Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Domácí počítačová síť

Martin Uher

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Martin Uher

Systémové inženýrství

Název práce

Domácí počítačová síť

Název anglicky

Computer network at home

Cíle práce

Cílem této bakalářské práce je, na základě získaných poznatků z odborné literatury, sestavit domácí počítačovou síť. Teoretická část je věnována využívaným prvkům, možným topologiím, protokolům, standardům apod. Dále zde bude charakteristika řešení zabezpečení počítačové sítě a jejich porovnání. V praktické části bude charakterizována reálná domácnost, kde je síť zkonstruována. Následně zde bude popsán výběr a nastavení prvků, konstrukce sítě, nastavení zabezpečení a připojení dalších zařízení domácnosti do sítě.

Metodika

Metodikou práce bude analýza a následná syntéza získaných poznatků o tématu z odborné literatury. Následně budou porovnávána možná technologická řešení.

Doporučený rozsah práce

40

Klíčová slova

LAN, WLAN, zabezpečení sítě, síťové prvky, síťové standardy

Doporučené zdroje informací

HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3

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

NORTHCUTT, Stephen. Inside network perimeter security. 2nd ed. Indianapolis, Ind.: Sams Pub., c2005. ISBN 0672327376

SPURNÁ, Ivona. Počítačové sítě: praktická příručka správce sítě. Kralice na Hané: Computer Media, c2010. ISBN 978-80-7402-036-0

Předběžný termín obhajoby

2015/16 LS – PEF

Vedoucí práce

Ing. Tomáš Vokoun

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 21. 10. 2016

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 10. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 27. 11. 2016

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Domácí počítačová síť" jsem vypracoval(a) 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(ka) 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(a) bych touto cestou poděkoval(a) Ing. Tomášovi Vokounovi za odborné vedení, cenné rady a užitečné připomínky pro vypracování této bakalářské práce.

Domácí počítačová síť

Souhrn

Cílem této práce je konstrukce domácí počítačové sítě. Jsou charakterizovány síťové prvky, používané protokoly a technologie, které se používají při stavbě domácí počítačové sítě. Dále jsou charakterizovány možnosti zabezpečení domácí sítě. V praktické části jsou uvedeny vybrané síťové prvky včetně konfigurace prvků a zařízení. Následně jsou uvedeny zvolené možností zabezpečení domácí sítě. Dále je provedeno měření přenosové rychlosti technologií a jejich porovnání. Na základě výsledků a dalších křitérií je vytvořeno doporučení té nejvhodnější pro stavbu domácí počítačové sítě.

Klíčová slova: LAN, WLAN, zabezpečení sítě, síťové prvky, síťové standardy

Computer network at home

Summary

The goal of this thesis is to build computer network at home. There are described network elements, network protocols and technologies used to build local area networks. There are also described possible network security options. In practical part, there are described used network elements and configuration of network elements and devices. Then there are described used network security options. Hereafter, there is tested bandwidth of used technologies and then they are compared. Based on results of comparison and other criteria, the recommendation, of which technology is the best to use in computer network at home, is made.

Keywords: LAN, WLAN, network protection, network elements, network standards

Obsah

1 Úvod 10

2 Cíl práce a metodika 12

2.1 Cíl práce 12

2.2 Metodika 12

3 Teoretická východiska 13

3.1 Síťové prvky 13

3.1.1 Aktivní síťové prvky 13

3.1.2 Pasivní síťové prvky 14

3.2 Topologie sítě 17

3.3 Síťové protokoly 19

3.3.1 ISO/OSI model 19

3.3.2 TCP/IP model 20

3.3.3 Aplikační vrstva 21

3.3.4 Transportní vrstva 21

3.3.5 Síťová vrstva 22

3.3.6 Vrstva síťového rozhraní 25

3.4 Síťové standardy 26

3.4.1 Ethernet 26

3.4.2 WiFi 27

3.4.3 PLC (Power Line Communication) 28

3.5 Zabezpečení sítě 29

3.5.1 SPI Firewall 29

3.5.2 Denial of Service útoky 30

3.5.3 Filtrování podle MAC adres 31

3.5.4 DMZ (De-Militarized Zone) 31

3.5.5 IDS a IPS 32

3.5.6 Zabezpečení WiFi provozu 32

4 Vlastní práce 35

4.1 Konstrukce sítě 35

4.2 Nastavení zabezpečení 37

4.3 Testování technologií 38

4.3.1 Charakteristika testovacích programů a podmínek testování 38

4.3.2 Provedení měření 41

4.3.3 Obecné doporučení 49

5 Výsledky a diskuse 50

6 Závěr 52

7 Seznam použitých zdrojů 53

8 Přílohy 55

Seznam obrázků

Obrázek 1 - Schéma STP kabelu 14
Obrázek 2 - Schéma ScTP kabelu 15
Obrázek 3 - Schéma UTP kabelu 15
Obrázek 4 - Schéma hvězdicové topologie 18
Obrázek 5 - Schéma hierarchické topologie 18
Obrázek 6 - Schéma topologie mesh 19
Obrázek 7 - Struktura paketu IPv4 23
Obrázek 8 - Struktura paketu IPv6 24
Obrázek 9 - Rámec Ethernet II a IEEE 802.3 26
Obrázek 10 - Frekvence 2.4GHz s používanými kanály 27
Obrázek 11 - Nastavení statické IP adresy 36
Obrázek 12 - Původní nastavení filtrování paket 37
Obrázek 13 - Nastavení sítě pro hosty 38
Obrázek 14 - Spuštění Iperf serveru 39
Obrázek 15 - Uživatelské rozhraní programu NetStress 40
Obrázek 16 - Měření přes ethernetový kabel (Iperf) 41
Obrázek 17 - Měření přes ethernetový kabel (NetStress) 41
Obrázek 18 - Měření přes WiFi (Iperf) 42
Obrázek 19 - Měření přes WiFi (NetStress) 42
Obrázek 20 - Měření přes s ethernetovým kabelem z powerline bez a se zatížením, stejná fáze (Iperf) 43
Obrázek 21 - Měření přes s ethernetovým kabelem z powerline bez a se zatížením, stejná fáze (NetStress) 44
Obrázek 22 - Měření přes WiFi z powerline bez a se zatížením, stejná fáze (Iperf) 45
Obrázek 23 - Měření přes WiFi z powerline bez a se zatížením, stejná fáze (NetStress) 45
Obrázek 24 - Měření přes s ethernetovým kabelem z powerline bez a se zatížením, různá fáze (Iperf) 46
Obrázek 25 - Měření přes s ethernetovým kabelem z powerline bez a se zatížením, různá fáze (NetStress) 47
Obrázek 26 - Měření přes WiFi z powerline bez a se zatížením, různá fáze (Iperf) 48
Obrázek 27 - Měření přes WiFi z powerline bez a se zatížením, různá fáze (NetStress) 48

Seznam tabulek

Tabulka 1 - Kategorie UTP kabelu 16
Tabulka 2 - Porovnání TCP/IP a ISO/OSI modelu 20
Tabulka 3 - Pohlcení WiFi signálu různými materiály 28
Tabulka 4 - Výběr technologie metodou pořadí 49

1 Úvod

Počítačové sítě jsou v dnešní době neodmyslitelnou součástí téměř všech domácností. Nejde ale jen o několik počítačů připojených k routeru a jejich přístupu k Internetu, součástí této lokální sítě (označované také jako LAN) mohou být tiskárny, chytré telefony, televize a mnoho dalších zařízení. Surfování po internetu, vzdáleně připojení do firemní sítě pro práci z domova, tisknutí dokumentů na bezdrátové tiskárně nebo kopírování souborů na externí datové uložiště, využití počítačových sítí v domácnosti je široké. S neustálým vývojem se objevují nové možnosti a vylepšení, která mohou pomoci uživatelům zlepšit výkon své domácí sítě nebo nabízí nové možnosti, jako je technologie PLC. Ovšem při špatném zabezpečení může být počítačová síť vystavena nebezpečí útoků, například za účelem krádeže soukromých dat, nebo k používání cizího připojení k Internetu a to často bez dlouhodobého vědomí majitele.

Práce se zaměřuje na konstrukci počítačové sítě v konkrétní domácnosti za použití vhodných prvků a nastavení zabezpečení. Práce je rozdělena do dvou částí, na teoretickou a praktickou. V teoretické části jsou charaktetizovány základní pojmy, se kterými se člověk v domácích počítačových sítích může setkat, jako jsou například používané prvky, jejich možné typy a možnosti jejich zapojení. Dále jsou charakterizovány procesy a protokoly, které se v lokálních sítích používají, a technologie používané při stavbě počítačové sítě spolu s jejich výhodami a nevýhodami. Jsou zde také charakterizovány nejen základní možnosti zabezpečení, které lze při konfiguraci zvolit, ale také pokročilejší způsoby, které mohou být zvoleny pro zvýšení úrovně zabezpečení.

V praktické části této bakalárské práce je nejdříve charakterizována domácnost, ve které je počítačová síť zkonstruována. Dále je charakterizována konstrukce sítě, vybrané prvky, jejich vlastnosti a použité technologie pro připojení jednotlivých zařízení. Následně je charakterizována konfigurace zabezpečení sítě. V další kapitole praktické části jsou pomocí 2 testovacích programů otestovány přenosové rychlosti použitých technologií v konkrétní domácnosti. U PLC technologie využívající elektrickou síť domácnosti byla měření provedena za různých podmínek za účelem zjištění, jak může stav eletktrické sítě, popřípadě
zvýšení odběru elektrického proudu, ovlivnit přenosovou rychlost přes elektrickou síť. Nakonec byla sestavena tabulka, kde byly jednotlivé technologie ohodnoceny podle

vybraných kritérií a na základě celkového hodnocení těchto kritérií bylo vytvořeno obecné doporučení, která z technologií by měla být preferována při tvorbě domácí počítačové sítě.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této bakalářské práce je, na základě získaných poznatků z odborné literatury, sestavit domácí počítačovou síť. Teoretická část je věnována využívaným prvkům, možným topologiím, protokolům, standardům apod. Dále zde bude charakteristika řešení zabezpečení počítačové sítě a jejich porovnání. V praktické části bude charakterizována reálná domácnost, kde je síť zkonstruována. Následně zde bude popsán výběr a nastavení prvků, konstrukce sítě, nastavení zabezpečení a připojení dalších zařízení domácnosti do sítě.

2.2 Metodika

Metodikou práce bude analýza a následná syntéza získaných poznatků o tématu z odborné literatury. Následně budou porovnávána možná technologická řešení.

3 Teoretická východiska

3.1 Síťové prvky

Síťové prvky jsou komponenty podílející se na přenosu dat uvnitř lokální sítě. Obecně je můžeme rozdělit na aktivní a pasivní. Aktivní prvky jsou zařízení, která s přenášeným signálem nějakým způsobem pracují – např. router pošle obdržená data na správný cílový počítač. Pasívní síťové prvky jsou prvky podílející se na přenosu dat, ale žádným způsobem s ním nepracují, jde tedy především o strukturovanou kabeláž.

3.1.1 Aktivní síťové prvky

Síťová karta

Pro vnější komunikaci počítače je potřeba síťová karta, která je v dnešní době bežné integrovaná na základní desce počítače. Každá síťová karta má unikátní fyzickou adresu tzv. MAC adresu (Media Access Control) – jde o 48bitovou adresu zapsanou hexadecimálně po dvojci znaků oddělenými dvojtečkou, popř. pomlčkou. Prvních 24 bitů identifikuje výrobce, zbylých 24 bitů identifikuje dané zařízení. Je důležitá v mnoha případech, např. při přidělování IP adresy a filtrování pomocí MAC adres, proto je důležité, aby každé koncové zařízení mělo vlastní MAC adresu, jinak může docházet k problémům v síti kvůli adresaci. Pracuje na druhé vsrtvě OSI modelu.

Repeater (opakovač)

Repeater je zařízení, které přijímá signál, opravuje jeho časování, kvalitu a sílu a vysílá ho dále. Po určité vzdálenosti je obnova signálu zapotřebí, neboť dochází k útlumu a šumu. S přibývající vzdáleností přenosového média se však zvětšuje zpoždění a s tím může docházet v kolizní doméně k více kolizím vysílaných signálů. Pracuje na první vrstvě OSI modelu.

Hub (rozbočovač)

Toto zařízení funguje na principu repeatru, ale k hubu může být připojeno několik počítačů najednou. Přijatý signál, který opraví, rozešle všem připojeným počítačům, bez ohledu na to, zda byl pro ně určený. To zbytečně zahlcuje síť, tudíž v dnešní době se příliš nepoužívají a jsou spíše nahrazeny switchy. Pracuje na první vrstvě OSI modelu.

Switch (přepínač)

Zařízení které pracuje obdobně jako bridge, pouze rozhodování provádí hardwarově, které je rychlejší. Na začátku si také vytváří tabulku MAC adres, podle které následně filtruje data. Každý port představuje jednu kolizní doménu, což je velmi výhodné, protože kolize jedné kolizní domény neovlivní chod na ostatních portech. Některé switche dokáží rozhodovat i na základě IP adresy. Pracuje na druhé vrstvě OSI modelu.

Router (směrovač)

Jde o zařízení, kterým lze spojit 2 a více sítí. O tom, kam přijatá data poslat, nerozhoduje pomocí MAC adresy, ale na základě síťové adresy koncového zařízení. Router si vytváří tzv. routovací tabulku, kde si vede nejlepší cesty do daných sítí pomocí routovací metriky. Síťová adresa je určena na základě IP protokolu, jde o 4 čísla oddělená tečkou v rozsahu 0-255. Zároveň router může sloužit jako spojení lokální sítě s vnější (Internet). V dnešní době routery používané v domácnostech fungují také jako tzv. přístupové body (access point) pro zajištění bezdrátového přenosu. Pracuje na třetí vrstvě OSI modelu. (Spurná, 2010, s. 25-31; Horák, Keršláger, 2013, s. 84)

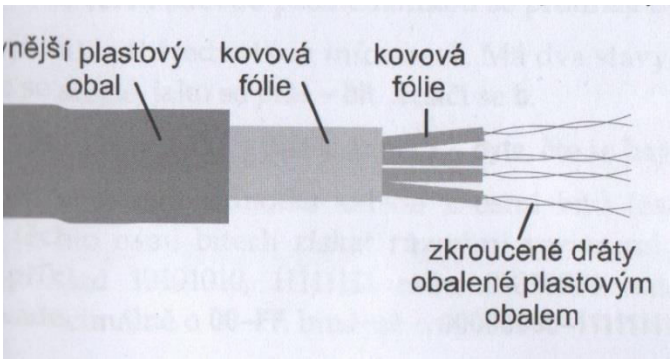
3.1.2 Pasivní síťové prvky

<u>Kroucená dvojlinka</u>

Kroucená dvojlinka se skládá ze 4 párů vodičů, kde každý pár je stočen dohromady. Dle úrovně stínění ji můžeme dělit na:

STP – Stíněná kroucená dvojlinka

Zdroj: (Spurná, 2010)

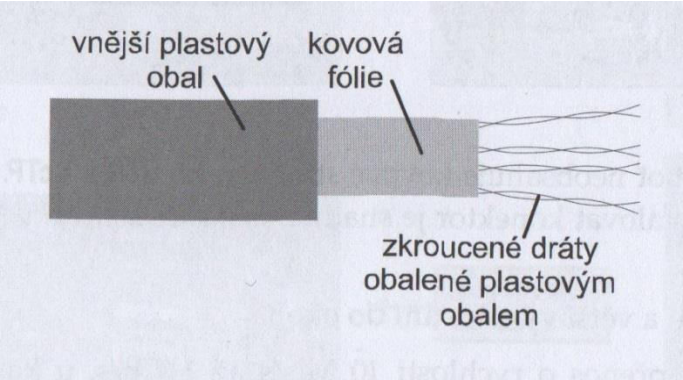


Obrázek 1 - Schéma STP kabelu

U tohoto typu je každý pár vodičů obalen kovovým obalem a následně jsou páry vodičů obaleny dohromady dalším kovovým obalem. Problematické je zde zakončení kabelu, který musí být správně uzemněn, jinak bude docházet k velkému rušení. Rychlost přenosu 10 až 100 Mbps, dosah signálu až 100 metrů.

