Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Zabezpečení malé domácí sítě

Bakalářská práce

Autor: Viktor Míčka
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Pavel Blažek, Ph.D.

Jilemnice Březen 2020

Prohlášení:

Prohlašuji, že jsem práci zpracoval samostatně. Použity byly pouze uvedené prameny v seznamu literatury.

vlastnoruční podpis

V Jilemnici dne 15.11.2020 Viktor Míčka

Poděkování:

Rád bych poděkoval svému vedoucímu práce, Ing. Pavlu Blažkovi, Ph.D., za pomoc, ochotu a zpětnou vazbu při vypracování této práce. Velký dík také patří celé rodině za podporu.

Abstrakt

Hlavním cílem této bakalářské práce je představit základní principy bezpečnosti v počítačových sítích, jejich fungování a návrh, jak takový příklad zabezpečení domácí sítě může vypadat. V úvodní části práce se pojednává o počítačové síti a jejích prvcích, jsou zde představeny standardy a principy, jak počítačová síť funguje, a také rozdělení sítí. Následně jsou popsány možnosti zabezpečení a ochrany proti těm nejnebezpečnějším hrozbám i samotné ochranné mechanizmy. Nakonec je zde ukázán návrh konkrétního routeru ASUS RT-N12D1, a to včetně představení domácí sítě, konfigurace jejího nastavení, demonstrace bezpečnostních prvků, síťových nástrojů a provedení testů.

Abstract

Title: Home network security

The main goals of this bachelor‘s thesis are to introduce basic principles of home network security, its management and a suggestion of home network security. In the beginning the thesis explains a computer network and its network devices, how the whole computer network and its principles work and also its partitioning. Next up there are described options of security and protection against the most dangerous network threats as well as security mechanisms themselves. Final part shows the home network security via the specific ASUS-RTN12D1 router, featuring the introduction of home network, its configuration settings, demonstration of security features, network tools and testing.

Obsah

Seznam obrázků

1 Úvod

S narůstající vlnou kybernetických hrozeb a internetové kriminality se běžný uživatel denně potýká s velkým nebezpečím. Byť se technologie vyvíjejí stále směrem kupředu i po stránce zabezpečení, je mnohdy pouze otázkou času, kdy to, co je bezpečné dnes, nebude bezpečné zítra. Útočníci jsou si však této skutečnosti často vědomi a zaměřují se spíše na slabiny člověka, jeho zvědavost a hloupost, což je v mnoha případech daleko jednodušší a časově méně náročné než překonávat současné technologie zabezpečení.

Online svět se rok od roku rozrůstá – téměř každé zařízení je připojeno do světa internetu. Běžně dnes v domácnosti nalezneme několik takových zařízení na jednoho člověka. Přibývá stále více inteligentních zařízení, počínaje jednoduchými senzory či snímači a konče komplexními chytrými domácnostmi. Bezpečnost ve světě internetu se tak stává citlivou a zranitelnou součástí života člověka.

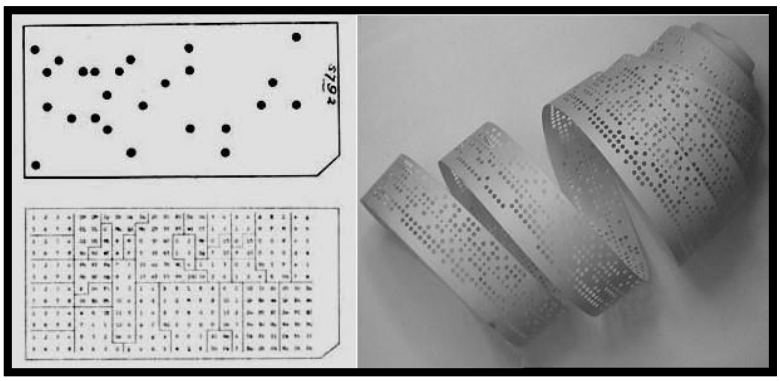
Stále populárnější a častější se také rok od roku stává „home office“ neboli práce z domova, kdy se potřeba mít spolehlivé, a především bezpečné připojení, stává důležitější, něž kdykoliv jindy. Součástí spousty domácích bezdrátových sítí jsou také rodiny s dětmi, které může správně nastavená a zabezpečená síť zachránit od toho nejhoršího. Bezpečnost v sítích není přitom nic složitého, stejně tak jako základně zabezpečit svou domácí síť – přesně tím se zabývá i tato práce.

2 Počítačová síť a její prvky

2.1 Princip a rozdělení sítí

Základním principem počítačové sítě je vzájemné propojení zařízení (počítačů) takovým způsobem, že mezi sebou mohou vést komunikaci, a to již při dvou zařízeních.

V počátcích se data zpočátku sdílela pomocí přenosových médií, jako jsou děrné štítky, pásky či diskety. Takové systémy byly nazývány nespřaženými, neboť veškeré dění probíhalo offline. Vzhledem k vývoji ve světě informačních technologií a narůstajících nároků na přenosovou rychlost a vzdálenost je však zanedlouho nahradily systémy spřažené – online. [1]



Obrázek 1 *Děrný štítek (vlevo) a děrná páska (vpravo), zdroj: [1]*

Existuje celá řada technologií, jak může být počítačová síť propojena, počínaje natažením drátů či kabelů, přes optická vlákna či telefonní linky až po bezdrátové způsoby jako je např. Wi-Fi[1] technologie. Nejčastěji se však tyto technologie v praxi kombinují a vhodně doplňují. To nejdůležitější pak představují tzv. síťové prvky, ty se starají jak o zajištění a realizaci spojení, tak i o samotnou výměnu dat mezi připojenými zařízeními. [2]

[1] Wi-Fi označuje standardy pro bezdrátovou komunikaci v počítačových sítích

Obrázek 2 *Počítačová síť, zdroj: Obrázek [2]*

2.1.1 Standard IEEE 802.11

802.11 je označená standardizace, často také nazývána jako Wi-Fi standard, za jejímž vývojem stojí dodnes standardizační komise IEEE, přesněji tedy IEEE 802. Tato skupina standardů definuje bezdrátové rozhraní, jak probíhá síťový přenos mezi koncovými bezdrátovými zařízeními a přístupovými body pracovních stanic – díky těm se Wi-Fi zařízení dokážou připojit do sítě. Rozhraní se také vztahuje ke dvěma či více bezdrátovým klientům. Komise IEEE však vyvíjí souběžně celou řadu dalších standardů, jako je například standard 802.3 pro Ethernet. [3]

Tyto standardy hrají ve skutečnosti velmi důležitou roli v sítích. Slouží totiž pro všechny výrobce a dodavatele v tomto oboru jako vodítkem pro předpisy a specifikace, které je nutno dodržet, aby byly jejich produkty plně kompatibilní. Stejně tak se tím i zajišťuje, aby si veškerá zařízení rozuměla mezi sebou a dokázala si předávat informace. [3]

Vůbec první standard IEEE vznikl poprvé v roce 1997 pod původním označením 802.11 a dnes je již zastaralý a nepoužívaný. Nejnovější standardizací je v současnosti IEEE 802.11ac, nazývaná také Wi-Fi 5. [3]

2.1.2 Rozdělení z hlediska velikosti

Jeden ze způsobů, jak můžeme dělit počítačové sítě je dle jejich rozsahu a velikosti. Historicky se v oblasti sítí odkazuje ke strukturám sítí jako k samostatným typům. Mezi nejznámějšími a nejčastěji používanými zástupci jsou LAN a WAN sítě.

2.1.2.1 LAN

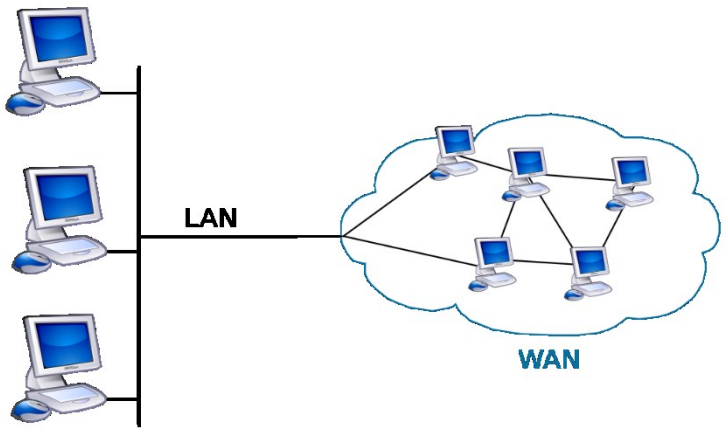
LAN (Local Area Network) neboli lokální sítě propojují zařízení napříč kratšími vzdálenostmi. Typickým příkladem jsou kancelářské budovy, školy, byty či domy, kde se topologie obvykle skládá z jedné LAN sítě. Jsou však případy, kdy je vhodnější diverzifikovat a použít naopak několik menších LAN sítí, kde jedna LAN síť může pokrýt několik budov současně, záleží vždy na konkrétní topologii.

LAN síť obvykle vlastní a spravuje jedna a tatáž fyzická osoba nebo organizace.

2.1.2.2 WAN

Zkratkou WAN (Wide Area Network, někdy také Worldwide Area Network), jak již název napovídá, se nazývají rozsáhlé, někdy také celosvětové sítě. Největší takovou WAN síť představuje Internet, který je ukázkovým příkladem, jež spojuje celý svět. WAN síť je tedy konzistentní shluk LAN sítí. Síťový prvek nazývaný router se stará o propojení dílčích LAN sítí do právě jedné WAN sítě.

WAN síť se od LAN sítě liší hned v několika důležitých aspektech. Většina WAN sítí (stejně jako Internet) není nikým vlastněna a existuje ve společném a sdíleném vlastnictví a správě. [4]



Obrázek 3 *Vztah LAN & WAN sítí, zdroj: Obrázek [3]*

2.1.3 Rozdělení z hlediska typu připojení

Dalším způsobem, jak můžeme dělit počítačové sítě, je dle typu nebo způsobu připojení. Počítače v síti mohou být připojeny hned několika způsoby. Jedním z nejběžnějších je metalické připojení. V metalickém připojení jsou veškerá zařízení připojena k síti pomocí drátové kabeláže (nejčastěji koaxiální kabely či kroucené dvojlinky). Tento způsob patří z hlediska nákladovosti k těm levnějším, hojně se proto používá pro připojení v pevných rozvodech sítí různých budov. Limitujícími faktory jsou zde však přenosová rychlost a také omezení maximální délky kabeláže, na které lze realizovat spolehlivý přenos. Možným řešením je varianta optického připojení, kde jsou zařízení připojena k síti pomocí optických kabelů. S tímto řešením však často přichází i vyšší náklady a cena. V poslední řadě se nabízí připojení bezdrátovou formou – ta najde své využití především při mobilních připojeních nebo pro rychlé a krátkodobé připojení periferií.[2] Spadají sem například Wi-Fi, radiové vlny, Bluetooth a další. [16]

Obrázek 4 *Koaxiální kabeláž (samice/samec), zdroj: Obrázek [4]*

2.1.4 Fyzická topologie

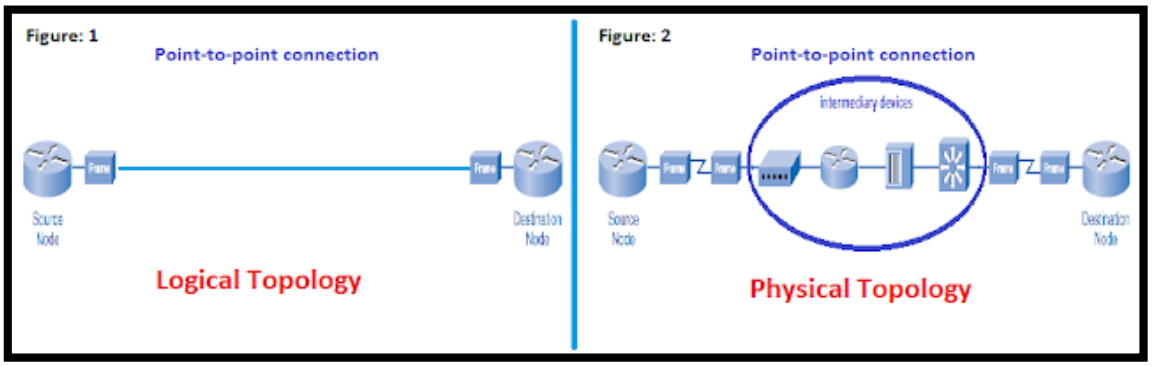
Fyzická topologie v počítačové síti představuje veškerý hardware a jeho konstrukci, která odpovídá realitě. Ve fyzické topologii se dokumentuje umístění daných zařízení, jejich uzly[3], vedení veškeré kabeláže a způsob propojení jednotlivých zařízení. Topologií existuje hned několik. Dle výběru a zvolení

[2] Periferie jsou veškerá zařízení a součásti připojující se k počítači
[3] Uzly bývají součástí fyzické topologie a znázorňují spoje a návaznost propojení celé topologie

topologie či kombinací vícero topologií, se následně odvíjí další náležitosti, jako je vybavení, kterým bude síť disponovat, možnosti použití tohoto vybavení, způsob, jakým bude síť spravována či způsob samotné komunikace v síti. Jelikož se však volba topologie řeší primárně u středně velkých až velkých sítí, je zmíněná problematika mimo rozsah této práce.

