Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Návrh domácí počítačové sítě

Václav Kykal

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Václav Kykal

Informatika

Název práce

Návrh domácí počítačové sítě

Název anglicky

Design of Home Computer Network

Cíle práce

Cílem práce je vytvořit rešerši o současných domácích počítačových sítích, jejich typech a topologiích, popsat výhody, nevýhody a možnosti zabezpečení. Praktická část práce se bude zabývat vlastním návrhem konkrétní domácí počítačové sítě včetně jejího připojení k internetu a vhodného zabezpečení.

Metodika

1. Vytvořte rešerši současných teoretických poznatků na základě studia odborné literatury
2. Zanalyzujte typy a topologie sítí, výhody a nevýhody a možnosti zabezpečení
3. Na základě získaných znalostí navrhněte vlastní domácí počítačovou síť a její vhodné zabezpečení

Doporučený rozsah práce

30-40 stran

Klíčová slova

počítačová síť, počítač, internet, notebook, Wi-Fi, smartphone, router, UTP kabel, bezpečnost sítě

Doporučené zdroje informací

BARKEN, Lee. Wi-Fi: jak zabezpečit bezdrátovou síť. Vyd. 1. Brno: Computer Press, 2004, 174 s. ISBN 80-251-0346-3.

HORÁK, Jaroslav. Vytváříme domácí bezdrátovou síť. Vyd. 1. Brno: Computer Press, 2011, 293 s. ISBN 978-80-251-2977-7.

HORÁK, J. – KERŠLÁGER, M. *Počítačové sítě pro začínající správce*. Brno: Computer Press, 2003. ISBN 80-7226-876-7.

Předběžný termín obhajoby

2016/17 ZS – PEF (únor 2017)

Vedoucí práce

Ing. David Buchtela, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 20. 2. 2016

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 20. 2. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 22. 01. 2017

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Návrh domácí počítačové sítě" 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. Davidovi Buchtelovi, Ph.D. za vedení mé práce.

Návrh domácí počítačové sítě

Souhrn

Tato bakalářská práce se zabývá návrhem domácí počítačové sítě. První část práce se zabývá studiem lokálních počítačových sítí. Zabývá se historií těchto sítí, typy topologií a referenčními modely OSI a TCP/IP. Jsou zde zmíněny aktivní a pasivní hardwarové prvky sítí, síťový software a jednotlivé standardy pro síťovou komunikaci. Dále práce pojednává o možnostech zabezpečení lokálních sítí.

Praktická část práce se zabývá tvorbou návrhu konkrétní počítačové sítě. Tato síť musí splňovat požadavky klienta, pro kterého je síť vytvořena. V návrhu je obsažena lokalizace prostoru, pro který je síť vytvořena, seznam potřebného hardwaru pro realizaci sítě a hardwaru, který se do sítě bude připojovat. Jako hlavní část práce je zde vytvořeno schéma vedení kabelů a umístění ostatních síťových prvků. Dále je v práci navrženo vhodné zabezpečení této sítě pomocí nastavení routerů a zapojení domácího síťového úložiště.

Klíčová slova: počítačová síť, počítač, internet, notebook, Wi-Fi, smartphone, router, UTP kabel, bezpečnost sítě

Design of Home Computer Network

Summary

This thesis describes the design of a home computer network. The first part deals with the study of local computer networks and their history. This part concerns network types and topologies and the reference models OSI and TCP/IP. Types of active and passive network hardware components are mentioned, as well as networking software and individual network standards for network communication. Furthermore, the thesis also discusses some possibilities of effective security of computer network.

The second part deals with creating the design of home computer network. The network must meet the client's requirements. The description of space, for which is the network created, forms a part of design. There is also the list of required hardware for network implementation and hardware that will be connected to the network. As the main part of this work, the schema of the cable placement and the placement of other active network components is designed. The work also describes appropriate security of this home computer network using setting of the routers and the network storage connection.

Keywords: computer network, computer, internet, notebook, Wi-Fi, smartphone, router, UTP cable, security of computer network

Obsah

1 Úvod

V dnešní době je počítač součástí téměř každé domácnosti. Již dávno je pryč doba, kdy to byl pouze jeden stolní počítač, využívaný spíše jako psací stroj, či přehrávač videí a hudby. I přesto, že si pod pojmem počítač většina lidí představí právě zmíněný stolní PC, jedná se dnes o mnohem širší pojem. Všichni nosíme svůj vlastní počítač v kapse v podobě smartphonu, vlastníme soukromý či služební notebook, na zdech obýváků nám visí počítače ve formě chytrých televizí. Počítače jsou dnes ale samozřejmě i v chytrých autech, nositelné elektronice a elektrospotřebičích.

Abychom však naplno využili potenciál všech těchto zařízení, musíme je přimět k tomu, aby komunikovala mezi sebou. K potřebnému propojení slouží počítačové sítě. V rámci jedné domácnosti či instituce se jedná o lokální sítě. Tyto sítě mohou být realizovány pomocí kabelových rozvodů nebo bezdrátově. Nejčastěji je to však kombinace obou dvou možností.

Lokální sítě však umožňují pouze komunikaci mezi přístroji v této síti. Pro komunikaci mimo lokální síť je potřeba propojení s celosvětovou sítí, zvanou internet. Internet pak propojuje jednotlivé lokální počítačové sítě v jednu, díky které spolu mohou zařízení komunikovat napříč celým světem.

První, teoretická, část této práce se zabývá studiem a rozborem lokálních sítí, jejich historií a vývojem, dále jednotlivými typy topologií, komunikačními protokoly a možnostmi zabezpečení.

Na základě těchto nastudovaných teoretických znalostí je zpracována druhá, praktická část, která se zabývá návrhem konkrétní domácí počítačové sítě.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem této práce je vytvořit konkrétní návrh domácí počítačové sítě. Tento návrh bere v potaz požadavky zadavatele a bude sloužit jako finální podklad pro její budoucí realizaci v reálném prostředí.

Mezi vedlejší cíle této práce patří vytvoření rešerše o současných počítačových sítích, jejich typech a topologiích a jejich konkrétních výhodách a nevýhodách. Dále je zaměřena na možnosti zabezpečení těchto sítí.

2.2 Metodika

Na základě nastudované odborné literatury se zpracuje teoretická část práce. Jako první se zaměří na rešerši současných počítačových sítí. Zabývat se bude jednotlivými typy a topologiemi sítí, jejich konkrétními výhodami a nevýhodami. Zmíněny budou jednotlivé komunikační protokoly, síťové standardy a referenční modely.

Další část teoretické práce se bude zabývat síťovým hardwarem, aktivními i pasivními prvky, používanými pro tvorbu domácích počítačových sítí. Dále bude zmíněn síťový software a možnosti zabezpečení lokálních sítí.

Na základě teoretické části práce bude zpracována část praktická. Ta se bude zabývat postupně od prvotního výběru hardwarových komponent, přes výběr vhodných tras strukturované kabeláže, připojení sítě k internetu, až po její zabezpečení.

3 Teoretická východiska

3.1 Historie počítačových sítí a internetu

Historie internetu a počítačových sítí začíná již na počátku šedesátých let minulého století. Tehdejší nejrozsáhlejší sítí byla telefonní síť. Ta pro vzájemný přenos informací využívala technologii přepínání okruhů, díky které bylo možné přenášet hlas konstantní rychlostí. V souvislosti s vývojem počítačů nastala potřeba jejich vzájemného propojení, a to kvůli sdílení informací mezi vzdálenými stanicemi. Technologie přepínání okruhů však pro nárazovou komunikaci počítačů nebyla vhodná.

Jako alternativa k přepínání okruhů byl zahájen vývoj technologie přepínání paketů. Začátkem roku 1969 byl organizací Advanced Research Project Agency (ARPA) instalován první přepínač paketů a během tohoto roku pak další tři. Tato síť byla nazvána ARPANET a během následujících tří let čítala až 15 uzlů. Pro koncové systémy byl vyvinut první protokol, pojmenovaný network-control protocol (NCP), který umožnil psát první aplikace. V roce 1972 byl napsán první e-mailový program.

Nezávisle na sobě však vznikalo více takto uzavřených počítačových sítí. Na jejich vývoji pracovaly mimo jiné firmy jako IBM, dále vznikaly sítě jako ALOHANET, Telenet, Cyclades a další. S rostoucím počtem těchto sítí přišla vize propojení těchto sítí dohromady a vytvoření jednotné architektury a společných protokolů.

Organizace Defense Advanced Research Projects Agency (DARPA) vytvořila návrh na propojení těchto sítí a poprvé použila pro název této práce výraz internetting. Zásady vycházející z této práce byly začleněny do rodiny protokolů TCP. Během vývoje došlo k oddělení protokolu IP od TCP a k rozvoji protokolu UDP. Koncem sedmdesátých let byly tyto tři internetové protokoly koncepčně hotové.

Ve stejné době byla na Havaji vyvíjena paketová rádiová síť zvaná ALOHANET. Tato síť umožňovala komunikaci vzdáleným lokalitám na Havajských ostrovech. Protokol ALOHA byl první protokol, který umožňoval sdílet jednu rádiovou frekvenci pro přístup několika uživatelů a položil základy pro dnešní bezdrátové sítě. V návaznosti na tento vícepřístupový protokol byl vyvinut protokol Ethernet pro kabelové sítě, kvůli potřebě propojení více počítačů, sdílených tiskáren a disků. Tím vznikl základ pro dnešní sítě LAN.

V osmdesátých letech se počet zařízení připojených k internetu dostal na hranici 100 000 počítačů. To bylo způsobeno hlavně vývojem sítí, které spojovaly jednotlivé

univerzity a vývojem sítě NSFNET, která poskytovala přístup k superpočítačovým centrům. Roku 1983 byl nasazen TCP/IP jako nová norma protokolu pro ARPANET a vyvinut byl dnes známý systém DNS pro párování IP adres s jejich textovými názvy.

Souběžně s ARPANETem byl vyvíjen francouzský systém Minitel, který se skládal z veřejné paketové sítě, serverů a přístupových terminálů. Francouzská vláda rozdávala terminály Minitelu zdarma všem, kdo projevili zájem. V polovině devadesátých let Minitel nabízel přes 20 000 služeb a byl velice rozšířený.

V devadesátých letech proběhl obrovský internetový rozmach. ARPANET přestal existovat, velkou událostí byl vznik aplikace World Wide Web, a vývoj čtyř hlavních složek webu, a to jazyku HTML, protokolu HTTP, webového serveru a prohlížeče. Díky tomu mohly mít přístup k internetu miliony domácností. Touto dobou začal i vývoj prohlížečů s grafickým rozhraním (GUI) a vznikl známý Internet Explorer od Microsoftu, kterým byl vytlačen tehdejší nejpoužívanější prohlížeč Netscape.

V druhé polovině devadesátých let už vypadal internet tak, jak ho známe dnes. Služby jako například e-mail včetně příloh, procházení webu, internetové obchodování, chatování a sdílení souborů přes peer-to-peer sítě, již byly běžně dostupné. Celosvětová síť internet se stala terčem podnikání, vývoje a neustálého zlepšování služeb.

(Kurose, Ross, 2014)

3.2 Dělení sítí podle rozlehlosti

Sítě se dají dělit podle mnoha kritérií, jedno z hlavních je dělení podle rozlehlosti. Dle tohoto kritéria dělíme sítě do třech skupin, jsou to sítě WAN, MAN a LAN.

WAN (Wide area network)

Propojením jednotlivých menších sítí dohromady vznikne rozlehlá síť WAN. Může to být síť jednoho většího města. Dále mezi tyto sítě můžeme zařadit síť firmy, která má pobočky v různých městech nebo kontinentech. Nejznámější a nejrozlehlejší síť, která patří do sítí WAN, je internet.

LAN (Local area network)

Do této kategorie spadají malé sítě. Patří sem sítě v jednotlivých domácnostech, bytech či domech, ale i sítě menších firem. Jsou však omezené na jedno lokální místo. Jejich hlavním cílem je propojení zařízení za účelem sdílení tiskáren, dat nebo aplikací. Tato práce se zabývá zejména těmito lokálními sítěmi.

MAN (Metropolitan area network)

Městská síť je rozlehlejší než LAN, ale menší než WAN. V praxi je však těžké nastavit hranici, kde přesně končí síť WAN a začíná MAN, a tak se tyto pojmy často prolínají, udává se však hranice okolo 75 km.

3.3 Topologie sítí

Způsob propojení jednotlivých aktivních síťových prvků a zařízení nazýváme fyzická topologie sítě. Síť můžeme popisovat i z hlediska logické topologie. Ta zobrazuje trasu, kterou urazí jednotlivé pakety od jednoho zařízení k druhému. Následující kapitola se zaměřuje na fyzickou topologii, která ukazuje fyzickou stavbu sítě neboli způsob, jakým jsou mezi sebou jednotlivé prvky propojeny.

Sběrnicová topologie

V této topologii jsou jednotlivá zařízení propojena průběžným vedením. Druhé zařízení je připojeno za prvním, třetí za druhým až k poslednímu zařízení, a to pomocí odbočovacích pasivních prvků. Propojení se nejčastěji realizuje koaxiálním kabelem.