ScTP – Částečně stíněná kroucená dvojlinka

Zdroj: (Spurná, 2010)

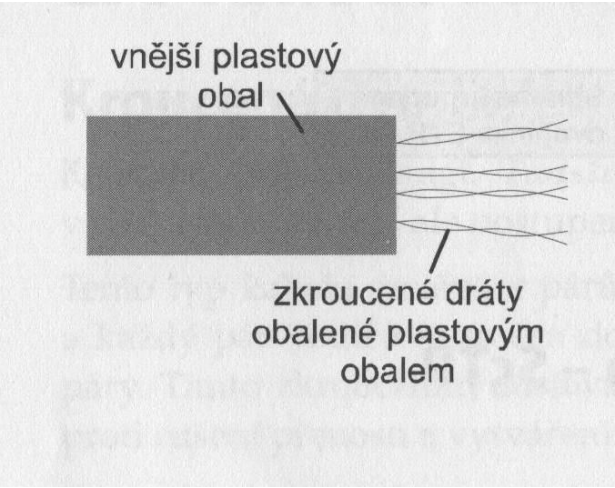


Obrázek 2 - Schéma ScTP kabelu

Stínění je zde zajištěno kovovým obalem kolem všech párů vodičů dohromady, oproti STP zde tedy chybí samostatný kovový obal pro každý pár vodičů. Rychlost přenosu 10 až 100 Mbps, dosah signálu až 100 metrů.

UTP – Nestíněná kroucená dvojlinka

Zdroj: (Spurná, 2010)



Obrázek 3 - Schéma UTP kabelu

Tento typ kabelu nemá stínění, nepotřebuje tedy ani žádné uzemnění, naopak je zde větší sklon k rušení signálu. Rychlost přenosu 10 Mbps až 1 Gbps, dosah signálu až 100 metrů. Dělí se do kategorií v závislosti na využití a rychlosti přenosu dat.

Zdroj: Vlastní zpracování

Kategorie	Využití
1	Telefonní rozvody, nikoliv přenos dat
2	Do rychlosti 4 Mb/s bylo možno přenášet i data
3	Přenos dat do rychlosti 10 Mb/s na lokálních sítích s technologií Ethernet
4	Přenos dat do rychlosti 16 Mb/s na lokálních sítích s technologií TokenRing
5	Přenos dat do rychlosti 100 Mb/s na lokálních sítích s technologií Ethernet
5e	Přenos dat do rychlosti 1 Gb/s na lokálních sítích s technologií Ethernet
6	Přenos dat do rychlosti 10 Gb/s na lokálních sítích s technologií Ethernet (pouze na kratší vzdálenost - přibližně 55 metrů)
6a	Přenos dat do rychlosti 10 Gb/s na lokálních sítích s technologií Ethernet (umožňuje vést až na 100 metrů)

Tabulka 1 - Kategorie UTP kabelu

Optický kabel

Optické kabely mají oproti metalickým několik výhod. Sígnál není ovlivňován elektromagnetickým rušením z okolí a ani ho negeneruje. Díky tomu zde není takový útlum a signál lze přenášet na podstatně větší vzdálenosti bez potřeby jeho obnovy. Signál je přenášen pomocí světelných impulzů v infračerveném spektru. Kabel se skládá ze skleněného jádra okolo kterého je skleněný obal s nižší optickou hustotou oproti optické hustotě jádra. Signál je vyslán jádrem pod určitým úhlem tak, aby docházelo k absolutnímu odrazu od obalu a paprsek se nelámal ven z vlákna. Kabel obsahuje dvě vlákna pro souběžné vysílání a přijímání. Skleněná vlákna mohou být nahrazena plastovými, ale dochází zde k většímu útlumu. Optické vlákno lze dělit na:

Jendovidové vlákno

Paprsek je do vlákna vyslán souběžně s vláknem, v případě zahnutí vlákna dochází k odrazu. Cesta signálu je minimální a dochází k minimálnímu útlumu, oproti mnohovidovému vláknu lze signál přenášet na větší vzdálenosti a to až 100 km. Jádro má v průměru 9 µm a jeho skleněný obal má průměr 125 µm.

Mnohovidové vlákno

Paprsky jsou vysílány do vlákna do určitého úhlu, aby docházelo k absolutnímu odrazu. Průměr vlákna je oproti jednovidovému podstatně vyšší. Variantou tohoto typu je tzv.

gradientní vlákno, kde vlákno má v krajích nižší optickou hustotu, než ve středu, signál tedy po krajích cestuje rychleji. Výhodou toho je, že paprsky vyslány pod různými úhly dorazí na konec přibližně ve stejný okamžik, bez ohledu na délku trasy. Maximální délka mnohovidového vlákna jsou 2 km. Samotné jádro může mít průměr 62,5 nebo 50 µm a jeho skleněný obal má průměr 125 µm. (Spurná 2010, s. 21-24; Horák, Keršláger 2013, s. 18-21)

WDM (Wavelength division multiplexing)

WDM, v českém překladu vlnový multiplex, je technologie, pomocí které lze v jediném optickém vlákně multiplexovat více signálů na základě použití různých vlnových délek pro každý ze signálů. WDM požaduje multiplexer ve vysílači pro spojení signálů a demultiplexer v přijímači pro jejich separaci. Díky tomu lze docílit zvýšení toku v síti bez nutnosti pokládat další optické kabely. WDM se používá ve dvou variantách CWDM a DWDM.

CWDM (Coarse wavelength division multiplexing)

Při CWDM jsou použity větší mezery mezi používanými vlnovými délkami. Lze tedy využít až 16 vlnových délek v jediném optické vláknu - 1270 až 1610 nm s mezerami 20 nm mezi kanály. Díky menšímu počtu použitelných vlnových délek lze použít levnější typy laseru, které nemusí být teplotně regulované a je cenově dostupnější**.** Přenosová rychlost vlákna se pohybuje v řádu desítek Gbps a používá se na vzdálenosti v řádu desítek km.

DWDM (Dense wavelength division mutliplexing)

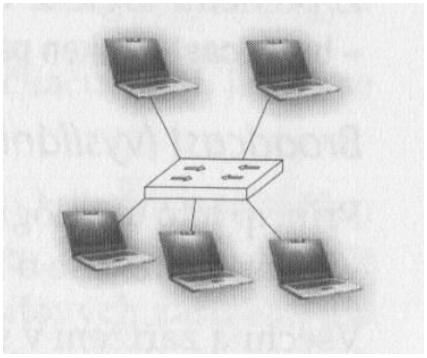
Tato varianta využívá velmi malých mezer mezi kanály, respektive jednotlivými vlnovými délkami, a to méně než 1nm. Díky tomu je možné vměstnat do optického vlákna i přes 100 kanálů, je ale nutné chlazených laserů. Rychlost jedné vlnové délky může být až několik desítek Gbps, celková rychlost vlákna může dosahnovat přes Tbps. Dosah vysílaného signálu je v řádu stovek až tisíců km. (lupa.cz, 2003)

3.2 Topologie sítě

Topologie typu hvězda

Počítače jsou samostatně připojeny k centrálnímu prvku (switch/hub/router). Velkou výhodou této topologie je, že v případě závady na jednom z počítačů není ohrožena funkčnost celé sítě, naopak při výpadku centrálního prvku je nefunkční celá síť.

Zdroj: (Spurná, 2010)

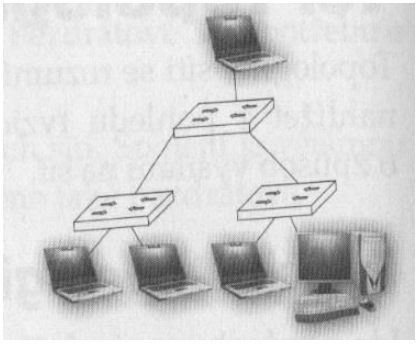


Obrázek 4 - Schéma hvězdicové topologie

Hierarchická topologie

Tento typ fyzické typologie (někdy nazývaný stromovou topologií) vychází z hvězdicové typologie. Centrální prvky jsou spojovány prvky vyšší úrovně sítě. K nejvyššímu prvku může být připojen počítač spravující celou síť. Využíváno především pro rozsáhlejší sítě, například ve firmách.

Zdroj: (Spurná, 2010)



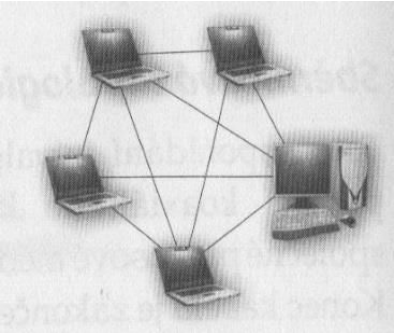
Obrázek 5 - Schéma hierarchické topologie

Topologie mesh

Při tomto typu zapojení jsou všechny počítače propojeny každý s každým. Výpadek jednoho z počítačů nemá vliv na provoz celé sítě. Přidání dalšího počítače do sítě je ovšem

velice nevýhodné z důvodu rapidního nárůstu nutné kabeláže. Proto se nevyužívá úplná topologie mesh, ale pouze částečná, kde se oproti té úplné se některá propojení vynechávají. (Spurná, 2010, s. 133-134)

Zdroj: (Spurná, 2010)



Obrázek 6 - Schéma topologie mesh

3.3 Síťové protokoly

Síťové protokoly pracují na různých úrovních síťových zařízení, proto byly vytvořeny síťové modely, které představují určitou standartizaci v komunikaci zařízení různých typů a výrobců. Jednotlivé vrstvy mezi sebou spolupracují a modely tyto vztahy mezi vrstvami definují. Zároveň jsou ale nezávislé a jejich implementace není předurčena. Nejznámější jsou dva modely – ISO/OSI a TCP/IP (Spurná, 2010, s. 35). Důležité protokoly jsou detailně popsány v rámci struktury TCP/IP modelu.

3.3.1 ISO/OSI model

Tento model byl vytvořen organizací ISO za účelem standartizace počítačových sítí a různých systému. Model se dělí do sedmi vrstev a podrobně popisuje funkce jednotlivých vrstev.

Aplikační vrstva

Umožňuje vzájemnou komunikaci aplikací koncových zařízení (např. vzdálený přístup k tiskárně, přístup k souborům na vzdáleném počítači).

Prezentační vrstva

Připravuje příchozí či odchozí data tak, aby byla správně prezentována v aplikaci na daném či cílovém počítači. Zároveň data kryptuje, aby nebyla v síťových meziprvcích čitelná. V praxi často splývá s vrstvou relační.

Relační vrstva

Má na starosti vytváření, udržování a ukončování relací mezi dvěma stranami.

Transportní vrstva

Přidává k odesílaným datům informace o zdrojovém a cílovém portu. Pomocí portů je identifikována aplikace, která má daná data obdržet. Zároveň kontroluje kvalitu přenosu dat. Data jsou rozdělěna do paket a na cílovém zařízení opět složena.

Síťová vrstva

Přidává k odesílaným datům informace o zdrojové a cílové síťové adrese, to je důležité při přenosu dat mezi různými lokálními sítěmi. Zajišťuje také volbu trasy mezi jednotlivými uzly.

Spojová vrstva

Přidává k odesílaným datům informace o zdrojové a cílové fyzické adrese. Zajišťuje doručení dat v rámci lokální sítě. V případě, že data putují mimo síť, je cílovou adresou adresa okrajového zařízení sítě (např. router).

Fyzická vrstva

Zajišťuje odesílání dat v rámci bitů a jejich časováním. (Spurná 2010, s. 39-40; Horák, Keršláger, 2013, s. 24)

3.3.2 TCP/IP model

TCP/IP je model je souborem protokolů, který je používán sítí Internet. Některé vrstvy ISO/OSI modelu slučuje do jedné, má tedy pouze 4 vrstvy. (Spurná, 2010, s. 35, 38-39)

Zdroj: Vlastní zpracování

TCP/IP model	ISO/OSI model
Aplikační vrstva	Aplikační vrstva
	Prezentační vrstva
	Relační vrstva
Transportní vrstva	Transportní vrstva
Síťová vrstva	Síťová vrstva
Vrstva síťového rozhraní	Spojová vrstva
	Fyzická vrstva

Tabulka 2 - Porovnání TCP/IP a ISO/OSI modelu

3.3.3 Aplikační vrstva

DNS (Domain Name System)

Jde o systém skládající se z DNS serverů a DNS protokolu, který slouží k překladu URL adresy na správnou IP adresu serveru. DNS servery si své seznamy průběžně aktualizují a navzájem sdílejí. Pakliže počítač zažádá o webovou stránku, ale nezná její IP adresu, pošle požadavek na svůj DNS server. Ten v případě, že požadovanou IP adresu nezná, předá požadavek na svůj nadřazený DNS server. DNS servery si tyto nově získané IP adresy uchovávají ve své DNS cache, takže při příštím požadavku na stejnou adresu se již nemusí dotazovat dalšího DNS serveru. DNS pracuje na portu 53. (Spurná, 2010, s. 45-48)

DHCP (Dynamic Host Configuration Protocol)

Tento protokol umožňuje síťovým zařízením získat informace o síťovém nastavení. Počítač (v případě, že má povoleno získávat informace o síti z DHCP serveru) kontaktuje DHCP server a zažádá si o údaje. Server mu může poskytnout, respektive přiřadit IP adresu, masku podsítě, adresu brány, adresu primárního či sekundárního DNS serveru, apod. Tato síťová nastavení mohou být přiřazena počítači jen na dobu určitou, proto musí počítač zaslat ke konci platnosti požadavek o jejich opětovné přidělení. V případě, že server nezjistí, že by mohlo dojít ke konfliku adres, prodlouží platnost nastavení. DHCP využívá porty 67 a 68. (Spurná 2010, s. 51-52)

3.3.4 Transportní vrstva

TCP (Transmition Control Protocol)

Tento protokol transportní vrstvy vytváří před začátkem přenosu oboustranné spojení, to zajišťuje doručení dat ve správném pořadí. Díky jeho spolehlivosti je využíván například webovými prohlížečí, aplikacemi pro transport souborů. Spolehlivosti je dosaženo tím, že TCP přidává do hlavičky odesílaného datového segmentu 20 bitů dat s dodatečnými informacemi – zdrojový a cílový port, číslo sekvence, číslo potvrzení, délka hlavičky, okno, kontrolní součet, ukazatel důležitosti a další dodatečné informace.