2.1.5 Logická topologie

Logická topologie se zabývá naopak datovým tokem, komunikací a tím, jak jednotlivá zařízení přistupují k datům a informacím v síti a jakým způsobem je po síti přenáší. Logická topologie je zcela nezávislá na fyzické topologii a pokud to situace vyžaduje, mnohdy se obě navzájem liší. Mezi nejvíce používané metody logické topologie patří tzv. „Broadcast“ aneb „kdo dřív přijde, ten dřív vysílá“ a „Token passing“, kde má možnost vysílat pouze takové zařízení, které má u sebe v daný okamžik žeton obíhající v síti. Z obou zmíněných technologií je patrné, že v jeden okamžik může po určité části sítě vysílat pouze jedno zařízení. [4]



Obrázek 5 *Příklad fyzické a logické topologie, zdroj: Obrázek [5]*

2.1.6 Topologie LAN & Home Networking

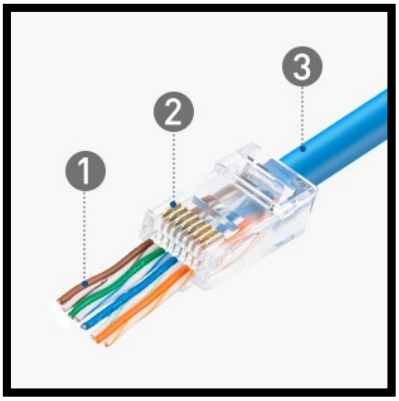
V LAN sítích a menších domácích sítích jsou zpravidla dva standardy síťových technologií či topologií, které zajišťují služby a určují princip, jakým síťová komunikace mezi zařízeními probíhá. Těmi jsou Ethernet a Token ring. [4]

2.1.6.1 Ethernet

Ethernet představuje technologii, která je známa již řadu let. Běžně je používána u kabelově řešených LAN sítí. Jedná se o síťový protokol, který se stará

o způsob řízení přenosu dat v LAN síti. V domácnostech se pak také sítě s touto technologií nazývají právě Ethernet LAN. Většina zařízení jako jsou počítače a notebooky jsou dnes již vybavena plnohodnotnou integrovanou ethernetovou kartou (nazývanou taktéž síťová karta), takže jsou připravena se bez problému připojit k domácí Ethernet LAN síti bez nutnosti dalšího zásahu. A co je k takové Ethernet LAN síti potřeba? [4]

- Počítače či jiná zařízení – Ethernet dokáže připojit jakýkoliv počítač či jiné zařízení k síti za předpokladu, že zařízení disponuje Ethernetovým adaptérem či síťovou kartou.
- NIC neboli síťové karty – nejběžnějším provedením je ve většině případů již integrovaná síťová karta v zařízení, nicméně může stát i jako samostatný hardware v počítači. Síťová karta má samostatné výstupní porty, kam se dají přímo připojit kabely
- Router (viz 2.2.3)
- Kabeláž – UTP kabeláž (známá také jako kroucené dvojlinky) představuje klasické řešení v Ethernet LAN sítích. Kabel je charakteristický osmi zakroucenými vodiči, které jsou rozlišeny barvami. Na konci kabelu nalezneme koncovku RJ-45, která je běžně používaným standardem síťového kabelu. V případě větších vzdáleností se naopak využívá kabel koaxiální, který nalezneme například i u televizorů.
- Software pro spravování sítě – je důležitou součástí dohledu a řízení sítí. Nemusí se jednat o specializovaná zařízení. Software může být řešen i formou aplikací běžících v běžných operačních systémech, jako je MS Windows, Linux či macOS. Mnohé z nich nástroje základní správy nabízejí, avšak lépe je na tom Linux.



Obrázek 6 *UTP Kabel s koncovkou RJ-45, zdroj: Obrázek [6]*

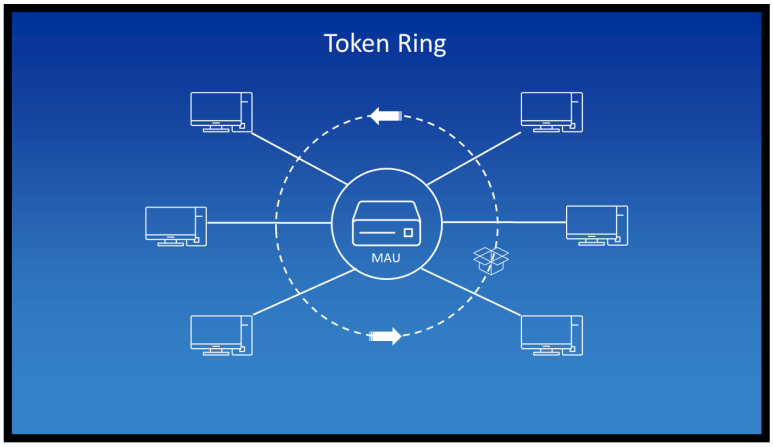
Obrázek 7 *Síťová karta (externí), zdroj: Obrázek [7]*

2.1.6.2 Token Ring

Technologie nebo spíše topologie Token Ring, známa také jako kruhová topologie, byla původně vyvinuta v 80. letech. Za jejím vznikem stojí dodnes fungující společnost IBM.

Hlavní příčinou jejího vzniku bylo alternativní řešení výše zmíněného Ethernetu. Token Ring je datově spojovou technologií zejména v LAN sítích, kde jsou zařízení připojena ve hvězdicovém či kruhovém systému, jak lze vidět na Obrázek 8. Princip spočívá v kolování tokenů, které se skrývají v hlavičkách rámců (paketů). Zařízení, které drží tzv. „token frame“ (rámec označen tokenem) rozhoduje, zdali pošle zprávu, a pokud ano, vloží do rámce data a vrací ho zpět do LAN sítě. V opačném případě se rámec, označený tokenem, vzdá dalšímu zařízení, které následuje v kruhu. [4]

Na rozdíl od Ethernet sítě si Token Ring síť dokáže poradit s více zařízeními, která mohou mít totožnou MAC adresu, aniž by to v síti způsobilo problémy. Mají navíc možnost nakonfigurovat určité uzly s vyšší prioritou, což Ethernet neumí. Náklady na kabeláž a zajištění výpočetní techniky jsou však v Token Ring sítích značně vyšší, a to včetně síťových karet a dalšího příslušenství. Začátkem 90. let oblíbenost tohoto řešení postupně upadala, jelikož dominantní technologií v designu LAN sítí se začala stávat právě ethernetová technologie. Průmyslová iniciativa, zvaná „High-speed token ring" (HSTR) reagovala vylepšením Token Ring standardů, čímž posunula možnosti přenosové rychlosti z původních 16Mb/s na 100Mb/s. Další práce a vývoj projektu „HSTR Token Ring" byly opuštěny z důvodů nedostatečné poptávky na trhu. [4]



Obrázek 8 *Token Ring princip, zdroj: Obrázek [8]*

2.2 Síťové prvky

2.2.1 Aktivní síťové prvky

Aktivní síťové prvky tvoří část počítačové sítě, která se aktivně podílí na práci se signály (zajišťuje např. jejich zesilování, modifikaci, vyhodnocování atp.). V sítích typicky představují konkrétní zařízení, která jsou umístěna v důležitých uzlech sítě. [5]

V každé počítačové síti je nezbytné minimum aktivních síťových prvků. Ty nejenže řídí tok dat či signálu v síti, ale podílejí se také ve velké míře na zajištění bezpečnosti. Mnohdy se jedná o mikropočítače nebo čipy, na nichž běží určitý software, který obsluhuje a řídí nějakou konkrétní oblast. Efektivní výkonnost pak

závisí nejen na kvalitě hardwaru, ale také na kvalitě samotného řídícího softwaru. [5]

Mezi zařízení nazývané aktivními síťovými prvky se řadí jak jednodušší zařízení, jako jsou například repeatery (opakovače) či jednodušší switche (přepínače), které se pouze starají o zprostředkování přenosu dál, tak i chytřejší zařízení jako jsou routery (směrovače), které už dokážou pracovat s daty na vyšší úrovni a v mnoha případech zabránit i kybernetickým hrozbám a jiným útokům. [5]

2.2.2 Pasivní síťové prvky

Pasivní síťové prvky jsou opakem prvků aktivních. Zajišťují tedy, jak se fyzicky řeší přenos dat v počítačové síti. Nespotřebovávají pro svoje fungování žádnou elektrickou energii ani nijak nezasahují do dat, která jsou přes ně přenášena. Patří sem především kabeláž, různé zásuvky a další konektory. [6]

Stejně tak jako aktivní síťové prvky, i pasivní jsou v sítích nezbytně důležité – představují totiž také základ ethernetových sítí. I přes to, že se dnes stávají stále dominantnějšími bezdrátové technologie, jsou stálým základním kamenem pro realizaci přenosu dat. Kabeláž je totiž skvělým prostředkem pro přenos velkého objemu dat na dlouhé vzdálenosti, kde má ve srovnání s bezdrátovým přenosem bezespornou výhodu, a to nejen v přenosových rychlostech, ale i díky tomu, že kabeláž vzhledem ke svému provedení a izolaci nepodléhá žádným vzájemným rušením. [6]

2.2.3 Router

Router, taktéž známý jako směrovač, je dosud nejpoužívanějším a nejinteligentnějším aktivním zařízením v síti. Právě router je zařízením, které zná nejlépe síť a její topologii. Router se hojně využívá jak ve WAN sítích, tak i lokálních, menších sítích LAN. Často uváděným modelovým příkladem bývá představa, že switche neboli přepínače, představují cesty, které propojují všechna města ve státě, a routery pak značí hraniční přechody mezi státy. [7]

Routerem však nemusí být nutně jen samostatně stojící zařízení, jsou případy, kdy je jako router používán server, který softwarově podporuje proces

síťování. V dnešní době jsou již v provozu speciální počítače se specifickým hardwarem či různá provedení routerů podporující specializované funkce. [7]

Jak již název napovídá, primárním úkolem routeru je směrování (routování). Jde o proces, kdy router určuje cestu datových informací (datagramů) v síti. Jeho primárním úkolem je tedy najít co možná nejoptimálnější a nejefektivnější cestu, jak doručit data k cíli. Nicméně síťová infrastruktura je mezi odesílatelem a příjemcem mnohdy velmi složitá a zdlouhavá, proto router vždy řeší cestu jen k dalšímu uzlu.

Router má v sobě určitou sadu pravidel, díky kterým ví, jak a kudy se mají zasílané pakety předat postupně až k cíli. Těmto informacím, které router využívá při procesu směrování, se také říká tzv. „routing tables“ (směrovací tabulky). Ty si každý router udržuje a průběžně aktualizuje. Nejdůležitější faktory zde představuje nalezení správných cest a jejich jednoduchost a efektivnost, kde router reaguje na případné změny, které mohou nastat (změna trasy, její přerušení atd.). [7]

Obrázek 9 *Domácí router nejnovější generace s podporou tří zesilujících antén, zdroj: Obrázek [9]*

2.2.4 Repeater

Opakovač, známý spíše pod původním označením repeater, je nejjednodušší aktivní zařízení v síti. Stará se o regeneraci přenášeného signálu, tzn. například o jeho zesilování či úpravu. Ve světě počítačových sítí představuje něco jako primitivní digitální zesilovač. [7]

Princip repeateru spočívá v přístupu k přijímaným signálům. Repeater totiž přeposílá veškerý přijímaný signál do všech k němu připojených segmentů.

Díky tomu se však rozšiřuje již zmiňovaná kolizní doména[4]. Na trhu je hned několik druhů repeaterů. Některé jsou vhodné pro jediný specifický typ přenosového média, jiné představují speciální typy jako například transceivery (převodníky), které umí převádět signál z jednoho typu na druhý (například z klasické kroucené dvojlinky na optický kabel) a mohou fungovat jako samostatné plnohodnotné zařízení, případně jako součást jiného aktivního síťového prvku. [7]

Repeater našel své využití v online světě především díky fyzikálním vlastnostem přenosových médií (také pasivních prvků). Po určité době totiž dojde k tzv. „útlumu či zkreslení", kdy přenášený signál po určité vzdálenosti ztrácí na síle a je tak problém z něj vyčíst, jakou informaci přenášené bity značí. Tuto vzdálenost ovlivňuje především druh přenosového média (koaxiální kabel, kroucená dvojlinka, optika…) a poté i samotná přenosová rychlost a charakter signálu. [7]

Obrázek 10 *Klasický starší repeater (vlevo) a novější v kombinaci se zesilující anténou (vpravo), zdroj: [7]*

2.3 Domácí Wi-Fi routery

Bezdrátové neboli Wi-Fi routery jsou běžnou součástí domácností. Pro poskytovatele internetu slouží jako univerzální řešení připojení svých zákazníků ke své kabelové nebo xDSL[5] internetové síti a kombinují funkce routeru a bezdrátového AP[6]. Dle [10] nazývané také „desktopové Wi-Fi routery", jsou

[4] Kolizní doména vyjadřuje doménovou část sítě, ve které může nastat kolize v komunikaci mezi zařízeními. Čím větší je kolizní doména, tím větší část sítě bude v případě kolize postihnuta.
[5] DSL je označení pro technologii přenosu dat pomocí telefonických rozvodů; xDSL pak slouží jako souhrnné označení pro různé druhy DSL technologie
[6] Access Point (AP) je tzv. přístupový bod – režim, v kterém mohou routery pracovat. Router je typicky připojen ethernetovým kabelem k jinému vysílajícímu zařízení (routeru) a rozšiřuje signálové pokrytí pro síťové klienty

obvykle malá zařízení osazená jednou či více anténami, které pomáhají vysílat signál a zajišťovat pokrytí napříč prostory.