Výhody: Největší výhodou je malá spotřeba kabelu, jelikož ten vede od zařízení k zařízení.

Nevýhody: V této topologii však převažují nevýhody. Velký počet spojů v kabelu zapříčiňuje velkou poruchovost. S tím souvisí další nevýhoda. V případě, že dojde k poruše, je velmi obtížné lokalizovat její výskyt. Nastane-li totiž porucha, dojde k havárii celé sítě.

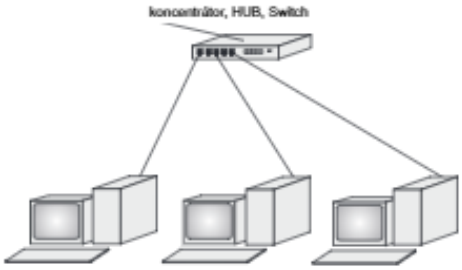
Obrázek 1: Sběrnicová topologie

Hvězdicová topologie

Pro realizaci této topologie je potřeba centrální rozbočovací aktivní prvek, například switch nebo router. K tomuto prvku je pak každé zařízení připojené vlastním kabelem, nejčastěji se zde používá kroucená dvojlinka. V praxi se však často jednotlivé topologie propojují dohromady, vzniká tak topologie hybridní. Hvězda je dnes nejpoužívanějším způsobem propojení více zařízení.

Výhody: Výhodou je malá pravděpodobnost chyby, zároveň pokud se poruší kabel, přístup k síti ztratí pouze jedno zařízení, ostatní mohou nadále bez omezení pracovat. Lokalizace poruchy je tedy také mnohem jednodušší.

Nevýhody: Nevýhodou této topologie je větší spotřeba kabelu a potřeba centrálního aktivního prvku. S tím souvisí větší finanční náklady na realizaci takovéto sítě.



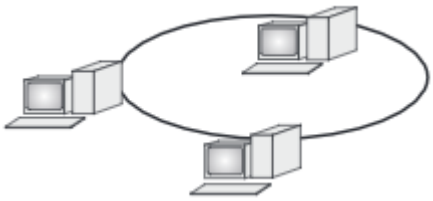
Obrázek 2: Hvězdicová topologie

Kruhová topologie

Stejně jako u sběrnicové topologie je u topologie kruhové použito průběžné vedení. V tomto případě však vedení utváří souvislý kruh. V tomto kruhu koluje token. Token je speciální paket, který se postupně pohybuje od stanice ke stanici. Zařízení, u kterého se zrovna token zastaví, má povoleno vysílat a přijímat data v síti. Tím je vyřešen možný vznik kolizí při přenosu dat.

Výhody: Výhodou je podobně jako u sběrnice menší spotřeba kabelu. Zároveň je síť velmi odolná proti zahlcení i při velkém zatížení. Díky tokenu se totiž zařízení vzájemně neruší a každé z nich dostává přístup v pravidelném intervalu.

Nevýhody: Při přerušení kabelu havaruje celá síť, to je možno řešit zdvojováním kabelu, avšak tím se vytěsňuje výhoda nízké nákladovosti. Další nevýhoda spočívá v nižší rychlosti sítě, část její činnosti je totiž zaplněna obíhajícím tokenem.



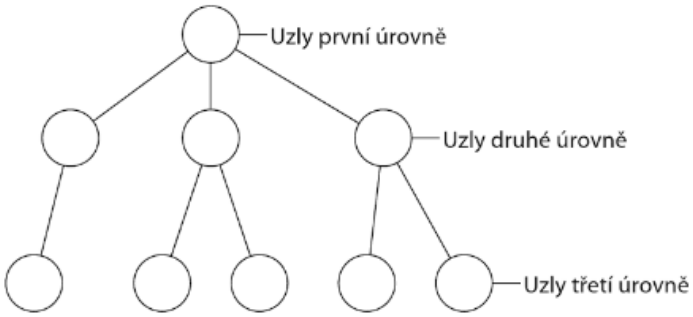
Obrázek 3: Kruhová topologie

Stromová topologie

Ve stromové topologii existuje vždy výchozí kořenová úroveň. V té je pouze jeden uzel, na který navazují uzly druhé úrovně. Na ty pak navazují uzly třetí úrovně a tak dále. Pokud by existovaly méně než tři úrovně, byla by to topologie hvězdy.

Výhody: Pokud dojde k poruše, neselže celá síť, ale pouze uzly, které jsou na porušené větvi závislé. Je zde jednodušší identifikovat místo poruchy.

Nevýhody: Čím výše se uzel ve stromu nachází, tím je vytíženější, zatěžuje ho provoz uzlů nižších úrovní, které nemají jinou možnost komunikace než skrze něj. Síť postavená na stromové topologii je tedy náchylná k havárii z důsledku přetížení.



Obrázek 4: Stromová topologie

CSMA-CD

Jak již bylo zmíněno, o tom, kdy bude mít jednotlivé zařízení v síti přístup k odesílání a přijímání dat, rozhodují přístupové metody. V sítích s kruhovou topologií o tom rozhoduje kolující token. Této výše popsané metodě se říká token ring. U sítí se sběrnicovou topologií je to také token, avšak ten koluje podle konkrétního adresování zařízení v síti. Díky tomu zde není potřeba kruhová topologie. Této metodě se říká token bus.

Nejrozšířenější topologií je u lokálních sítí topologie hvězdy. V této topologii se používá přístupová metoda CSMA-CD (Carrier-sense Multiple Access with Colision Detection) neboli metoda náhodného přístupu. Tato metoda se používá u standardu Ethernet.

Pokud chce nějaké zařízení vysílat, zkontroluje, jestli vedením neprochází nějaké signály jiného zařízení. Pokud ne, samo začne vysílat. Pokud ano, zařízení počká a o vysílání se pokusí později. V případě volného vedení mohou začít vysílat dvě různá zařízení. Proto zařízení, které vysílá, zároveň kontroluje, jestli signály procházející vedením pochází od něj. Pokud ne, zařízení se musí o vysílaní pokusit znovu, bylo totiž předběhnuto zařízením jiným.

K tomu, aby se nestalo, že bude síť přehlcena příliš mnoha pokusy o vysílání, slouží aktivní síťové prvky. Tyto prvky se postarají o to, aby nebyly pakety vpuštěny do částí sítě, kam nepatří. Tím se sníží pravděpodobnost kolizí.

(Horák, Keršláger 2013), (Sosinsky 2011)

3.4 Referenční model ISO/OSI

Jelikož byly počítačové sítě zpočátku vyvíjeny více firmami nezávisle na sobě, jednotlivé systémy mezi sebou nebyly kompatibilní. Cílem počítačových sítí je však propojení zařízení mezi sebou, nezávisle na jejich typech a výrobcích. Z tohoto důvodu byl mezinárodním ústavem ISO (International Standards Organization) vytvořen referenční model OSI (Open Systems Interconnection), kterým byla práce v síti rozdělena do sedmi spolupracujících vrstev. Jsou to aplikační vrstva, prezentační vrstva, relační vrstva, transportní vrstva, síťová vrstva, linková vrstva a vrstva fyzická.

Tento model pracuje s takzvaným zapouzdřováním. Nejvyšší vrstva zpracovávaná data zapouzdří a připojí k nim svou informaci ve formě hlavičky. Tato data pak putují do nižší vrstvy, ve které se data opět zapouzdří a jsou opatřena další hlavičkou vrstvy, která data aktuálně zpracovala. Takto prostupují data až do nejnižší vrstvy. Jakmile jsou data opatřena hlavičkami ze všech sedmi vrstev, je možné je odeslat jinému zařízení. Toto zařízení poté zopakuje stejný postup jako před odesláním, jen v opačném pořadí. Každá vrstva si vezme informaci z té hlavičky, která je pro ni určená, až v nejvyšší vrstvě zbydou pouze původně odeslaná data.

Aplikační vrstva

Do aplikační vrstvy spadají konkrétní síťové aplikace. Jedná se například o aplikace umožňující správu sítě, přístup k síťovým tiskárnám či e-mailům.

Prezentační vrstva

Jelikož stejná data mohou být na různých sítích různě kódována, má prezentační vrstva na starosti konverzi těchto přenášených dat. Dále může data komprimovat, případně šifrovat.

Relační vrstva

Tato vrstva navazuje spojení a po skončení přenosu ho ukončí. Dále může ověřovat uživatele a zabezpečovat přístup k zařízení.

Transportní vrstva

Funkce této vrstvy spočívá u odesílacího zařízení v dělení přenášených dat na jednotlivé pakety. U přijímacího zařízení tato vrstva naopak z přijatých paketů opětovně poskládá původní data.

Síťová vrstva

Pokud mezi odesílacím a přijímacím zařízením nebo mezi jednotlivými sítěmi neexistuje přímé spojení, zajišťuje tato vrstva směrování neboli routing. Routing spočívá ve volbě nejvhodnější trasy pro odesílání paketů, jelikož vždy existuje více možných cest.

Linková vrstva

Linková neboli spojová vrstva pracuje s fyzickými MAC adresami síťových karet. Odesílá a přijímá pakety. Kontroluje cílové adresy jednotlivých přijímaných paketů a poté rozhodne, zda je předá vyšší vrstvě. Odesílané pakety naopak opatřuje výchozími a cílovými adresami.

Fyzická vrstva

Vrstva, která popisuje fyzickou podobu přenášených signálů. Určuje, jakým signálem je zastoupena logická jednička a nula nebo jak přijímací stanice rozezná začátek bitu. Dále pak popisuje typ konektoru a konkrétní použití jednotlivých vodičů v kabelu.

(Horák, Keršláger, 2013), (Kurose, Ross, 2014)

3.5 TCP/IP

3.5.1 Referenční model TCP/IP a jeho porovnání s OSI

Přesto, že byl tento model mnohokrát kritizován za nedostatečnou obecnost, je na modelu TCP/IP je založena velká většina dnešních sítí a zařízení. Je tomu tak z důvodu, že na tomto modelu stojí dominantní standardy a nejpoužívanější síťové protokoly, byl totiž původně navržen pro síť internet. Model OSI v praxi rozšířen není, avšak díky své flexibilitě nám pomáhá lépe porozumět síťové komunikaci.

Oproti sedmivrstvému modelu OSI je TCP/IP rozdělen do čtyř vrstev. Je to vrstva síťového rozhraní, síťová, transportní a aplikační vrstva. Zatímco druhá, třetí a čtvrtá vrstva jsou reprezentovány samostatnými protokoly, činnost první vrstvy má na starosti samotný hardware. Ten pracuje v tomto modelu podle standardu Ethernet nebo Wi-Fi. Tyto standardy budou podrobněji zmíněny v kapitole síťové standardy. V modelu OSI je tato vrstva rozdělena na vrstvu linkovou a fyzickou. Druhá vrstva, síťová, je zastoupena i v modelu OSI a stejně je tomu u vrstvy třetí, transportní. Na rozdíl od modelu OSI, nenajdeme v TCP/IP vrstvu relační a prezentační. Čtvrtá vrstva, aplikační, je již zastoupena v obou modelech.

Vrstvy TCP/IP	Vrstvy OSI
Aplikační	Aplikační
	Prezentační
Transportní	Relační
	Transportní
Síťová (IP)	Síťová
Vrstva síťového rozhraní	Linková
	Fyzická

Tabulka 1: Porovnání modelů

3.5.2 Síťové protokoly jednotlivých vrstev

Pravidla komunikace a výměny dat v síti jsou definována síťovými protokoly. Aby síť správně fungovala, všechna zařízení v síti musí používat protokol stejný. Nejrozšířenější skupinou protokolů je TCP/IP.

Spolupráce jednotlivých protokolů napříč vrstvami probíhá stejně jako u modelu OSI. V případě potřeby navázání spojení mezi zařízeními odešle aplikační vrstva požadavek transportní vrstvě. Zde se data rozdělí na segmenty a naváže se spojení, poté jsou data předána do síťové vrstvy. Ta segmenty zabalí a odešle. Při přijímání dat je tomu přesně naopak.

Aplikační vrstva

Do aplikační vrstvy patří mnoho protokolů, které spolupracují s konkrétními programy. Mezi nejpoužívanější protokoly této vrstvy patří například protokol HTTP, který se používá pro uspořádání www stránek. Dále je to třeba protokol FTP, který se používá pro přenos souborů. Mezi další důležité služby patří elektronická pošta, jejíž činnost zajišťují protokoly SMTP a POP3. Za zmínku stojí i protokol DNS, který páruje textové názvy serverů s jejich IP adresami.

Transportní vrstva

Tato vrstva obsahuje pouze dva protokoly. Jsou to protokoly TCP a UDP, které mají podobnou funkci.

Protokol TCP dostane data od aplikační vrstvy, rozdělí je na segmenty a seřadí. Než však začne s kontrolou a vysíláním, naváže spojení s transportní vrstvou cílového zařízení. Poté předává segmenty síťové vrstvě, která je odesílá. Naopak při přijímání dat kontroluje příchozí segmenty a zda nějaký nechybí. Pokud ano, zažádá si o jeho opětovné zaslání. Pokud ne, poskládá ze segmentů data, která předá aplikační vrstvě. Ta je pak předá konkrétnímu programu.

