrů. Pomocí PowerLine je možné přenést data pouze na stejném elektrickém okruhu. Pro přenos mezi patry domu se tak většinou příliš nehodí. Při průchodu přes jističe nebo elektroměr je signál velmi utlumen nebo se dokonce ztrácí. Zároveň nastává problém s rušením přenosu v elektrické síti ostatními připojenými zařízeními (PC, televize, kuchyňské spotřebiče atd.).

Testování rychlosti přenosu

Testování probíhalo se sítí standardu FastEthernet a pro tři možnosti zapojení. **Test č. 1** je zapojení obou PowerLine adaptérů do stejné zásuvky, **test č. 2** v rámci jedné místnosti, **test č. 3** mezi různými místnostmi a nakonec **test č. 4**, kdy byla v cílové místnosti použita jiná zásuvka než u testu č. 3. První dvě zapojení jsou pouze pro potřeby testu, v praxi je jediné přínosné zapojení mezi jednotlivými místnostmi. Test probíhal s připojenými běžnými spotřebiči po celém bytě, tímto jsou zajištěny podmínky reálného provozu. Byl přenášen testovací soubor ve formátu ISO o velikosti 3,7 GB. Dosahované průměrné rychlosti jsou zaznamenány v tabulce č. 1.

Výsledky ukazují, že již v rámci jedné místnosti klesá rychlost o polovinu a mezi různými místnostmi již na pětinu, maximální možné rychlosti této sítě (100 Mbit/s). V závislosti na rychlosti připojení k internetu je možné jeho rozšíření pomocí PowerLine adaptérů, ovšem pro přenos dat plnou rychlostí mezi zařízeními v síti je velice nevhodné. Dosahované rychlosti pomocí PowerLine adaptérů jsou závislé na kvalitě a materiálu elektrického rozvodu, jeho rozvržení do různých okruhů, přítomnosti jističů nebo elektroměru a dalších vlivech. Dále jak ukázal test č. 4 jsou rozdíly i v rámci jedné místnosti s použitím pouze různých zásuvek. Proto není možné vhodnost použití tohoto řešení zobecnit, je nutné buďto znát přesně schéma elektrického obvodu nebo vždy otestovat v konkrétním případě.

	Doba přenosu (sekundy)	**Průměrná rychlost (Mbit/s)**
Test č. 1	361	82
Test č. 2	604	49
Test č. 3	1345	22
Test č. 4	1057	28

Tabulka 1 - Test rychlosti PowerLine adaptérů (autor)

4.1.2 Testování prostupnosti Wi-Fi signálu

Kvalita bezdrátového přenosu pomocí technologie Wi-Fi je narušována různými vlivy. Jedním takovým je rušení od ostatních vysílaných sítí na stejné frekvenci. Dalším je útlum prostředí šíření signálu a také odrazy a pohlcování signálu v různých materiálech, se kterými

se lze setkat v domácnostech. Ve stavbách z určitého materiálu je nutno počítat s většími útlumy, a tudíž vyššími nároky na výkon bezdrátové sítě.

Autor se zabývá testováním útlumu Wi-Fi signálu na frekvenci 2,4 GHz. Metodikou je umístění vysílače 3 metry od zkoumaného materiálu, změření referenční hodnoty signálu 3 metry od vysílače a poté zjištění 5 hodnot signálu ihned za měřeným materiálem a jejich zprůměrování. Tato metodika byla zvolena z důvodu testování v různých podmínkách domácností. Zprůměrování více měřených hodnot je prováděno pro odstranění co největšího množství zkreslení. Testování probíhá na zařízení Nexus 5.

Jsou otestovány nejčastější stavební materiály, se kterými se lze v domácnostech setkat. Výsledné naměřené útlumy jsou zachyceny v tabulce č. 2. Jako nejvhodnější materiál k šíření signálu uvnitř domácnosti je dle testu vyhodnocen pórobeton, naopak jako nejhorší se ukázal železobeton a velmi tlusté nosné cihlové zdi. Vzhledem ke své malé tloušťce je také velice pohlcující sádrokartonová příčka, která vstřebává vlhkost a ta je pro šíření signálu velkým problémem. Pro rozšíření signálu mimo domácnost, například na zahradu je dle testu velkou překážkou bezpečnostní okno s železnou mříží.

Materiál	**Síla (cm)**	**Útlum (dB)**
Cihlová zeď	10	7
	25	12
	66	26
Pórobeton	10	5
Sádrokartonová příčka	10	11
Železobeton	15	17
Bezpečnostní okno s mříží		25

Tabulka 2 - Útlumy materiálů (autor)

Pro zjištění útlumu prostředí šíření (vzduch) v decibelech na určitou vzdálenost, lze využít výpočet:

$$FSPL\ (dB) = 20\log_{10} d + 20\log_{10} f - 147{,}55$$

d = vzdálenost od vysílače (m) a f = frekvence vysílání (Hz)

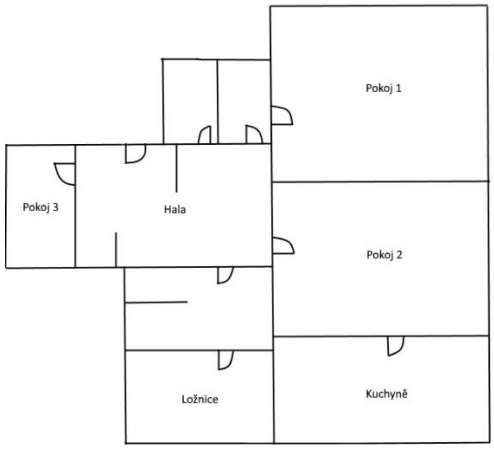
Výpočtem pro vzdálenost 3 metry a frekvenční pásmo 2,4 GHz dostaneme útlum 50 dB. Testováním byl naměřen útlum průměrně 53 dB. Lze tedy říci, že v praxi se útlum velmi blíží teoreticky vypočtené hodnotě a je možno s výpočtem pracovat při návrhu bezdrátové sítě ve volném prostoru.