Vyvstává však otázka, proč mít doma vlastní Wi-Fi router. Většina internetových poskytovatelů dodává jako součást svých služeb lidem do domovů i bezdrátový router – často spolu s kabelovým nebo DSL modemem[7]. Pověřený technik dorazí na místo, vše zapojí, nastaví a internet funguje. To je vše v pořádku, jsou případy, kdy router od dodavatele internetu slouží tak, jak má, zvlášť je-li to součástí smlouvy a uživatel je pak dlouhodobě spokojen. Pokud ovšem není jiná cesta než si od poskytovatele zařízení zapůjčit nebo zakoupit, je zde prostor využít peníze i alternativě. [11]

2.3.1 Rozhodující faktory výběru

Kdy tedy sáhnout po vlastním Wi-Fi routeru, podle čeho zvolit a jak vybírat, záleží na celé řadě faktorů. Uživatel zde musí mít především jasno, co od sítě očekává a jak vypadají její topologie. Každý z rozebíraných faktorů bude mít po stránce bezpečnosti případ od případu jinou důležitost.

2.3.1.1 Single-band a Dual-band

Komunikace v bezdrátovém přenosu funguje na principu radiových vln, které si lze představit jako pomyslné cesty, po nichž putují data. Zatímco routery do verze standardu 802.11g fungovaly výhradně v pásmu frekvence 2.4GHz, 5GHz pásmo přišlo až s ostřejší verzí standardu 802.11n a následně bylo přeneseno také do nejnovějších verzí standardu 802.11ac a 802.11ax. Důvodem vzniku 5GHz pásma byla neustála navyšující se zátěž 2.4GHz pásma, což vedlo ke stále častějším výchylkám a rušením síťového provozu. [11]

Single-band routery jsou tedy zařízení s podporou původního a jediného 2.4GHz přenosového pásma, zatímco Dual-band routery mohou pracovat jak s pásmem 2.4GHz, tak i s 5GHz. Obecně platí, že pásma s nižší frekvencí disponují nižší přenosovou rychlostí a menším pokrytím, vyšší frekvence naopak značí širší

[7] Modem převádí analogový signál na digitální a naopak. Přenos může probíhat například koaxiálním kabelem nebo přes telefonní přípojku

pokrytí a značně vyšší přenosovou rychlost. 5GHz pásma mají však také jisté nevýhody. Vyšší frekvence kmitočtu totiž způsobuje, že má signál větší tendenci ztrácet na síle a hůře se tak přenáší přes překážky jako zdi nebo nábytek. Novodobé routery však mají techniku tzv. „beamformingu“, která směřuje signál směrem k vysílajícímu zařízení namísto běžného všesměrového vysílání. [11]

V praxi mají tedy obě pásma svá pro a proti. Pásmo 5GHz a jeho vyšší potenciál rychlosti přenosu a dosahu bude ideální volbou do hustě obydlených oblastí, zatímco 2.4GHz lépe prochází přes překážky a dosah se v poměru ke vzdálenosti ztrácí v mnohem menším měřítku, může zde však docházet ke zmiňovanému vzájemnému rušení. Až na výjimky je tedy dodnes levnější a dostačující investicí volba single-band routerů.

2.3.1.2 Oblast pokrytí

Je také potřeba uvážit, jak velká oblast by měla být pokryta. Ve velkých stavbách a domácnostech může být zajištění Wi-Fi konektivity všem klientům a zařízením náročným krokem, zvlášť pokud síť běží právě v 5GHz pásmu. Pro menší bydlení a domácnosti bezpochyby vystačí jediný router s osazením několika antén, uživatel už má mnohdy i představu, zdali síť v minulosti fungovala bez problému, nebo bylo již něco v této souvislosti řešeno. Rozhodně je na místě před výběrem nejprve všechny tyto věci vyzkoušet a vyhnout se koupi něčeho zbytečně drahého, kde uživatel nemusí plně využít potenciál daného zařízení. Dobrým způsobem, jak si mnohdy udělat představu o vlastnostech routerů, jsou recenze, ať už od kurátorů, firem nebo běžných uživatelů, kteří již produkt zakoupili. [11]

2.3.1.3 Softwarové a bezpečností součásti

Na základě informací, které uživatel o své budoucí síti ví, by se měl také soustředit na softwarové a bezpečností součásti routeru. Pokud bude potřeba mít nad routerem plnou kontrolu a starat se o provoz, je záhodno sáhnout po variantách s pokročilým firmwarem, které obsahují základní firewall a nabízí další rozšíření, jež mohou přijít vhod. V případě rodinného routeru, kdy může dojít ze strany dětí k přístupu k nevhodným informacím na Internetu, by uživatel měl věnovat

pozornost funkcionalitám jako je vestavěná rodičovská kontrola nebo podobné režimy. Některé routery umožňují mimo jiné spravovat internetový přístup formou různých časových nebo obsahových omezení. A co víc, pokud router umí vytvářet také tzv. „hostované sítě“, mohou se uživatelé a hosté připojovat k síti skrze oddělené segmenty sítě s jinými přístupovými údaji a správce jim tak nemusí poskytovat žádné citlivé nebo přístupové údaje primární Wi-Fi sítě. [11]

Výrobci čas od času vydávají na svá zařízení také tzv. aktualizace firmwaru. Ty zpravidla řeší bezpečnostní trhliny, stabilitu a výkonnost zařízení či rozšíření o nové funkce. Firmware je totiž velmi důležitým, specifickým typem softwaru. Nachází se zpravidla ve speciální paměti zařízení k tomu určené. Zařízení mají různý způsob přístupu a práce s firmwarem a jeho špatně provedená aktualizace může skončit nesprávnou funkčností a vážným poškozením celého zařízení. [19]

3 Zabezpečení

3.1 Hrozby v počítačové síti

Počítačová síť je pro mnoho lidí velkou neznámou. Není zde žádný zákon ani pravidla, jak by se měl uživatel chovat, co smí a nesmí, co představuje onu hranici apod. Ve spoustě případů není vlastně ani koho potrestat či jakkoliv postihnout, neboť síť sama o sobě je ve výsledku stejně tak jako celý Internet velmi anonymním místem.

To, jak dodržovat zásady bezpečnosti v online světě a pohybovat se bezpečně v domácí síti nebo kdekoliv na internetu člověka dnes běžně nikde nenaučí. Byť se technologie a zabezpečení stále vyvíjí vpřed, hackeři a útočníci neustále přichází s novými nápady a způsoby, jak tyto věci obejít. Obvykle se jedná o dva druhy hackerů – v lepším případě jsou to ti, kteří chtějí poukázat na slabiny určitého systému, jeho nedostatky nebo jeho funkcionality bez škodlivého úmyslu, v horším případě jsou tu ti, co mají v plánu uškodit dotyčné osobě nebo instituci různou formou.

Hrozeb, které denně kolují počítačovou sítí, je nespočet – hackeři, viry a různý zákeřný software představují jen zlomek toho, co je skutečným nebezpečím. Je až děsivé, jak jednoduchým způsobem může běžný uživatel přijít o svou identitu

během několika okamžiků třeba jenom tím, že otevřel nesprávný odkaz na internetovou adresu nebo špatný e-mail. [8]

3.1.1 Malware (zákeřný software)

Malicious software, zkráceně také Malware, je označení určitého druhu zákeřného či škodlivého softwaru, který se bez vědomí uživatele dostane na jeho zařízení, typicky formou stažení do zařízení s jinými soubory nebo spolu s instalací jiného programu, způsobů je mnoho. Dopady na systém, který malware nakazil, se projeví zejména zpomalením chodu celého systému, automatickým odesíláním emailů bez vědomí uživatele, náhodnými restarty či spouštěním různých algoritmů[8] a programů na pozadí. [9]

Malware má mnoho podob. Souhrnně se malwarem nazývají veškeré počítačové viry, spadají sem i viry známých typů jako „trojský kůň“ nebo například tzv. „ransomware“, který dokáže zamknout a znepřístupnit uživateli celé zařízení s daty, dokud nezaplatí výkupné (angl. ransom). S malwarem se lze často setkat u výhružných, tzv. „phishingových“ e-mailů, kdy útočnici zasílají ve zprávě odkazy na různé neznámé weby nebo posílají e-mail s přílohou, která se může tvářit zcela neškodně. Pak už jen stačí, až nic netušící uživatel malware spustí, ten aktivuje škodlivý kód v zařízení a malware tak získá tak kontrolu nad zařízením či nad celou sítí. [9]

3.1.2 Sociální inženýrství

Útoky formou sociálního inženýrství se za poslední roky staly jedním z nejpopulárnějších a nejsnazších způsobů, jak zaútočit v online světě. Pro útočníka je totiž daleko snazší obejít zabezpečení a bezpečností protokoly tak, že využije uživatelovu nedbalost a hloupost, než volit složitější cestu a pokoušet se prolomit nějaké silnější zabezpečení s menší šancí na úspěch. [9]

Sociální inženýrství se tak stalo celkem lukrativním byznysem pro schopné hackery. Lidé a firmy tak díky časté neznalosti základů bezpečnosti světa sítí mohou nenávratně přijít k fatálním ztrátám a škodám za nevyčíslitelné částky. V praxi je

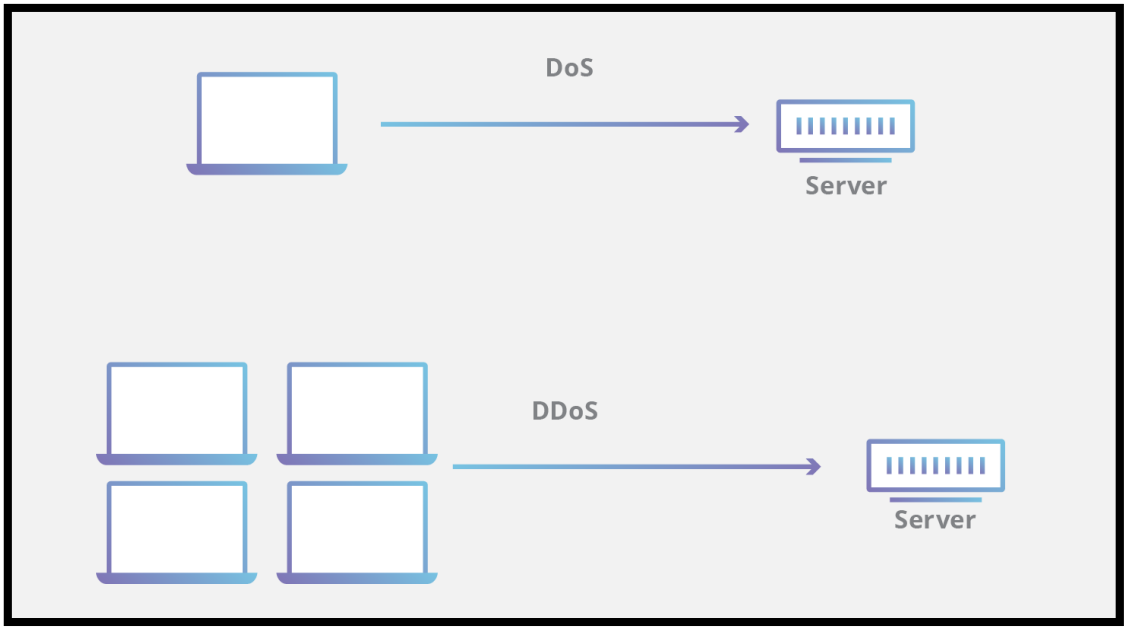
[8] Algoritmus představuje určitý postup, skládající se z jednotlivých po sobě jdoucích kroků

způsobů sociálního inženýrství nespočet. Nepříjemnou záležitostí pak jsou i výše zmíněné „phishingové“ e-maily, lákající uživatele k poskytnutí citlivých osobních údajů. [8][9]

3.1.3 DoS (odmítnutí služeb)

DoS, útok, v počítačové síti nazýván také jako „odmítnutí služeb“ (z anglického Denial-of-Service), představuje největší nebezpečí především pro servery a veškeré síťové služby. Základní princip tohoto útoku spočívá v záměrném přetížení síťové komunikace cílového zařízení. Kapacita takového zařízení, která dokáže zpracovat v jeden okamžik jen omezené množství požadavků, je zahlcena do bodu, kdy server nedokáže obsloužit a zpracovat standardní provoz. [12]

Pro útok DoS je také charakteristické, že je možné ho realizovat již za pomocí jediného počítače v síti. Existuje také nadstavba, a sice DDoS neboli distribuovaný DoS – viz Obrázek 11. Jak již název napovídá, rozdíl spočívá ve způsobu distribuce – útok probíhá z více zdrojů současně. Rozpoznat, zda je počítačová síť pod DoS útokem, není příliš složité. Síť je zpomalena až do takových extrémů, kdy je prakticky nepoužitelná a nenačte ani obyčejné webové stránky. Dochází také k narušení stability sítě a zařízení se začínají náhle odpojovat. [12]