Stejnou činnost jako TCP má na starosti protokol UDP. Ten však nenavazuje spojení s přijímacím nebo odesílacím zařízením ani nekontroluje úspěšnost přenosu jednotlivých segmentů. Po rozdělení dat na segmenty je pouze předá síťové vrstvě. Tento protokol není tolik spolehlivý jako TCP, neřídí tok dat ani zahlcení. Jeho výhoda spočívá v rychlosti.

Segment, obohacený o hlavičku z transportní vrstvy se nazývá datagram.

Síťová vrstva

Vrstva síťová zodpovídá za přenos datagramů mezi zařízeními. Pracuje zde protokol IP, který dostává požadavky od transportní vrstvy. Tento protokol připojí k datagramu svoji

hlavičku, která obsahuje IP adresu odesilatele a příjemce. Má na starost adresaci a směrování datagramů. Protokol IP je nespolehlivý, nekontroluje odeslané nebo doručené datagramy, to má na starosti protokol TCP.

I přesto, že se síťové vrstvě často říká IP vrstva, neobsahuje pouze protokol IP. Jsou zde směrovací protokoly, které určují, kterou z možných cest budou datagramy cestovat od výchozího k cílovému uzlu.

Vrstva síťového rozhraní

Fyzický přenos dat mezi zařízeními má na starosti vrstva síťového rozhraní. Tato vrstva přenáší již jednotlivé bity, v závislosti na použitém připojení. Například pro kabelové připojení slouží standard Ethernet. Ten používá jiný protokol pro přenos po kroucené dvojlince, jiný pro optická vlákna a jiný pro koaxiál.

(Sosinsky 2011), (Horák, Keršláger 2013), (Kurose, Ross 2014)

3.6 Síťové standardy

Jak už bylo řečeno, k tomu, aby byly jednotlivé sítě kompatibilní, slouží standardy. Tyto normy definuje organizace IEEE (Institute of Electrical and Electronics Engineers). Jednotlivé normy podrobně popisují mimo jiné přístupovou metodu, topologii sítě, rychlost přenosu dat, typ kabelu, jeho délku a typ konektoru.

Standardy pro lokální sítě jsou:

- **IEEE 802.3** Sítě Ethernet (topologie hvězdy), CSMA-CD
- **IEEE 802.4** Sítě sběrnicové, Token bus
- **IEEE 802.5** Sítě kruhové, Token ring
- **IEEE 802.11** Bezdrátové sítě

3.6.1 Kabelové síťové standardy

Ethernet

Ethernet je nejrozšířenější standard lokálních počítačových sítí. V modelu TCP/IP je reprezentován vrstvou síťového rozhraní, v modelu OSI vrstvou fyzickou a linkovou. Jako

přístupovou metodu používá již zmíněnou metodu CSMA-CD. Jednotlivé specifikace Ethernetu se zabývají použitím různých typů kabelů a topologií.

Pojmenování jeho jednotlivých typů se skládá ze tří částí. První číslice udává maximální přenosovou rychlost. Druhé je slovo BASE, které značí signalizační metodu. Koncové písmeno popisuje typ kabelu, pro který je navržen.

Nejstarší standard byl vytvořen pro přenosovou rychlost 10 Mb/s. Zde jsou jeho jednotlivé typy:

- **10BASE-5** Tlustý koaxiál, sběrnicová topologie
- **10BASE-2** Tenký koaxiál, sběrnicová topologie
- **10BASE-T** Kroucená dvojlinka, topologie hvězdy
- **10BASE-F** Optický kabel, další 3 podtypy podle použití

Fast Ethernet

Dnes asi nejrozšířenější norma Ethernetu je navržená pro rychlost 100 Mb/s. Pro tuto normu již není možné použití koaxiálního kabelu.

Tato norma má tři varianty:

- **100BASE-TX** – Varianta pracující s kroucenou dvojlinkou kategorie 5. Využívá 2 páry a maximální délka kabelu je 100 metrů.
- **100BASE-FX –** Tato varianta používá optický kabel. Pro mnohovidové kabely je maximální délka 412 metrů, pro jednovidové až 10 000 metrů.
- **100BASE-T4** – Starší norma pro kroucenou dvojlinku kategorie 5, 4 a 3. Využívá všechny 4 páry a maximální délka je 100 metrů.

Gigabit Ethernet

Původně byl používán pro páteřní vedení a připojení serverů, dnes je však čím dál rozšířenější i v lokálních sítích. Jeho maximální přenosová rychlost je až 1000 Mb/s. Opět je standardizovaný pouze pro kroucené dvojlinky nebo optické kabely.

Existují zde 2 základní typy:

- **1000BASE-X (802.3z)** - Norma pro optické kabely, dále se dělí na 2 typy.

    - **1000BASE-SX** – Zdrojem světla je zde LED dioda, jejíž světlo je přenášeno mnohovidovými kabely. Používá se u krátkých horizontálních vedení a krátkých páteřních vedení. Maximální délka kabelu je 220 metrů.
    - **1000BASE-LX** – Světlo je generované laserovým zdrojem a může být přenášeno mnohovidovým i jednovidovým kabelem. Při použití mnohovidového kabelu je jeho maximální vzdálenost 550 metrů a používá se u krátkých horizontálních nebo krátkých páteřních vedení. Pro jednovidový kabel je maximální délka až 5 kilometrů a využívá se pro dlouhá páteřní vedení, dlouhá horizontální vedení a propojování mezi budovami.

- **1000BASE-T (802.3ab)** - Norma pro použití kroucené dvojlinky kategorie 5 a 5e, přičemž je doporučena novější kategorie 5e. Oba tyto typy využívají všechny 4 páry vodičů.

10 Gigabit Ethernet

Standardy vycházející z této normy byly pojmenovány 802.3ae pro optické kabely a 802.3an pro kroucenou dvojlinku. Jeho maximální přenosová rychlost je 10 Gb/s. Jeho využití není jen v sítích lokálních (LAN), ale díky své velké maximální vzdálenosti i v sítích metropolitních (MAN) a rozlehlých (WAN).

Rozdělení:

- **10GBASE-X (802.3ae)** - Pro optické kabely.

    - **10GBASE-SR** – Standard pro mnohovidový kabel na kratší vzdálenosti, až do 82 metrů.
    - **10GBASE-LX4** – S mnohovidovým kabelem dosáhne vzdálenosti do 300 metrů, s jednovidovým až 10 kilometrů.

- **10GBASE-LR a -ER** – Jeho maximální vzdálenost je až 40 kilometrů a pracuje pouze s jednovidovými kabely.

- **10GBASE-T (802.3an)** - Standard pro kroucené dvojlinky. Rychlost 10 Gb/s je schopný dosáhnout s kabely kategorie 5e, 6 a 7. Liší se pouze maximální možná délka podle použité kabeláže. S dnes nejrozšířenějšími kabely kategorie 5e je to 40-50 metrů, s kabely kategorie 6 je to 50-60 metrů. Dosáhnout můžeme až vzdálenosti 100 metrů, to však pouze s kroucenou dvojlinkou kategorie 6a a 7.

(Ptáček 2006), (Horák, Keršláger 2013)

3.6.2 **Bezdrátové síťové standardy**

U zařízení, jako jsou například notebooky, smartphony a tablety, je hlavní výhodou jejich mobilita. Potřeba zapojeného kabelu pro spojení s internetem by však eliminovala tuto výhodu. V takových případech se používají bezdrátové sítě.

V bezdrátových sítích se signál přenáší elektromagnetickým vlněním o určité vlnové délce a frekvenci. Využití elektromagnetických vln, jakožto přenosového média, je velmi rozšířenou metodou. Stejným způsobem jsou distribuovány například rozhlasové, televizní a telekomunikační služby. Aby spolu zařízení vzájemně komunikovala, musí vysílat a přijímat vlny na stejné frekvenci. Bezdrátové sítě komunikují na 2,4 GHz a 5 GHz frekvenci. Zatímco 2,4 GHz frekvence je volně použitelné pásmo, provoz v pásmu 5 GHz je regulován Českým telekomunikačním úřadem.

Jelikož je třeba, aby spolu komunikovala jednotlivá zařízení různých výrobců, bylo potřeba stanovit pravidla provozu takovýchto sítí. Požadavky, které musí splňovat jednotlivá zařízení, definovala aliance výrobců zvaná WECA (Wireless Ethernet Compatibility Aliance). Každý výrobek, který tyto požadavky splní, dostane certifikát Wi-Fi, který zaručuje kompatibilitu s ostatními produkty se stejným certifikátem.

Standard byl odvozen z Ethernetu, takže má jisté podobné znaky, jako například přístupovou metodu CSMA/CD. Jednotlivé standardy Wi-Fi, definuje, tak jako u kabelových sítí, organizace IEEE. Pro Wi-Fi sítě je to norma IEEE 802.11, která se dále dělí.

Zde jsou vypsány nejpoužívanější standardy od nejstarších po nejnovější, jejich používané pásmo a teoretická maximální rychlost:

• **IEEE 802.11a**	5 GHz	54 Mb/s
• **IEEE 802.11b**	2,4 GHz	11 Mb/s
• **IEEE 802.11g**	2,4 GHz	54 Mb/s
• **IEEE 802.11n**	2,4 nebo 5 GHz	600 Mb/s
• **IEEE 802.11ac**	2,4 GHz	450 Mb/s
	5 GHz	1 Gb/s

Normy IEEE 802.11n a ac pracují na bázi vysílání více signálů použitím více antén. Tento model se nazývá MIMO (Multiple Input Multiple Output). Přidáváním více antén lze pak zvyšovat datovou propustnost, pro vnitřní prostředí se však většinou používají 2 až 4 antény.

(Horák, Keršláger 2013)

3.7 Síťový hardware

Pro realizaci sítě je potřeba síťový hardware. Podle toho, jestli síťový prvek signál nějakým způsobem zpracovává nebo signál pouze přenáší, rozdělujeme dvě základní kategorie. Jedná se o aktivní síťové prvky a prvky pasivní.

3.7.1 **Pasivní prvky**

Mezi pasivní prvky patří všechen hardware, díky kterému jsme schopni šířit signál na různá místa. Tyto prvky však signál nijak neovlivňují. Jeho činnost pak řídí prvky aktivní. Mezi pasivní prvky tak patří například síťové zásuvky.

Nejdůležitějšími pasivními prvky jsou však přenosová média. Existují různé druhy přenosových médií, po kterých můžeme šířit signál. Způsob přenosu signálu po jednotlivých médiích definují výše zmíněné standardy.

V domácích počítačových sítích jsou používány tři typy těchto přenosových médií, optický kabel, metalický kabel a vzduch, kterým se šíří elektromagnetické vlnění bezdrátových sítí. Dříve používané koaxiální kabely jsou již zastaralá technologie.

Optický kabel

Data jsou v optických kabelech přenášena světelnými impulsy ve světlovodivých optických vláknech. Tato vlákna jsou chráněna sekundární ochranou proti mikro a makroohybům, které by omezovaly průchod světelného paprsku vláknem. Okolo sekundární ochrany je vrstva konstrukční, která zvyšuje pevnost kabelu. Plastový vnější obal již jen vše kryje. Optických vláken musí být v kabelu sudý počet, po jednom vlákně se impulsy odesílají, po druhém přijímají. Může to být pouze jeden pár, avšak běžně je v optických kabelech páru hned několik.

Obrázek 5: Optický kabel

Podle konstrukce optického vlákna v kabelu rozeznáváme dva typy optických kabelů:

- **Jednovidové (SMF)** - Single Mode Fiber

Index lomu mezi jádrem a pláštěm vlákna je velmi malý, přičemž vláknem prochází pouze jeden světelný paprsek bez ohybů. Díky tomu má jednovidový kabel velkou přenosovou kapacitu a je schopen nést signál až na desítky kilometrů. Takové kabely se u lokálních sítí příliš nevyskytují, a to především kvůli jejich ceně. Zdrojem světla je totiž u těchto kabelů laser.

- **Mnohovidové (MMF)** - Multi Mode Fiber

Jelikož u mnohovidových kabelů není index lomu ve všech částech kabelu stejný, mají horší optické vlastnosti. Světlo se kvůli ohybům rozpadá na části, vidy, ty pak způsobují zkreslení signálu, protože na konec kabelu nedorazí najednou.

Mnohovidové kabely jsou schopny nést signál jen na stovky metrů, jsou však levné a v lokálních sítích dostačující. Zdrojem světla je levná LED dioda.

Převážně se používají dva druhy normovaných koncovek. Hranatý konektor SC a kulatý konektor ST. Tyto koncovky mají výběžek, který se zapojuje do příslušného konektoru, říká se mu ferule. Ta je chráněna krytkou, protože by se při práci s kabelem mohla zašpinit, což by utlumilo průchod signálu.