Vysoký útlum jednotlivých prostředí by bylo teoreticky možné kompenzovat například vyšším výkonem vysílače. V praxi toto bohužel možné není, z důvodu regulace maximálního vysílaného výkonu zařízení v pásmech 2,4 GHz až 66 GHz, ze strany Českého telekomunikačního úřadu. Tento maximální vyzářený výkon je roven 100 mW. Po přepočtu na decibely se rovná 20 dBm. (ČTÚ, 2010)

Pomocí výše uvedených hodnot lze vypočítat přibližný útlum Wi-Fi signálu pro tvorbu sítě. Pro příklad je uveden výpočet pro průchod signálu přes dvě zdi a jednu místnost. Jedna zeď je z železobetonového panelu o tloušťce 15 cm, druhá cihlová o tloušťce 25 cm a místnost mezi stěnami o šířce 4 metry. Budeme uvažovat maximální možný vyzářený výkon na frekvenci 2,4 GHz, čehož jsou i domácí routery schopny dosáhnout a umístění vysílače 3 metry od jedné ze stěn. Vyzářený výkon je tedy 20 dBm, útlum vzduchu dle výše uvedeného vzorce je pro celkovou vzdálenost 7 metrů 57 dB a útlumy stěn budeme uvažovat, dle provedeného měření 17 a 12 dB. Poté stačí od vyzářeného výkonu odečíst uvedené útlumy a vyjde nám síla signálu ihned za zdí. V tomto případě: $20 - 57 - 17 - 12 = -66$ dBm. Pro plnou rychlost bezdrátového připojení je považováno za hraniční přibližně -60 dBm, v tomto případě tedy teoreticky nebude spojení probíhat maximální možnou rychlostí. Celý výpočet je však pouze přibližný, nezahrnuje různé odrazy vln a rušení od okolních sítí a zařízení.

4.2 Návrh sítě v konkrétním případě

Byt tvoří celkem 7 místností. U vchodu se nachází hala a s ní sousedící menší místnost, která je využívána jako pracovna. Vedle haly leží koupelna a za ní ložnice. Na druhé straně se nachází dva pokoje, z toho jeden obývací a na konci bytu leží kuchyně. Celý byt je situován ve staré zástavbě tvořené cihlovými domy. Tento materiál je dle poznatků získaných z měření útlumu oproti modernějším stavbám z betonových panelů s železnými výztuhami vhodnější pro šíření bezdrátových sítí. Mezi pokojem č. 3 a halou je pouze příčka, stejně tak mezi koupelnou a ložnicí. Kuchyně od pokoje č. 2 je taktéž oddělena příčkou, všechny ostatní zdi jsou nosné. Na obrázku č. 13 je nákres bytu, ve kterém bude síť realizována.



Obrázek 13 - Nákres bytu (autor)

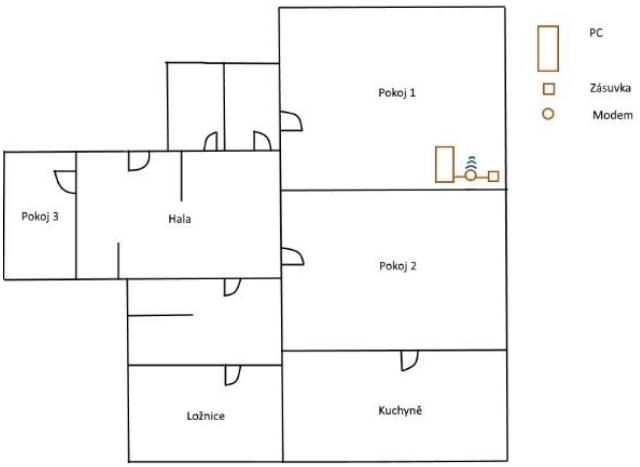
4.2.1 Analýza technologií

V této kapitole se autor zabývá analýzami jednotlivých možností pro vybudování této domácí počítačové sítě. Dle výsledků je poté navržena architektura sítě v daném případě.

Rozbor a otestování stávající sítě

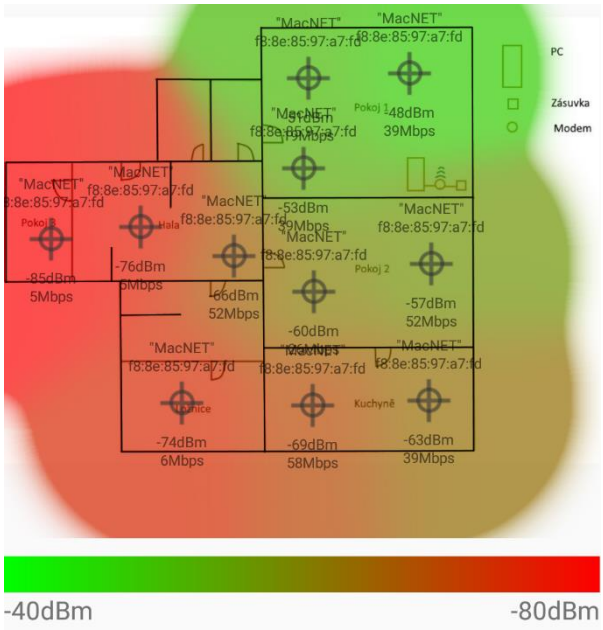
Stávající počítačová síť je tvořena pouze v pokoji č. 1. Nachází se zde internetová zásuvka a Wi-Fi modem od poskytovatele internetu a jeden stolní počítač, který je připojen pomocí kabelu přímo k modemu. Rychlost připojení k internetu od poskytovatele je pro stahování 40 Mbit/s a pro nahrávání 5 Mbit/s. Tuto síť bylo potřeba rozšířit až do pokoje č. 3 a na

druhou stranu přes pokoj č. 2 do kuchyně. Mezi pokojem č. 1 a halou se nachází přibližně 60 cm široká nosná zeď. Na základě předchozích měření útlumů lze předpokládat velmi slabý signál bezdrátové sítě v hale, případně v pokoji č. 3.