Navazování spojení vzniká procesem three-way handshake. Uživatel zašle serveru žádost o synchronizaci (SYN) s úvodním číslem sekvence (SEQ). Server zašle potvrzení žádosti o synchronizaci (ACK) a to s hodnotou o jedná vyšší, než bylo číslo sekvence zaslané uživatelem. Také odešle uživateli vlastní žádost o synchonizaci s vlastní hodnotou čísla sekvence. Uživatel potvrdí číslo sekvence zaslané serverem plus jedna a tím je spojení navázáno. Zároveň se obě strany dohodnou na velikosti okna – počet bitů, kolik je možné zaslat, než je vyžadováno potvrzení o přijetí dat. To se může v průběhu přenosu měnit v závislosti na velikosti ztrát dat při přenosu. Díky tomu se předchází zahlcení spojení potvrzováním zbytečně malých segmentů. V případě, že nějaká data k cílovému počítači nedorazila, zašle potvrzení přijetí dat s hodnotou posledního správně přijatého bitu plus jedna. Spojení je ukončeno tím, že obě strany si musí navzájem zaslat žádost o ukončení, kterou musí obě strany potvrdit. (Spurná, 2010, s. 56-60)

UDP (User Datagram Protocol)

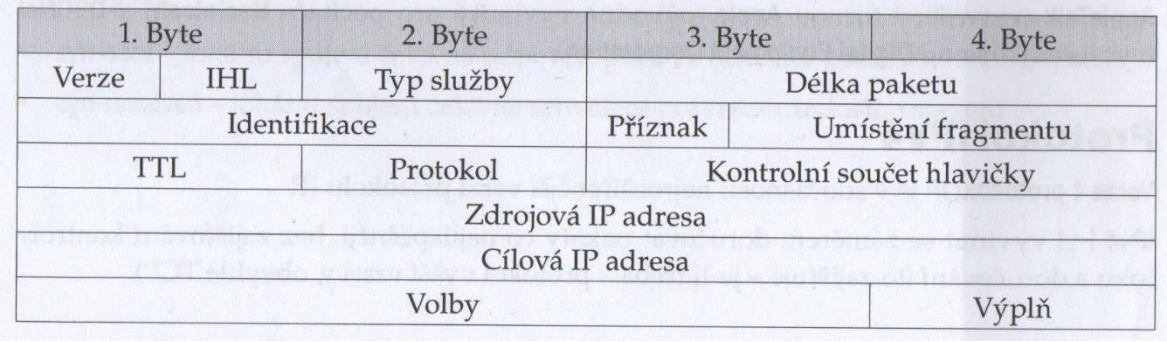
Před zahájením přenosu dat tímto protokolem se obě strany nedomlouvají na parametrech přenosu. V průběhu přenosu dat cílový počítač nezasílá druhé straně informace o tom, v jakém stavu data dorazila, nebo zda-li vůbec dorazila. Je tedy patrné, že se nejedná o spolehlivý přenos. Pokud cílový počítač (resp. cílová aplikace) vyžaduje seřazení dat, musí si to zprostředkovat sám. Tento protokol je používán například u některých on-line her, nebo streamování. UDP přidává do hlavičky 8 bitů informací, ale některé z nich mohou být pro povahu protokolu vynechány. V případě, že cílový počítač neobdrží nějáký důležitý datagram (datová jednotka tohoto protokolu), zažádá si o něj a požadovaná data jsou ihned zasílána. (Spurná, 2010, s.60)

3.3.5 Síťová vrstva

IPv4 (Internet Protocol version 4)

Účelem tohoto protokolu je doručování dat (pakety) co nejrychleji. Jedná se o protokol nespojový, není tedy vytvořeno mezi dvěma zařízeními žádné spojení, při kterém by byl ověřován tok dat. V případě ztráty dat může kontrolu zajistit protokol TCP. Tím se přenáší méně dat a k zahlcení sítě nedochází tak často, jako při kontrole přenosu dat. Adresa IPv4 je 32 bitové číslo zpravidla zapsané jako čtyři čísla decimální soustavy oddělené tečkou. S nastavením IP adresy pro koncové zařízení úzce souvisí adresy masky podsítě a výchozí brány. Adresa výchozí brány je adresa hraničního zařízení sítě, obvykle se jedná o router. Všechna zařízení v síti mají stejnou výchozí bránu. Maska podsítě je číslo, které svou strukturou říká, jaká část IP adresy představuje identifikaci sítě a jaká část identifikuje koncové zařízení. Jde o 32 bitové číslo v binárním zápisu začínající zleva jedničkami. Jedničky určují část pro identifikaci sítě, nuly část pro identifikaci koncového zařízení. V případě, že v části IP adresy identifikující cílové zařízení jsou pouze nuly, jedná se o adresu sítě. Pakliže ve stejné části jsou samé jedničky, jde o adresu broadcastu. IP adresu, masku podsítě a výchozí bránu lze nastavit manuálné, nebo si tyto adresy lze nechat přidělit pomocí DHCP. V lokálních sítích se využívá především adresace IPv4, protože je naprosto dostačující. (Spurná, 2010, s. 63-70, 96)

Zdroj: (Spurná, 2010)



Obrázek 7 - Struktura paketu IPv4

NAT (Network Address Translation)

Jde o překlad mezi lokální adresou koncového zařízení a veřejnou adresou. Router musí přeložit adresu když koncové zařízení zasílá dotaz na zařízení umístěné například v síti Internet. Při komunikaci se zaměňují lokální adresa za veřejnou, protože případná odpověď, kde by byla cílovou adresou adresa lokální, bude zahozena (Spurná, 2010, s. 90-

91). Často se využívá pro přístup více počítačů v lokální síti na Internet přes jednu veřejnou IP adresu, to však často vytváří problémy a některé aplikace nemusí fungovat správně.

IPv6 (Internet Protocol version 6)

Jedním z rozdílů IPv6 oproti IPv4, je možnost adresace mnohem většího počtu zařízení – u IPv4 bylo možné adresovat 2^{32} zařízení (cca přes 4 miliardy), u IPv6 je možné adresovat až 2^{128} zařízení. Adresa IPv6 je tedy 128 bitové číslo zapsané jako osm skupin čtyř číslic v hexadecimální soustavě oddělených dvojtečkou. Lze vynechávat nuly zleva, popřípadě je-li skupina tvořena čtyřmi nulami, lze ji celou vynechat – v adrese tedy budou dvě dvojtečky po sobě. Adresy IPv6 se dělí do 3 kategorií.

- **Unicast**
  Adresa přidělena právě jednomu síťovému rozhraní. Data posílaná na tuto adresu jsou doručena kontrétnímu zařízení.
- **Multicast**
  Adresa přidělena určité skupině zařízení. Data posílaná na tuto adresu jsou doručena všem zařízením této skupiny.
- **Anycast**
  Adresa přidělena určité skupině zařízení. Oproti multicastu se liší tím, že data zaslaná na tuto adresu dorazí jen k nejbližšímu zařízení dané skupiny. To je z důvodu snížení zahlcení a ochrany proti útokům cíleným k zahlcení adresy.

Jako u IPv4, adresa se dá rozdělit na část identifikující síť a část identifikující síťové rozhraní. Adresa sítě je určena prefixem, tedy číslem za lomítkem, které vyjadřuje počet bitů zleva určující adresu sítě. (Spurná 2010, s. 93-95)

Zdroj: (Spurná, 2010)

Verze 6 (4 bity)	Dopravní třída (8 bitů)	Pojmenování toku (20 bitů)
Délka těla (16 bitů)	Následující hlavička (8 bitů)	Limit přeskoků (8 bitů)
Zdrojová adresa (128 bitů)		
Cílová adresa (128 bitů)		

Obrázek 8 - Struktura paketu IPv6

Porty

S IP adresami také souvisí i porty. Jde o šestnáctibitové číslo, které identifikuje zdrojovou či cílovou aplikaci, mezi kterými přenos dat probíhá (na jakém portu aplikace naslouchá). Porty lze rozdělit do 3 skupin:

- 0 – 1023 (Dobře známé porty) – Porty přidělené kontrétním aplikacím. Jedná se především o systémové procesy a aplikace spuštěné uživatelem s vysokým oprávněním, například HTTP, DNS, DHCP, aj.
- 1024 – 49151 (Registrované porty) – Porty dynamicky přidělované procesům a aplikacím spuštěné uživatelem s běžnými oprávněními
- 49152 – 65535 (Dynamické porty) – Porty dynamicky přidělované procesům a aplikacím zahajující spojení

(Spurná, 2010, s. 61)

ICMP (Internet Control Messaging Protocol)

Protokol pro zasílání kontrolních či chybových zpráv, je používán například příkazem „ping“. Hlavička paketu ICMP se skládá z typu (8 bitů), kódu (8 bitů) a kontrolního součtu (16 bitů). Protokol může zaslat zprávy typu:

- ICMP Echo Request – žádost o odpověď cílového zařízení
- ICMP Echo Reply – odpověď na žádost cílového zařízení
- Destination Unreachable – nedostupnost sítě, specifický problém je upřesněn kódem v hlavičce paketu
- Time Exceeded – překročení časového limitu, v případě, že je přijat paket s TTL roven 0
- Redirect – přesměrování, router informuje zdrojový počítač, že do cíle existuje lepší cesta, než je původně zvolená, zdrojový počítač poté začne posílat paketu lepší cestou
- Source Quench – zahlcení cílového zařízení popřípadě routeru, zahlcené zařízení odešle na zdrojové zprávu o zahlcení, ten poté může upravit rychlost zasílání paket.
- Další typy zpráv (datagramů) jsou spíše výjimečné

ICMP zprávy bývají často využívány k průzkumu a útoku na ochranné prvky počítačové sítě, proto je jejich užití často filtrované či blokované.

(Spurná, 2010, s. 119-121; Northcutt, 2005, s. 32)

3.3.6 Vrstva síťového rozhraní

Ačkoli CSMA není protokolem, jde o důležitou metodu řízení provozu v síti. Dokáže detekovat možné kolize, zahlcení linky a řešit tyto problémy.

CSMA/CD (Carrier Sense Mulitple Access / Collision Detection)

Tato metoda je využívána technologií Ethernet (pokud funguje ve full-duplexu, pak se tato metoda nevyužívá). Zařízení, které chce vysílat přes společné přenosové médium, nejdříve naslouchá, zda je na lince provoz či nikoliv. Jakmile není provoz, začíná vysílat. Může se ale stát, že zařízení žačnou vysílat ve stejný okamžik, tím dojde ke kolizi a data se musí odesílat znovu. Pakliže dojde ke kolizi, nebo zájemce o vysílání zjistí, že na lince je provoz, řídí se tzv. backoff algoritmem – ten vybere náhodnou dobu, po kterou zařízení čeká, než se pokusí znovu o vysílání svého signálu. Díky tomu, že čekací doba pro vysílání je náhodná, výrazně snižuje nebezpečí výskytu kolize. (Spurná, 2010, s. 127)

CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)

Tato metoda je používána u bezdrátového přenosu. Zařízení, které chce vysílat přes společné přenosové médium, nejdříve naslouchá, zda je na lince provoz či nikoliv. Jakmile není provoz, zašle informaci všem ostatním zařízením na médiu, že se chystá vysílat. Následně může začít vysílat. Nemůže zde dojít ke kolizi při vysílání, pouze ke kolizi o zasílání informace o tom, že se zařízení chystá vysílat. V tom případě se opět zařízení řídí backoff algoritmem. (Spurná, 2010, s. 127)

3.4 Síťové standardy

V této kapitole jsou charakterizovány možné technologie při stavbě počítačové sítě a popsány jejich výhody a nevýhody.

3.4.1 Ethernet

Jde o počítačovou síť, kdy je jako přenosové médium využito kabelů kroucené dvojlinky a optických kabelů. V rámci ISO/OSI modelu Ethernet představuje jeho fyzickou a spojovou vrstvu. Ethernet je standardizován pod 802.3 a kromě ethernetového rámce tohoto standardu se spíše využívá ethernetový rámec Ethernet II. Jeho hlavní rozdíl je, že místo pole Délka má pole Typ, kde je uveden typ protokolu v datovém poli. Ethernet II je

podporován pouze pro nespojovanou komunikaci. Nejčastěji je využívána typologie typu hvězda, kdy v centrálním prvkem je hraniční router sítě.

Zdroj: (Spurná, 2010)

Ethernet II					
Preambule	Cílová adresa	Zdrojová adresa	Typ	Data	FCS
8 B	6 B	6 B	2B	46–1500 B	4 B

IEEE 802.3						
Preambule	SFD	Cílová adresa	Zdrojová adresa	Délka	Data	FCS
7 B	1 B	6 B	6 B	2 B	46–1500 B	4 B

Obrázek 9 - Rámec Ethernet II a IEEE 802.3

Ethernet můžeme dle přenosové rychlosti rozdělit na:

- 10Mbps (10Base-T)

  Původní verze Ethernetu, dnes již zastaralá a nepoužívá se.

- 100Mbps (Fast Ethernet)

  Aktuálně nejrozšířenější verze Ethernetu, používají se UTP kabely s minimální karegorií 5 a optické kabely.

- 1Gbps (Gigabit Ethernet)

  Používají se UTP kabely s minimální kategorií 5 a optické kabely, vyšší pořizovací cena zařízení podporující tento typ, full-duplexový typ vysílání.

- 10Gbps (Ten Gigabit Ethernet)

  Přenos především před optický kabel, je možné pouze full-duplexové vysílání, kromě využití v LAN lze použít i pro MAN nebo WAN.