S optickými vlákny je třeba zacházet opatrně. Pokud ohneme vlákno v devadesátistupňovém úhlu, může dojít ke špatnému odrazu signálu a tím jeho zhoršení. Taková deformace se nazývá mikroohyb. Makroohyb je naopak přílišné zmáčknutí vlákna a způsobuje stejné potíže jako mikroohyb.

Na každém konci optického kabelu tak musí být převodník, ten je součástí aktivního prvku, ne kabelu. Převodník převádí světelné paprsky na elektrické impulzy a naopak. Optický kabel jde spojit i s kroucenou dvojlinkou. Pomocí konvertoru, elektroniky v něm umístěné, můžeme konvertovat optický signál na elektrický.

Výhody: Mezi výhody optické kabeláže patří vysoká kapacita přenášených dat, vysoká rychlost a přenos dat na velké vzdálenosti. Jsou odolné proti elektromagnetickému rušení, a navíc se optické signály nedají odposlouchávat.

Nevýhody: Největší nevýhoda je v ceně. Velmi drahé a složité je především konektorování. Samotný kabel tak drahý není, ostatní prvky kabeláže však ano.

Kroucená dvojlinka

Kroucená dvojlinka je metalický kabel, který se skládá ze čtyř párů měděných vodičů. Jak z názvu vyplývá, každý pár kabelů je navzájem zakroucen a tyto páry jsou zkroucené s ostatními páry. Měděné vodiče by se mohly vzájemně rušit, díky kroucení střídají vzájemnou polohu, a tak se minimalizuje riziko vzájemného ovlivnění.

Z ethernetových standardů vyplývá, že kroucenou dvojlinku lze použít pro různé přenosové rychlosti až do 10 Gb/s, v závislosti na kategorii použitého kabelu a ostatních pasivních i aktivních síťových prvků.

Zde jsou jednotlivé kategorie kabelů, jejich přenosová rychlost a šířka pásma:

- **Cat5** **100 Mb/s** **100 MHz**
- **Cat5e** **1 000 Mb/s** **125 MHz**
- **Cat6** **10 Gb/s** **250 MHz**
- **Cat7** **10 Gb/s** **600 MHz**

Podle provedení kabelu se odlišují tři typy:

- **UTP** - (Unshielded Twisted Pair)

  Nestíněná kroucená dvojlinka je u domácích sítí nejpoužívanějším typem kabelu. Jednotlivé páry vodičů jsou kryty pouze vnější izolací.

- **STP** - (Shielded Twisted Pair)

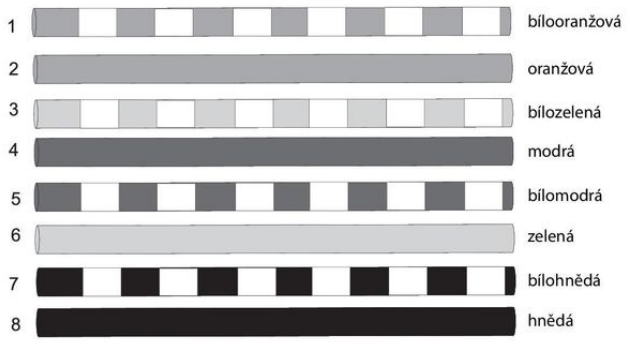
  Stíněná kroucená dvojlinka zvyšuje ochranu proti vnějšímu rušení izolací. Vodiče jsou uloženy v kovovém opletu, teprve potom ve vnějším obalu. Stíněny mohou být všechny páry zvlášť nebo je odstíněn pouze plášť kabelu. Takové kabely nesou označení ScTP.

- **FTP** - (Foiled Twisted Pair)

  Kroucená dvojlinka stíněná metalickou fólií.

V kroucené dvojlince jsou tedy čtyři páry vodičů. Pro připojení při rychlosti do 100 Mb/s jsou využity pouze dva páry, zbylé zůstávají nevyužité. Z těchto dvou párů jsou první dva vodiče použity pro vysílání a druhé dva pro přijímání. Pro připojení rychlostí 1000 Mb/s se již používají všechny páry. Při této rychlosti pracuje všech osm vodičů v obousměrném provozu.

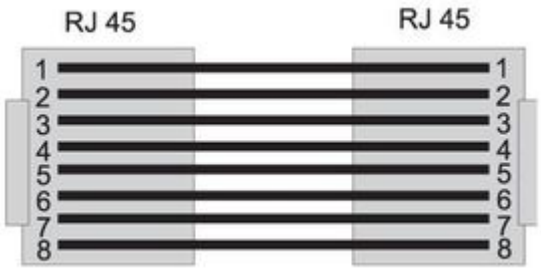
Všech osm vodičů je od sebe barevně rozlišeno. Kvůli lepší identifikaci páru mají dva vodiče stejnou barvu, přičemž na jednom z nich jsou bílé pruhy pro odlišení. Značení barev pro zapojení v konektoru, zásuvce či patch panelu, určují normy TIA/EIA 568-A a TIA/EIA 568-B. Druhá norma je u nás rozšířenější.



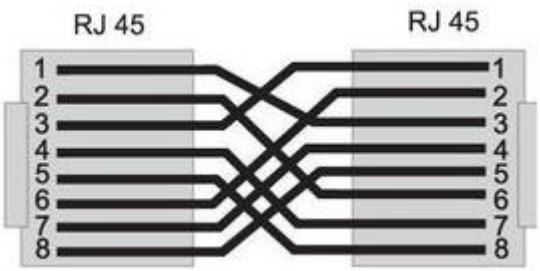
Obrázek 6: Schéma TIA/EIA 568-B

U prvního typu barevného schématu je zelený pár vyměněn s oranžovým, ostatní barvy zůstávají stejné. Na každém konci kabelu je použita koncovka RJ 45, do které jsou jednotlivé vodiče připojeny podle použití.

Při propojování počítače se zásuvkou nebo routerem či switchem se jednotlivé vodiče zapojují na obou koncích stejně. Pokud je však potřeba propojit dva počítače přímo, bez použití aktivního propojovacího prvku, je potřeba zapojit vodiče křížově.



Obrázek 7: Přímé zapojení



Obrázek 8: Křížené zapojení

U kříženého zapojení pro rychlost 100 Mb/s křížíme pouze vodiče 1, 2, 3 a 6.

3.7.2 **Aktivní prvky**

Funkci kabeláže řídí aktivní prvky, ty aktivně ovlivňují průchod signálů. Model OSI definuje vše, co je třeba zařídit pro úspěšnou síťovou komunikaci. Síťová, linková a fyzická vrstva zajišťují základní komunikaci a velkou část jejich činnosti má na starosti přímo síťová karta zařízení. Kontrolu paketů a rozhodnutí o tom, kudy paket dorazí do cíle a kam bude vpuštěn, mají na starosti další aktivní prvky v síti.

Repeater

Nejjednodušší prvek je opakovač (zesilovač). Ten má jeden vstup a jeden výstup. Signál, který do něj vstoupí, zesilovač zopakuje a odešle na výstup. Tím se zvýší dosah kabelu. Pracuje ve fyzické vrstvě modelu OSI.

Transceiver

Převodník zesiluje signál jako zesilovač. Zároveň je schopen signál převést například z optického kabelu na kroucenou dvojlinku. Stejně jako opakovač, pracuje převodník ve vrstvě fyzické.

Hub

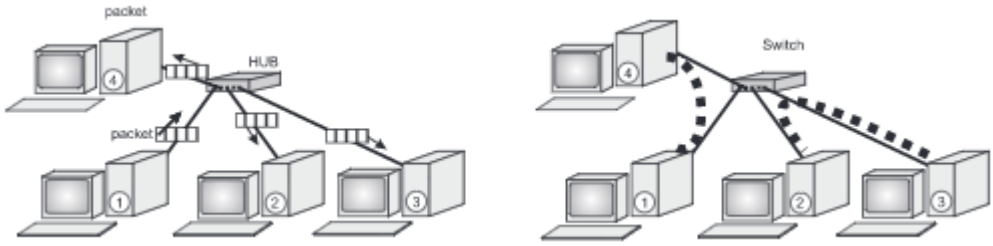
Pro hvězdicovou topologii je nutný rozbočovač, hub. Ten pouze větví síť a rozbočuje signál. Hub také pracuje ve vrstvě fyzické.

Bridge

Bridge neboli most odděluje síťové segmenty. Pokud jsou v síti odeslána data jedním počítačem, hub je pouze přijme a odešle všem připojeným zařízením. Přijme je pak pouze počítač, pro který byla data určena. Při použití bridge mezi dvěma huby jsou data přijata bridgem a ten podle cílové adresy odešle data pouze hubu, ve kterém je cílové zařízení připojeno. Most tedy minimalizuje přetížení sítě. Most pracuje v linkové vrstvě OSI, není ovlivněn fyzickou odlišností sítí, a tak je schopen propojit i dvě různé sítě.

Switch

Switche plně nahradily huby, jakožto rozbočovače pro hvězdicové topologie. Switch používá standard ethernet, a tedy přístupovou metodu CSMA-CD. Jeho práce je podobná, jako práce při kombinaci hubu a mostu. Switch však neodesílá data celé větvi, ale pouze jednomu konkrétnímu zařízení. Tak jako most, pracuje v linkové vrstvě.



Obrázek 9: Síť s hubem (vlevo) a síť se switchem (vpravo)

Router

Mezi aktivními prvky je směrovač ten nejinteligentnější. Slouží pro propojení domácí sítě s internetem a pracuje v síťové vrstvě OSI. Zajišťuje výběr vhodné trasy pro pakety a jejich filtraci. Dokáže propojit více LAN sítí.

Dnešní domácí routery mají integrované DHCP servery pro přidělování IP adres, firewally pro ochranu sítě a samozřejmě access pointy. Access point je zařízení, ke kterému se připojujeme s bezdrátovými zařízeními díky anténám, vysílajícím Wi-Fi. Ve velmi malé síti, například pro jeden menší byt, je tedy možné postavit síť pouze na routeru. Ten je schopen plnit funkci všech výše zmíněných zařízení dohromady.

Nejdůležitější funkcí routeru v síti však zůstává takzvané routování, směrování paketů, datagramů, v síti.

Gateway (Brána)

Zařízení, které slouží k propojování LAN sítí s odlišnými sítěmi, používajícími jiný hardware a protokoly. Pracuje v aplikační vrstvě OSI.

(Horák, Keršláger 2013), (Kurose, Ross 2014)

3.8 Síťový software

Aby síťový hardware správně pracoval, je třeba ho oživit softwarem. Kombinace hardwaru a softwaru nám umožní vytvořit provozuschopnou síť. Podle toho, zda je v naší síti umístěn server nebo ne, rozlišujeme dva základní typy sítí. Jsou to sítě peer-to-peer a klient-server.

3.8.1 **Peer-to-peer sítě**

Tento typ sítě je nejpoužívanější u domácích počítačových sítí a u sítí malých firem, přibližně do deseti počítačů. Síť je tvořena jednotlivými počítači, které jsou si navzájem rovné. Jednotlivá zařízení si mohou povolit přístup k jednotlivým diskům nebo jejich částem, dělit se mohou i o jednu síťovou tiskárnu. Síť peer-to-peer je obsažena v běžných operačních systémech, není tedy potřeba pořizovat síťový operační systém.

Výhody: Toto řešení je levné, jelikož není potřeba pořizovat síťový operační systém ani nákladný server. Správa takové sítě navíc není náročná a zvládne ji i mírně pokročilý uživatel.

Nevýhody: Čím více počítačů v síti sdílí své soubory nebo celé disky, tím těžší je udržet přehled o tom, kde jsou která data uložena. Nastavení přístupových práv je jednoduché a méně bezpečné, data tedy nejsou dostatečně chráněna proti zneužití.

3.8.2 **Sítě klient-server**

Všechna data v této síti jsou uložena na jednom místě, počítači, serveru. Tam jsou data důkladně zabezpečena a nabízena ostatním zařízením v síti, podle přidělených přístupových práv.

Tato přístupová práva organizuje síťový operační systém, který je nainstalován na serveru. Server tedy může být jakýkoliv počítač na kterém je takový systém nainstalován. Jelikož však server obsluhuje všechna zařízení v síti, kdykoli o to požádají, jsou na něj kladeny mnohem větší hardwarové nároky než na běžná zařízení, ze kterých se na něj přistupuje.

Mezi nejpoužívanější síťové operační systémy patří buďto různé linuxové distribuce nebo jednotlivé verze Windows Server od firmy Microsoft.

Výhody: Data v síti jsou vysoce zabezpečena a centralizována na jednom místě. Konfigurace přístupu nových i stávajících zařízení k síti je snadno proveditelná na jednom místě.

Nevýhody: Nevýhody zde spočívají v ceně, jelikož je potřeba nakoupit výkonný server a licenci k síťovému operačnímu systému. Dále potřebujeme správce sítě, který se o ni bude starat, jelikož obsluha sítě klient-server už vyžaduje odbornou znalost.

(Horák, Keršláger 2013)

3.9 Zálohování dat

Zálohování dat je velmi důležitá součást jakékoli práce s důležitými soubory. Zapisovací média se mohou nečekaně porouchat. Ke ztrátě nebo zašifrování dat může však dojít i v důsledku napadení nějakým škodlivým softwarem nebo z důvodu chyby samotného uživatele. Ve výše zmíněných případech přijde vhod záloha dat.