Obrázek 14 - Stávající síť (autor)

Stávající modem Comtrend VR-3026e v2 od poskytovatele připojení se autor rozhodl zachovat díky jeho dostatečné výbavě a vysoké ceně pořízení nového modemu. K otestování bezdrátové sítě byly použity dvě aplikace na mobilní telefon se systémem Android a to *„Wifi Analyzer“ a „Wi-Fi Visualizer“*. Byly vybrány na základě kladných hodnocení a dobré zkušenosti autora s těmito aplikacemi. Po otestování dosahu stávající Wi-Fi sítě byla vytvořena tzv. heatmapa pokrytí. Jedná se sice o metodu pouze orientační, ale dle autora naprosto dostačující pro reálné mapování pokrytí bytu Wi-Fi signálem. Při testování byly zavřeny všechny dveře nacházející se v bytě, tímto byly vytvořeny nejhorší možné podmínky, které mohou v daném místě nastat. Dále byl při měření omezen pohyb osob, a to z důvodu



Obrázek 15 - Síla Wi-Fi signálu na stávající síti (autor)

zkreslení měření. Podle této mapy lze lehce určit rozmístění dalších prvků. Bylo zjištěno, že v pokoji č. 3 je signál tak slabý, že občas vypadává připojení k síti, v ložnici je připojení stabilnější, ale signál je velmi slabý a přenosové rychlosti dosahují zlomku požadované rychlosti. Je tedy nutné instalovat druhý přístupový bod Wi-Fi.

Analýza technologií

Vzhledem ke konstrukci bytu a výsledku testování stávající sítě autor vybral jako vhodné místo k umístění sekundárního Wi-Fi routeru halu. Tímto bude poskytnuto dobré pokrytí pracovny (pokoj č. 3) a zvýšení síly signálu v ložnici. Dle nabytých teoretických poznatků se autor rozhodl síť zkonstruovat jak pomocí bezdrátových technologií, tak i metalickou kabeláží. Pro tuto bude využita kroucená dvojlinka kategorie 5e, a to především díky přijatelné ceně a budoucí možnosti vylepšení sítě pomocí výměny starších aktivních prvků za prvky podporující standard Gigabitového Ethernetu, bez nutnosti výměny kabeláže.

Pro zavedení metalické sítě bylo otestováno moderní řešení rozvodu dat pomocí PowerLine adaptérů, které přenášejí data silnoproudým rozvodem v bytě. K tomuto kroku autora vedla především možnost zjednodušení celé sítě, bez nutnosti rozvádění strukturované kabeláže přes celý byt a možnost použití pouze krátkých kabelů v rámci jednotlivých místností.

K tomuto testu jsou využity PowerLine adaptéry renomované firmy TP-LINK model TL-PA2010. Nejdříve proběhl referenční test pomocí přímého zapojení dvou PC do modemu Comtrend VR-3026e v2 a přenosu testovacího souboru ve formátu ISO o velikosti 3,7 GB mezi těmito dvěma počítači. Tento test zaručil schopnost daného modemu dosahovat maximální udávané rychlosti standardu Fast Ethernet. Po připojení adaptéru k modemu v pokoji č. 1 a spárování s druhým adaptérem v hale byl proveden test přenosové rychlosti se stejným souborem. Bylo zjištěno, že přenosová rychlost dosahuje v průměru maximálně 20 Mbit/s. Jedná se o polovinu rychlosti připojení k internetu v daném bytě a o pětinu maximální možné rychlosti přenosu dat po této síti.

S ohledem na možnost budoucí investice a vylepšení sítě na standard Gigabitového ethernetu, je po zhodnocení testu možnost rozvodu sítě pomocí PowerLine adaptéru zavrhnuta. Síť tedy bude realizována pouze pomocí kroucené dvojlinky kategorie 5e a bezdrátové sítě Wi-Fi.

S těmito poznatky autor přistoupil k výběr vhodného Wi-Fi routeru k posílení signálu bezdrátové sítě. Hlavními požadavky pro jeho výběr byla díky přijatelné ceně a připravenosti pro budoucí vylepšení podpora standardu Gigabitového Ethernetu. A možnost připojení USB zařízení, a to z důvodu použití sdílené tiskárny nebo úložiště dat. Dalším omezením byla cena, která činí maximálně 2000 Kč. S těmito parametry vybral autor do užšího výběru 4 zařízení. Jedná se o 3 zařízení firmy TP-LINK, konkrétně modely Archer C1200, Archer C2 AC750 a TL-WR1043ND. Posledním routerem je Edimax BR-6478AC V2.

Výběr je proveden pomocí vícekriteriální analýzy variant, kde autor zvolil pro něj podstatná kritéria a to cenu, rychlost Wi-Fi a výbavu routeru.

	Cena	**Rychlost Wi-Fi**	**Výbava (body)**
TP-LINK Archer C1200 Dual Band	1800 Kč	1200 Mbit/s	3
TP-LINK Archer C2 AC750 Dual Band	1400 Kč	750 Mbit/s	3
TP-LINK TL-WR1043ND	1300 Kč	450 Mbit/s	1
Edimax BR-6478AC V2	1500 Kč	1200 Mbit/s	2

Tabulka 3 - Parametry Wi-Fi routerů (autor)

Výsledek analýzy je získán pomocí metody bodovací s vahami. Jednotlivé parametry jsou obodovány pomocí stupnice 1-4 body, kde více bodů značí lepší parametr. Nejlepší zařízení má nejvyšší celkový součet bodů, vynásobených vahami kritérií. Analýza určila jako nejvhodnější router TP-LINK Archer C2 AC750 Dual Band.

Váhy kritérií	0,5	0,3	0,2	
	Cena	**Rychlost Wi-Fi**	**Výbava**	**Celkem**
TP-LINK Archer C1200 Dual Band	1	4	3	2,3
TP-LINK Archer C2 AC750 Dual Band	3	2	3	**2,7**
TP-LINK TL-WR1043ND	4	1	1	2,5
Edimax BR-6478AC V2	2	4	2	2,6

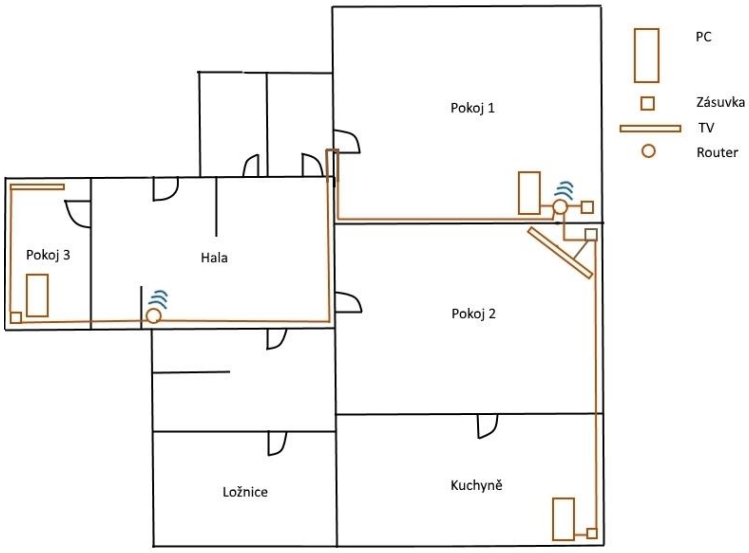
Tabulka 4 - Výběr Wi-Fi routeru (autor)