Obrázek 11 *Schémata DoS a DDoS útoků, zdroj: [12]*

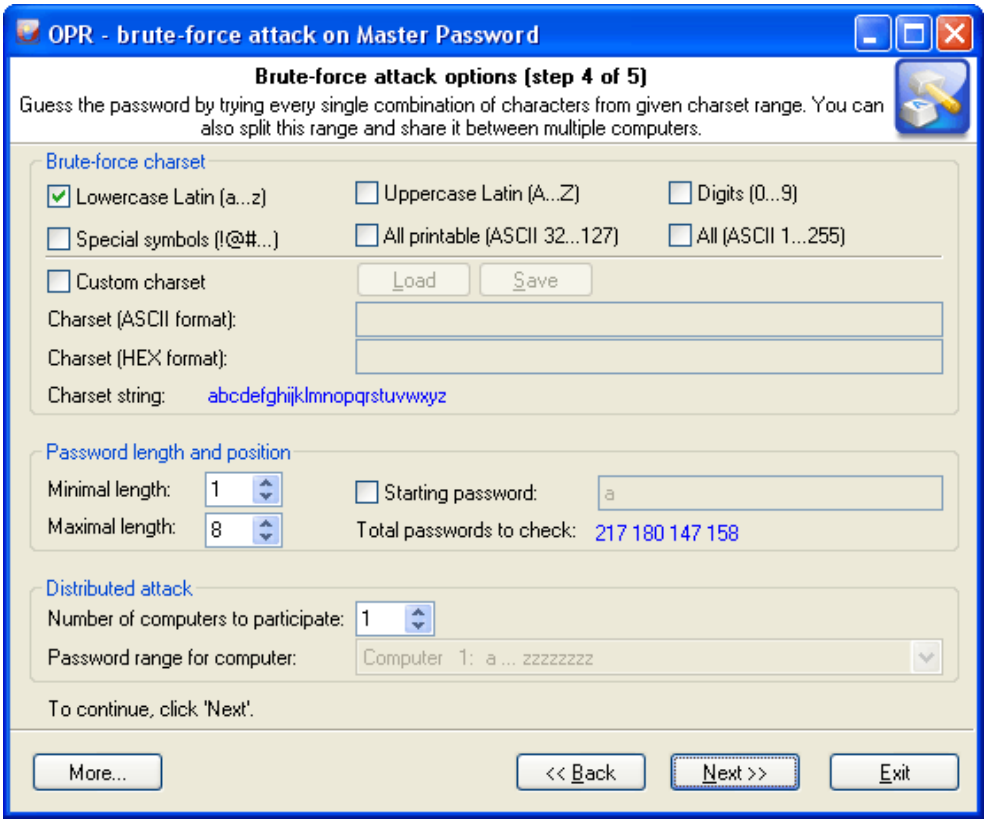
3.1.4 Brute-force útok

Tzv. „brute-force“ útok je starý, avšak dodnes stále známý a zneužívaný útok. Svůj název „útok hrubou silou“, dostal proto, že se při něm útočník se pokouší doslova vloupat do zařízení za pomocí opakovaných útoků hrubou silou. Obvyklé scénáře zahrnují systematické postupy, jak prolomit uživatelovo heslo zkoušením nespočetného množství různých slov nebo jejich kombinací. Útočník pak často sází na nekomplexní a jednoduchá hesla, která nezabere moc času vypátrat a prolomit. [13]

Začátkem většiny útoků hrubou silou je rozsáhlý seznam slov. Ty jsou posbírané napříč Internetem z různých zdrojů, např. z veřejně dostupných databází odcizených hesel z různých jiných útoků. Takové seznamy slov se mohou pohybovat v řádech desetitisíců až statisíců. Útočník pak pouze spustí program nebo skript, který seznam slov postupně prochází zkoušením jednotlivých slov nebo celých kombinací. Jakmile software nalezne správnou kombinaci hesla nebo přihlašovacích údajů, ohlásí útočníkovi výsledek. V tento moment útočník získává přístupové údaje a může se tedy přihlásit do systémů, jak to běžně dělá uživatel. [13]

Útoky formou hrubé síly nejsou po většinu času nic víc než to, že útočník zahájí proces hádání uživatelova hesla za pomocí zákeřného softwaru, díky němuž je usnadněna spousta práce a celý proces útoku je systematický. Taktikou, jak se před takovými útoky chránit a zabezpečit, je volba bezpečného a složitého hesla. Jelikož seznam slov většinou tvoří ta nejjednodušší a nejvíce používaná slova z uniklých databází hesel nebo ze slovníků, uživatel může předejít prolomení svých údajů složitými hesly, která kombinují velká a malá písmena, čísla a speciální znaky. Čím složitější kombinace znaků v hesle, tím déle zabere útočníkovi je uhádnout. Výhodou je i to, že s prolomením posloupností náhodných znaků až na výjimky nepomůže žádný slovník. [13]

„Brute-force“ útokům se dá také zabránit i jinak. Mnoho systémů nebo softwaru nabízí možnosti omezit počet pokusů na úspěšné přihlášení. Systém nebo software se poté zablokuje či nějakým způsobem znepřístupní další pokusy o přihlášení.



Obrázek 12 *Brute-force attack software, zdroj: Obrázek [12]*

3.1.5 Zastaralý a neaktuální software

Aktualizace a bezpečností záplaty jsou pravidelnou součástí údržby vývojářů softwaru či operačních systémů. Zajišťují tak svůj software před chybami a možnými bugy[9], které mohou vést k bezpečnostním dírám a nedostatkům. Některé aktualizace mohou představovat miliony řádků algoritmů a programového kódu, které jsou bohužel nezbytné pro správnou optimalizaci a nasazení softwaru do praxe. Z takových důvodů vývojáři průběžně pracují na tzv. „záplatách“, aby mohli případně v co nejbližší době zajistit software co možná nejbezpečnější, ať už se jedná o výkonnostní či funkcionální záležitosti. [9]

Správa jakéhokoliv softwaru z hlediska zabezpečení je dlouhodobá a náročná. Dominantní společnosti ve světovém měřítku jako jsou např. Facebook, Apple či Microsoft, vydávají bezpečností záplaty prakticky denně. Bojují tak nejen

[9] Bug způsobuje nežádoucí chování nějakého programu nebo jeho funkcionality, ať se jedná o vizuální, funkcionální či jiný druh bugu

proti přibývajícím kybernetickým hrozbám, ale také samy proti sobě, kdo dokáže držet lepší krok s aktuální dobou. [9]

Za zmínku stojí i tzv. „end of life dates“ (EOL), resp. životní cyklus softwaru. Prodejci softwaru a hardwaru oznamují tuto skutečnost obvykle s vydáním první stabilní, ostré verze softwaru. Důvodem uvádění životního cyklu je především ekonomika dané společnosti, neboť po určitém čase produkt už není výdělečný a stojí společnost dodatečné zdroje v podobě práce vývojářů, kteří udržují podporu produktu. Pokud tedy nějakému produktu skončí podpora životního cyklu, do budoucna to znamená spoustu otázek po stránce zabezpečení. Běžným a doporučovaným způsobem řešení je přejít nebo aktualizovat na novější, aktuální software. [9]

3.2 Antivirový software

Vývoj antivirových programů za poslední roky značně pokročil. Internet už dávno není jen místem pro zábavu a trávení volného času, ale také velkým byznysem. Nachází se zde mnoho cenných informací a dat, pro velké množství lidí dnes znamená internet i živobytí a velkou část jejich života. Antivirový software tak stále zůstává vysoce důležitou formou ochrany počítačů, která sice nedokáže garantovat stoprocentní ochranu, ale markantně přidává na její hodnotě před jakýmkoliv zákeřným typem viru a dokáže takto zachránit spousty zařízení.

Antivirus provádí aktivní ochranu takovým způsobem, že běží nepřetržitě po celou dobu, kdy je počítač zapnutý (obvykle jako program na pozadí) a v pravidelných intervalech vykonává kontroly a skenování virů, které se mohou snažit dostat do e-mailů, souborů nebo přímo do kritických částí samotného operačního systému. Kvalitní antivirové programy dostávají pravidelné aktualizace, které zajišťují imunitu počítače proti těm nejnovějším a nejzákeřnějším, denně vznikajícím virům.

Při výběru kvalitního antivirového softwaru je třeba mít na paměti určité věci. Je dobré vždy vědět něco o společnosti a samotném produktu, za kterým společnost stojí. Některé antiviry mohou být komplexní a nabízet široké možnosti ochrany, jež využije jen zkušený uživatel, jiné zase nabídnou snadné nastavení a základní balíčky ochrany, která pro běžného uživatele stačí. Nejdražší antivirové

programy nemusí vždy automaticky znamenat nejlepší ochranu, všeobecně jde o dobrou investici, která se zúročí. [8]

3.3 Firewall

Velmi důležitou oblastí je také Firewall. Firewall, někdy také nazýván jako brána firewall, je důležitou a kritickou součástí zabezpečení každého zařízení připojeného do sítě již od počátků Internetu. Jeho podstatu lze přirovnat k pomyslné „ochranné zdi“ na Obrázek 13, která stojí mezi uživatelem a celosvětovou sítí. Jeho hlavní starostí je kontrola toku paketů, a to ve veškeré síťové komunikaci. Díky tomu tak plní pomyslnou roli „kontrolního bodu“ veškerých hrozeb. Existuje mnoho typů firewallů, nicméně v rámci této práce je představena ta nejdůležitější čtveřice.

Obrázek 13 *Brána Firewall, zdroj: Obrázek [13]*

3.3.1 Filtrování paketů

Firewall s přístupovou metodou tzv. „filtrace paketů“ přezkoumává a kontroluje každý packet, který cestuje danou sítí – ať už se jedná o pakety odchozí nebo příchozí. To provádí na základě definovaných příchozích a odchozích pravidel. Vše probíhá na síťové vrstvě, kde každý paket obsahuje zdrojovou a cílovou IP adresu, na základě kterých se následně provoz filtruje. Tento typ firewallu je poměrně efektivní a přímočarý, ale jeho uživatelská konfigurace může být v mnoha případech složitá. [25][26]

3.3.2 Filtrování na úrovni okruhů

Tento typ firewallu využívá bezpečnostních mechanizmů transportní vrstvy, konkrétně se zde pracuje s tzv. čísly portů (port numbers), kdy dochází k navázání spojení skrze TCP či UDP protokoly a následně ke zjištění přímo cílové aplikace. Firewall poté filtruje provoz dle jeho režimu konfigurace. Může provádět filtrování například na základě čísla portu cílové aplikace nebo toho, zdali se jedná o typ příchozího či odchozího provozu v síti atp. Je zde tedy více způsobů, jak definovat to, do jaké míry bude moci firewall manipulovat a vynaložit s příchozími pakety. [25][26]

3.3.3 Filtrování na úrovni proxy serveru

Tento firewall spolupracuje s protokoly na aplikační vrstvě. Filtruje se zde provoz například za pomocí HTTP nebo FTP protokolů. Firewall je zde zpravidla nakonfigurován tak, že pomocí 2 předešlých metod filtrování umožňuje řídit webový provoz, který běží standardně na portu s číslem 80. Takový firewall pak může spravovat veškerý síťový provoz z aplikací, které právě skrze port 80 navazují TCP spojení s proxy serverem[10]. Jsou zde opět široké možnosti, jak lze přizpůsobit konfiguraci. Firewall může například kontrolovat protokoly na aplikační vrstvě nebo přímo data každého paketu – díky tomu může vymezit provoz pouze danému protokolu (např. HTTP). Výsledkem bude zablokování proxy provozu od ostatních aplikací či programů. [25][26]

V praxi je tento způsob filtrování znatelně náročnější a komplexnější nežli filtrace paketů nebo na úrovni okruhů. Je totiž zapotřebí, aby byla konfigurace provedena pro každý z jednotlivých protokolů, na kterém bude filtrování provozu probíhat. Router, který tak například disponuje firewallem jakožto nadstavbou se v mnoha případech na úrovni tohoto filtrování nevyplatí používat. Může to zpomalit celý proces routování a router tak může ztratit cenný čas navíc tím, že bude nucen provádět další filtrování. [25][26]

---

[10] Proxy serverem je myšlena specifická brána skrývající skutečné adresy zařízení, která se napříč sítí připojují. Tato brána se připojuje k internetu, provádí veškeré spojení a požadavky a zpracovává data, která jsou směrována zařízením stojícím za ní. [25]

3.3.4 Stavová kontrola

Firewall se stavovou kontrolou přichází s tím nejlepším, co dnes mezi firewally najdeme. Takovému firewallu se také někdy říká tzv. „stavový firewall“, neboť má tu schopnost, že si uchovává a shromažďuje informace o každém paketu, se kterým pracuje. To mu dále pomáhá odlišit datové pakety a pracovat s nimi tak na základě dříve získaných informací. [25][26]

Díky těmto vlastnostem by si stavový firewall tak měl dokázat hravě poradit třeba s DoS útoky. Firewall si inicializuje a zaznamená počet žádostí o spojení na server za určitou jednotku času od jednotlivých IP adres síťových klientů. Na základě toho následně dokáže rozlišit opakované žádosti a v případě, že rozpozná nadměrné množství požadavků od menšího množství klientů, zablokuje komunikaci s těmito klienty. [25][26]

3.3.5 Hardwarové a softwarové firewally

Běžně se rozlišují hardwarové a softwarové firewally. Ty v praxi často využívají a kombinují dvě či více z výše zmíněných přístupových metod. S Hardwarovým firewallem se lze setkat nejčastěji u routerů, kde chrání veškerá zařízení připojená k síti a je navržen tak, aby mohl neustále kontrolovat síťový provoz z Internetu. Naopak firewally softwarové najdeme v operačních systémech jako MS Windows či macOS. Jsou ve výchozím stavu zapnuté automaticky, pokud ovšem není na zařízení nainstalovaný například antivirový software, který často nahrazuje vestavěný firewall svým vlastním. Takové firewally mohou mít rozšířené možnosti a nadstavby, kdy mohou poskytovat ochranou na více úrovních a zachytávat malware nebo jiné zákeřné programy. [14][25]

3.4 Zálohování

Základním principem jakékoliv ochrany dat je redundance. Data jsou pro každého z nás tím nejhodnotnějším majetkem ve virtuálním světě digitalizace. Je proto zlatým pravidlem mít je uložena v jednu dobu na několika místech současně. Díky technologiím a možnostem, které se dnes nabízejí, je to relativně snadné a zvládnutelné pro každého. Provedením zálohy dat však teprve vše začíná. To, co je zde nejdůležitější, je pravidelnost.