Data se dají zálohovat na optická média CD či DVD, USB flash disky nebo externí harddisky či páskové jednotky. Přímo v počítači může být i druhý záložní disk. Velmi oblíbené jsou dnes síťová úložiště NAS.

NAS neboli Network Attached Storage je samostatný počítač s pevnými disky připojený v síti LAN. Takové úložiště je možné použít pro sdílení multimediálního obsahu v lokální síti, může fungovat i jako soukromý cloud pro přístup k datům mimo lokální síť. Hlavně poskytuje dostatek místa pro ukládání záloh ostatních počítačů, které samy dostatek místa pro tyto účely neposkytují.

V operačních systémech Windows je možné nastavit automatické zálohování souborů na námi zvolené médium. Jako médium s dostatečnou kapacitou je možné použít právě NAS. Pomocí nástroje zálohování a obnovení je možné pravidelně ukládat dokumenty, fotky, hudbu, videa a také bitové kopie systému. Bitová kopie systému přijde vhod tehdy, když z nějakého důvodu přestane správně fungovat operační systém. Bitová kopie obsahuje přesný obraz disku a umožňuje tedy obnovení zhrouceného systému na předchozí zálohovanou verzi. Uživatel má možnost si sám zvolit, jak často se budou soubory nebo bitové kopie zálohovat.

Pokud dojde k porouchání pevného disku v počítači, je možné nahráním bitové kopie na disk nový obnovit počítač do téměř stejného stavu jako před poruchou. Selže-li pevný disk v NASu, který zálohovaný není, data budou ztracena. Z toho důvodu se vyrábějí NASy s několika pozicemi pro disky. NAS si pak dokáže sám zálohy vytvářet pomocí diskových polí a v případě selhání jednoho disku stačí vadný kus vyměnit za nový. Na nový disk se po jeho zapojení opět automaticky zálohuje disk nebo disky, které již v NASu jsou. Vždy záleží na tom, jakým způsobem jsou disky zapojeny, jaká jsou použita disková pole a jak je zálohování nastaveno.

Disková pole:

- **RAID 0 –** Toto pole žádné bezpečí dat nevytváří. Disky zapojené v tomto poli se jeví jako samostatné. Při havárii disku uživatel přijde o všechna data na něm uložená
- **JBOD –** Při zapojení disků v tomto poli se všechny disky jeví jako jeden velký. Data jsou zapisována postupně od prvního k poslednímu disku. Při havárii disku se ztratí pouze část dat, na něm zapsaná.
- **RAID 1 (Zrcadlení) –** Při použití tohoto pole se ztratí polovina kapacity disků. Data ukládaná na jeden disk se zapisují i na disk druhý. Při havárii jednoho z disků jsou všechna data na druhém. Po výměně vadného disku za nový se data z prvního disku zkopírují na disk nový.
- **RAID 5 –** Na rozdíl od předchozích polí vyžaduje toto pole minimálně tři disky. Předchozí pole vyžadují dva. Kapacitu jednoho z disků zabírají samoopravné kódy, které jsou střídavě uloženy na všech členech. Při výpadku jednoho z disků a následné výměny za disk nový jsou data dopočítána z opravných kódů a znovu nakopírována na disk nový.

Existují i další disková pole, zmíněna jsou ta v praxi nejpoužívanější.
(Horák 2011), (Horák, Keršláger 2013)

3.10 Zabezpečení sítí

Internet je dnes natolik rozšířený, že se jen velmi málo vidí počítač, který k němu nemá přístup. Domácí sítě a jejich připojení k internetu přináší velké množství výhod, byla by tedy škoda je nevyužít. Nejsou to však pouze výhody, které připojením k počítačové síti získáme. Připojením počítače k síti, internetu, výrazně snižujeme zabezpečení takového zařízení. K napadení není třeba fyzický přístup k počítači, jelikož počítač komunikuje s okolím, a tak může být ohrožen skrze síť. Hrozí nám ztráta dat, napadení viry a spywary, či vniknutí do soukromí skrze webové kamery a mikrofony.

Je velmi důležité domácí síť správně zabezpečit. Zatímco v pouze kabelových sítích je signál šířen pouze zařízením, která jsou v síti připojená, v sítích bezdrátových se signál

šíří do okolí, a tak může být zachycen kýmkoli v dosahu vysílání. U sítí Wi-Fi je zabezpečení zvláště důležité, existuje mnoho ochranných prvků, které výrazně snižují riziko napadení.

3.10.1 **Preventivní ochrana před útoky**

Chránit počítač před různými typy útoků musí především sám uživatel. Nejdůležitější je jeho chování při používání daného zařízení. Neuvážené akce uživatele zvyšují riziko napadení počítače. Patří mezi ně například otevírání neověřených příloh e-mailů od neznámých odesilatelů, klikání na neznámé odkazy, instalace neověřeného softwaru, navštěvování pochybných www stránek a další. Před nevědomostí a nerozvážností uživatele samotného se dá počítač ochránit jen těžko. Dodržováním několika následujících pravidel můžeme alespoň snížit rizika napadení.

Aktualizace

K přístupu do cizího počítače se dají zneužít jak softwarové aplikace, tak operační systém samotný. Vývoj softwaru proto nikdy nekončí datem uvedení do prodeje, ale ukončením softwarové podpory, která může trvat desítky let. Postupem času se odhalují bezpečnostní mezery v softwaru a prací vývojářů je tyto mezery eliminovat. Pravidelnými aktualizacemi softwaru není distribuována pouze jeho nová funkčnost či modernější vzhled, ale hlavně zásadní bezpečnostní záplaty. Je tedy důležité udržovat všechen používaný software, zejména operační systém, aktualizovaný.

Antivirový a antispywarový program

Zařízení jsou nejčastěji ohrožována počítačovými viry a spywarem. Četnost napadení člověkem za účelem odcizení dat je v poměru s výše zmíněnými hrozbami malá. Počítačový virus je program, který nějakým způsobem škodí počítači. Virus se dokáže sám šířit, například elektronickou poštou, odkazy v internetových prohlížečích i přes přenosná média. Spyware je program, který, aniž by o tom uživatel věděl, odesílá z počítače konkrétní informace. Mohou to být hesla k účtům, e-maily, ale i číslo kreditní karty. Spyware je však využíván i legální cestou, a to například softwarovými společnostmi. Ty využívají například anonymní informace o tom, jakým způsobem jsou využívány jejich produkty. Díky takové zpětné vazbě mohou zlepšovat své služby.

Existuje velké množství antivirových programů, placených, ale i freewarových. Freewarové antiviry jsou sice ochuzeny o některé dodatečné funkce, které nabízejí verze placené, avšak pro použití v domácích sítích jsou naprosto dostatečné. V žádném počítači by takový program neměl chybět. Microsoft integruje antivirovou ochranu přímo do operačního systému od verze Windows 8. Tento program najdeme pod názvem Windows Defender, uživatel si samozřejmě může vybrat antivirus, zapnutý však zůstává vždy jen jeden.

Antispywarových programů je také hodně a uživatel si může vybrat. Ve Windows obstarává antispywarovou ochranu Windows Defender, který je v něm integrován od verze Windows Vista. Od verze Windows 8 obstarává i ochranu před viry.

Samozřejmě je třeba udržovat takový software aktuální a pravidelně stahovat aktualizované virové a spywarové databáze. Dnešní antiviry zvládají tyto aktualizace spravovat bez zásahu uživatele.

Firewall

Firewall je pomyslná zeď mezi domácí sítí a internetem, která reguluje propustnost komunikace jednotlivých programů. Programy, které potřebují komunikovat skrz, mají vytvořené výjimky. Firewall pracuje na pozadí a kontroluje jednotlivé porty, skrze které komunikují programy se sítí. Ve Windows je integrovaný jako Brána Windows firewall.

Nejen jednotlivé počítače mají integrovanou tuto ochranu. Většina dnešních routerů má také integrovaný firewall. Ten chrání síť proti neoprávněným přístupům z internetu.

3.10.2 Nastavení bezdrátové sítě

Středem domácí sítě je přístupový bod, na který se připojují všechna zařízení v síti. Zde je zároveň propojena kabelová síť s bezdrátovou, tato kombinace je u dnešních domácích sítí nejčastější. Nastavení a správné zabezpečení routeru je tedy velice důležité, a přesto bývá toto často podceňováno.

Pro přístup k routeru slouží jeho IP adresa v lokální síti, kterou lze zjistit z návodu od výrobce, či přímo na štítku zařízení. Tato adresa vypadá například 192.168.0.1, přičemž poslední dvě trojčíslí se mohou podle výrobce lišit. Tuto IP adresu zadáme do webového

prohlížeče a poté se přihlásíme výchozím přihlašovacím jménem a heslem. Tyto přihlašovací údaje je potřeba změnit, aby neměl k nastavení přístup nikdo jiný.

SSID

Jako první je třeba povolit vysílání bezdrátového signálu a nastavit SSID (Service Set ID). To je název přístupového bodu a identifikátor bezdrátové sítě, ke které se zařízení připojují. Vysílání SSID může být buďto povoleno nebo zakázáno. Pokud bude povoleno, všechna zařízení v dosahu síť uvidí pod tímto názvem. Pokud bude vypnuto, nikdo název neuvidí a síť bude skryta. V tom případě musí uživatel znát tento název, aby se k takové síti mohl připojit.

Možnosti vysílače

Prvně se nastavuje vysílací frekvence rádiového signálu. Většinou je to frekvence 2,4 GHz, u novějších routerů je to i 5 GHz frekvence, které vysílá router současně.

Dále se dá ručně nastavit kanál, kterých je na každé frekvenci vyhrazeno více. Uživatel si může ručně nastavit číslo kanálu, který bude používat nebo je možné vybrat možnost auto. V takovém případě router skenuje, jaké sítě vysílají v jeho dosahu a na jakém kanálu. Automaticky pak vybírá nejméně vytížený kanál.

Jako další je potřeba nastavit šířku vysílaného pásma, která se u 2,4 GHz frekvence volí mezi 20 a 40 MHz. U 5 GHz frekvence je to 20, 40 a 80 MHz. Čím větší šíře pásma je nastavena, tím méně kanálů je možné na dané frekvenci střídat. V hustě obydlených oblastech, kde se překrývá větší množství jednotlivých Wi-Fi sítí, je tedy lepší nastavit menší šířku pásma, díky které bude signál méně rušen a připojení bude stabilnější.

Šifrování

Dále je třeba nastavit šifrování přenášených dat. V dnešní době je nejpoužívanější a nejdokonalejší šifrovací protokol WPA2, který vychází z předchozího WPA. Prostřednictvím této metody je kontrolován přístup nového zařízení do sítě a všechna přenášená data jsou šifrována klíčem. WPA2 používá pro šifrování velmi pokročilý algoritmus AES (Advanced Encryption Standard). Mezi starší a již překonané protokoly patří například protokol WEP.

WPA2-PSK

Pre-Shared Key je přístupové heslo, které je potřeba vyplnit při přihlašování nového zařízení do sítě. Je vhodné zvolit dostatečně dlouhé heslo, které obsahuje velká a malá písmena, číslice a nejlépe i takzvané speciální znaky.

MAC filtr

K ještě vyššímu zabezpečení existuje možnost použití MAC filtru. Ten kontroluje MAC adresy zařízení, která se pokouší připojit k síti. MAC adresa je jedinečný identifikátor síťového zařízení, který je mu přiřazen již ve výrobě. Říká se jí také adresa fyzická.

V nastavení routeru je tedy možno nastavit seznam MAC adres zařízení, která bude přístupový bod kontrolovat při připojování zařízení do sítě. Tento filtr může být vypnutý, pokud je však zapnutý, jsou na výběr dvě možnosti jeho použití. Seznam MAC adres může sloužit jako seznam pouze těch zařízení, kterým je přístup do sítě povolen. V opačném případě je možno konkrétním zařízením přístup do sítě zakázat.

MAC adresa mobilních zařízení, například u Androidu, se dá zjistit v nastavení WiFi nebo v informacích o zařízení. U zařízení s operačním systémem Windows je adresa napsána ve správci zařízení, přímo u konkrétní síťové karty, ethernetové, či bezdrátové. Nejrychlejší způsob je spuštění příkazového řádku a vložení příkazu „getmac /v“ nebo „ipconfig /all“.