Návrh sítě

Pomocí těchto vybraných zařízení je navržen rozvod metalické sítě. Primárním prvkem celé sítě je modem umístěný v pokoji č. 1, který slouží zároveň jako přístupový bod do internetu. Tento modem je připojen do internetu pomocí VDSL splitteru[11] přes telefonní přípojku. Dále v jednom LAN konektoru je připojen stolní počítač, v dalším spoj ke druhému routeru, a poslední dva LAN konektory jsou obsazeny kabely vedoucími do pokoje č. 2 a do kuchyně. Vedení strukturované kabeláže se autor rozhodl řešit především pomocí stávajících okrasných podlahových lišt, které jsou však uzpůsobené i pro vedení kabeláže. Tímto jsou ušetřeny finance a není třeba provádět větší stavební úpravy. Mezi pokojem č. 1 a halou je kabeláž vedena v malých lištách posuvnými dveřmi, které toto umožňují. Jediné drobné stavební úpravy, které je nutné provést, jsou otvory ve zdech pro průchod kabeláže mezi halou a pokojem č. 3 a pokoji č. 1, 2 a kuchyní. Do těchto otvorů budou instalovány

[11] VDSL splitter – zařízení umožňující vzájemné využívání pevné telefonní linky a připojení k internetu.

průchodky, tzv. „husí krky“ a to pro usnadnění případné nutné výměny kabeláže. Návrh sítě je zakreslen na obrázku č. 16.



Obrázek 16 - Návrh sítě (autor)

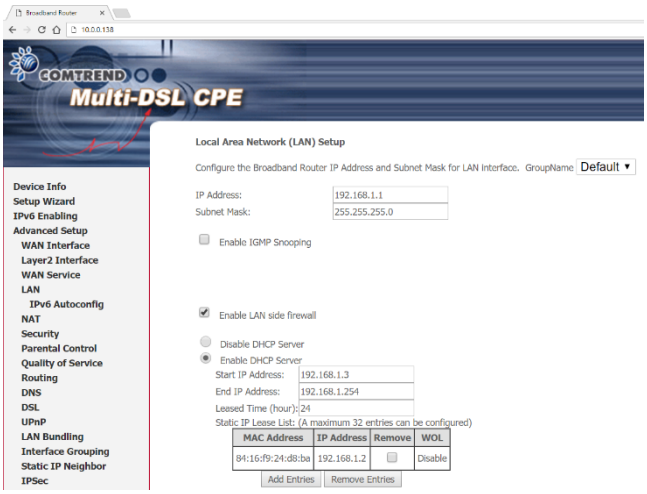
4.2.2 **Zapojení a nastavení sítě**

Podle návrhu je třeba celou síť nejdříve nakonfigurovat. Postupně bude nakonfigurován Wi-Fi modem Comtrend VR-3026e v2 a poté také výše vybraný sekundární směrovač TP-LINK Archer C2 AC750 Dual Band.

Konfigurace primárního modemu

Jako první je provedeno nastavení hlavního aktivního prvku celé sítě, modemu Comtrend VR-3026e v2, který celou síť připojuje do internetu. K tomuto je využito přímé připojení PC do LAN konektoru modemu. Do webového rozhraní konfigurace routeru se přistupuje přes výchozí IP adresu 10.0.0.138, která je daná výrobcem modemu. Po zadání výchozích přihlašovacích údajů admin/admin, můžeme přistoupit ke konfiguraci.

Jako první a nejdůležitější věc, na kterou mnoho lidí zapomíná je zabezpečit modem před neoprávněným vstupem do konfigurace. Jedná se o nejzákladnější prvek zabezpečení sítě. Toto provedeme v záložce *Management → Access control,* kde zvolíme dostatečně silné heslo. Poté je důležité zkontrolovat aktuálnost firmwaru zařízení. Pro většinu i nových zařízení je vždy dostupný aktuálnější firmware, který podstatně zvyšuje celé zabezpečení sítě. Dále je možné přejít k nastavení celé sítě. Nejdříve nastavíme IP adresu celé naší lokální sítě. Autor vybral pro tuto síť třídu IP adres C, která se využívá pro menší lokální sítě. Celá síť má adresu 192.168.1.0 s maskou sítě 255.255.255.0, to nám dává 254 adres pro zařízení v rámci dané sítě. Pro modem je nastavena první adresa z tohoto rozsahu. Autor se vzhledem k častému připojování různých zařízení do sítě rozhodl namísto statického přidělení IP adres využít dynamické přidělování pomocí serveru DHCP. Rozsah přidělování je nastaven na adresy 192.168.1.3 - 192.168.1.254. Adresu 192.168.1.2 autor vyhradil pro druhý router. Celé nastavení je vidět na obrázku č. 17.

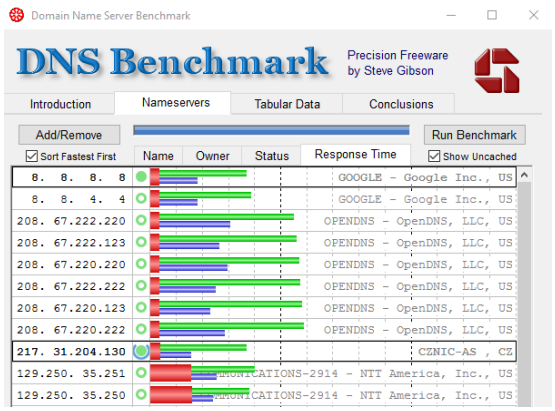


Obrázek 17 - Nastavení DHCP serveru (autor)

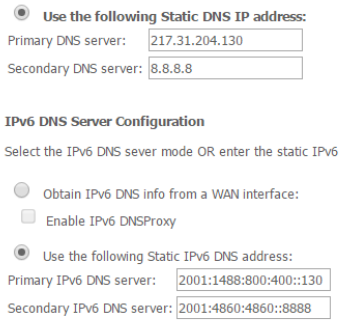
Pro pokračování v konfiguraci je třeba se do konfigurace přihlásit přes nově nastavenou adresu 192.168.1.1. Dále je nastaven WAN port na VDSL připojení, přes tuto technologii je od poskytovatele umožněno připojení k internetu, zároveň je zapnuta podpora nového standardu IPv6. Modem umožňuje připojení jedné nebo dvou IPTV od poskytovatele, toho však v tomto případě není využito, a tak jsou nastaveny všechny 4 LAN porty na poskytování internetu. V neposlední řadě je zapnuta technologie QoS (Quality of Service), která zajišťuje řízení datových toků a dělí přenosovou kapacitu, dle aktuálního vytížení sítě tak, aby nedocházelo k zahlcení.