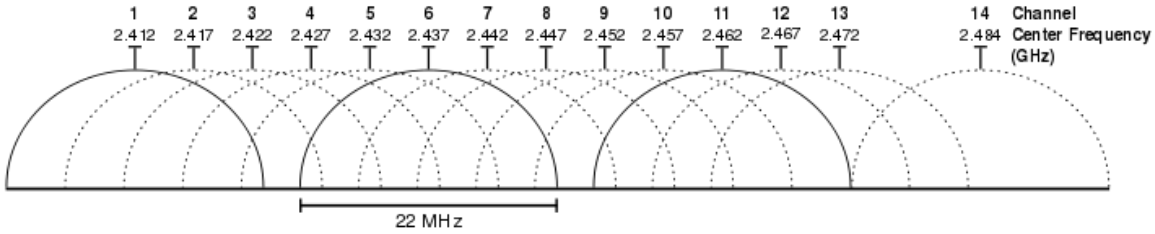
(Spurná, 2010, s. 128, 152-156; Horák, Keršláger, 2013, s. 31-35)

3.4.2 WiFi

Nejpoužívanější technologie při konstrukci počítačových sítí v domácnostech a to především díky jejich jednoduché realizaci. Základem je tzv. přístupový bod neboli access point, který vysílá signál prostřednictvím atmosféry jako přenosového média. Vysílání probíhalo dříve pouze na frekvenci 2.4 GHz, na této frekvenci ale pracují, respektive komunikují, i jiná bezdrátová zařízení, jako například dětské chůvičky, nebo bezdrátová myš či klávesnice. Zároveň se signál může rušit s dalšími sítěmi v okolí – operační pásmo

2.4 GHz je 2412-2472 MHz o šířce jednotlivého kanálu 5MHz. Tím tedy vzniká 13 vysílacích kanálů, ale minimální šířka kanálu standardů pro tuto frekvenci je 22MHz, je tedy zřejmé že může docházet k rušení.

Zdroj: moxa.cz



Obrázek 10 - Frekvence 2.4GHz s používanými kanály

Vznikla tedy druhá možnost a to vysílání na frekvenci 5GHz. Hlavní výhodou je, že vysílání na této frekvenci není rušeno spotřebiči, nebo jinými bezdrátovými přístroji. Jednotlivé vysílací kanály byly oproti 2.4GHz uzpůsobeny tak, aby se navzájem nerušily. Přenosová ryhlost je oproti 2.4GHz vyšší, ale signál na této frekvenci není dostatečně silný na to, aby prošel například několika zdmi. Pokrytí 5GHz bude ze stejného AP menší, než pokrytí 2.4GHz. Různé typy materiálu pohltí vysílaný signál různou silou, tabulka č.1 zobrazuje míru pohlcení signálu zdmi z různého materiálu dle Horáka(2011, s. 16). Bezdrátový přenos je standardizován podle IEEE 802.11 – v rámci počítačových sítí v domácnostech jsou nejdůležitější 802.11a/b/g/n/ac zabývající se oběma pásmy. (Spurná, 2010, s. 131; Horák, Keršláger, 2013, s. 52-55)

Zdroj: (Horák, 2011)

materiál	projde [% signálu]	útlum [% signálu]
dřevěná zeď	95	5
hliník	90	10
sklo	75	25
cihly	70	30
beton	60	40
sádrokartón	50 (výborně pohlcuje především záření 2,4 GHz)	50

Tabulka 3 - Pohlcení WiFi signálu různými materiály

3.4.3 PLC (Power Line Communication)

Jde o technologii vysílání signálu přes rozvodnou síť 230V (pro domácnosti pojmenováno jako skupina HomePlug). Jeden z adapterů připojených do rozvodné sítě je zároveň připojen ethernetovým kabelem k routeru a vysílá signál, který lze zachytit druhým adaptérem připojeným v jakékoliv zásuvce domu – odtud může být veden opět ethernetovým kabelem do cílového zařízení, nebo některé adaptéry jsou schopné vytvářet access point pro bezdrátový přenos. Pakety se vysílají na podstatně vyšší frekvenci, než kterou využívá elektrický proud – pakety na rozmezí 1 – 30 Mhz, elektrický proud na 50 Hz. Nejnovější verze této technologie uvádí přenosovou rychlost 500Mbit/s u typu HomePlug AV a dokonce 1Gbit/s u typu AV2. Tato teoretická rychlost je ale ovlivněna mnoha faktory, které mohou výrazným způsobem snížit reálnou rychlost přenosu. Jedním z nich je kvalita elektrické rozvodné sítě v domácnosti. Lepšího přenosu a dosahu lze docílit měděnými dráty, naopak, dříve používané, hliníkové dráty mohou ryhlost a dosah zmenšit. Adaptéry by měli být připojeny přímo do zásuvky, připojení přes prodlužovačku snižuje výkon připojení. K dispozici jsou již adaptéry se stíněnou průchozí zásuvkou, tedy případnou prodlužovačku je možné připojit přes adaptér. Pokud je to možné, je vhodné vyčlenit zásuvku pouze pro adaptér, další připojené spotřebiče a přístroje opět mohou zapříčinit pokles výkonu. Další velmi důležitou podmínkou je, aby zásuvky vysílacího i přijímacího adaptéru byly připojeny na stejnou fázi (v domácnosti mohou být využívány až 3 fáze), v opačném případě může být problém s navázáním spojení mezi adaptéry, nebo dosahovaná přenosová rychlost je velice nízká. Běžně bývá uváděn dosah signálu mezi adaptéry až 300 metrů, nicméně opět jde spíše o vzdálenost teoretickou, reálný dosah je podobně jako rychlost ovlivněn faktory výše uvedenými. Konfigurace adaptéru je velice intuitivní, adaptéry se mezi sebou spárují, s případě adaptéru fungujícím zároveň jako AP, lze konfiguraci pro WiFi zkopírovat přes WPS funkci. Samotné nastavení adaptéru (například skrytí SSID) lze provést dměna způsoby. Pokud je konfigurace na adaptéru jiná, než na routeru (jiný název sítě), pak se lze k adaptéru přihlásit napsáním stránky do prohlížeče (podobné přihlašování jako k routeru), zde po přihlášení je možné SSID skrýt. V případě shody jmen musí být na stránkách výrobce stažen program pro daný typ powerline a pomocí něj lze měnit nastavení adaptéru. Výhodou této technologie je, že lze signál šířit v místech, kde nelze vést ethernetový kabel či řušení bezdrátového signálu je příliš velké. Nejnovějším typem PLC je HomePlug Green PHY – nejde ovšem o pokrok

v přenosové rychlosti, naopak HomePlug GP dosahuje maxima pouhých 10 Mbps, ale spotřebuje až o 75% méně energie. Její využití se plánuje u nových zařízení v regulaci topení, ventilace a klimatizace (anglická zkratka HVAC – heating, ventilating, air-conditioning) nebo u zařízení pro automobily. Tato technologie je standardizována podle 1901-2010 – IEEE Standard for Broadband over Power Line Networks. (Schmidt, Kubeš, 2014; Evans, 2014)

3.5 Zabezpečení sítě

Zabezpečení počítačové sítě je důležitou částí při její tvorbě. Používané prvky nejsou stoprocentní jistotou, že nevyžádaný uživatel nezíská přístup k síti. Jde ale o vytvoření několika vrstvé obrany, kterou musí útočník překonat a to ho může odradit.

3.5.1 SPI Firewall

Tento firewall, jinak nazývaný stavový firewall, kontroluje nová spojení i již spojení navázaná, nehledě na to, zda se jedná o TCP či UDP přenos. Udržuje si přehled o aktuálních spojení v tabulce navázaných spojení a blokuje pakety, které nejsou součástí některého z navázaných spojení. To napomáhá blokovat pakety sloužící k skenování obrany počítačové sítě. Firewall má vlastní databázi pravidel, určující zdrojové a cílové IP adresy a porty, které mohou navázat spojení. SPI Firewall je dnes již běžnou součástí kvalitních routerů. Jako rozšíření či alternativu lze využít proxy firewallu, který funguje na stejném principu jako SPI firewall, ale oproti tomu slouží jako prostředník mezi webovým serverem a uživatelem, tedy obě strany nekomunikují přímo spolu, ale nejdříve s proxy firewallem. To napomáhá k zabránění přijímání i odesílání škodlivých dat. (Northcutt, 2005, s. 32-33)

3.5.2 Denial of Service útoky

Jde o typ útoku, kde různými způsoby lze docílit nadměrného provozu v cílové síti a tím zahltit počítač nebo, pokud je veden útok na webový server, znepřístupnit webové stránky. Kromě standardního DoS útoku, který je veden z jednoho počítače, existuje tzv. DDoS útok (Distributed Denial of Service), kde útok je veden z velkého množství počítačů, často bez vědomí jejich majitelů a to kvůli generování vyššího množství dotazů na cílovou adresu a tedy většího zahlcení. V některých typech DoS útoků dochází k tzv. IP spoofingu,

kdy útočník do odesílaného paketu zadá jako zdrojovou IP adresu jinou adresu. (Northcutt, 2005, s. 32, 366) Filtrování níže uvedených útoků lze na moderních routerech provést pomocí nastavení určitého povoleného počtu daných paket za vteřinu.

ICMP flood

Mezi nejčastější útoky pomocí ICMP jsou ping flood a smurf attack. Ping flood je útok, kdy je na cílovou adresu zasílán ICMP Echo Request (žádost o odezvu příkazem ping) paket. Pakety se odesílají bez toho, aniž by čekaly na odpověď. Pakliže má útočník rychlejší připojení k internetu než cílový počítač, dokáže zahltit cíl tímto dotazem.

Druhým typem je smurf attack, kdy útočník zašle falešný ICMP Echo Request nějčastěji na broadcast segmentu sítě s předpokladem, že každý počítač v segmentu zašle zpět odpověď. V paketu je jako zdrojová IP adresa uvedena adresa cíle, který chce útočník zahltit, takže všechny odpovědi se odešlou na cílové zařízení a zahltí ho. (Northcutt, 2005, s. 32)

UDP flood

Dalším typem útoku je UDP flood, kdy je využito procesu kominukace UDP protokolu. Útočník zasílá UDP pakety cíli na náhodné porty. Ten musí zjistit, jestli nějaká z aplikací nenaslouchá na daném portu a pak zaslat odpověď ICMP Destination Unreachable. Tento provoz zahltí cílové zařízení. Zdrojová adresa zasílanách paket může být navíc upravena tak, aby se útočníkovi nevraceli odpovědi. (Hanák, 2015; Juniper.net, 2012)

TCP flood

Tento typ útoku využívá princip fungování TCP protokolu. K útoku lze využít všechny 3 možnosti třícestného navázání spojení. Pokud útočník zasílá FIN pakety, cíl je bude zahazovat, protože žádné takové spojení navázané není, ale i toto ověření vyžaduje určité množství práce. SYN flood funguje na způsobu, kdy pomocí IP spoofingu je změněna zdrojová IP adresa a tak cíl odesílá SYN-ACK pakety na jinou adresu a zpětného ACK paketu se nedočká. Tím se vytváří mnoho napůl navázaných TCP spojení a cíl je zahlcen. (Hanák, 2015)

3.5.3 Filtrování podle MAC adres

Filtrování pomocí MAC adres zařízení je efektivním způsobem, jak kontrolovat přístup zařízení do sítě. Filtrování může být vedeno dvěma způsoby, buď je možné vytvořit tzv. blacklist MAC adres, neboli seznam MAC adres, kterým bude odepřen připojení k síti. Druhou variantou je vytvořit whitelist, seznam zařízení s MAC adresami, které mají naopak povolený vstup do sítě, jakýmkoliv ostatním zařízení bude přístup odepřen. (Horák, Keršláger, 2013, s. 57) Nicméně filtrování MAC adres, lze překonat pomocí MAC spoofingu - změna MAC adresy (Northcutt, 2005, s. 372). Whitelist varianta je v malé počítačové síti praktičtější, protože získat MAC adresy několika vlastních zařízení je velmi jednoduché, naopak přidávat do blacklist seznamu MAC adresy nevyžádaných uživatelů se jeví jako nereálné.

3.5.4 DMZ (De-Militarized Zone)

DMZ je prostor před firewallem vniřní sítě do kterého jsou umístěny většinou servery provozovaných služeb. I když je DMZ před vnitřním firewallem je zpravidla pod ochranou dalšího firewallu hraničního routeru. Spolu s tím úzce souvisí pojem screened subnet – rozdílem oproti DMZ je to, že servery jsou umístěny za stejným firewallem a jsou izolovány od vnitřní sítě. (Northcutt, 2005, s. 29-30) Na domácích routerech lze nalézt možnost vytvoření DMZ, ale zde je funkcí to, že se otevřou všechny porty počítače (je nutné, aby měl nastavenou statickou IP adresu a vyplé přidělování z DHCP serveru).

3.5.5 IDS a IPS

Intrusion Detection System je systém, který se snaží detekovat a upozornit na poderzřelé či škodlivé události v síti. V případě detekování nějakého podezřelého chování může být upozorněn administrátor sítě. Tento systém může být tvořen několika IDS senzory, které se umístí na důležitá místa dané sítě. IDS lze rozdělit na dva základní typy – Network-based Intrusion Detection System (NIDS) a Host-based Intrusion Detection System (HIDS). NIDS kontroluje provoz na síti a to jak příchozí, tak i odchozí (všech zařízení). Například kontrola provozu na firewallu, zda-li se někdo nepokouší o jeho prolomení. HIDS je umístěn na jednotlivých serverech nebo zařízeních a monitorují příchozí a odchozí komunikaci daného zařízení.

Intrusion Prevention System je systém, který se snaží detekovat a zabránit útokům na síť. Rozdílem oproti IDS je to, že při detekci IPS se automaticky snaží odrazit útok bez toho, aniž by byla vyžadována nějaká činnost ze strany administrátora. Za IPS je také často označována kombinace IDS a firewallu. (Northcutt 2005, s. 27-28, 34)

3.5.6 Zabezpečení WiFi provozu

Nejzranitelnější je počítačová síť přes bezdrátové vysílání a to hlavně z toho důvodu, že přenosové médium je pro každého dostupné. Je tedy třeba zvolit správnou konfiguraci AP a předejít tak připojení nevyžádaného uživatele.