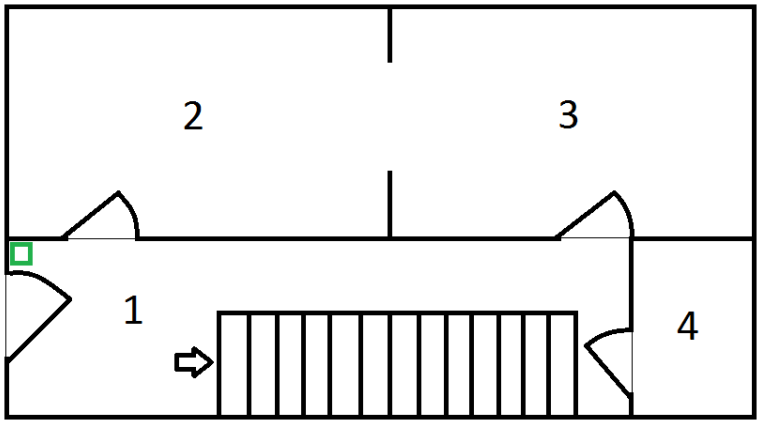
(Horák 2011), (Horák, Keršláger 2013), (Sosinsky 2011)

4 Vlastní práce

4.1 Zmapování domu

Návrh domácí počítačové sítě je vytvořen pro starší malý rodinný domek v Praze. Tato síť je vytvořena kombinací kabelové sítě realizované pomocí UTP kabelu a bezdrátového Wi-Fi pokrytí. Do domu je přivedena internetová přípojka od poskytovatele UPC s maximální poskytovanou rychlostí připojení k internetu 200 Mb/s. Dům má dvě nadzemní podlaží, tedy přízemí a první patro. Celý dům je zděný z cihel.

V prvním nadzemním podlaží se nachází obývací pokoj, kuchyň, koupelna a chodba. V chodbě jsou schody do druhého podlaží. Přípojka k UPC internetu a televizi se nachází v chodbě, v blízkosti vstupních dveří. V návrhu je tato přípojka vyobrazena v podobě zeleného čtverce.

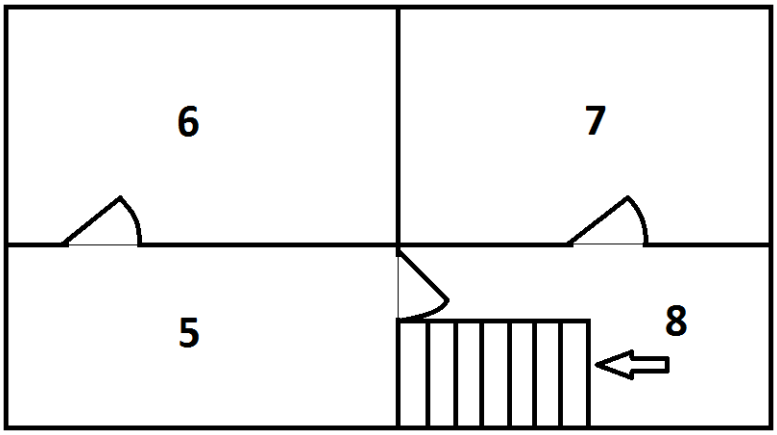


Obrázek 10: 1NP – Půdorys

1. Chodba
2. Obývací pokoj
3. Kuchyň
4. Koupelna a WC

□ Přípojka UPC

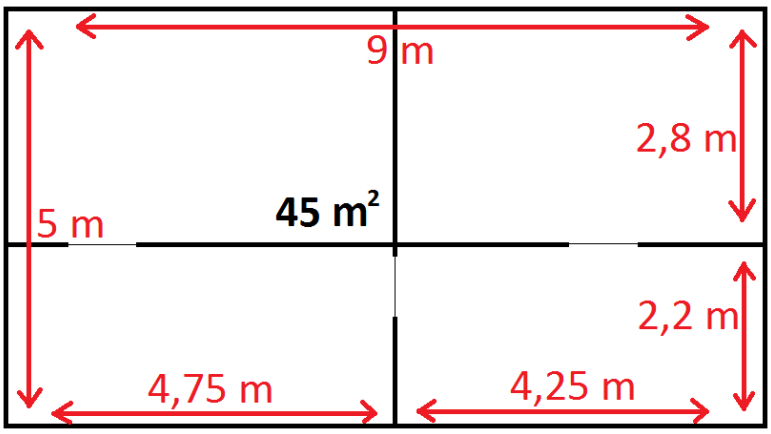
V druhém podlaží se nachází pracovna, ložnice, dětský pokoj a chodba, do které vedou schody z prvního podlaží.



Obrázek 11: 2NP – Půdorys

5. Pracovna
6. Ložnice
7. Dětský pokoj
8. Chodba

Celý dům byl změřen s následujícími výsledky. Rozloha jednoho podlaží je 45 metrů čtverečních, obě patra mají stejné rozměry. Celková plocha pro pokrytí bezdrátovou Wi-Fi sítí je 90 čtverečních metrů.



Obrázek 12: Rozměry jednoho podlaží

4.2 Souhrn požadavků klienta

Klient koupil starší malý rodinný domek v Praze, do kterého se bude stěhovat. Jelikož dům odkoupil již po rekonstrukci, požaduje vytvoření domácí sítě s co nejmenším finančním zatížením a s minimálními stavebními zásahy. Nepřeje si tedy, aby byly síťové rozvody ve zdech. Vysekávání rozvodů do zdí by bylo finančně nákladné a oddálilo by termín možného nastěhování. Vybudování funkční sítě požaduje klient za co nejkratší dobu a celkové náklady na síť včetně úložiště nesmí přesáhnout 10 000 Kč. Klient si přeje naplno využít maximální propustnost internetové přípojky, zakoupí si tedy paušál s rychlostí 200 Mb/s pro připojení k internetu.

Mezi další požadavky patří vysoká propustnost kabelové lokální počítačové sítě. Klient počítá s využitím domácího síťového úložiště, a to nejen pro zálohování rodinných fotografií a dokumentů. Úložiště by rád využíval jako multimediální server, ze kterého by rád sdílel obsah pro svou chytrou televizi.

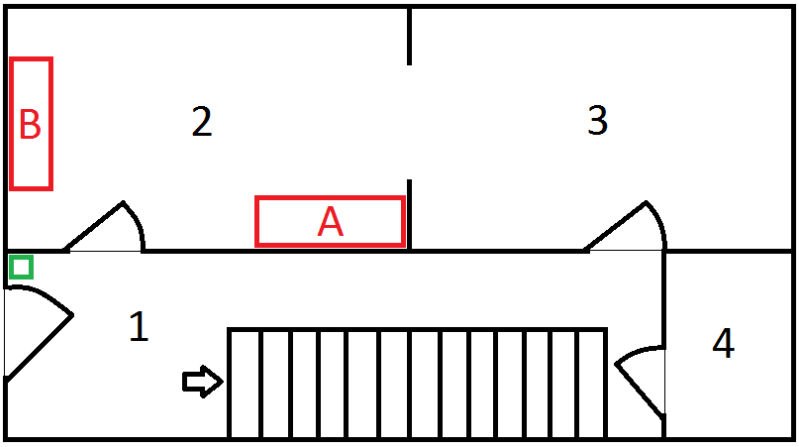
Jelikož k multimediálním souborům budou přistupovat i další členové domácnosti, a to z různých zařízení, propustnost bezdrátové Wi-Fi sítě musí být také vysoká. Bezdrátovým signálem chce mít samozřejmě pokrytý celý dům

Zároveň by rád využíval toto úložiště jako vlastní cloud, do kterého by mohl přistupovat zvenčí. Klient nejčastěji pracuje doma na All in One počítači a mimo domov používá smartphone nebo skladný notebook. Přístup k datům bez nutnosti kopírování na fyzická přenosná média mu značně ušetří čas. Jelikož se však jedná o důležitá data, požaduje automatickou zálohu souborů. Minimální využitelná požadovaná kapacita úložiště je 2 TB.

Domácnost má tři členy, jsou to klient, jeho žena a šestiletý syn. Všichni budou přistupovat do domácí sítě z vlastních zařízení. Oba rodiče mají vlastní smartphone, žena má i druhý služební. Žena má také svůj notebook. V domě bude jeden All in One počítač a v nejbližší době další stolní počítač. Syn má pouze smartphone, ale do budoucna je třeba počítat s tím, že bude mít vlastní notebook.

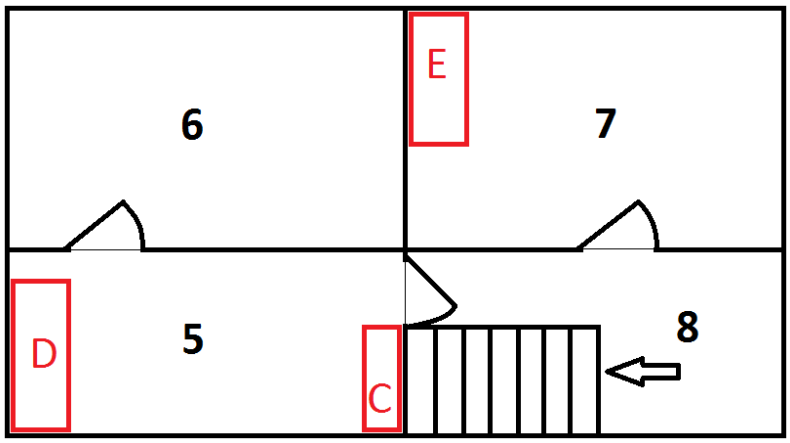
Klient chce mít ve své kanceláři tiskárnu. Žena a v budoucnu i syn by také rádi využívali možnost tisku. Klient však z důvodu šetření místa i financí chce mít pouze jednu tiskárnu. Přeje si tedy využít možností tiskárny síťové, na kterou budou mít přístup všichni a dokumenty na ni budou moci posílat odkudkoliv z domu.

Následující obrázky zobrazují rozmístění jednotlivých míst v domě, ze kterých se bude přistupovat do domácí počítačové sítě.



Obrázek 13: 1NP – Zařízení

V přízemí se budou hlavní zařízení vyskytovat v obývacím pokoji (2). Na místě označeném písmenem A bude pracovní stůl, na který by klient v budoucnu rád umístil stolní počítač, který by mohla využívat jeho žena a syn, než bude mít vlastní notebook. Na místě označeném písmenem B bude televizní stolek, na kterém bude stát chytrá televize.



Obrázek 14: 2NP – Zařízení

V druhém podlaží jsou zařízení soustředěna do pracovny (5). Na místě označeném písmenem C bude skříňka, na které bude umístěna tiskárna. Zadavatel si nepřeje plýtvat místem na svém pracovním stole. Jeho pracovní stůl bude umístěn na místě označeném

písmenem D. Na tomto stole bude jeho soukromý All in One počítač. Písmeno E v dětském pokoji (7) označuje pracovní stůl. Na něm bude v budoucnu umístěn notebook pro syna.

4.3 Hardware

Na klienta doléhá velká finanční vytíženost z nedávné koupi domu. Do budoucna sice plánuje nákup stolního PC a poté i notebooku pro syna, nyní se však zaměřil na vybudování stabilní sítě.

Při budování sítě by rád využil router z předchozí domácnosti, který je téměř nový, a tak svými parametry splňuje požadavky pro stavbu této domácí počítačové sítě. Největší část nákladů bude směřována k nákupu domácího síťového úložiště NAS a samozřejmě kabelů a zásuvek.

Jako poskytovatel internetu se nabízí společnost UPC, která má díky předchozímu majiteli v domě přípojku. Poskytovatel internetu nabízí ke svým tarifům pronájem Wi-Fi routeru v ceně měsíčního paušálu.

Hardware pro realizaci sítě

Router z předchozí domácnosti:

TP-LINK Archer C2 AC750

- 4 LAN porty ethernet 10/100/1000Base-T
- IEEE 802.11a/b/g/n/ac dual band
- USB 2.0 port + printserver

Kabelový modem a router pronajatý od společnosti UPC:

Compal CH7465LG

- 4 LAN porty ethernet 10/100/1000Base-T
- IEEE 802.11b/g/n/ac dual band

Dle specifikací routerů a dle požadavků klienta na vysokou propustnost domácí sítě bude celá síť postavena pro přenosovou rychlost 1000 Mb/s. Pro kabelové síťové rozvody bude použit UTP kabel kategorie 6. V případě budoucí potřeby zvyšování propustnosti sítě pak nebude nutné měnit kabelové rozvody.

Kabel bude pořízen v padesátimetrové roli, koncovky RJ 45 zvlášť. Pomocí krimpovacích kleští se pak na nastříhaný kabel nacvakají podle potřeby. Dále bude třeba zakoupit dvě síťové zásuvky pro konektory RJ 45 ve verzi na omítku, aby nebylo třeba sekat do zdi.

Pro zálohu dat a využívání funkcí multimediálního serveru byl vybrán NAS dle několika požadavků. První požadavek byla gigabitová síťová karta kvůli využití rychlosti sítě. Dále byla nutná přítomnost minimálně dvou šachet pro pevné disky a možnost zrcadlení, RAID 1, kvůli záloze dat při případném selhání jednoho z disků. Samozřejmě také funkce domácího cloudu s přístupem zvenčí.

Jako nejlevnější varianta pro splnění všech požadavků byl vybrán tento NAS:

QNAP TS-228

- 1 Gb/s LAN
- 2 šachty pro pevné disky
- RAID 0, 1, JBOD
- myQNAPcloud pro připojení mimo lokální síť

NAS je prodáván samostatně bez disků, disky bude tedy třeba koupit zvlášť. Klient požaduje minimální kapacitu úložiště 2 TB. Pro použití RAID 1 je třeba dvou stejných disků. S ohledem na cenu byly vybrány dva disky vhodné pro použití v serverech NAS s kapacitou 2 TB.