Vzhledem ke špatné zkušenosti autora s DNS servery poskytovatele byly otestovány různé DNS servery pomocí programu *„Domain Name Server Benchmark“*. Dle těchto výsledků, zobrazených na obrázku č. 18, byly vybrány dva DNS servery. Jeden hlavní od CZ.NIC,

správce domény .cz a druhý záložní od společnosti Google. Dva DNS servery byly vybrány z důvodu zajištění stabilního připojení. V případě využití jenom serverů od CZ.NIC a jejich výpadku by nebyl umožněn přístup k internetu. Proto je jako záložní využit DNS Google. V připojených zařízení poté stačí zapnout v nastavení síťového adaptéru automatické získávání DNS serverů. Nastavení adres DNS, včetně jejich IPv6 verzí je zobrazeno na obrázku č. 19.



Obrázek 18 - Testování DNS serverů (autor)



Obrázek 19 - Nastavení DNS serverů (autor)

Konfigurace bezdrátové sítě

Pro šíření bezdrátového pokrytí bude sloužit jak stávající modem, tak i nově koupený router. V konfiguraci modemu po zapnutí bezdrátové sítě je nastaveno SSID[12] Wi-Fi na „*MacNET*“. Zabezpečení bylo zajištěno pomocí dostatečně silného hesla (14 znaků, kombinace velkých a malých písmen včetně čísel). A zapnutí šifrování pomocí WPA2-PSK AES. Filtrování MAC adres nebylo použito, protože poskytuje pouze malou úroveň zabezpečení, lze snadno naklonovat MAC adresu povoleného zařízení. Toto zabezpečení bylo použito dle nabytých znalostí autora z teoretické části této práce. Jako další možností pro přihlašování do sítě je zde technologie WPS. Jedná se o technologii, která umožňuje jednodušší přihlášení k síti bez nutnosti pamatování si složitého přístupového hesla. Například pomocí 8místného PIN kódu nebo fyzického tlačítka na routeru. Tato technologie je bohužel velmi slabě

[12] SSID – identifikátor bezdrátové sítě Wi-Fi.

zabezpečená a lze ji se 100 % úspěšností prolomit mezi 3-5 hodinami. Díky tomuto bezpečnostnímu riziku autor technologii deaktivoval. (OCCUPYTHEWEB, 2016)

Všechna ostatní nastavení bezdrátové sítě (kanál, šířka pásma atd.) byla prozatím ponechána na výchozích hodnotách. Po konfiguraci celé sítě bude provedeno otestování a podle výsledků budou tato nastavení případně upravena.