Skrytí SSID

Vzhledem k faktu, že připojit se k bezdrátové síti je velmi jednoduché, skrytí SSID vysílání představuje rychlý způsob, jak zvýšit zabezpčení své počítačové sítě. Každý AP je defaultně nakonfigurován tak, že vysílá SSID (Service Set Identifier), tedy identifikátor, který říká svému okolí, že jde o připojitelný AP. Skrytím tohoto SSID vysílání pak uživatel, který by se chtěl pokusit připojit k síti neuvidí daný AP v nabídce. Tato možnost je ovšem nutná aplikovat na všech AP, kterými síť disponuje, aby byla celá síť skryta. Možnou nevýhodou může být, že v případě skryté SSID se nový uživatel, respektive nové zařízení musí připojit manuálně (je nutné znát název sítě, typ zabezpečení a přístupové heslo). Je nutné mít na vědomí, že toto nedělá AP absolutně bezpečnými, existují programy a metody, které dokáží cílovou síť detekovat. (Northcutt, 2005, s. 370-371)

WPA (WiFi Protected Access)

Zabezpečení, které bylo vydáno po prolomení v té době využívaného WEP zabezpečení. Problémem WEP bylo, že klíče pro šifrování komunikace byly statické, tedy při získání dostatečného vzorku dat byl útočník schopen získat šifrovací klíč. WPA používá stejné kliče jako WEP, ty jsou ale dynamicky vytvářeny a obměňovány, útočník tedy nezíská takové množství dat šiforvaných stejným způsobem, aby ho mohl získat. WPA bylo vytvořeno tak, aby bylo možné ho implementovat na stávající zařízení a nebyla tak nutná hardwarová obměna. Zabezpečení WPA využívá protokol TKIP (Temporal Key Integrity Protocol), jehož dynamicky generované šifrovací klíče jsou známy pouze zařízení, ke kterému se uživatel připojuje a po ukončení spojení se smažou. Po určité době byly

nalezeny způsoby pro prolomení tohoto zabezpečení a je doporučeno používat bezpečnější WPA2. (Horák, Keršláger, 2013, s. 57; Northcutt, 2005, s. 369)

WPA2 (WiFi Protected Access 2)

Jde o nadstavbu WPA, kde je použito lepší a podstatně bezpečnější šifrování a je dnes vyžadováno, aby všechna vyrobená AP zařízení podporovala WPA2 zabezpečení. U WPA2 je protocol TKIP nahrazen standardem AES (Advanced Encryption Standard), který je celosvětově uznávaný šifrovací standard. WPA2 je součástí standardu IEEE 802.11i. Novější AP umožňují nastavit kromě klasického WPA+TKIP a WPA2+AES i možnost WPA+WPA2 mixed – AP se s uživatelem připojí defaultně přes WPA2, pokud zařízení uživatele nepodporuje WPA2, přejde na WPA. (Northcutt, 2005, s. 369)

IEEE 802.1x

Jde o protokol, charakterizující zabezpečení vstupu uživatele do počítačové sítě. Uživateli, který se připojí do sítě, je blokována veškterá kominukace v síti, kromě komunikace s EAS (Extensible Authentication Protocol). Uživatel musí zadat uživatelské jméno a heslo, které ověří RADIUS protokol podle seznamu povolených uživatelů na RADIUS serveru a v případě shody uživateli povolí přístup. To umožňuje efektivně blokovat přístup nevyžádaným uživatelům do sítě. Často je tento způsob popisován jako WPA2-Enterprise, protože jeho využití je převážně ve firmách. (Horák, Keršláger, 2013, s. 57)

PSK (Pre-Shared Key)

Jde o způsob přístupu uživatele do počítačové sítě, kdy je nutné znát předem sdílený klíč (heslo). Složitost klíče musí být dostatečná, aby klíč odolal útokům o prolomení a o jeho podobě rozhoduje administrátor sítě. Klíč je pro každého uživatele stejný. Býva taky označováno jako WPA2 – Personal, protože je používáno hlavně v malých firmách a domácnostech. (Northcutt, 2005, s. 369)

4 Vlastní práce

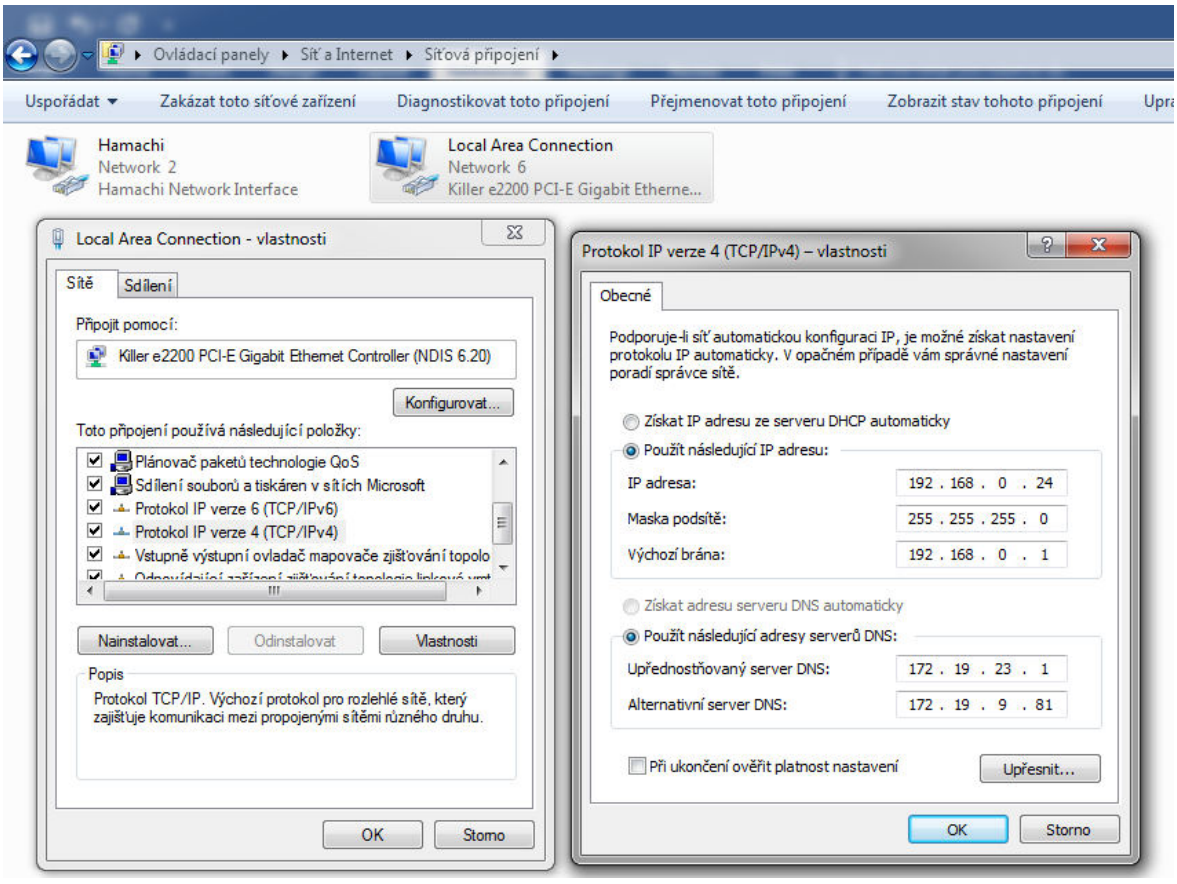
4.1 Konstrukce sítě

Dům, kterém byla počítačová síť zkonstuována se nachází Kostelci nad Labem – Jiřicích. Jedná se o patrový rodinný dům, kde žijí 3 osoby. Uživatelé používají počítače k běžnému surfování po internetu, hraní počítačových her a připojování se do firemních sítí a systémů přes VPN. Kromě stolního počítače, popřípadě notebooku, jsou k síti připojena další zařízení jako například tiskárna a satelitní HDTV přijímač.

Jako hraniční router byl pořízen TP-LINK Archer C58, který slouží zároveň jako access point pro bezdrátová zařízení. Je schopný vysílat souběžně na 2.4 Ghz a 5 Ghz frekvenci s teoretickou rychlostí 450 Mbps pro 2.4 Ghz frekvenci a 867 Mbps pro 5 Ghz frekvenci. Tři všesměrové antény zajišťují kvalitní dosah signálu. Kanál a šířka kanálu u obou frekvencí byla nastavena na automatický režim, v případě, že by docházelo k výpadkům, je možné tuto konfiguraci upravit manuálně. Router disponuje dalšími funkcemi jako například síť pro hosty, funkce DMZ, UPnP, nebo VPN server. K routeru je připojen powerline adaptér (TP-LINK TL-PA4010), který vysílá signál v elektrické síti. Druhý adaptér (TL-WPA4220), který tento signál přijímá, má dva 10/100Mbps Ethernet porty a zároveň funguje jako tzv. WiFi extender – tedy funguje jako další access point vysílající na 2.4 Ghz s rychlostí 300 Mbps. Oba PLC adaptéry jsou přípojeny do stejného elektrického obvodu, jsou tedy ve stejné fázi. Přenosová rychlost mezi adaptéry udávaná výrobcem je 500Mpbs (jedná se o čistě teoretickou rychlost). Byla vybrána PLC technologie, protože satelitní HDTV přijímače je možné připojit pouze přes ethernetový kabel a k jednomu z nich není fyzicky možné natáhnou kabel přímo z routeru. Konfigurace PLC adaptérů byla velmi jednoduchá, nejdříve bylo nutné spárovat adaptéry (dle pokynů výrobce), poté bylo možné nakonfigurovat adaptér s WiFi extenderem stejně jako je nastavený hraniční router a to pomocí funkce WPS (přesný proces opět podle pokynů výrobce). Počítače a satelitní přijímače jsou připojeny kabelem (byly použity ethernetové kabely kategorie 5e) tiskárna a TV jsou připojeny bezdrátově. Pro připojení tiskárny k lokální síti byl potřeba nejdříve k tiskárně připojit datovým kabelem počítač, který je zároveň do lokální sítě připojen. Tiskárna si poté zkopírovala konfiguraci a připojila se samostatně.

Pro přidělování IP adres zařízením je povolen DHCP server s rozsahem IP adres 192.168.0.100 – 192.168.0.199, pouze jeden z počítačů má statickou IP adresu (kvůli otevírání specifických portů pro daný počítač) mimo rozsah DHCP serveru, aby nedošlo ke konfliktu adres. Nastavení statické IP adresy lze provést na daném zařízení následujícím postupem (operační systém Windows) – Ovládací panely -> Síť a Internet -> Síťová připojení, zde se lze nalézt všechna síťová zařízení daného počítače. Poté je potřeba otevřít vlastnosti a rozkliknout řádek „Protokol IP verze 4“ (IP adresy dle IPv4 jsou pro domácí počítačovou síť naprosto dostačující, není pravděpodobné, že by byl využit celý rozsah adresace). V nově otevřeném okně je potřeba označit možnost „Použít následující IP adresu:“ a vyplnit příslušná políčka. Při nastavení statické IP adresy je také nutné zadat adresy DNS serverů.

Zdroj: Vlastní zpracování

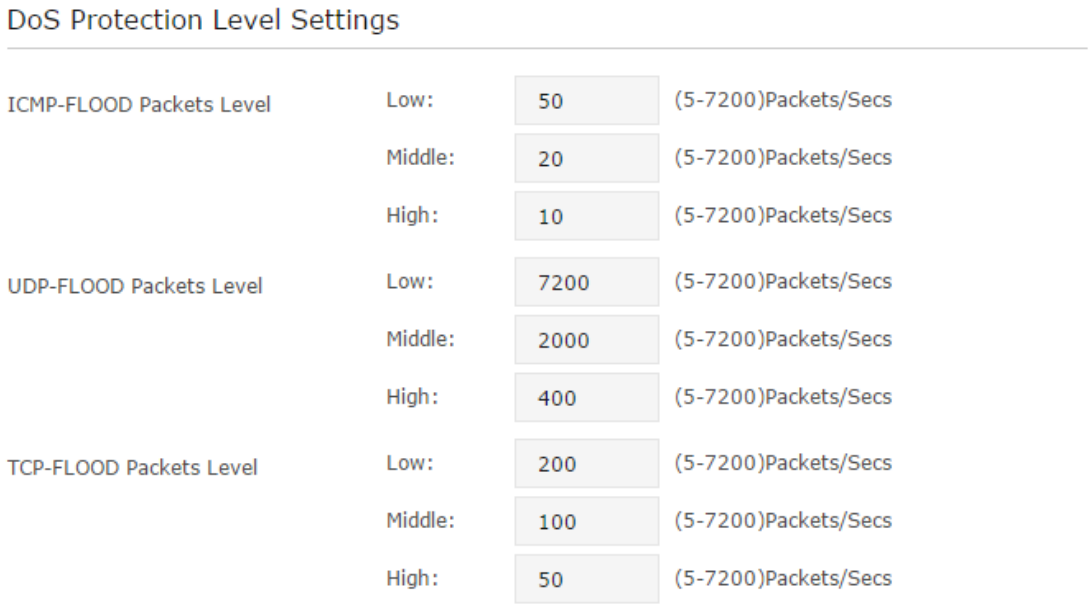


Obrázek 11 - Nastavení statické IP adresy

Podobně jako nastavení statické IP adresy je nutné zadat i IP adresu, masku podsítě, výchozí bránu a DNS servery do routeru pro připojení k Internetu. Tyto informace byly zaslány lokálním poskytovatelem internetového připojení

4.2 Nastavení zabezpečení

Router je zabezpečen několika způsoby, které tvoří komplexní obranu. Běží zde SPI firewall, nabízí obecnou ochranu před DoS útoky a lze upravit filtrování některých typů útoků na základě počtu obdržených paket. Lze zvolit nízkou, střední nebo vysokou úroveň filtrování. Rozsah pro vytvoření hranice je 5 až 7200 paketů za vteřinu, hranici pro jednotlivé úrovně filtrování lze ručně změnit. Obrázek č. 12 ukazuje původní nastavení.
Zdroj: Vlastní zpracování

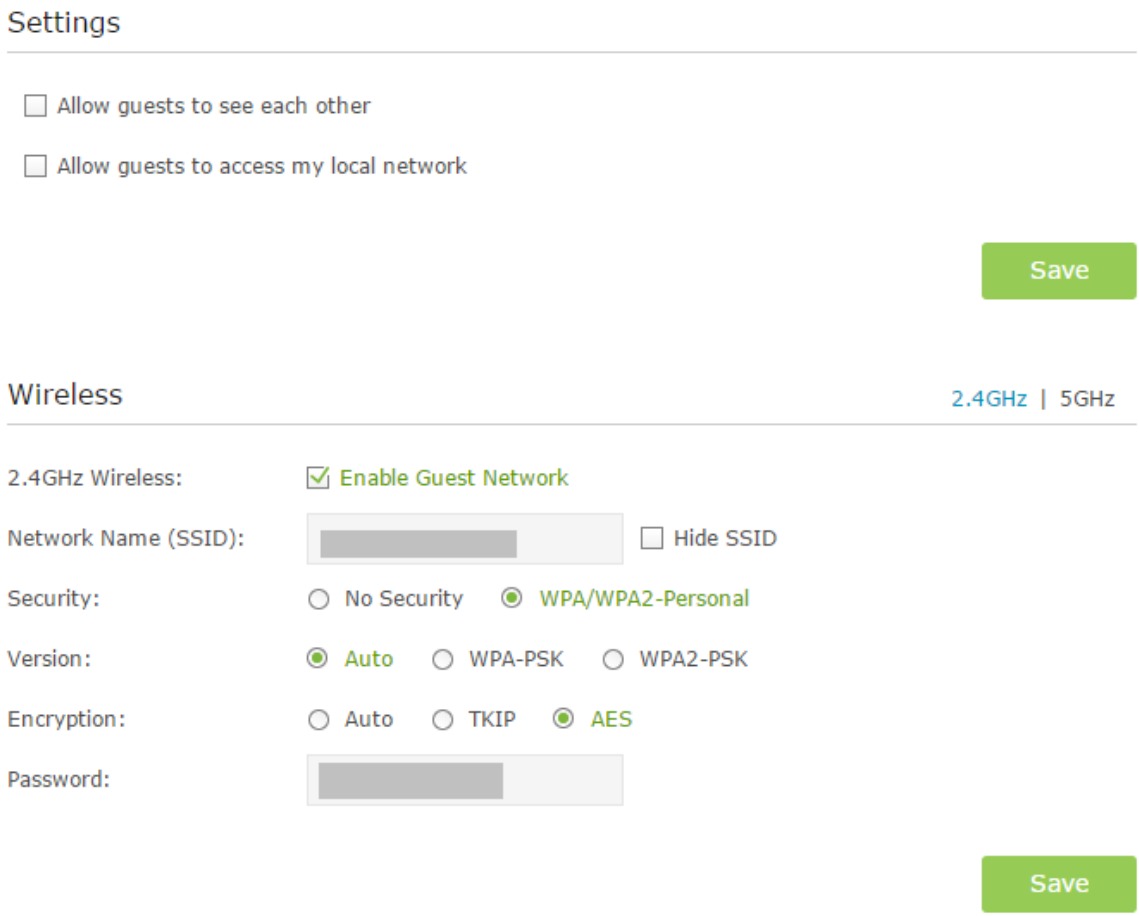


Obrázek 12 - Původní nastavení filtrování paket
Byla zvolena střední úroveň filtrování pro všechny tři typy útoků. Také bylo nastaveno, aby router jakékoliv ping pakety, které jdou z vně lokální sítě, ignoroval. Naopak ping pakety uvnitř sítě jsou povoleny. Router si v případě jákéhokoliv útoku zaznamená IP adresu a MAC adresu, ze které útok přišel a tu přidá do seznamu blokovaných adres, což ale díky možnému spoofingu nemusí zaručit, že útočník nebude moci útok zopakovat.