Vybrané disky:

2x WD Red 2TB

Následující tabulka vyčísluje celkové náklady na realizaci domácí sítě:

Zařízení	Typ	Množství	Cena za kus
NAS	QNAP TS-228	1	3 393 Kč
Harddisk	WD Red 2 TB	2	2 480 Kč
Kabel	Datacom UTP, cat 6, 50 m	1	603 Kč
Koncovka RJ 45	Datacom RJ 45, cat 6, 10 ks	1	117 Kč
Zásuvka	Netrack RJ 45, cat 6	2	36 Kč
Celkem			**9 145 Kč**

Tabulka 2: Finanční náklady

(Ceny převzaty z webu Heureka)

Routery není třeba kupovat, v tabulce tedy nejsou zaneseny. Klient si přál realizovat síť s maximálními náklady na hardware ve výši 10 000 Kč, do těchto nákladů se návrh vešel.

Hardware, který se bude k domácí síti připojovat

K domácí síti se budou připojovat následující zařízení. Klient má All in One počítač, smartphone a notebook. První zařízení bude připojeno UTP kabelem, ostatní dvě budou připojena bezdrátově. Žena má notebook, soukromý smartphone a služební smartphone. Syn má pouze smartphone. Tato zařízení budou připojena bezdrátově. V obývacím pokoji bude chytrá televize, připojena UTP kabelem. V pracovně bude UTP kabelem připojen NAS. Tiskárna v pracovně se bude připojovat přímo k routeru pomocí USB rozhraní.

Zařízení, která budou připojená kabelem a rychlost připojení síťové karty:

- **Smart TV LG 50LF652V** 100 Mb/s
- **HP ProOne 400 G2 AIO** 1 000 Mb/s
- **NAS QNAP TS-228** 1 000 Mb/s

Zařízení, která budou připojená bezdrátově, jejich majitel a standard připojení:

- **Samsung Galaxy S4 mini** Syn 802.11a/b/g/n
- **Samsung Galaxy A3** Žena 802.11b/g/n
- **iPhone 4s** Žena 802.11b/g/n

• **HP Pavilion 15**	Žena	802.11b/g/n
• **Samsung Galaxy S6**	Klient	802.11a/b/g/n/ac
• **Dell Inspiron 11z touch**	Klient	802.11b/g/n

Ze seznamu je vidět, že všechna bezdrátová zařízení podporují standard minimálně 802.11n. V nastavení routerů se tedy budou moci ostatní standardy opomenout a nastavit vysílání na režim 802.11n/ac. Dále je patrné, že na 5 GHz Wi-Fi se budou připojovat dvě zařízení, smartphone klienta a syna.

Poslední zařízení, které se bude k síti připojovat je tiskárna. Klient má k dispozici pouze tiskárnu s rozhraním USB. Je to tiskárna Canon Pixma MX375. Uvažuje tedy o koupi tiskárny síťové.

4.4 Návrh sítě

Návrh sítě je tvořen postupně od přípojky poskytovatele, přes přízemí až po první patro domku. Vzhledem k požadavku klienta a dispozici domu budou kvůli dostatečnému pokrytí použity dva Wi-Fi routery, každý pro pokrytí jednoho patra.

Router pronajatý od společnosti UPC bude v přízemí. Používán bude za prvé jako kabelový modem, do kterého bude přiveden koaxiální kabel od internetové přípojky. Tento router lze používat zároveň jako access point. Za druhé bude tedy použit jako přístupový bod pro bezdrátové připojení v přízemí.

Položení kabeláže

Jako první je potřeba zvolit vhodnou pozici pro umístění routeru. Kvůli dobrému Wi-Fi pokrytí je ideální pozice ve středu podlaží. Pro jeho umístění byl vybrán pracovní stůl (A) v obývacím pokoji, který leží v téměř ideálním středu podlaží.

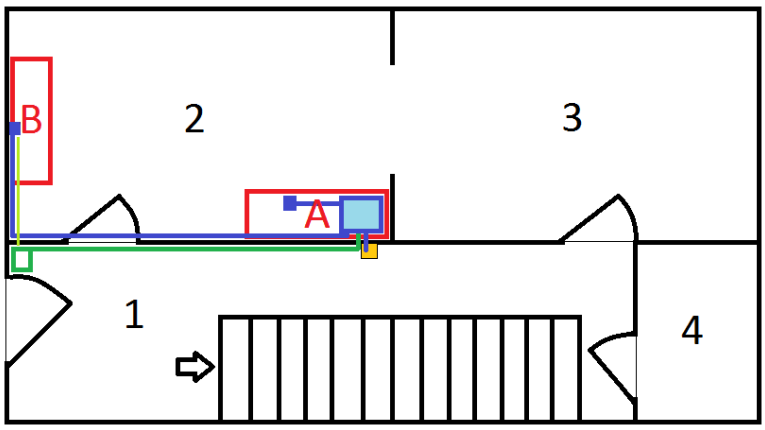
Od přípojky UPC povede internetový koaxiální kabel pod prahem a dále v podlahové liště podél zdi chodby. Na následujícím návrhu je značen zelenou barvou. V úrovni pracovního stolu bude provrtán otvor a koaxiál bude vyveden přímo za stolem, na kterém bude router stát. Koaxiál pro připojení kabelové televize je znázorněn na následujícím obrázku světle zelenou barvou. Ten vede od přípojky skrz zeď přímo do obývacího pokoje k televiznímu stolku.

Otvor za pracovním stolem bude také použit pro UTP kabel, který propojí přízemí a první patro. Jeden z ethernetových portů UPC routeru bude tedy použit pro propojení s druhým routerem v prvním patře.

Druhý ethernetový port bude použit pro UTP kabel, který povede podél místnosti v podlahových lištách a pod prahem až k televiznímu stolku. Za ním bude umístěna síťová zásuvka pro připojení chytré televize.

Třetí port zůstane prázdný, bude však připravený pro budoucí zapojení stolního počítače, který se klient chystá zakoupit. Čtvrtý ethernetový port zůstane nevyužitý jako rezerva pro případnou budoucí potřebu rozšiřování sítě. Například by mohl sloužit pro zavedení síťové zásuvky v kuchyni.

UTP kabel, který povede do prvního patra, bude v chodbě veden po zdi přímo ke stropu v liště. Přímo nad otvorem ve zdi na úrovni pracovního stolu na straně chodby, bude provrtán otvor stropem do prvního patra. Stropní otvor je znázorněn žlutým čtvercem, UTP kabely jsou modré.



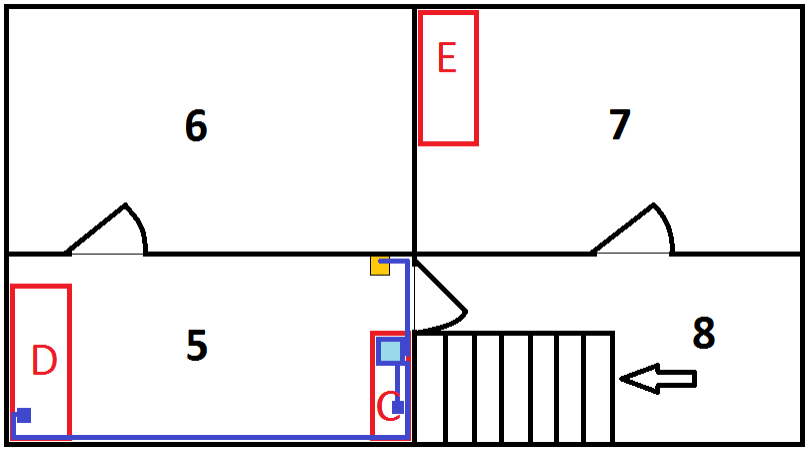
Obrázek 15: 1NP – Rozvody

V prvním patře bude umístěn router na podobném místě. Aby nemusel být v ložnici, bude umístěn na skříňce (C), za dveřmi do pracovny. UTP kabel k němu povede od stropního otvoru pod dveřním prahem a v podlahové liště. Tím vyplníme první ethernetový port horního routeru.

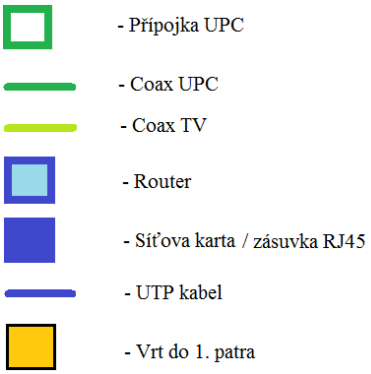
Od routeru povede UTP kabel z druhého ethernetového portu v podlahových lištách podél zdi až za pracovní stůl (D). Tam bude síťová zásuvka pro připojení klientova pracovního All in One počítače.

Vedle routeru bude umístěna tiskárna a v odvětrané skříňce pod ním bude NAS. NAS bude připojen do třetího ethernetového portu. Kvůli snížení rozpočtu, bude použita klientova stávající tiskárna s rozhraním USB. Tím klient ušetří za síťovou tiskárnu a zároveň zanechá jeden volný ethernetový port, pro případné budoucí rozšiřování sítě. Například pro síťovou zásuvku v dětském pokoji.

Pro připojení tiskárny pomocí rozhraní USB, a zároveň splnění klientových požadavků na síťovou tiskárnu, použijeme USB vstup horního routeru. Tiskárnu připojíme pomocí USB přímo k routeru, který nabízí funkci printserver, sdílení připojené tiskárny v lokální síti.



Obrázek 16: 2NP – Rozvody



Obrázek 17: Legenda

4.5 Nastavení a zabezpečení domácí sítě

Compal UPC

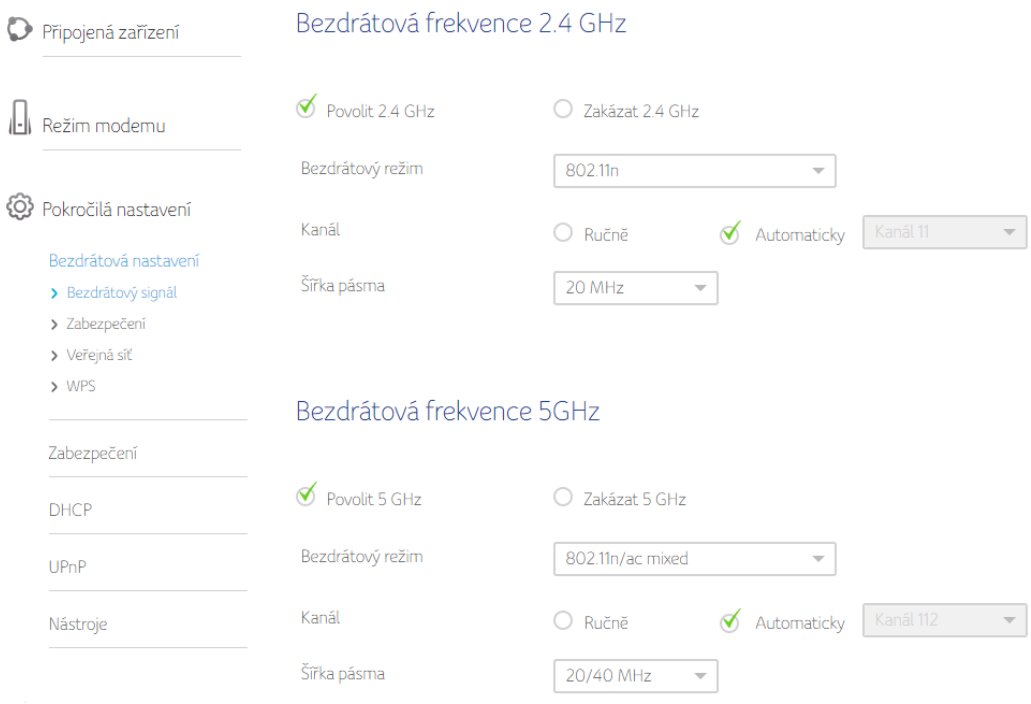
Jako router v přízemí, bude použit Compal od UPC. Ten bude plnit funkci kabelového modemu, routeru a bezdrátového přístupového bodu. Zároveň to bude zařízení, které oddělí síť WAN od domácí sítě LAN.

Jeho IP adresa bude 192.168.0.1 a zapnut na něm bude DHCP server a firewall. Kabelem do něj bude připojena televize a router v druhém patře. Zároveň bude zajišťovat bezdrátové pokrytí v přízemí.

Pro přihlášení do administrace routeru je třeba použít jeho IP adresu. Ta se vloží do webového prohlížeče ve formátu http://192.168.0.1. Po prvním přihlášení bude změněno výchozí přihlašovací jméno a heslo k administraci. Původní přihlašovací údaje jsou k nalezení v balení routeru od UPC a na spodní straně routeru samotného.

Zařízení Compal se může používat ve dvou režimech, a to v režimu modem a režimu router. Režim modem se používá v případě využití vlastního routeru, který bude směrovat provoz až za modemem. Zde bude použit režim router, díky tomu není třeba kupovat další aktivní síťové zařízení. Využity budou tedy všechny funkce routeru.