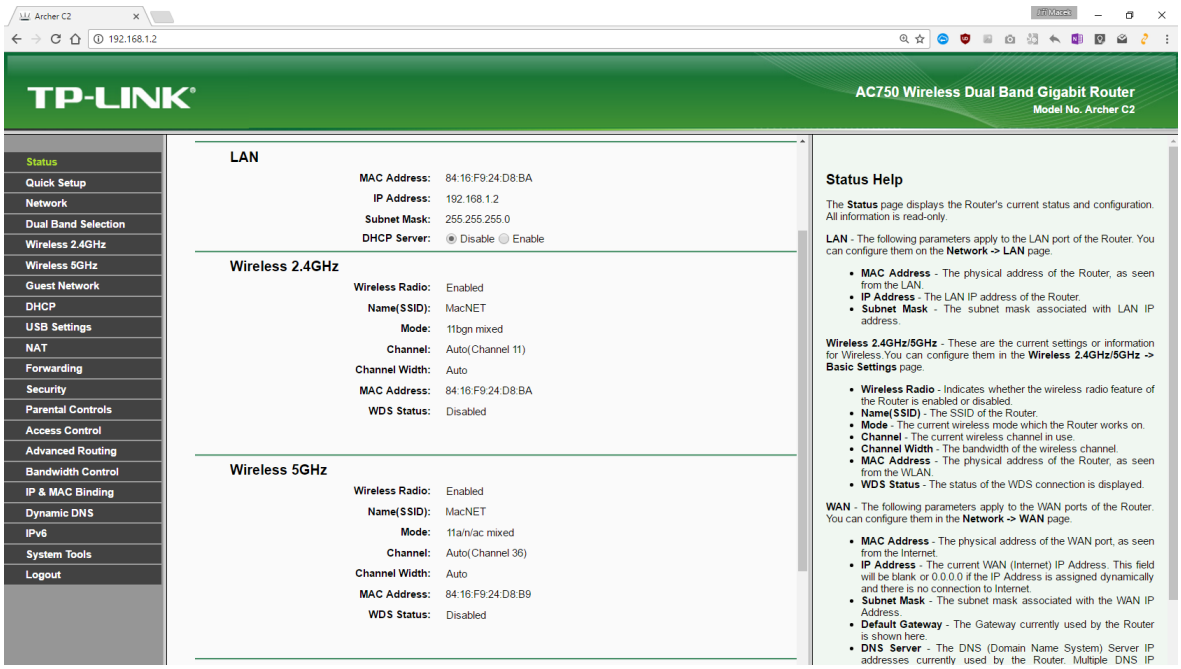
Konfigurace sekundárního routeru

Po zapojení routeru TP-LINK Archer C2 AC750 Dual Band, k již nakonfigurovanému modemu Comtrend VR-3026e v2, můžeme přejít také k jeho konfiguraci. První možností je opět přímé zapojení počítače přes LAN konektor, ale je také možné na tento router přistoupit přes PC zapojeném do hlavního modemu. Toho také autor využil. Router má od výrobce nastavenou výchozí IP adresu 192.168.0.1, přes tuto se dostaneme obdobně jako v prvním případě do konfigurace. První přihlášení je stejné, přihlašovací údaje jsou nastaveny na admin/admin. Jako první opět změníme přihlašovací údaje, tento router podporuje navíc kromě změny hesla i změnu přihlašovacího jména. Bylo však ponecháno beze změny, a to z důvodu zanechání stejných přihlašovacích jmen do obou aktivních prvků v síti. Jak již bylo výše zmíněno, je i u nových zařízení nutné zkontrolovat aktuálnost firmware, i v tomto případě je dostupná bezpečnostní aktualizace. V nastavení LAN je zařízení přidělena adresa 192.168.1.2 s maskou 255.255.255.0. Jedná se o vyhrazenou adresu z DHCP serveru na primárním modemu. Router podporuje připojení USB periférií, byl to hlavní požadavek autora při vícekriteriální analýze na výběr zařízení. Připojena bude především tiskárna, a tak v nastavení USB portu zapneme možnost print serveru. Poté stačí tiskárnu na počítači přidat jako síťovou, nalezneme ji pod IP adresou routeru 192.168.1.2. Po uložení je nutné se znovu přihlásit pomocí nové IP adresy zařízení a nových přihlašovacích údajů.

Dále je potřeba aby router fungoval pouze jako switch, toho je docíleno nastavením IP adresy routeru na adresu 192.168.1.2, která je mimo rozsah přidělovaných adres DHCP serverem, běžícím na hlavním modemu. Poté je deaktivován DHCP server na tomto routeru. Toto nastavení je nutné z důvodu přidělování síťových adres pouze jedním aktivním prvkem v síti. O přidělování IP adres zařízením se tak stará pouze primární modem.

Konfigurace bezdrátové sítě

Router TP-LINK Archer C2 AC750 Dual Band podporuje Wi-Fi standardu 802.11n v pásmu 2,4 GHz a standardu 802.11ac v pásmu 5 GHz. Konfigurace bezdrátové sítě je provedena obdobně jako u hlavního modemu. Jméno sítě neboli SSID je nastaveno na „MacNET“, zabezpečení je také nastaveno se stejnými údaji, se šifrování WPA2-PSK AES a stejným heslem. Autor se rozhodl i na tomto routeru nezapínat filtrování MAC adres a deaktivoval technologii WPS, z důvodu vyšší bezpečnosti. Takto nastavený router umožňuje připojovaným zařízením vidět celou bezdrátovou síť jako celek, a ne jednotlivé přístupové body. Díky tomu je umožněno při průchodu bytem automatické přihlašování připojeních zařízení k přístupovému bodu se silnějším signálem. Ostatní nastavení jsou do finálního otestování sítě prozatím také nechána na výchozích hodnotách. Souhrn nastavení druhého routeru je zobrazen na obrázku č. 20.



Obrázek 20 - Souhrn nastavení sekundárního routeru (autor)

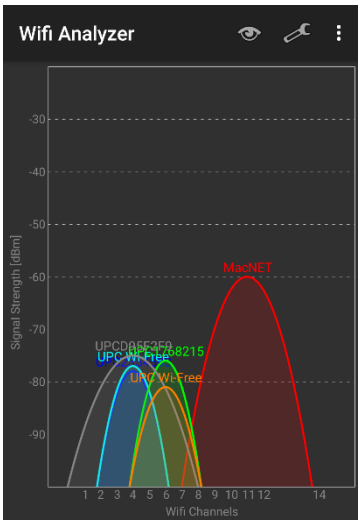
4.2.3 Testování výsledné sítě

Po finální konfiguraci a zapojení celé sítě je třeba tuto síť otestovat. Pro testování dosažitelnosti zařízení a počtu ztracených paketů po cestě je využita metodika pomocí

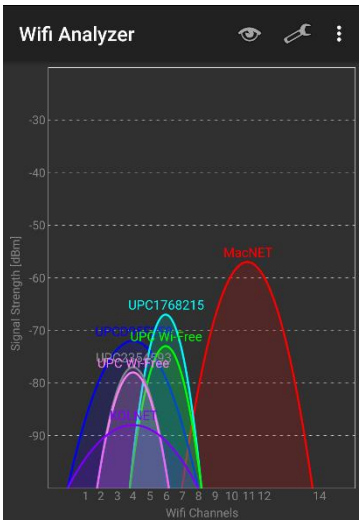
programu ping, kde je stanovena tolerance pro ztrátu paketů 1 % a průměrná odezva max. 150 ms. Tolerance je stanovena na základě doporučených hodnot pro VoIP a streaming zvuku a videa. (Szigeti, 2004) Pro zjištění zahlcenosti jednotlivých kanálů Wi-Fi je využita aplikace *„Wifi Analyzer“*. A pro zmapování pokrytí bytu signálem je vytvořena heatmapa signálu pomocí aplikace *„Wi-Fi Visualizer“*, obě tyto aplikace jsou spuštěny na Android zařízení Nexus 5.

Analýza kanálů Wi-Fi

V konfiguraci routeru zůstalo nastavení kanálů na režim auto, kdy router sám vybírá nejvhodnější kanál. To však dle zkušeností autora většinou nefunguje příliš spolehlivě, a tak je na dvou místech bytu proveden test zahlcenosti kanálů. Test je proveden pomocí aplikace *„Wifi Analyzer“* na zařízení Nexus 5. Je zjištěno, že většina cizích Wi-Fi sítí je provozována na kanálech 2-6. Naše Wi-Fi využívá 40MHz pásmo, a tak je kanál nastaven na poslední možný a to číslo 11. Na tomto kanálu prozatím žádné sítě v okolí nevysílají, a tak je zaručen nerušený signál. Měření kanálu na obou místech je zobrazeno na obrázkách č. 21 a 22.