Zabezpečení WiFi signálu obou frekvencí na routeru je pomocí WPA/WPA2-PSK s šifrováním pomocí AES standardu a zároveň jsou obě SSID skryty. Přístup k access pointu PLC adaptéru je taktéž zabezpečen WPA/WPA2-PSK, následně byla skryta SSID. Samotná komunikace mezi powerline adaptéry je zabezpečena 128-bitovým AES šifrováním (uvádí výrobce). Dále je celý přístup do sítě regulován na základě filtrování MAC adres. Byl vytvořen whitelist zařízení, která jsou stabilně nebo pravidelně připojena

v síti. Samozřejmě se může stát, že příjde nějaká návštěva a nikdo z nich by se nemohl připojit v této domácnosti k síti, potažmo k Internetu. Byla tedy vytvořena síť pro hosty, která je vysílána na 2.4 GHz frekvenci (je i možné vytvořit síť pro hosty na 5 Ghz frekvenci, není pro ní ale v tomto případě využití), s viditelným SSID. Je zabezpečena stejným způsobem, tedy WPA/WPA2-PSK, ovšem s jiným přístupovým heslem, než mají ty se skrytým SSID. Dále je zakázáno, aby zařízení připojená v síti pro hosty měla přístup do lokální sítě, slouží tedy čistě k tomu, aby návštěvníci měli přístup k Internetu.

Zdroj: Vlastní zpracování



Obrázek 13 - Nastavení sítě pro hosty

4.3 Testování technologií

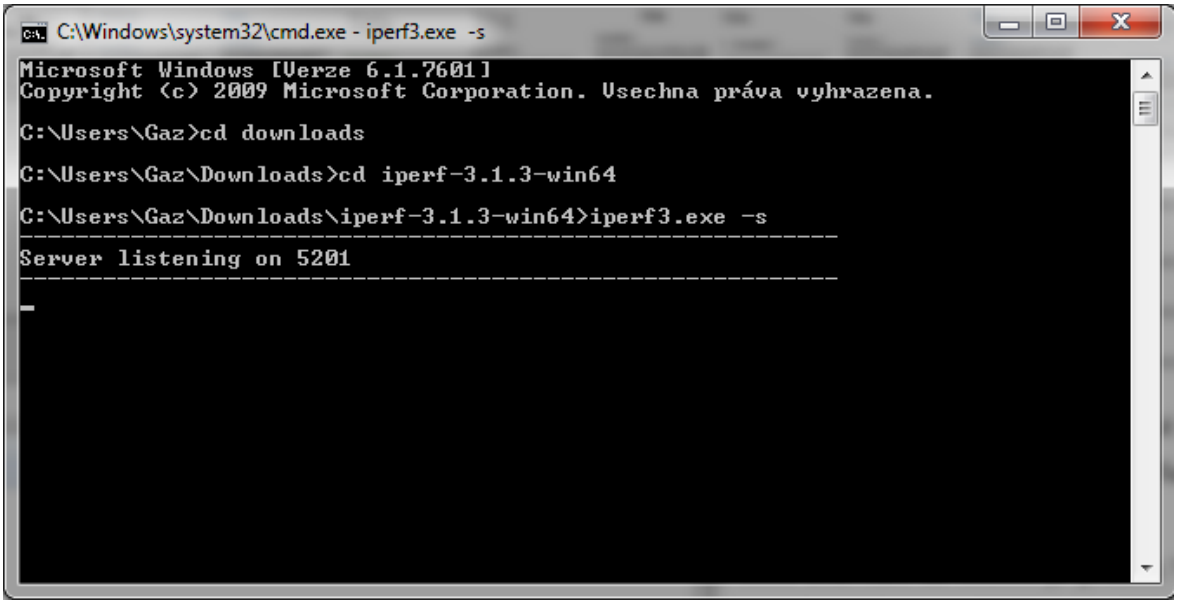
4.3.1 Charakteristika testovacích programů a podmínek testování

Po konstrukci a zabezpečení sítě byla otestována přenosová rychlost při různých variantách použitých technologií pro připojení počítače k lokální síti. Pro testování byly použity dva

freewarové programy – Iperf a NetStress. Oba programy vyžadují, aby byl program spuštěn (NetStress je nutné nainstalovat) souběžně na dvou počítačích. První počítač funguje jako server, pomocí něj testujeme druhý počítač, který je uváděn jako klient. Serverový počítač byl ve všech měřeních připojen k routeru ethernetovým kabelem a to z důvodu, aby na tomto úseku byla co nejmenší ztrátovost. Pro minimalizaci provozu na síti byl odpojen ethernetový kabel z WAN portu zajišťující připojení k Internetu a všechna ostatní zařízení byla odpojena, nebo vypnuta. Jak na serverovém, tak i na klientském počítači byly vypnuty soukromé firewally, aby nedošlo k nechtěnému blokování komunikace.

Nastavení serverového počítače u programu Iperf je jednoduché. Příkazy jsou zadávány přes Windows příkazovou řádku. Server je založen spuštěním souboru iperf.exe s příslušným parametrem. Poté stačí na testovaném počítači spustit stejný soubor s parametrem pro klientský režim, popřípadě dalšími parametry jako doba testování, velikost poslaných testovacích dat a další. Server naslouchá na portu 5201.

Zdroj: Vlastní zpracování



Obrázek 14 - Spuštění Iperf serveru

U programu NetStress se po jeho spuštení dá nastavit, zda počítač má být trasmitter (posílat data) nebo receiver (přijímat data). Podobně jako u Iperf, i zde je možné měnit nastavení měření jako například zda budou posílány data přes TCP nebo UDP protokol (TCP je výchozí), nebo objem dat a další. Na jednom z počítačů pak stačí nastavit IP adresu počítače druhého a je možné začít měření.

Zdroj: Vlastní zpracování

Obrázek 15 - Uživatelské rozhraní programu NetStress

Na testovaném počítači byla měřena přenosová rychlost při zapojení přes:

- Ethernetový kabel k routeru
- WiFi routeru
- Ethernetový kabel k powerline adaptéru
- WiFi powerline adaptéru

Protože využití PLC technologie závisí na stavu rozvodné sítě, bylo při jejím použití testováno zapojení obou powerline adaptérů na stejné fázi (ve stejném obvodu) a zapojení v různé fázi (signál musí projít přes rozvodnou skříň). V obou situacích bylo provedeno měření, kdy v zásuvce byl nejdříve připojen pouze powerline adaptér a poté byla do stejné zásuvky připojena zařízení – notebook s připojeným nabíjecím adaptérem, telefon s připojeným nabíjecím adaptérem a rychlovarná konvice, která v době měření ohřívá vodu. Při testování přes WiFi bylo vždy na druhém access pointu zakázáno vysílání bezdrátového signálu, aby nedošlo k připojení k jinému access pointu, než který byl testován. Rychlost byla testována pouze na 2,4 GHz frekvenci, protože testovaný počítač nepodporuje standardy pro 5 GHz frekvenci. Programem Iperf, byla rychlost testována desetivteřinovými intervaly s třemi opakováními, u programu NetStress byl testován třicetivteřinovým intervalem.

4.3.2 Provedení měření

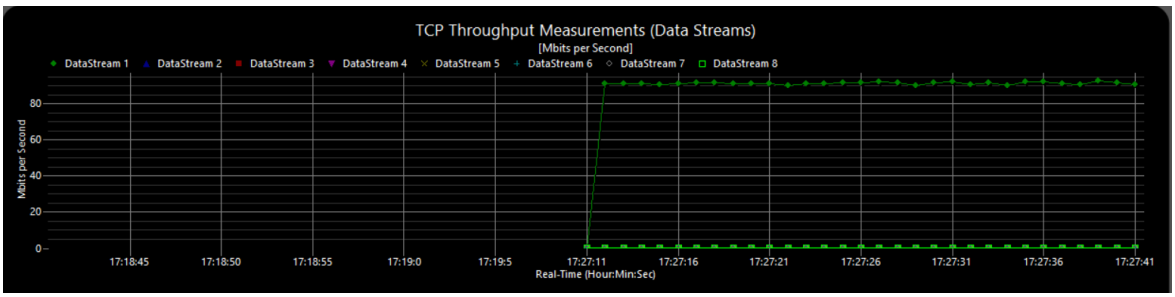
Přípojení testovaného počítače přes etheretnový kabel k routeru, ke kterému je připojen i server, je z hlediska přenosové rychlosti ta nejlepší varianta. Reálná rychlost se pohybuje pouze o trochu níže, než teoretických 100 Mbps. Pomocí Iperf bylo naměřena rychlost okolo 93-94 Mbps. Program NetStress naměřil stabilně podobné hodnoty (obrázek č. 16 a 17).

Zdroj: Vlastní zpracování

```
C:\Users\Uher\Desktop\iperf-3.1.3-win64>iperf3.exe -c 192.168.0.24
Connecting to host 192.168.0.24, port 5201
[  4] local 192.168.0.113 port 58843 connected to 192.168.0.24 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.01   sec  11.4 MBytes  94.6 Mbits/sec
[  4]   1.01-2.01   sec  11.0 MBytes  91.8 Mbits/sec
[  4]   2.01-3.01   sec  11.1 MBytes  93.9 Mbits/sec
[  4]   3.01-4.00   sec  11.1 MBytes  93.7 Mbits/sec
[  4]   4.00-5.01   sec  11.4 MBytes  94.8 Mbits/sec
[  4]   5.01-6.00   sec  11.2 MBytes  95.0 Mbits/sec
[  4]   6.00-7.01   sec  11.4 MBytes  94.9 Mbits/sec
[  4]   7.01-8.01   sec  11.1 MBytes  93.3 Mbits/sec
[  4]   8.01-9.00   sec  11.2 MBytes  94.9 Mbits/sec
[  4]   9.00-10.00  sec  11.1 MBytes  93.2 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.00  sec   112 MBytes  94.0 Mbits/sec                  sender
[  4]   0.00-10.00  sec   112 MBytes  93.9 Mbits/sec                  receiver

iperf Done.
```

Obrázek 16 - Měření přes ethernetový kabel (Iperf)

Zdroj: Vlastní zpracování



Obrázek 17 - Měření přes ethernetový kabel (NetStress)

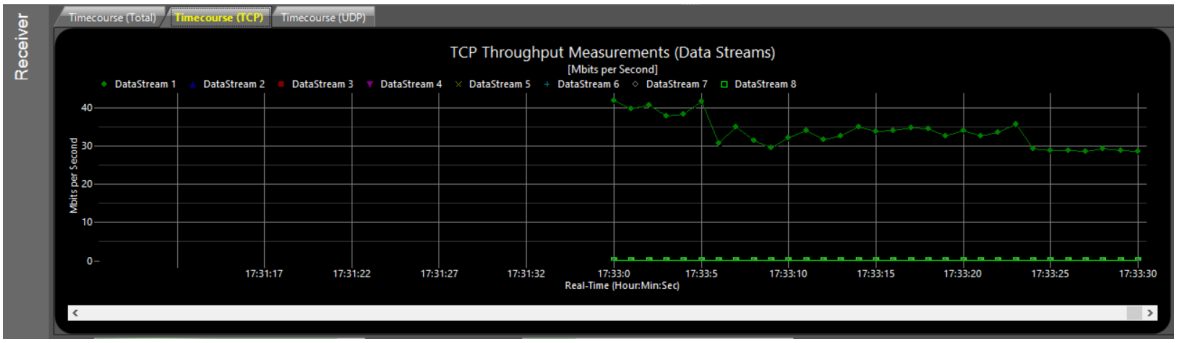
V dalším měření byl počítač připojen k WiFi na vzdálenost několika metrů, přenosová rychlost byla nižší, než u ethernetového kabelu a na naměřených hodnotách bylo patrné, že i méně stabilní. Hodnoty v programu Iperf se pohybovaly přibližně mezi 37 až 46 Mbps (obrázek č.18), NetStress naměřil hodnoty přibližně mezi 28 až 42 Mbps (obrázek č.19).

Zdroj: Vlastní zpracování

```
C:\Users\Uher\Desktop\iperf-3.1.3-win64>iperf3.exe -c 192.168.0.24
Connecting to host 192.168.0.24, port 5201
[  4] local 192.168.0.121 port 58802 connected to 192.168.0.24 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.01   sec  5.50 MBytes  45.5 Mbits/sec
[  4]   1.01-2.01   sec  5.12 MBytes  43.2 Mbits/sec
[  4]   2.01-3.00   sec  5.38 MBytes  45.4 Mbits/sec
[  4]   3.00-4.01   sec  5.38 MBytes  44.6 Mbits/sec
[  4]   4.01-5.00   sec  5.25 MBytes  44.6 Mbits/sec
[  4]   5.00-6.00   sec  5.50 MBytes  46.1 Mbits/sec
[  4]   6.00-7.00   sec  3.88 MBytes  32.5 Mbits/sec
[  4]   7.00-8.00   sec  1.88 MBytes  15.7 Mbits/sec
[  4]   8.00-9.01   sec  1.50 MBytes  12.5 Mbits/sec
[  4]   9.01-10.00  sec  5.25 MBytes  44.2 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.00  sec  44.6 MBytes  37.4 Mbits/sec                  sender
[  4]   0.00-10.00  sec  44.6 MBytes  37.4 Mbits/sec                  receiver

iperf Done.
```

Obrázek 18 - Měření přes WiFi (Iperf)

Zdroj: Vlastní zpracování



Obrázek 19 - Měření přes WiFi (NetStress)

U použití powerline adaptérů se naměřené hodnoty velmi liší. Jako první byla testována rychlost při zapojení adaptérů na stejné fázi. Při připojení počítače k adaptéru ethernetovým kabelem se přenosová rychlost v programu Iperf pohybovala okolo 70 Mbps. Při připojení dalších zařízení do zásuvky rychlost klesla na 60 až 65 Mbps (obrázek č.20).