Na kolik si dat uživatel váží, tak často by je měl i zálohovat. Existuje celá řada softwaru, který si hravě poradí např. i s každodenním zálohováním. Díky tomu je možné být vždy o krok napřed před jakoukoliv katastrofou, která by mohla data postihnout. Lze využít cloudové služby[11], externí pevné disky či nespočet dalších úložných médií. Uživatel má dnes rozmanité možnosti, a to s relativně nízkými až nulovými náklady. Je proto vhodné ukládat data jak ve fyzické podobě, tak i online formou.

Desítky společností nabízejí v dnešní době poměrně široké portfolio cloudových služeb, které jsou pro nenáročné uživatele snadno dostupné za rozumné ceny. Existují však i řešení, kdy má uživatel možnosti využívat cloudové úložiště a jejich služby zcela zdarma. Všichni majitelé účtů Google mají například ke svým účtům automaticky dostupných 115 GB úložného prostoru v cloudu zdarma, to samé platí např. i pro službu OneDrive, kde se v základním bezplatném programu možnosti pohybují pouze v několika GB, avšak v případě kancelářského balíčku Office 365, který může být dostupný zdarma pro studenty nebo spoustu pracujících, se uživatel dostává na solidní 1 TB (1000 GB) úložného prostoru. [15]

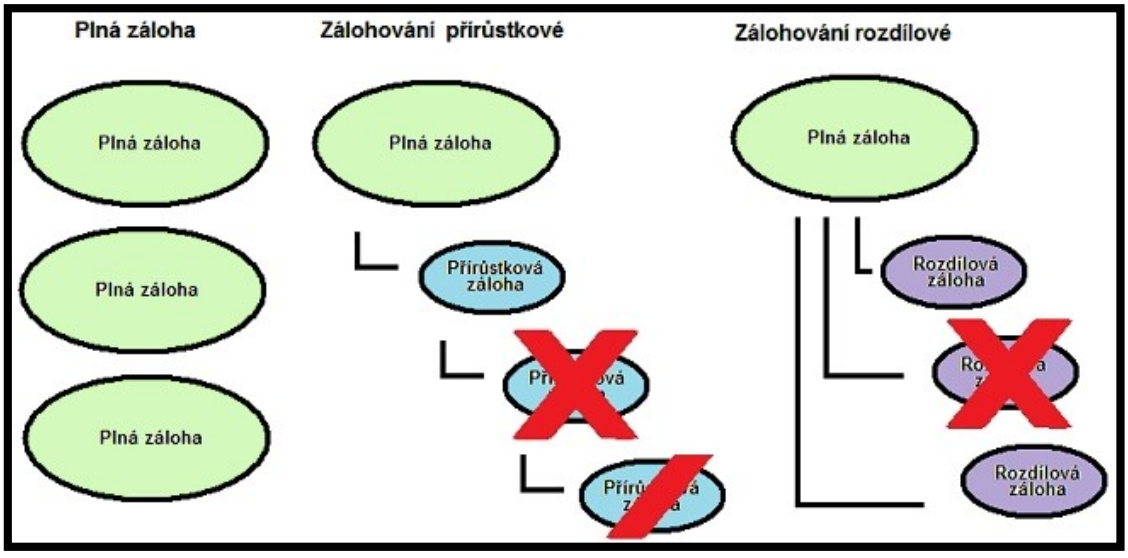
3.4.1 Metody zálohování

S dlouhodobým a pravidelným zálohováním je důležitá také volba optimální zálohovací strategie. Odvíjí se vždy dle požadavků a potřeb v konkrétní situaci, kdy každá ze 3 základních metod nabízí své výhody, nevýhody a efektivnost.

První metodě se říká tzv. „full backup“ neboli úplná záloha. Tato strategie zálohování je pro většinu uživatelů tou nejznámější a nejzákladnější. Jedná se o kompletní zálohu všech souborů a složek, kdy lze data poměrně snadno spravovat a v případě potřeby obnovit. Z dlouhodobějšího hlediska se však jedná o metodu časově velmi náročnou, zvláště když pak záloha probíhá i po síti, protože při každé záloze se kopírují všechna data. Úplná záloha je tak i tou nejvíce náročnou variantou z hlediska úložného prostoru a pro její nejbezpečnější využití se často doporučuje zvážit i její šifrování. Druhou metodou je tzv. inkrementální záloha, někdy také

[11] Cloudové služby nabízí online ukládání dat, odděleně od lokálních zařízení, typicky na vzdálené internetové servery

uváděna jako přírůstková záloha. Jejím základem je alespoň jedna úplná záloha, ke které se následně zálohují jen ta data, která se změnila od předchozí zálohy. Bezespornou výhodou této metody je ušetření úložného prostoru – ze všech 3 metod je v tomto ohledu tou nejefektivnější. Avšak v případě obnovy je zde potřeba alespoň jedna úplná záloha a všechny následné inkrementální zálohy, a to ve správném pořadí tak, jak byly postupně vytvořeny. Nejen že je tato metoda tedy časově náročná na správu, ale pokud se jen jedna z inkrementálních záloh poškodí nebo ztratí, šance na plnohodnotné obnovení dat je nenávratně ztracena. Třetí metodou je tzv. diferenční záloha, resp. rozdílová záloha. Diferenční záloha kombinuje výhody úplné zálohy a inkrementální zálohy. Opět je zde nutnou podmínkou jedna úplná záloha. Tentokrát se však zálohují data, která se změnila od poslední úplné zálohy. V případě obnovy dat tedy stačí mít nejaktuálnější úplnou zálohu a pouze poslední diferenční zálohu. Není zde potřeba zálohovat více záloh, a tak se s každou zálohou diferenční záloha vždy přepisuje, což ušetří nejen úložný prostor, ale i spoustu času navíc při případné obnově. [24]



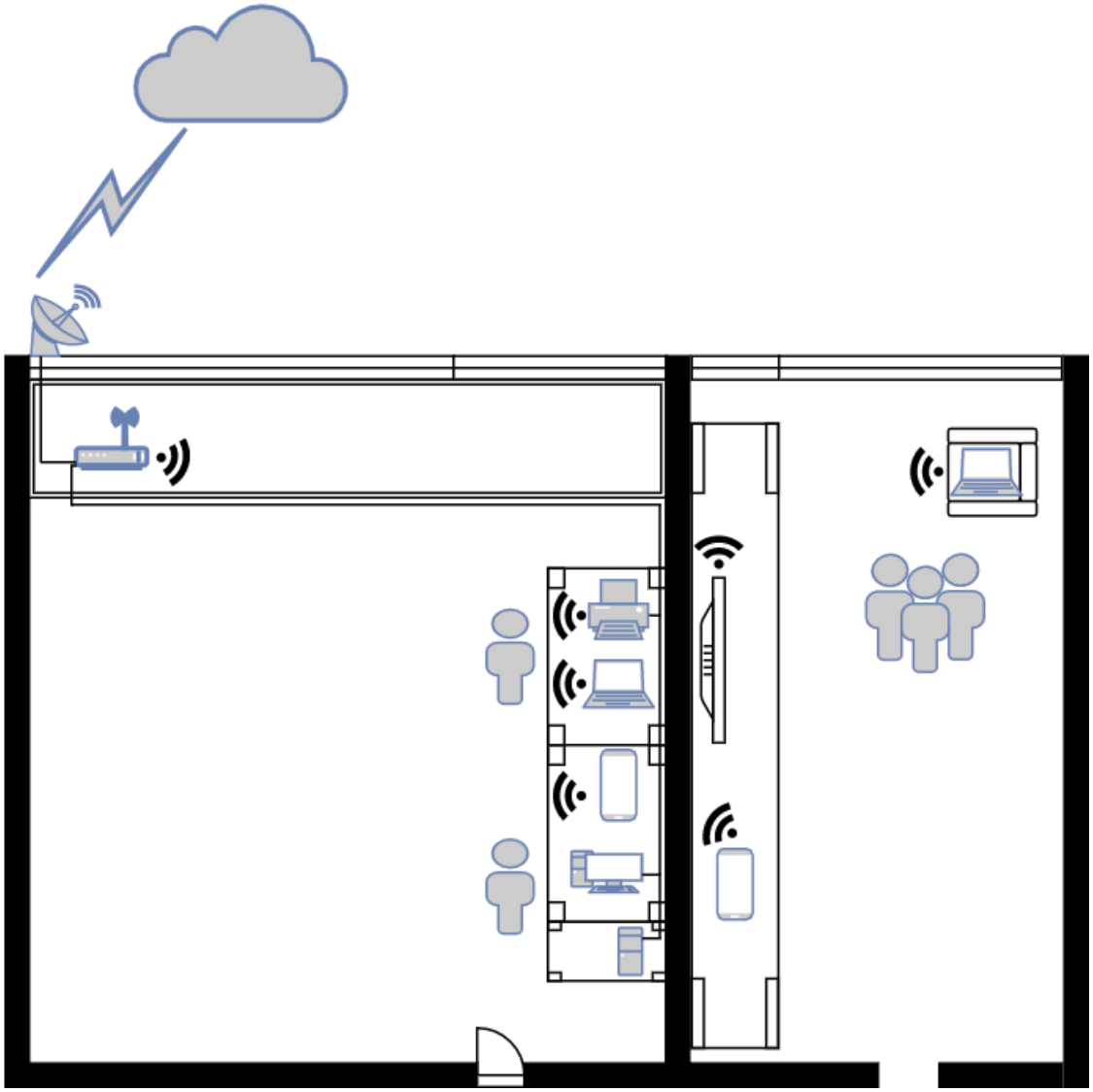
Obrázek 14 *Vizuální znázornění metod zálohování, zdroj: Obrázek [14]*

4 Návrh zabezpečení

4.1 Síť a periferie

V této části práce je předložen návrh konkrétního hardwaru, na kterém byly demonstrovány zabezpečovací prvky. Jako příklad bylo použito prostředí malé

domácí LAN sítě, která pokrývá v dané domácnosti pouze několik místností. Internetové připojení je zajišťováno místním poskytovatelem internetu bezdrátovou formou a kabeláží následně nataženo do bytu k zařízení. V síti se aktivně střídá a připojuje kolem pěti bezdrátových zařízení od notebooků až po telefony nebo tiskárnu a dva stolní počítače jsou připojeny napřímo síťovým kabelem. Pro návštěvy nebo hosty je připravena k použití také tzv. „hostovaná síť“, viz podkapitola 4.2.1.3 o hostované síti.



Obrázek 15 *Prostory a topologie domácí sítě, zdroj: Autor*

Síť není sice rozsáhlá či nijak komplexní, avšak vzhledem k lokalitě, kterou je centrum menšího města, je její zabezpečení o to důležitější a kritičtější. V blízkém

okolí se mimo jiné nachází celá řada podniků a jiných sítí, od dalších sítí v bytovém domě až po místní kavárny, což představuje další hrozby.

4.2 Router, jeho funkce a hrozby

Celou síť má na starosti pouze jediný router. Jedná se o bezdrátový, single-band 2.4GHz router od firmy Asus, konkrétně model RT-N12 D1 (viz Obrázek 16), který byl poprvé uveden na trh v roce 2012, prodává se dodnes a je ukázkovým příkladem dostačující volby alternativního routeru pro malou a nenáročnou domácnost. Nabízí pokročilou správu firmwaru se stálými aktualizacemi, vlastní zjednodušený firewall, hostovanou síť a v případě potřeby i režim rodičovské kontroly.