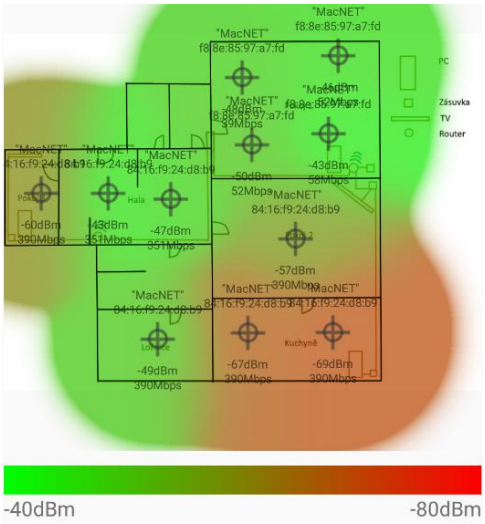
Obrázek 21 - Analýza Wi-Fi kanálů 1 (autor)



Obrázek 22 - Analýza Wi-Fi kanálů 2 (autor)

Heatmapa signálu

Jako další test je vypracována heatmapa pokrytí signálu. Vytvořena je pomocí stejné metody jako při prvotním testování sítě. Při měření jsou také zavřeny veškeré dveře pro zajištění nejhorších možných podmínek, které mohou nastat. Dle výsledků je zřejmé, že se povedlo rozšířit dostatečný signál po celém bytě a je vyřešen problém s vypadávajícím signálem v pokoji č. 3 a slabým signálem v ložnici. Nyní je nejslabší signál v kuchyni, ale stále dostatečně silný pro bezproblémový přenos. Heatmapa signálu nové konstrukce sítě je zobrazena na obrázku č. 23.

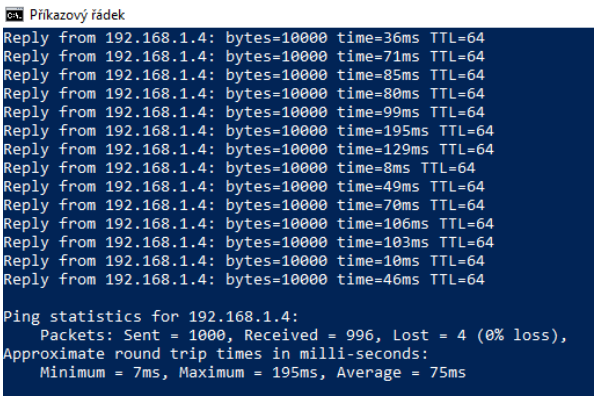


Obrázek 23 - Heatmapa signálu nové sítě (autor)

Testování ztráty paketů

Pomocí programu ping je otestována dostupnost veškerých zařízení v síti, připojených na metalické kabeláži. Toto je testováno pomocí výchozího nastavení programu ping, kde jsou na cílové zařízení odeslány 4 pakety o velikosti 32 B a očekává se jejich návrat. U všech testovaných zařízení je naměřena ztráta paketů 0 %, metalická síť je tedy 100 % spolehlivá.

Jako poslední je proveden test ztráty paketů na bezdrátové síti. Jako místo pro cílové zařízení byla na základě vytvořené heatmapy signálu vybrána kuchyně, a to z důvodu nejslabšího signálu. Jestliže bude v tomto místě ztráta paketů v toleranci, dá se předpokládat, že i kdekoli jinde v bytě bude Wi-Fi spolehlivé. Pomocí programu ping je odesláno 1000 paketů o velikosti 10 kB a je očekáván jejich návrat. Z 1000 odeslaných paketů se 996 vrátilo, což představuje ztrátu 0,4 %, tudíž stanovenou toleranci tato síť splňuje. Zároveň průměrná odezva se rovná 75 ms, která je rovněž v toleranci. Celý výsledek je zobrazen na obrázku č. 24.



Obrázek 24 - Testování pomocí ping (autor)

5 Závěr

Jako hlavním bodem vlastní práce bylo provedeno otestování dostupných technologií pro budování domácí počítačové sítě. Testován je přenos dat přes silnoproudý rozvod v domácnosti pomocí PowerLine adaptérů. Rychlost přenosu je dle výsledků velmi závislá na kvalitě elektrického vedení, jeho rozvržení do různých okruhů a vlivu dalších okolností. Vhodnost tohoto řešení je tak nutno vždy otestovat v konkrétním případě.

Dále jsou testovány útlumy signálu bezdrátové sítě na frekvenci 2,4 GHz v různých stavebních materiálech, se kterými se lze v domácnostech setkat. Zde byly zjištěny velké rozdíly a jakožto nejvhodnější materiál pro šíření signálu je vyhodnocen pórobeton, na druhou stranu nejhorším byl shledán železobeton. Jako velké překvapení se ukázala sádrokartonová příčka, která má vzhledem k malé tloušťce také značný útlum. Nakonec se autor zabývá názornou ukázkou přibližného výpočtu útlumu v určitém případě.

Poté je vypracován návrh konkrétní domácí počítačové sítě, konstruované především s ohledem na nízké finanční náklady. Po otestování dostupných technologií jsou pomocí vícekriteriální analýzy variant, jakožto jedné z metod analýz, vybrána síťová zařízení pro konstrukci sítě. Nakonec je síť pomocí několika metodik otestována. Dle výsledků testů je síť vyhodnocena jako stabilní a signál bezdrátové části sítě dostatečně silný pro pokrytí celé domácnosti.

I přes nízké finanční náklady lze vybudovat silnou domácí síť, která umožňuje rychlé sdílení dat a přístup k internetu kdekoli v domácnosti. Zároveň je celá síť připravena pro budoucí investici a vylepšení na standard Gigabitového Ethernetu. Návrh této sítě včetně metodiky pro výběr zařízení a otestování sítě je možno využít ve většině domácností.