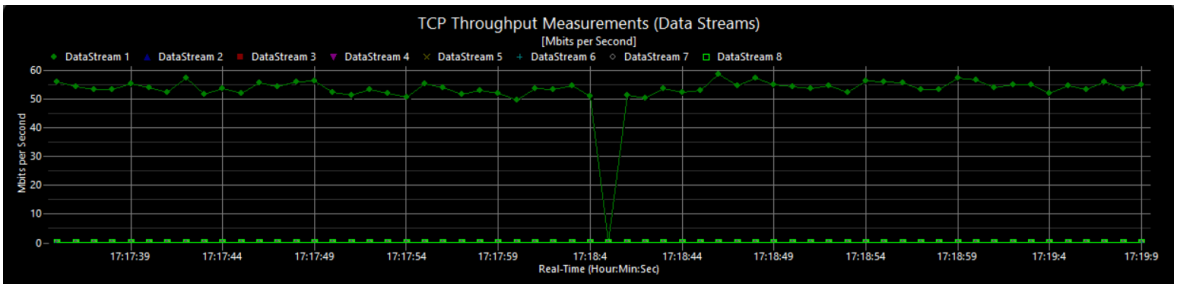
Zdroj: Vlastní zpracování

```
C:\Users\Uher\Desktop\iperf-3.1.3-win64>iperf3.exe -c 192.168.0.24
Connecting to host 192.168.0.24, port 5201
[  4] local 192.168.0.113 port 59181 connected to 192.168.0.24 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.01   sec  9.75 MBytes  80.8 Mbits/sec
[  4]   1.01-2.01   sec  8.00 MBytes  67.0 Mbits/sec
[  4]   2.01-3.00   sec  9.62 MBytes  81.8 Mbits/sec
[  4]   3.00-4.01   sec  9.12 MBytes  76.2 Mbits/sec
[  4]   4.01-5.00   sec  7.25 MBytes  61.1 Mbits/sec
[  4]   5.00-6.00   sec  8.75 MBytes  73.3 Mbits/sec
[  4]   6.00-7.00   sec  9.00 MBytes  75.3 Mbits/sec
[  4]   7.00-8.00   sec  7.62 MBytes  64.0 Mbits/sec
[  4]   8.00-9.00   sec  6.12 MBytes  51.6 Mbits/sec
[  4]   9.00-10.00  sec  8.25 MBytes  69.3 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.00  sec  83.5 MBytes  70.0 Mbits/sec                  sender
[  4]   0.00-10.00  sec  83.5 MBytes  70.0 Mbits/sec                  receiver

iperf Done.
C:\Users\Uher\Desktop\iperf-3.1.3-win64>iperf3.exe -c 192.168.0.24
Connecting to host 192.168.0.24, port 5201
[  4] local 192.168.0.113 port 59185 connected to 192.168.0.24 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.00   sec  5.75 MBytes  48.2 Mbits/sec
[  4]   1.00-2.00   sec  6.38 MBytes  53.4 Mbits/sec
[  4]   2.00-3.00   sec  7.38 MBytes  61.9 Mbits/sec
[  4]   3.00-4.01   sec  7.12 MBytes  59.5 Mbits/sec
[  4]   4.01-5.01   sec  7.38 MBytes  61.8 Mbits/sec
[  4]   5.01-6.00   sec  7.62 MBytes  64.2 Mbits/sec
[  4]   6.00-7.01   sec  7.75 MBytes  64.6 Mbits/sec
[  4]   7.01-8.01   sec  8.50 MBytes  71.1 Mbits/sec
[  4]   8.01-9.00   sec  7.88 MBytes  66.8 Mbits/sec
[  4]   9.00-10.00  sec  8.00 MBytes  67.0 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.00  sec  73.8 MBytes  61.8 Mbits/sec                  sender
[  4]   0.00-10.00  sec  73.7 MBytes  61.8 Mbits/sec                  receiver

iperf Done.
```

Obrázek 20 - Měření přes s ethernetovým kabelem z powerline bez a se zatížením, stejná fáze (Iperf)

Ovšem při testování za stejných podmínek s programem NetStress se přenosová rychlost pohybovala 60 až 50 Mbps bez ohledu na zatížení zásuvky dalšími zařízeními. Z grafu programu NetStress na obrázku č. 21 je patrné, že jeho první polovina (při zátěži el. sítě) se výrazně neliší od druhé poloviny (bez zátěže) grafu.

Zdroj: Vlastní zpracování



Obrázek 21 - Měření přes s ethernetovým kabelem z powerline bez a se zatížením, stejná fáze (NetStress)

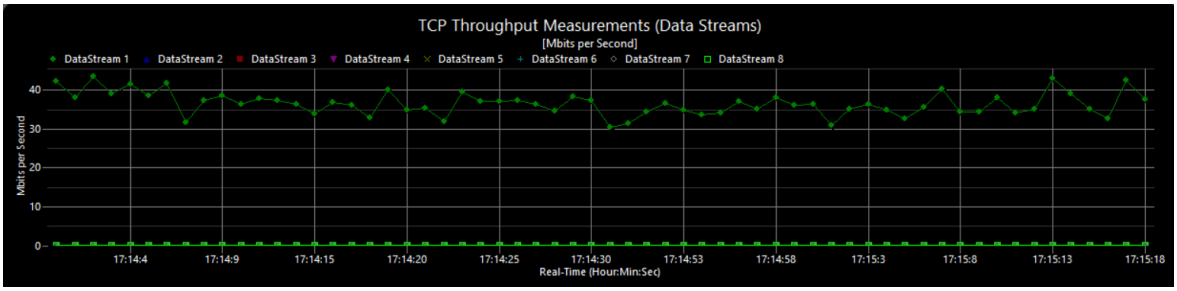
Při zapojení počítače k WiFi powerline adaptéru, který je zapojen ve stejné fázi, byly naměřené hodnoty podobné hodnotám naměřeným při připojení přes WiFi routeru. Iperf naměřil přenosovou rychlost mezi 30 až 36 Mbps bez zatížení zásuvky. Při zatížení rychlost klesla na rozmezí mezi 26 a 32 Mbps (obrázek č.22). Jako u připojení přes ethernetový kabel, i zde ale NetStress nenaměřil zásadní rozdíl v přenosové rychlosti, která se pohybovala mezi 30 a 45 Mbps (obrázek č.23).

Zdroj: Vlastní zpracování

```
C:\Users\Uher\Desktop\iperf-3.1.3-win64>iperf3.exe -c 192.168.0.24
Connecting to host 192.168.0.24, port 5201
[  4] local 192.168.0.121 port 59257 connected to 192.168.0.24 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.00   sec  3.12 MBytes  26.2 Mbits/sec
[  4]   1.00-2.01   sec  5.12 MBytes  42.6 Mbits/sec
[  4]   2.01-3.01   sec  3.88 MBytes  32.5 Mbits/sec
[  4]   3.01-4.01   sec  4.38 MBytes  36.6 Mbits/sec
[  4]   4.01-5.01   sec  4.38 MBytes  36.6 Mbits/sec
[  4]   5.01-6.01   sec  4.25 MBytes  35.9 Mbits/sec
[  4]   6.01-7.01   sec  4.12 MBytes  34.6 Mbits/sec
[  4]   7.01-8.01   sec  4.12 MBytes  34.4 Mbits/sec
[  4]   8.01-9.00   sec  4.00 MBytes  33.9 Mbits/sec
[  4]   9.00-10.01  sec  5.12 MBytes  42.7 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.01  sec  42.5 MBytes  35.6 Mbits/sec                  sender
[  4]   0.00-10.01  sec  42.5 MBytes  35.6 Mbits/sec                  receiver

iperf Done.
C:\Users\Uher\Desktop\iperf-3.1.3-win64>iperf3.exe -c 192.168.0.24
Connecting to host 192.168.0.24, port 5201
[  4] local 192.168.0.121 port 59249 connected to 192.168.0.24 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.01   sec  4.12 MBytes  34.3 Mbits/sec
[  4]   1.01-2.01   sec  3.75 MBytes  31.4 Mbits/sec
[  4]   2.01-3.00   sec  3.12 MBytes  26.4 Mbits/sec
[  4]   3.00-4.01   sec  4.75 MBytes  39.8 Mbits/sec
[  4]   4.01-5.01   sec  4.50 MBytes  37.5 Mbits/sec
[  4]   5.01-6.00   sec  2.75 MBytes  23.2 Mbits/sec
[  4]   6.00-7.01   sec  3.88 MBytes  32.5 Mbits/sec
[  4]   7.01-8.01   sec  0.00 Bytes  0.00 bits/sec
[  4]   8.01-9.00   sec  3.88 MBytes  32.7 Mbits/sec
[  4]   9.00-10.00  sec  6.50 MBytes  54.4 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.00  sec  37.2 MBytes  31.2 Mbits/sec                  sender
[  4]   0.00-10.00  sec  37.2 MBytes  31.2 Mbits/sec                  receiver

iperf Done.
```

Obrázek 22 - Měření přes WiFi z powerline bez a se zatížením, stejná fáze (Iperf)

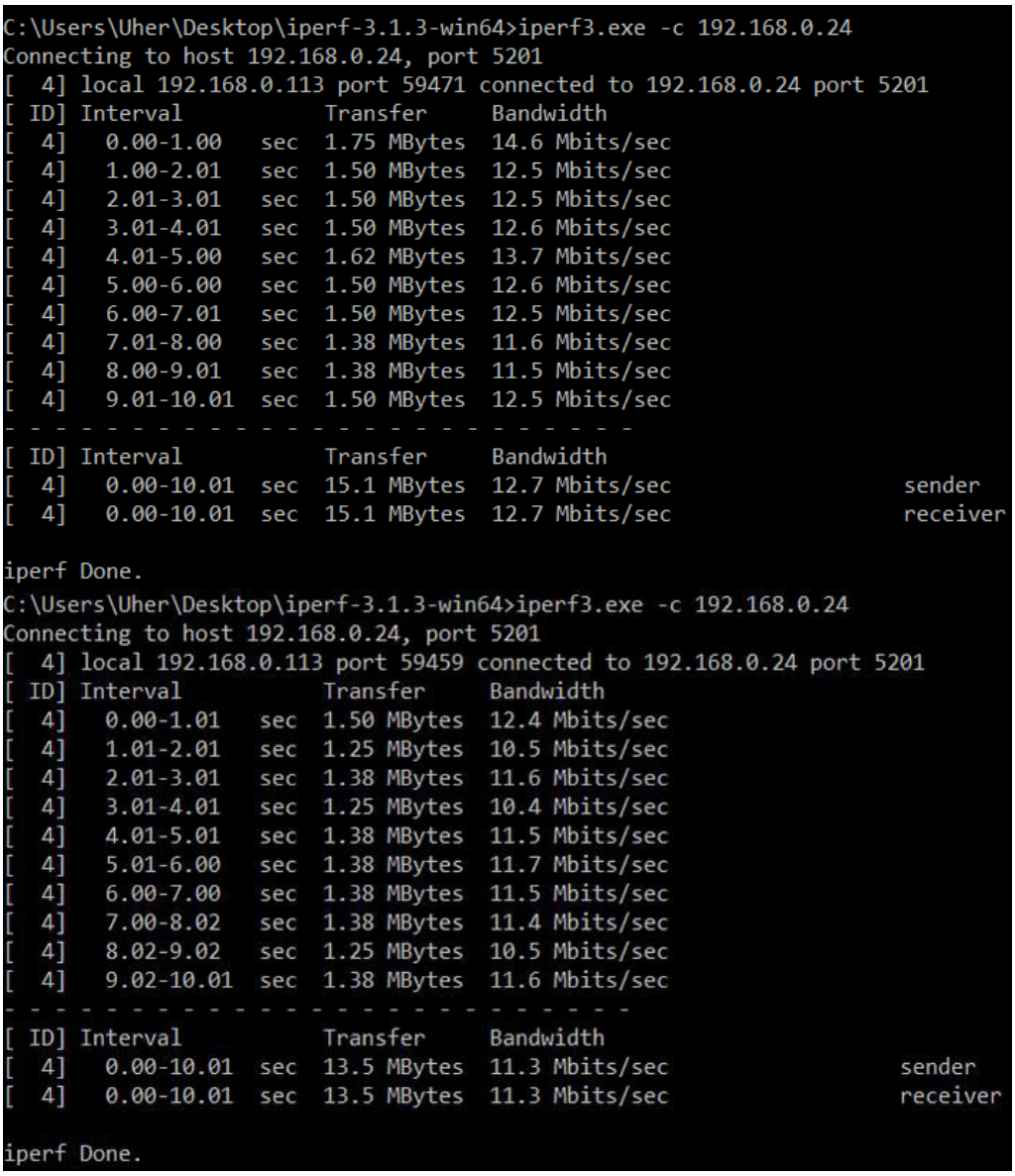
Zdroj: Vlastní zpracování



Obrázek 23 - Měření přes WiFi z powerline bez a se zatížením, stejná fáze (NetStress)

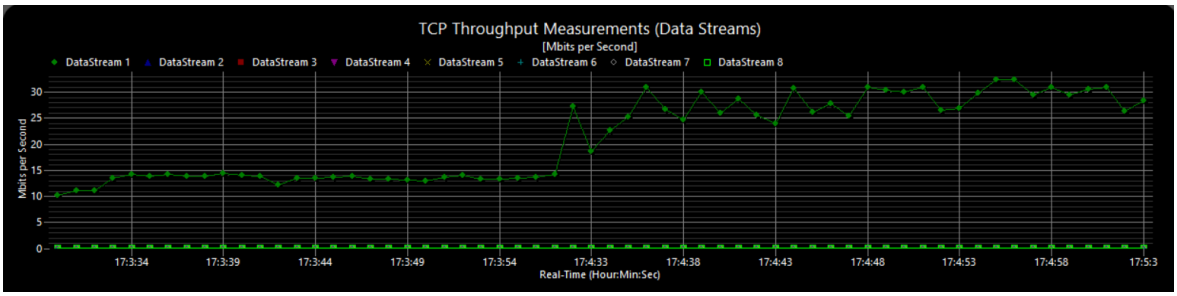
V případě, že byly powerline adaptér zapojeny v rozdílných fázích, naměřené rychlosti byly podstatně nižší, než u adaptérů zapojených ve stejné fázi. Při připojení k adaptéru ethernetovým kabelem se přenosová rychlost pohybovala pohybovala mezi 12 až 15 Mbps, při zatížení sítě rychlost klesla v řádu několika jednotek Mbps na 9 až 12 Mbps (obrázek č.24). Měření v NetStress odhalilo znatelný pokles rychlosti přenosu dat při zatížení sítě (obrázek č.25).