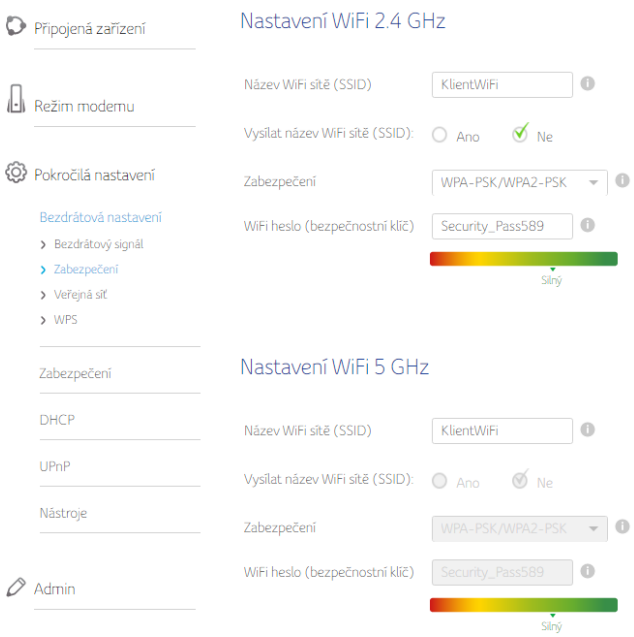
Dále je třeba nastavit bezdrátový signál. Ten lze nalézt v bočním menu v záložce Pokročilá nastavení / Bezdrátová nastavení / Bezdrátový signál. Na následujícím obrázku je vidět nastavení vysílání.



Obrázek 18: Compal – Nastavení vysílání

Poté se nastaví zabezpečení bezdrátové sítě v další záložce zabezpečení. Viz následující obrázek.

Název sítě zůstane kvůli lepšímu zabezpečení skrytý. Zabezpečení bude zvoleno WPA2, které je v současnosti nejbezpečnější. Dále bude zvoleno dostatečně silné heslo pro připojení k bezdrátové síti. Níže je možnost použití filtrování MAC adres v bezdrátové síti. To znamená, že zařízení budou filtrována pouze v bezdrátové síti, po připojení kabelu nebude hrát MAC filtr roli. Zde není třeba zjišťovat MAC adresy ručně, stačí se k zařízení připojit pomocí Wi-Fi a v administraci routeru vyhledat připojená zařízení. Všechna zařízení, kterým bude přístup povolen, se pak dají vybrat přímo ze seznamu. Příslušné MAC adresy budou tedy vloženy do tabulky a jako možnost nastavení MAC filtru bude nastaveno povolit přístup těmto zařízením. Tím dostanou do sítě přístup pouze uvedená zařízení.



Obrázek 19: Compal – Bezdrátové zabezpečení

V další záložce veřejná síť je možnost nastavení Wi-Fi sítě pro hosty. Díky ní nebudou mít hosté přístup do lokální sítě, ve které jsou sdílené soubory a tiskárny. Hostům bude umožněn pouze přístup na internet, navíc bez nutnosti přidávání jejich MAC adres do tabulky v routeru. Poslední možnost v sekci bezdrátová nastavení je WPS. WPS je možnost připojení k Wi-Fi síti bez nutnosti znát heslo. Na routeru je WPS tlačítko, které je možné zmáčknout při připojování zařízení. Zařízení se pak připojí bez žádosti o zadání hesla. Je možné nastavit i WPS pin, který bude sloužit místo hesla. V nastavení routeru bude ponecháno zapnuté pouze WPS tlačítko.

V záložce Pokročilá nastavení / Zabezpečení lze nastavit firewall, který je ve výchozím nastavení zapnut. Firewall bude ponechán zapnutý. Dále je zde možné nastavit filtrování MAC adres pro celou síť, tedy i kabelovou. Tento filtr se nastavovat nebude, MAC adresy v bezdrátové síti jsou již filtrovány a k připojení ke kabelové síti je třeba fyzický přístup do domu.

V záložce DHCP je nastavení přidělování IP adres v lokální síti. DHCP server zůstane zapnutý a přidělované adresy budou začínat adresou 192.168.0.10, o jeden řád výš, než je adresa routeru. V další záložce bude povoleno používání protokolů UPnP, kvůli přenosu multimediálních souborů v síti. Na těchto protokolech staví standard DLNA, používaný pro přehrávání síťového obsahu na chytrých televizích, či jiných zařízeních.

TP-LINK Archer

TP-LINK je potřeba nastavit jako přístupový bod, kterým bude rozšířena Wi-Fi síť z přízemí. Před zapojením je třeba ho správně nastavit tak, aby se obě Wi-Fi sítě chovaly jako jedna. Po připojení bezdrátového zařízení, například smartphonu, v patře k hornímu routeru a následnému přesunutí smartphonu do přízemí je třeba, aby se smartphone automaticky přepojil na router v přízemí. Všechna připojená zařízení by si tedy měla vždy vybrat výhodnější přístupový bod, během jejich pohybu domem, bez zásahu uživatele.

Pro přihlášení do administrace routeru Archer použijeme adresu http://192.168.0.1. Přihlašovací údaje jsou výrobcem nastaveny na admin / admin. Po přihlášení do administrace je třeba v záložce LAN nastavit IP adresu, která by měla být nastavena na 192.168.0.2. To proto, aby byla mimo rozsah přidělovaných adres DHCP serverem routeru Compal. Po uložení se bude k administraci přihlašovat pod adresou http://192.168.0.2. Jako další je třeba vypnout DHCP server. IP adresy bude přidělovat pouze router Compal, od kterého je Archer bude přebírat. V záložce DHCP settings tedy bude zaškrtnuta možnost Disable DHCP Server.

Po nastavení těchto zásadních možností je třeba nastavit bezdrátové vysílání. To bude nastaveno identicky podle routeru Compal v přízemí.

- Zapnuta 2,4 a 5 GHz Wi-Fi (Pro obě frekvence platí stejná nastavení)
- Šířka pásma pro 2,4 GHz: 20 MHz
- Šířka pásma pro 5 GHz: 20/40 MHz
- Mód vysílání: 802.11n/ac mixed
- Nastavené SSID: KlientWiFi a zakázané jeho vysílání
- Zvolené zabezpečení: WPA2
- Nastavené heslo pro přístup: Security_Pass589

Síť pro hosty bude vysílána pouze v přízemí, firewall bude zajišťovat router Compal.

Dále je třeba nastavit sdílení tiskárny. Tiskárna se připojí pomocí USB portu k routeru Archer, v administraci v záložce USB Settings / Printserver je třeba povolení printserveru. Pak už bude stačit nainstalovat správné ovladače tiskárny všem počítačům.

Po tomto nezbytném nastavení stačí router Archer zapojit do domácí sítě. Do routeru v prvním patře bude přiveden UTP kabel z routeru Compal. Zapojen bude do zdířky LAN, zdířka WAN zůstane při tomto způsobu využití routeru nevyužitá.

Nastavení NAS

Do horního routeru Archer bude připojen NAS QNAP. Do NASu budou nejprve vloženy harddisky, zapojené v režimu RAID 1. Díky tomu budou všechna data chráněna před havárií disku. Pokud havaruje jeden disk, data jsou zálohována na druhém, stačí pak dokoupit disk nový a při stejném zapojení budou data znovu zrcadlena na disk druhý.

Poté bude NAS připojen UTP kabelem k routeru. Pomocí aplikace Qfinder se počítač připojí k administraci NASu. Je třeba se přihlásit výchozím jménem a heslem. Poté se na dva nové disky nainstaluje firmware.

Po nainstalování firmwaru a původním nastavení NASu je možné nastavit přístupy pro jednotlivé uživatele. Uživatelské prostředí je velmi přehledné a podobné známým operačním systémům. Na výběr jsou instalace jednotlivých balíčků, jako například centrum stahování, vysílání médií pomocí DLNA, sdílení složek v síti, printserver nebo synchronizace se známými cloudovými službami jako je například Microsoft OneDrive, Google Disk, iCloud,

DropBox a další. Mezi další funkce patří například správa IP kamer a možnost vybudování vlastního domácího kamerového systému.

Veškerá nastavení proběhnou po realizaci sítě za přítomnosti klienta, kvůli zaškolení před jeho budoucí samostatnou správou NASu.

5 Závěr

V této práci byla navržena domácí počítačová síť, která bere v potaz požadavky klienta, pro kterého byla navržena. Klient si přál navrhnout realizaci sítě s minimálními stavebními úpravami. Pro realizaci sítě dle návrhu bude třeba vrtat do zdi pouze dvakrát, zbytek kabelů bude veden pod dveřními prahy a v existujících podlahových lištách podél zdí. Mezi další požadavky patřil nákup a využití domácího síťového úložiště a síťové tiskárny. Celkové náklady na realizaci sítě nesměly překročit stanovenou hranici 10 000 Kč. Síť byla navržena s celkovými potřebnými finančními náklady pro její realizaci 9 145 Kč. Pro realizaci sítě byly použity dva routery, každý pro bezdrátové pokrytí jednoho patra. Síťové rozvody byly vedeny pomocí UTP kabelu v kombinaci s bezdrátovou Wi-Fi sítí. Oba dva routery byly popsány včetně jejich správného zapojení, nastavení a zabezpečení.

Jako vedlejší cíl této práce byla vytvořena rešerše o lokálních počítačových sítích a historie těchto sítí. Rešerše se týká jednotlivých typů sítí, druhů topologií a jejich výhodami a nevýhodami. Dále byly popsány referenční modely OSI a TCP/IP, komunikační protokoly počítačových sítí a jednotlivé síťové standardy. Vyjmenovány byly jednotlivé aktivní i pasivní hardwarové síťové prvky. Zmíněny byly také možnosti zabezpečení lokálních počítačových sítí.

6 Seznam použitých zdrojů

1. *Heureka* [online]. Liberec: Rockaway, ©2000-2017 [cit. 2017-03-12]. Dostupné z: https://www.heureka.cz
2. HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. Dotisk 5. aktualizovaného vydání. Brno: Computer Press, 2013. ISBN 978-80-251-3176-3.
3. HORÁK, Jaroslav. *Vytváříme domácí bezdrátovou síť*. Brno: Computer Press, 2011. ISBN 978-80-251-2977-7.
4. KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.
5. SOSINSKY, Barrie. Mistrovství - Počítačové sítě. In: *Https://books.google.cz* [online]. Brno: Computer Press, 2011 [cit. 2017-03-12]. Dostupné z: https://books.google.cz/books?isbn=8025139166
6. Standard pro 10 Gigabit Ethernet po metalické kabeláži (10GBase-T) dospěl do finále. *Svět sítí* [online]. Praha: Josef Ptáček, 2006 [cit. 2017-03-12]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Standard-pro-10-Gigabit-Ethernet-po-metalicke-kabelazi-10GBase-T-dospel-do-finale-1962006

7 Přílohy

7.1 Seznam obrázků

7.2 Zdroje obrázků

[Obrázek 1] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. In: *Https://books.google.cz* [online]. Brno: Computer Press, 2013 [cit. 2017-03-12]. Dostupné z: https://books.google.cz/books?isbn=8025143961

[Obrázek 2] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. In: *Https://books.google.cz* [online]. Brno: Computer Press, 2013 [cit. 2017-03-12]. Dostupné z: https://books.google.cz/books?isbn=8025143961

[Obrázek 3] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. In: *Https://books.google.cz* [online]. Brno: Computer Press, 2013 [cit. 2017-03-12]. Dostupné z: https://books.google.cz/books?isbn=8025143961

[Obrázek 4] SOSINSKY, Barrie. Mistrovství - Počítačové sítě. In: *Https://books.google.cz* [online]. Brno: Computer Press, 2011 [cit. 2017-03-12]. Dostupné z: https://books.google.cz/books?isbn=8025139166

[Obrázek 5] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. In: *Https://books.google.cz* [online]. Brno: Computer Press, 2013 [cit. 2017-03-12]. Dostupné z: https://books.google.cz/books?isbn=8025143961

[Obrázek 6] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. In: *Https://books.google.cz* [online]. Brno: Computer Press, 2013 [cit. 2017-03-12]. Dostupné z: https://books.google.cz/books?isbn=8025143961

[Obrázek 7] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. In: *Https://books.google.cz* [online]. Brno: Computer Press, 2013 [cit. 2017-03-12]. Dostupné z: https://books.google.cz/books?isbn=8025143961

[Obrázek 8] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. In: *Https://books.google.cz* [online]. Brno: Computer Press, 2013 [cit. 2017-03-12]. Dostupné z: https://books.google.cz/books?isbn=8025143961

[Obrázek 9] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. In: *Https://books.google.cz* [online]. Brno: Computer Press, 2013 [cit. 2017-03-12]. Dostupné z: https://books.google.cz/books?isbn=8025143961

[Obrázek 10 – 19] Autor

7.3 Seznam tabulek

7.4 Zdroje tabulek

[Tabulka 1 – 2] Autor