6 Seznam použitých zdrojů

1. BOUŠKA, Petr, 2007. *TCP/IP - model, encapsulace, paket vs. rámec* [online]. In: . [cit. 2017-02-15]. Dostupné z: http://www.samuraj-cz.com/clanek/tcpip-model-encapsulace-paketu-vs-ramec/
2. CISCO, , 2015. 802.11ac: The Fifth Generation of Wi-Fi Technical White Paper. In: *Cisco* [online]. [cit. 2017-02-15]. Dostupné z: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.html
3. CISCO, , 2017. What Is a Network Switch vs. a Router?. In: *Cisco* [online]. [cit. 2017-02-15]. Dostupné z: http://www.cisco.com/c/en/us/solutions/small-business/resource-center/connect-employees-offices/network-switch-what.html
4. ČTÚ, , 2010. Všeobecné oprávnění č. VO-R/12/09.2010-12 k využívání rádiových kmitočtů a k provozování zařízení pro širokopásmový přenos dat v pásmech 2,4 GHz až 66 GHz. In: *Český telekomunikační úřad* [online]. Praha [cit. 2017-02-15]. Dostupné z: https://www.ctu.cz/cs/download/oop/rok_2010/vo-r_12-09_2010-12.pdf
5. DONAHUE, Gary, 2007. *Network warrior*. 1st ed. Sebastopol, CA: O'Reilly Media. ISBN 0596101511.
6. GOOGLE, , 2017. Secure your site with HTTPS. In: *Google console help* [online]. [cit. 2017-02-15]. Dostupné z: https://support.google.com/webmasters/answer/6073543?hl=en
7. HORÁK, Jaroslav a Milan KERŠLÁGER, 2011. *Počítačové sítě pro začínající správce*. 5., aktualiz. vyd. Brno: Computer Press. ISBN 9788025131763.
8. KOSTRHOUN, Aleš, 2001. *Stavíme si malou síť*. Vyd. 1. Praha: Computer Press. Všechny cesty k informacím. ISBN 8072265105.
9. KUROSE, James a Keith ROSS, 2014. *Počítačové sítě*. 1. vyd. Brno: Computer Press. ISBN 9788025138250.
10. MICROSOFT, , 2003. How TCP/IP Works. In: *Microsoft: TechNet* [online]. [cit. 2017-02-15]. Dostupné z: https://technet.microsoft.com/en-us/library/cc786128(v=ws.10).aspx
11. MITCHELL, Bradley, 2016. About 802.11g Wi-Fi for Wireless Computer Networking. In: *Lifewire* [online]. [cit. 2017-02-15]. Dostupné z: https://www.lifewire.com/history-of-wireless-standard-802-11g-816556
12. NIZAM, Ayesha, 2014. *NETWORKING BASICS* [online]. In: . [cit. 2017-02-15]. Dostupné z: http://www.networking-basics.net/mesh-topology/
13. OCCUPYTHEWEB, , 2016. Breaking a WPS PIN to Get the Password with Bully. In: *Wonderhowto: Fresh Hacks For A Changing World* [online]. [cit. 2017-02-15]. Dostupné z: https://null-byte.wonderhowto.com/how-to/hack-wi-fi-breaking-wps-pin-get-password-with-bully-0158819/

14. PETERKA, jiří, 2005a. *Báječný svět počítačových sítí, část II. - Taxonomie, aneb: škatulkování* [online]. In: . [cit. 2016-02-15]. Dostupné z: http://www.earchiv.cz/b05/b0300100.php3
15. PETERKA, Jiří, 2005b. Báječný svět počítačových sítí, část III. - Síťové architektury. In: *EArchiv.cz* [online]. [cit. 2017-02-15]. Dostupné z: http://www.earchiv.cz/b05/b0500001.php3
16. PETERKA, Jiří, 2005c. Báječný svět počítačových sítí, část IV. - Rodina protokolů TCP/IP. In: *EArchiv.cz* [online]. [cit. 2017-02-15]. Dostupné z: http://www.earchiv.cz/b05/b0600001.php3
17. PLEXO, , 2008. Technologie přenosu dat přes optická vlákna. In: *Pctuning.cz* [online]. [cit. 2017-02-15]. Dostupné z: http://pctuning.tyden.cz/hardware/site-a-internet/9994-technologie_prenosu_dat_pres_opticka_vlakna
18. SCARPATI, Jessica, 2017. Wireless security protocols: The difference between WEP, WPA, WPA2. In: *TechTarget* [online]. [cit. 2017-02-15]. Dostupné z: http://searchnetworking.techtarget.com/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2
19. SOLARIX, , 2016. 10GBASE-T a strukturovaná kabeláž. In: *Solarix* [online]. [cit. 2017-02-15]. Dostupné z: http://www.solarix.cz/info.jsp?name=10gbaset
20. SOSINSKY, Barrie, 2010. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Vyd. 1. Brno: Computer Press. ISBN 9788025133637.
21. SPURNÁ, Ivona, 2010. *Počítačové sítě: praktická příručka správce sítě*. Vyd. 1. Kralice na Hané: Computer Media. ISBN 9788074020360.
22. SZIGETI, Tim a Christina HATTINGH, 2004. Quality of Service Design Overview. In: *Cisco* [online]. [cit. 2017-02-15]. Dostupné z: http://www.ciscopress.com/articles/article.asp?p=357102

7 Zdroje obrázků

[Obr. 1–6] Introduction to Network Topology: The NEST of Knowledge, 2015. In: *Xathrya.ID: The NEST of Knowledge* [online]. [cit. 2017-02-15]. Dostupné z: https://xathrya.id/2015/12/11/introduction-to-network-topology/

[Obr. 7] PETERKA, Jiří, 1997. Sága rodů LAN a WAN. In: *EArchiv.cz* [online]. [cit. 2017-02-15]. Dostupné z: http://www.earchiv.cz/a708s600/a708s671.php3

[Obr. 8] PETERKA, Jiří, 1999. Rodina protokolů TCP/IP. In: *EArchiv.cz* [online]. [cit. 2017-02-15]. Dostupné z: http://www.earchiv.cz/anovinky/ai1592.php3

[Obr. 9] MARCELO, Barros, 2009. Network programming for PyS60 (XI). In: *HOME TO PYS60 DEVELOPERS* [online]. [cit. 2017-02-15]. Dostupné z: http://croozeus.com/blogs/?p=1075

[Obr. 10] MAGNET ACADEMY, 2014. Coaxial Cable – 1929. In: *Magnet academy* [online]. [cit. 2017-02-15]. Dostupné z: https://nationalmaglab.org/education/magnet-academy/history-of-electricity-magnetism/museum/coaxial-cable

[Obr. 11] TEKTEL, 2014. UTP vs. FTP cable. In: *Tektel communications* [online]. [cit. 2017-02-15]. Dostupné z: http://www.tektel.com/b1/faq/ethernet-cable-faqs/utp-vs-stp-cable-image/

[Obr. 12] IGS COMPUTERS, 2015. How to Choose The Right Wi-Fi Channel and Avoid Interference. In: *IGS Computers* [online]. [cit. 2017-02-15]. Dostupné z: https://igscomputers.co.uk/how-to-choose-the-right-wi-fi-channel-and-avoid-interference/