Zdroj: Vlastní zpracování



Obrázek 24 - Měření přes s ethernetovým kabelem z powerline bez a se zatížením, různá fáze (Iperf)

Zdroj: Vlastní zpracování



Obrázek 25 - Měření přes s ethernetovým kabelem z powerline bez a se zatížením, různá fáze (NetStress)

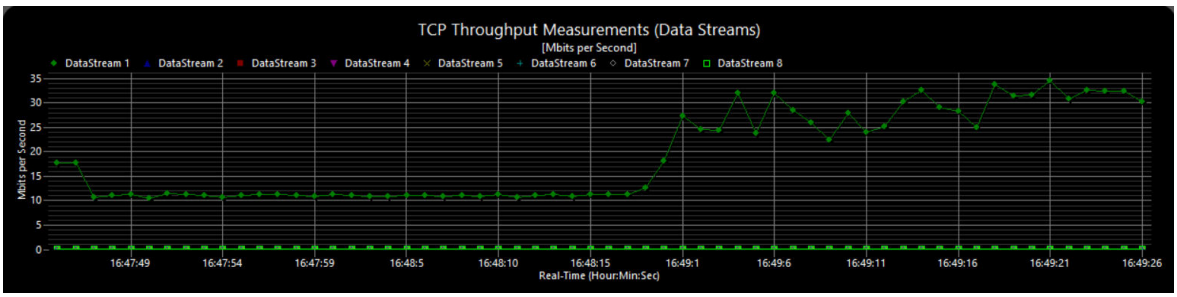
Při připojení k WiFi z powerline adaptéru přenosová rychlost klesla o několik jednotek Mbps, bez zatížení se pohybovala mezi 10 až 12 Mbps, při zatížení rychlost nepatrně klesla na hodnoty kolem 10 Mbps (obrázek č.26). Naopak měření v programu NetStress zaznamenalo větší výkyv v porovnávaných hodnotách, také je patrné, že rychlost po odpojení ostatních zařízení kolísala ve větším rozsahu než u zapojení přes ethernetový kabel (obrázek č.27).

Zdroj: Vlastní zpracování

```
C:\Users\Uher\Desktop\iperf-3.1.3-win64>iperf3.exe -c 192.168.0.24
Connecting to host 192.168.0.24, port 5201
[  4] local 192.168.0.121 port 59420 connected to 192.168.0.24 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.01   sec  1.38 MBytes  11.5 Mbits/sec
[  4]   1.01-2.00   sec  1.25 MBytes  10.5 Mbits/sec
[  4]   2.00-3.01   sec  1.25 MBytes  10.4 Mbits/sec
[  4]   3.01-4.00   sec  1.25 MBytes  10.5 Mbits/sec
[  4]   4.00-5.00   sec  1.50 MBytes  12.6 Mbits/sec
[  4]   5.00-6.01   sec  1.38 MBytes  11.4 Mbits/sec
[  4]   6.01-7.00   sec  1.50 MBytes  12.7 Mbits/sec
[  4]   7.00-8.01   sec  1.50 MBytes  12.4 Mbits/sec
[  4]   8.01-9.01   sec  1.62 MBytes  13.7 Mbits/sec
[  4]   9.01-10.01  sec  1.62 MBytes  13.6 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.01  sec  14.2 MBytes  11.9 Mbits/sec                  sender
[  4]   0.00-10.01  sec  14.2 MBytes  11.9 Mbits/sec                  receiver

iperf Done.
C:\Users\Uher\Desktop\iperf-3.1.3-win64>iperf3.exe -c 192.168.0.24
Connecting to host 192.168.0.24, port 5201
[  4] local 192.168.0.121 port 59424 connected to 192.168.0.24 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.00   sec  1.12 MBytes  9.41 Mbits/sec
[  4]   1.00-2.01   sec  1.12 MBytes  9.39 Mbits/sec
[  4]   2.01-3.01   sec  1.25 MBytes  10.5 Mbits/sec
[  4]   3.01-4.01   sec  1.25 MBytes  10.5 Mbits/sec
[  4]   4.01-5.01   sec  1.25 MBytes  10.5 Mbits/sec
[  4]   5.01-6.00   sec  1.38 MBytes  11.6 Mbits/sec
[  4]   6.00-7.01   sec  1.25 MBytes  10.4 Mbits/sec
[  4]   7.01-8.01   sec  1.38 MBytes  11.5 Mbits/sec
[  4]   8.01-9.02   sec  1.25 MBytes  10.5 Mbits/sec
[  4]   9.02-10.02  sec  1.38 MBytes  11.5 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.02  sec  12.6 MBytes  10.6 Mbits/sec                  sender
[  4]   0.00-10.02  sec  12.6 MBytes  10.6 Mbits/sec                  receiver

iperf Done.
```

Obrázek 26 - Měření přes WiFi z powerline bez a se zatížením, různá fáze (Iperf)

Zdroj: Vlastní zpracování



Obrázek 27 - Měření přes WiFi z powerline bez a se zatížením, různá fáze (NetStress)

4.3.3 Obecné doporučení

Následně bylo vytvořeno doporučení jaká technologie je, na základě vybraných kritérií, nejlepší pro stavbu domácí počítačové sítě. Na technologiích (Ethernet, WiFi, PLC) byla hodnocena tato kritéria – cena, dosah, rychlost, jednoduchost a zabezpečení. Byla použita metoda ordinálního typu – metoda pořadí.

Zdroj: Vlastní zpracování

Metoda pořadí

	Cena	Dosah	Rychlost	Jedno.	Zabezp.	SUM
Ethernet	2	2	1	3	1	9
WiFi	1	3	3	1	3	11
PLC	3	1	2	2	2	10

Tabulka 4 - Výběr technologie metodou pořadí

V kritériu cena byla hodnocena pouze pořizovací cena prvků potřebných k provozu sítě. U kritéria dosah je jako první PLC, protože se uvádí možnost šířit signál až 300 metrů, u Ethernetu jde o 100 metrů a u WiFi je díky použitému přenosovému médiu dosah značně ovlivněn prostředím, kterým se signál šíří, dosahuje zpravidla několika desítek metrů. U přenosové rychlosti je na druhém místě PLC díky výsledkům při měření (za správné konfigurace). Kritérium jednoduchost zahrnuje jednoduchost konstrukce sítě a připojení zařízení k síti – připojení může být u Ehternetu složitější kvůli nutnosti fyzicky táhnout kabel od centrálního prvku k cílovému zařízení. Zabezpečení představuje míru využití dané technologie k napadení sítě – WiFi je díky svému přenosovému médiu jako nejzranitelnější na poslední místě. K tomuto výpočtu nebyly využity metody využívající váhy jednotlivých kritérií z důvodu zachování jejich rovnocennosti. Metodou pořadí vyšla nejlépe varianta Ethernet, druhá PLC a třetí WiFi.

5 Výsledky a diskuse

Síť, která byla v domácnosti vytvořena, je dále předmětem sledování a případného vylepšování. Použité prvky je možné měnit za lepší za účelem zvýšení přenosu dat, šlo by například o instalaci gigabitového switche a tím dosáhnout GLAN, nebo šířit WiFi signál směrovými anténami, dále by bylo možné zvýšit zabezpečení přidáním dalších bezpečnostních funkcí jako například IDS/IPS (Intrusion Detection System/Intrusion Prevention System) nebo použitím DMZ (De-Militarized Zone).

Výsledky samotného měření přenosové rychlosti ukázalo zajímavé výsledky v porovnání Ethernetu a WiFi s kombinací powerline adaptérů. Propojení přes Ethernet je dle měření nejlepší variantou. Připojení přes WiFi dosáhlo horších výsledků, ale především díky své jednoduchosti šíření signálu jde stále o nejrozšířenější způsob tvorby domácí počítačové sítě. Ovšem měření při použití powerline adaptérů ukázalo, že při správné konfiguraci lze PLC technologii považovat za dobrou alternativu k šíření signálu v domácnosti. Výrobci kladou důraz na to, že propojené adaptéry musí být na stejné fázi pro dosažení dobré přenosové rychlosti – to měření potvdila. V situaci, kdy jsou adaptéry v rozdílných fázích, měření ukázala, že rychlost výrazně klesá. Problém rozdílné fáze by bylo možné řešit spojením fází patřičnou elektrosoučástkou. Jinak je nejspíše vhodné uvažovat o použití jiné technologie. Zajímavé bylo, že při měření přenosu přes powerline adaptéry byly naměřeny, v některých zásuvkách v rámci stejného obvodu, odlišné hodnoty (přibližne o 10 až 15 Mbps) i když zátěž daného elektrického obvodu zůstala neměnná. To by mohlo být zapříčiněno stavem elektrické sítě. Dále měření v programu Iperf ukázala, že zapojením dalších zařízení do stejné zásuvky, ve které je zapojen adaptér, klesla přenosová rychlost pouze v řádu několika jednotek Mbps. Naopak program NetStress ukázal, že při zatížení zásuvky byla přenosová rychlost výrazně nižší, ale pouze při zapojení v rozdílné fázi, při stejné fázi nebyla rychlost odlišná. Nutno však také podotknout, že při měření v rozdílné fázi program NetStress naměřil vyšší hodnoty bez zátěže, než naměřil program Iperf (např. u ethernetového kabelu Iperf přibližně 12-15 Mbps, NetStress 25-35 Mbps). Pro přesnější výsledky by mohlo být zvýšen počet opakování, nebo zvýšit časový rámec jednotlivého měření. Naměřené hodnoty obou programů byly porovnávány s několika webovými portály zabývající se počítačovou tématikou, které provedly podobná měření, a více skutečné vypadají hodnoty naměřené v programu Iperf.

Výsledky obecného doporučení využití technologií by se mohly lišit, pakliže by daná kritéria hodnotil jiný rozhodovatel, nebo kdyby byla zvolena jiná metoda. Zvolení určité technologie či jejich kombinací ale často závisí na prostředí a za jakým účelem je počítačová síť realizována.

6 Závěr

Cílem práce bylo zkonstruovat síť v domácnosti, zvolit vhodné síťové prvky a adekvátně domácí síť zabezpečit. V teoretické části byly charkterizovány používané síťové prvky a protokoly se kterými se lze setkat. Byly chrakterizovány možnosti zabezpečení bezdrátového přenosu a domácí počítačové sítě jako celku.

V praktické části byla charakterizována domácnost ve které byla síť realizována. Dále byl charakterizován výběr prvků spolu s jejich vlastnostmi a konfigurace síťových prvků a zařízení. Následně byla ukázána konfigurace zabezpečení celkové domácí sítě a konfigurace zabezpečení bezdrátového přenosu.

Poté bylo provedeno měření použitých technologií, které mělo porovnat využití technologie PLC používající k šíření signálu elektrickou síť s dalšími použitými jako jsou Ethernet a WiFi. Bylo testováno několik způsobů zapojení s důrazem na to, jak ovlivní přenosovou rychlost zvýšený odběr ve stejné zásuvce. Bylo zjištěno, že zvýšená zátěž ve stejné zásuvce snižuje přenosovou rychlost, ale pokles není výrazný. Dále bylo testováno zapojení do stejné a rozdílné fáze. Bylo zjištěno, že při měření v rozdílné fázi je přenosová rychlost výrazně snížena, naopak při stejné fázi dosahuje dobrých výsledků.

Nakonec byla sestavena kriteriální tabulka pro používané technologie a pomocí jednoduché rozhodovací metody byla doporučena nejlepší možnost pro konstrukci domácí počítačové sítě.

7 Seznam použitých zdrojů

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

HORÁK, Jaroslav, KERŠLÁGER, Miroslav. Počítačové sítě pro začínající správce. 5., aktualiz. vyd. Brno: Computer Press, 2013. ISBN 978-80-251-3176-3

NORTHCUTT, Stephen. Inside network perimeter security. 2nd ed. Indianapolis, Ind.: Sams Pub., c2005. ISBN 0-672-32737-6

SPURNÁ, Ivona. Počítačové sítě: praktická příručka správce sítě. Kralice na Hané: Computer Media, c2010. ISBN 978-80-7402-036-0

SCHMIDT, Christoph, KUBEŠ, Radek. Informace, testy a novinky o hardware, software a internetu – CHIP.cz [online]. Copyright ©2 [cit. 08.03.2017]. Dostupné z: http://www.chip.cz/soubory/dokumenty/01-14-046-powerline-wifi.pdf

HANÁK, Jiří. Postavte se velké vodě: Nejčastějšími DDoS útoky jsou SYN a UDP záplavy - Blog Master.cz. Server Hosting, Housing, Virtuální servery VPS - Master Internet [online]. Copyright © 2017 Master Internet, s.r.o. [cit. 08.03.2017]. Dostupné z: https://www.master.cz/blog/jak-funguji-ddos-utoky-typy-ddos-syn-udp-zaplavy/

Understanding UDP Flood Attacks - Technical Documentation - Support - Juniper Networks. 301 Moved Permanently [online]. Copyright © 1999 [cit. 08.03.2017]. Dostupné z: https://www.juniper.net/documentation/en_US/junos12.1x44/topics/concept/denial-of-service-network-udp-flood-attack-understanding.html

Čtyři nejdůležitější rady pro plánování bezdrátových sítí. Object moved [online]. Copyright © [cit. 08.03.2017]. Dostupné z: http://www.moxa.cz/NewsLetter/newsletter_2014_01_A.html

EVANS, Dean. Powerline networking: what you need to know: Page 2 | TechRadar. TechRadar | The source for tech buying advice | TechRadar [online]. Copyright © [cit. 09.03.2017]. Dostupné

z: http://www.techradar.com/news/networking/powerline-networking-what-you-need-to-know-930691/2

WDM v optických metro a přístupových sítích - Lupa.cz. Lupa.cz - server o českém Internetu [online]. Copyright © 1998 [cit. 12.03.2017]. Dostupné z: http://www.lupa.cz/clanky/wdm-v-optickych-metro-a-pristupovych-sitich/

8 Přílohy

Příloha A - Výsledky měření (Mbps) 55
Zdroj: Vlastní zpracování

Ethernet	WiFi
93,7	37,4
94,0	45,8
93,4	42,2
STEJNÁ FÁZE	ROZDÍLNÁ FÁZE
PLC + Ethernet	
70,0	12,7
72,5	14,3
74,8	13,1
PLC + Ethernet, zatížení	
64,7	11,3
61,8	9,8
63,2	10,8
PLC + WiFi	
35,6	11,9
31,4	10,3
30,8	10,8
PLC + WiFi, zatížení	
26,4	10,6
28,8	9,5
31,2	9,8

Příloha A - Výsledky měření (Mbps)