Obrázek 16 *Bezdrátový router Asus řady N, ASUS RT-N12 D1, zdroj: [17]*

Na tehdejší dobu disponoval mnoha inovativními technologiemi a nabízel celou řadu pokročilých funkcí. Měl například vestavený zesilovač s kombinací dvou 5dBi antén, díky čemuž dokázal pokrýt kvalitním signálem i větší prostory. [17]

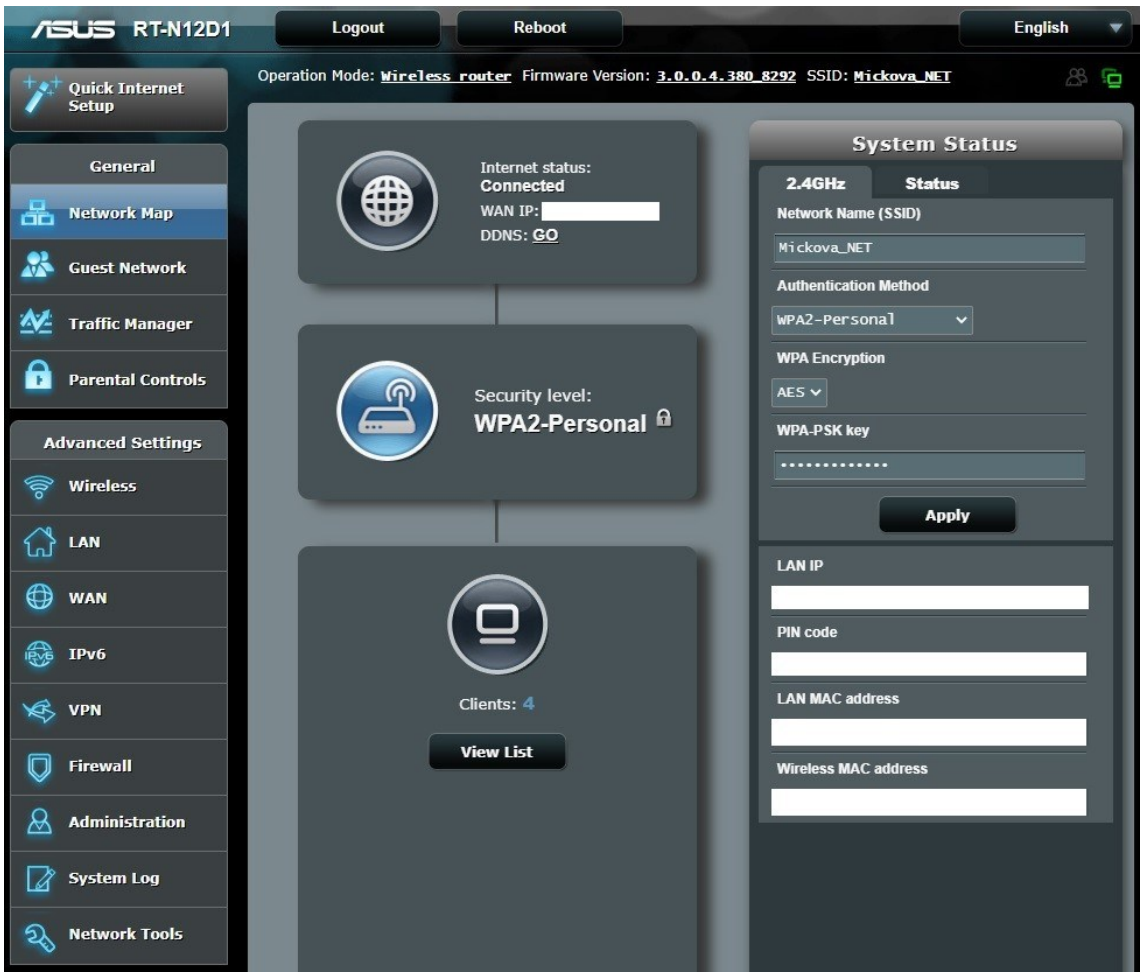
Router se ovládá velice intuitivně díky své jednoduchosti, za kterou vděčí svému grafickému uživatelskému rozhraní (GUI), nazývanému také „ASUSWRT“, které se stalo napříč uživatelskou komunitou velice oblíbené. ASUSWRT totiž jakožto webové rozhraní nepotřebuje ke své funkci žádnou další aplikaci – lze k němu tedy přistupovat i z mobilních zařízení či vzdáleně. [18]

Běžně takový domácí bezdrátový router čelí veškerým útokům a hrozbám v síti jako první. Je totiž tou první bránou, která má nějakou šanci zastavit

potenciální útok nebo průnik hrozby do sítě. Chrání tedy nejen sebe a svoji strukturu, ale také vše co stojí za ním – v tomto případě celou zdejší počítačovou síť, kde se mohou nacházet i desítky zařízení. Mnoho domácích routerů má nějakou zjednodušenou verzi integrovaného firewallu, který má v těchto případech právě pomoci zasáhnout, potažmo pak i jiné mechanizmy.

4.2.1 Jednotlivé prvky zabezpečení

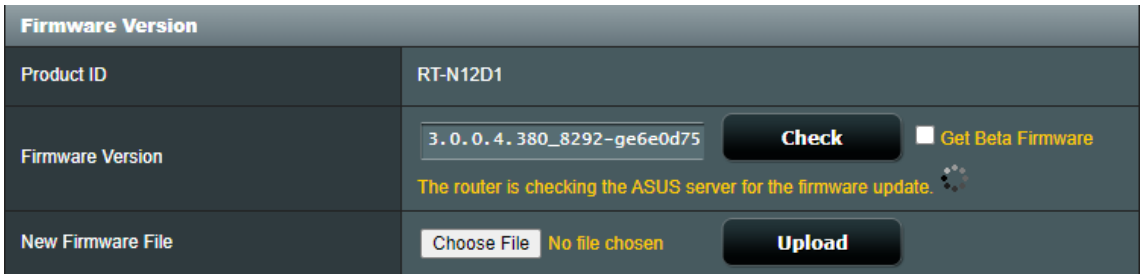
Jak je vidět na Obrázek 17, směrovač se ve výchozím zobrazení nachází v tzv. „mapě sítě“. Ta ukazuje přehled důležitých a často přistupovaných nastavení, stavu sítě a to, jakým způsobem síť funguje. Předností mapy sítě je především rychlý přístup k nastavení a kontrole, jaká zařízení jsou aktuálně v síti, a základní monitoring aktivity.



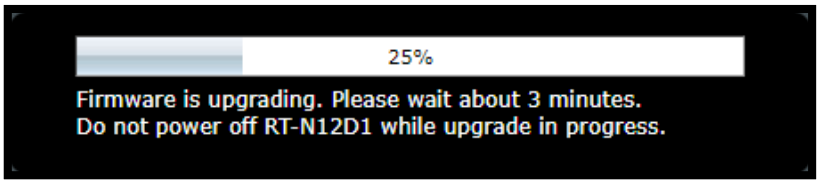
Obrázek 17 *Úvodní obrazovka s mapou sítě, zdroj: Autor*

4.2.1.1 Firmware

Na routeru Asus RT-N12 je proces správy firmwaru částečně automatizovaný (viz Obrázek 18) – výrobce v grafickém rozhraní routeru implementoval funkci, kdy si router za pomocí stisku tlačítka „check“ zkontaktuje oficiální servery výrobce, kde se nacházejí aktualizační soubory, a v případě, že existuje novější verze firmwaru, podá o ní informaci, nabídne aktualizaci a případně zahájí samotnou sekvenci aktualizace. Jako alternativa je zde samozřejmě možnost aktualizace standardní, ruční cestou, přes stažení z webu a následné nahrání ze souboru skrze výběr a tlačítko „upload“. Proces aktualizace firmwaru je vidět na Obrázek 19.



Obrázek 18 *Částečně automatizovaná aktualizace firmwaru na ASUS RT-N12, zdroj: Autor*



Obrázek 19 *Aktualizace firmwaru, zdroj: Autor*

4.2.1.2 Zabezpečení bezdrátové komunikace

To, čemu by měl uživatel věnovat největší pozornost hned po firmwaru, je Wi-Fi síť a bezdrátový přenos. Ke kvalitnímu zabezpečení bezdrátové sítě a jakýchkoliv zařízení obecně je žádoucí také kvalitní komplexnost hesla. Jelikož se jedná o údaj, který bude pravděpodobně velmi často využíván a poskytován pro nově připojovaná zařízení a pro hosty, je rozumné jeho volbu důkladně promyslet. V současné době není rozhodně doporučováno dávat do hesla ani jakékoliv celé slovo, natož pak úsměvně oblíbená data narození, číselné posloupnosti typu 123 apod. Co je zde klíčové jsou kombinace – a to velkých a malých písmen, čísel a speciálních znaků. Existují i online generátory hesel

nebo vzory pro hesla, které si může uživatel vygenerovat a následně upravit dle své libosti. Nicméně už jen to, že heslo bylo někde na internetu vygenerováno, mu na důvěryhodnosti moc hodnoty nepřidá.

„Network name“ neboli SSID značí název sítě, pod nímž bude viditelná a dostupná – ideální název by měl být pokud možno stručný a výstižný, neměl by ale opět obsahovat žádné osobní nebo citlivé údaje, neboť jsou to informace dostupné komukoliv v okolí. Pokud by bylo potřeba, lze zde zvolit i možnost „hide SSID“, která název sítě skryje.

„Wireless mode“ souvisí s podporou standardu IEEE 802.11 na jednotlivých zařízeních. Ve výchozím a optimálním nastavení automatického výběru si router volí sám rozhraní IEEE, dle kterého připojuje zařízení s podporou 802.11n, 802.11g nebo 802.11b. Zaškrtávací položka „b/g protection“ slouží pro podporu připojení starších zařízení, která mohou mít s novějšími verzemi standardu problémy.

„Channel bandwidth“ je volba frekvenční šířky pásma, která však stojí za pozornost pouze v případě problémů se stabilitou, kdy výrobce doporučuje vyzkoušet nastavení 20MHz, jinak opět automatické nastavení. To stejné platí i pro „control extension channel“, které mají na bezpečnost sítě nulový vliv a řeší se spíše v experimentálních případech.

Co však stojí za největší pozornost je „authentication method“ neboli nastavení autentizace[12] a režimu přístupu. Na výběr je zde ze dvou možností, a to WPA a WPA2.

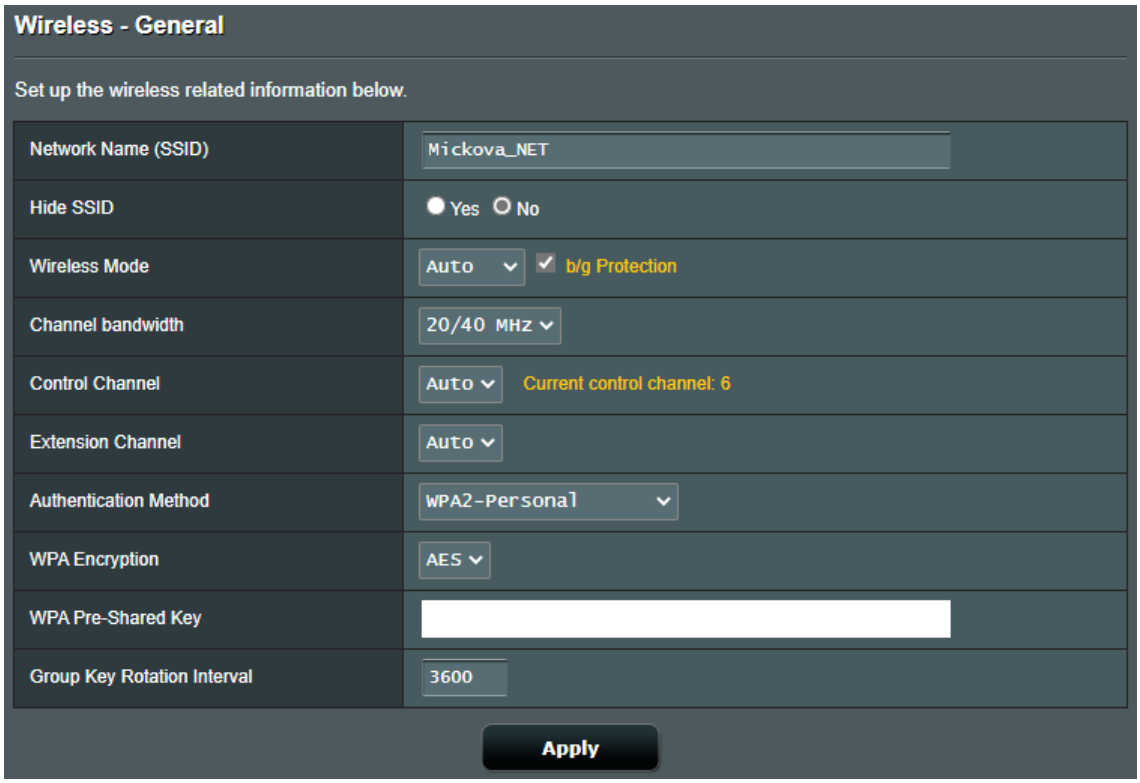
WPA (z anglického Wi-Fi Protected Access) metoda se stala standardem, který vychází z historicky originální specifikace zabezpečení 802.11 zvané WEP, vylepšené o šifrovací algoritmus, díky čemuž se stává hůře prolomitelnou. WEP se však sama o sobě dnes již nepovažuje za bezpečnou metodu a lze ji poměrně snadno prolomit, proto ji většina výrobců už ani nezahrnuje do svých routerů. [22]

[12] Autentizace je proces bezpečnostního opatření, který se stará o ochranu před falešnou identitou subjektu. Subjektem se myslí např. osoba či nějaký systém – ten musí prokázat svoji identitu. Existuje mnoho způsobů autentizace, která se odvíjí vždy od konkrétní situace. Subjekt může být autentizován například identifikační kartou, heslem či různými biometrickými údaji. [21]

Oproti tomu WPA2 je posledním současným standardem pro zabezpečení bezdrátových sítí. Využívá ke své práci pokročilý šifrovací protokol AES, který je v současnosti považován za dosud nejsilnější šifrovací protokol. [22]

Jak WPA, tak i WPA2 se dále dělí do režimů Personal a Enterprise. Režim Personal najdeme v domácích, malých kancelářských nebo firemních sítích. Uživatelé se identifikují pomocí „předsdíleného klíče PSK“ (Pre-shared key), který slouží jako heslo pro ověření s bezdrátovým routerem. Oproti tomu režim Enterprise nalezneme v podnicích a větších firmách, kdy se autentifikace řeší přes vyhrazený server za pomocí řady protokolů založených na standardu 802.11. [22]

WPA2-Personal tedy v současné době představuje nejlepší možnou volbu, jak může uživatel učinit svoji bezdrátovou síť co možná nejbezpečnější. Byť je už nějakou dobu známo, že i ta nejaktuálnější metoda autentifikace WPA2 je prolomitelná, zůstává i tak plnohodnotnou ochranou, která sice není stoprocentně spolehlivá, ale stále je lepším řešením nežli otevřený nezabezpečený Wi-Fi systém.



Obrázek 20 *Podrobnější nastavení bezdrátového přenosu, zdroj: Autor*

Další záležitostí Wi-Fi sítě, která stojí za zmínku, je WPS – Wi-Fi protected setup. Díky této funkci se může do sítě připojit jakékoliv bezdrátové zařízení s podporou WPS.

Použití WPS ovšem dodnes zůstává u síťových zařízení velkou otázkou. Tento standard má za sebou nechvalnou historii kvůli svému nezdařilému designu registračního protokolu a spoustě chyb při samotné implementaci do provozu. Jakmile se něco takového rozkřiklo po Internetu, odborníci i samotní výrobci zařízení vydávali důrazná doporučení WPS nepoužívat. Začaly probíhat „Brute force" útoky online i offline metodami nebo zneužívání slabin v systémech Windows, kdy se uživatel namísto připojování k routeru ve skutečnosti připojoval na podvodný přístupový bod a neměl ani tušení, že se právě úspěšně připojil k útočníkovi. [23]

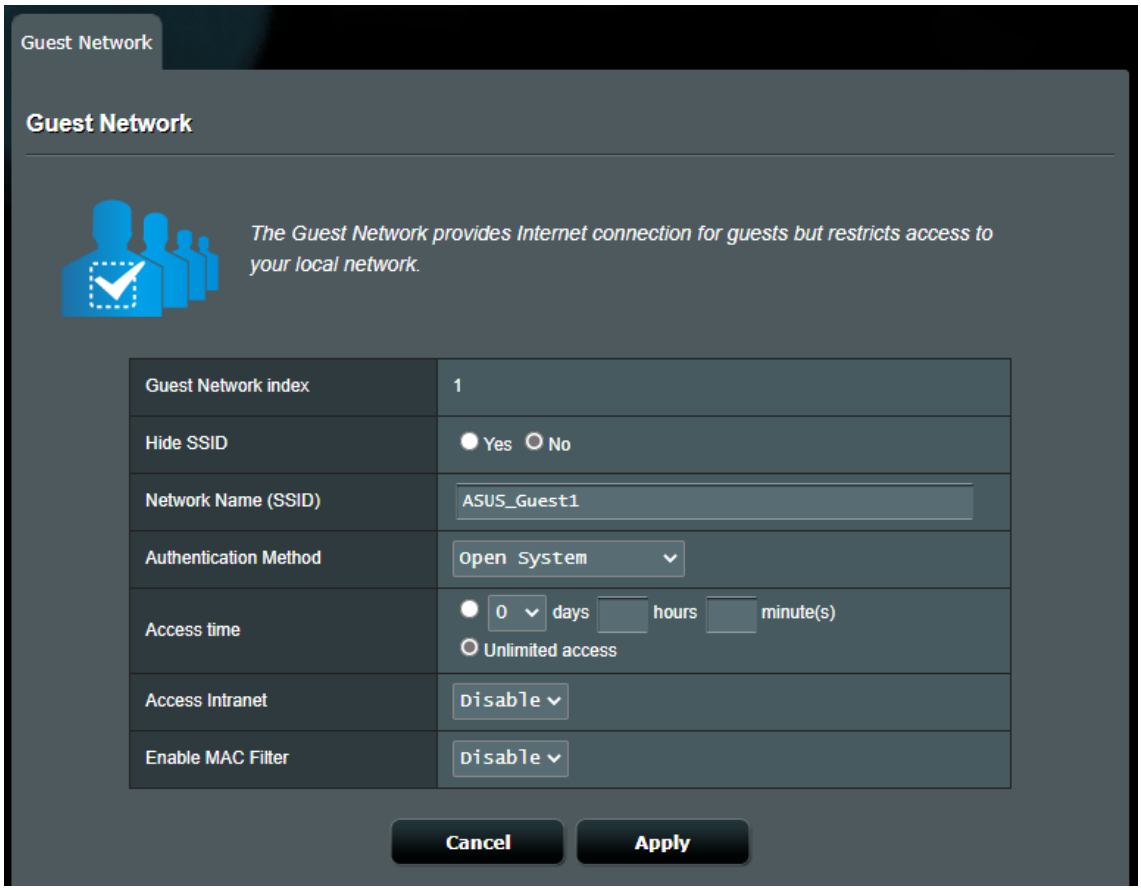
WPS je dodnes stále rozšířenou funkcí, kterou disponuje téměř každý bezdrátový router. Jako nouzové řešení tato funckionalita určitě potěší, avšak nežli zbytečně riskovat, je lepší sáhnout po sofistikovanějších řešeních jako je hostovaná síť.

4.2.1.3 Hostovaná síť

Samostatná síť pro hosty, tzv. „hostovaná síť", představuje způsob, jak oddělit správu a síťový provoz a zároveň mít lepší kontrolu nad zařízeními, která se do sítě připojují. Pokud je hostovaná síť zapnuta, zařízení se ve skutečnosti připojují do samostatné podsítě. Pro správce je to dlouhodobě efektivní a snazší řešení, protože může měnit nastavení a funkce pro celou síť s hosty, aniž by narušil strukturu a nastavení původní místní sítě.

Na Obrázek 21 je vidět, jak vypadá karta nastavení hostované sítě. „Guest Network Index" neboli index hostované sítě je systém indexování, pomocí kterého router rozpoznává, o jakou hostovanou síť se jedná. Zdejší model RT-N12 nabízí možnost současného běhu až tří hostitelských sítí. Dále tu jsou nastavení jako u běžné sítě, tj. správa SSID či výběr metody ověření a zabezpečení pro bezdrátové připojení. Zajímavou možností je i nastavení „Access Time" (přístupová doba), kdy lze omezit dostupnost dané hostované sítě na určitou dobu nebo „Access Internet", kdy lze omezit hostům přístup do vnitřní LAN sítě. Dále lze také v hostitelské síti

povolit či zamítnout přístup do intranetu a provádět základní filtrování na základě MAC[13] adres.



Obrázek 21 *Nastavení hostované sítě, zdroj: Autor*

4.2.1.4 Firewall

Jak již bylo zmíněno, Firewall je v počítačové síti po stránce bezpečnosti velmi důležitým prvkem. Zdejší model RT-N12 disponuje jednoduchým síťovým firewallem – viz Obrázek 22. To přináší celou řadu výhod – síťový provoz se například nejprve bude muset dostat přes firewall routeru, nežli se vůbec dostane k firewallu daného zařízení (např. u stolního PC). Další nadstavbou jsou pokročilé algoritmy, které by měly být dle výrobce schopny zastavit i základní DoS útoky či jiné pokusy o síťové útoky. Router v tomto případě dokáže i zaznamenávat do

[13] MAC adresa je jedinečným identifikátorem zařízení v hexadecimální podobě. Říká se jí také tzv. fyzická adresa, protože je obvykle přiřazována výrobci daných zařízení do různých forem fyzické paměti.

logů[14] jednotlivé pakety síťové komunikace. Logování lze nastavit na vícero úrovních, mohou se zaznamenávat jak všechny pakety, které firewallem projdou, tak jenom ty, které router z nějakého důvodu zamítl a zahodil, v případě potřeby i oba typy. Funkce logování se dá samozřejmě i kompletně vypnout.

Obrázek 22 *Nastavení firewallu a logování paketů, zdroj: Autor*

4.2.1.5 URL filtry

Za zmínku také stojí URL[15] filtrování, zajímavá funkce, která je součástí firewallu routeru. Nastavení není nijak složité, filtrování funguje na základě filtrační tabulky, kam se zadávají klíčová slova. Tu si uživatel definuje dle svých potřeb a následně potvrdí nastavení. Na základě zadaných informací v tabulce bude router filtrovat URL adresy, které obsahují tyto řetězce.

Filtrování lze nastavit dvěma způsoby: buď se jedná o tzv. „blacklist“, tedy černou listinu, kdy bude router filtrovat to, co je definované v tabulce, nebo je zde striktnější nastavení tzv. „whitelistem“, kdy bude router filtrovat veškeré URL adresy, které naopak nejsou definovány v tabulce. Filtr není stoprocentně spolehlivý, protože jak sám výrobce uvádí, některé druhy stránek, včetně HTTPS[16] protokolu nelze filtrovat.

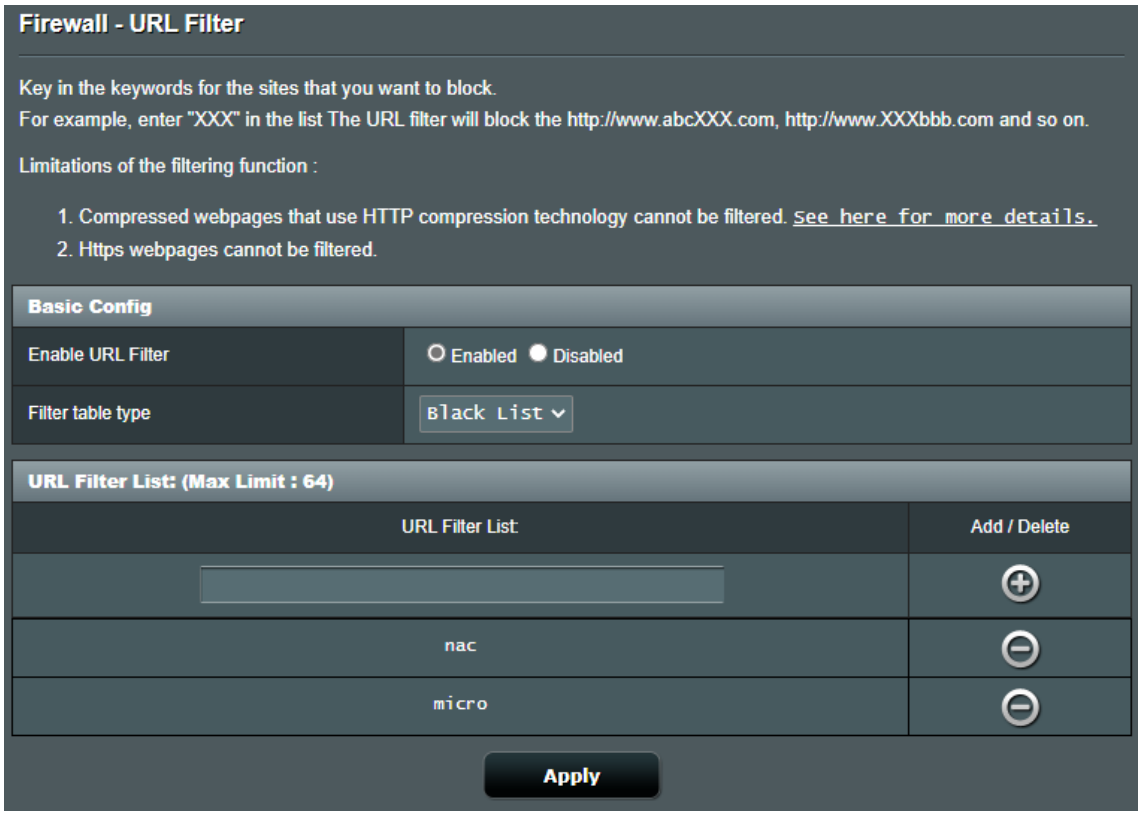
---

[14] Tzv. log a související pojem logování je zaznamenání informací o nějaké konkrétní činnosti do souboru

[15] URL je jednotná struktura, přes kterou se přistupuje k jednotlivým zdrojům na Internetu (webovým stránkám, souborům…)

[16] HTTPS je vylepšená (zabezpečená) forma komunikačního protokolu HTTP, který slouží pro přenos různých informací na webu

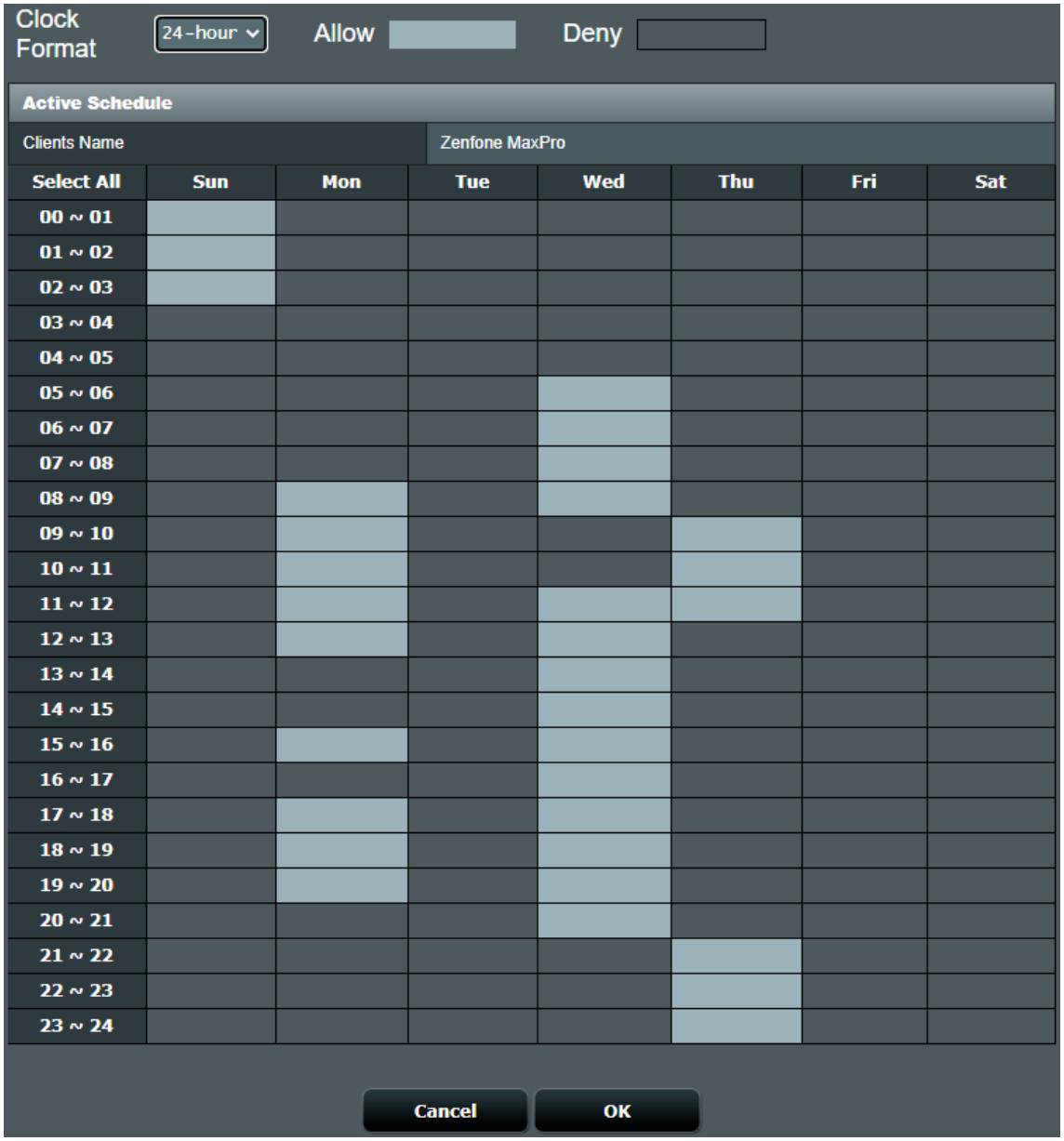
Na Obrázek 23 s filtrovacím režimem „blacklist“ lze vidět například filtr na klíčové slovo micro, což znamená, že kdokoliv v síti bude chtít na webové stránky společnosti Microsoft, bude zachycen filtrem a na stránku se nedostane.



Obrázek 23 *URL filtrování s filtrem v režimu blacklist, zdroj: Autor*

4.2.1.6 Rodičovská kontrola

Pokud je třeba, je zde i režim tzv. „rodičovské kontroly“. Jde o jednoduchý nástroj, jehož pomocí lze jednotlivým uživatelům vymezit dobu, po kterou mohou používat síť. Uvítají ho zejména rodinné a početné sítě. Filtrování probíhá obdobně jako u URL filtrování ve firewallu, tedy na základě zařízení a jejich MAC adres. Uživatel si dohledá zařízení, přidá ho do tabulky a následně se dostává do sekce „Time Management“. Upřesnění pak probíhá v tabulce časového rozpisu, kde jednotlivá pole představují den v hodinách. Uživatel zakliknutím příslušných oblastí zakazuje (prázdná pole) nebo povoluje (modře vyplněná pole), kdy je možné na daném zařízení používat síť – viz Obrázek 24.



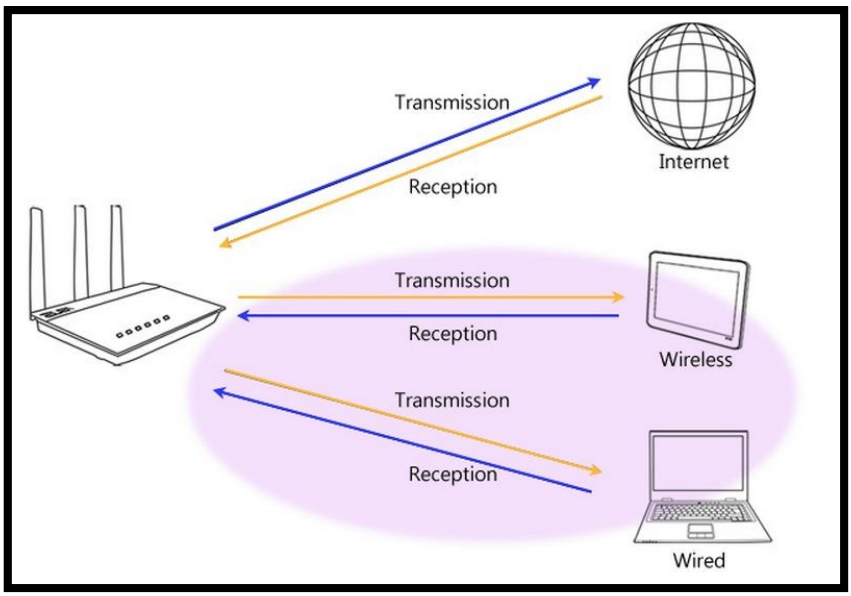
Obrázek 24 *Tabulka rozpisu rodičovské kontroly, zdroj: Autor*

4.2.2 Manažer síťového provozu

RT-N12 také v rámci rozšířených funkcí nabízí tzv. „Traffic manager“ – manažer síťového provozu. Jedná se o nástroj, který je schopen provádět základní měření, monitorování sítě, graficky vizualizovat tok dat a reprezentovat výsledky provozu celé sítě.

Konkrétně se zde monitoruje provoz příchozích a odchozích paketů.[17] Ten je rozdělen do tří kategorií, jak je vidno na Obrázek 25:

- Internetové pakety (Internet packets) – pakety, které jsou přenášeny mezi routerem a WAN sítí neboli internetem
- Pakety přenášeny po médiu (Wired packets) – pakety, které se přenáší přes klasický síťový kabel RJ-45 či jiné médium mezi routerem a připojeným zařízením
- Pakety přenášeny bezdrátově (Wireless packets) – veškeré pakety, které jsou přenášeny vzduchem mezi routerem a bezdrátově připojeným zařízením

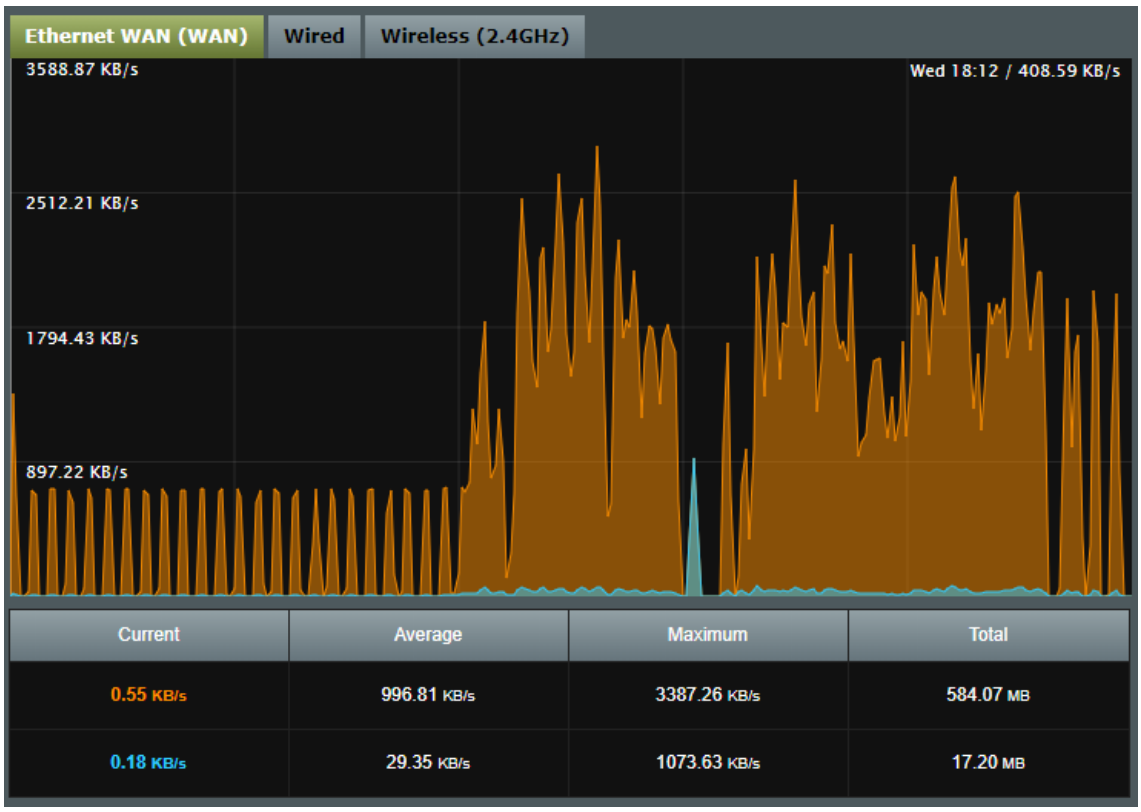


Obrázek 25 *Znázornění kategorií síťového provozu, zdroj: Obrázek [25]*

Router umí celkem tři režimy sledování síťového provozu. Prvním a zároveň výchozím režimem je sledování v reálném čase. Router automaticky zaznamenává síťový provoz po celou dobu svého provozu, avšak po vstoupení na hlavní stránku manažera síťového provozu začne také vykreslovat infografiku s daty, která právě putují napříč sítí v reálném čase, a po časových odskocích je zaznamenává do grafu. Graf je také doplněn jednoduchou tabulkou, která se průběžně aktualizuje a znázorňuje množství dat, která jsou přijímána a odesílána v daný okamžik,

[17] Paket představuje v počítačové síti balíček informací nebo dat, která jsou přenášena po síti.

průměrně, ve výkyvech a celkově. Na Obrázek 26 lze vidět ukázku monitorování v režimu reálného času, konkrétně tedy internetových paketů, kdy oranžově zvýrazněná část grafu značí příchozí pakety a modře zvýrazněná část naopak pakety odchozí.



Obrázek 26 *Real-time monitoring RT-N12, zdroj: Autor*

Druhým režimem sledování síťového provozu je 24h režim. Tento režim slouží především jako rychlý přehled toho, co se dělo v síti a kolik odešlo či dorazilo dat bezdrátovým či kabelovým přenosem. Aktivita je opět prezentována barevně odlišeným grafem a tabulkou s množstvím přenesených dat.

Jako poslední režim se zde nachází denní režim – viz Obrázek 27. Tento režim najde svou přidanou hodnotu především v sítích s omezením FUP,[18] kdy tak správce může sledovat průběžné vytížení a množství stahovaných dat. V denním režimu

[18] FUP (Fair User Policy) je politika internetových služeb, která by měla zajistit uživatelům stejnou kvalitu a dostupnost internetu. Jedná se typicky o sítě, kde je pásmo dat sdíleno s ostatními uživateli. Uživatel má k dispozici určitý objem dat a v případě jeho vyčerpání je patřičně omezen, nejčastěji formou snížení přenosové rychlosti. [20]

router sestavuje přehledové tabulky s množstvím přenesených dat za jednotlivé dny, a to až 30 dní zpět.

Date	Reception	Transmission	Total
2020-07-15	15.60 GB	6.93 GB	22.53 GB
2020-07-14	18.42 GB	8.16 GB	26.58 GB
2020-07-13	16.80 GB	7.39 GB	24.19 GB
2020-07-12	40.08 GB	35.53 GB	75.62 GB
2020-07-11	17.81 GB	9.08 GB	26.89 GB

Last 30 Days (2020-06-16 ~ 2020-07-15)	
Reception	394.20 GB
Transmission	213.04 GB
Total	607.24 GB

Obrázek 27 *Přehledové tabulky sestavené routerem, zdroj: Autor*

4.2.3 Připojovaná zařízení

Stav a stáří jednotlivých zařízení, která se k síti připojují může představovat další potenciální rizika. Byť není nezbytně nutné, aby na zařízeních byly nainstalovány nejnovější aktualizace samotných operačních systémů nebo příslušného aplikačního vybavení, je to vždy výrazně doporučováno. Nejen, že pak zařízení dokážou lépe spolupracovat s aktuálními technologiemi a standardy, ale chrání opět o to víc i samy sebe. Mimo to u starých zařízení může docházet k situacím, že například nebudou podporovat aktuálně běžící verzi Wi-Fi standardu 802.11. I na to však mají některé routery včetně zde demonstrovaného řešení, většinou formou nějaké vestavěné podpory v samotném programovém vybavení, nicméně není to nic, na co by se dalo vždy spolehnout. Co se týče podpory nejnovějších zabezpečovacích metod k zabezpečenému bezdrátovému připojení jako je např. WPA2, je zde možnost využít řešení jako je třeba již zmiňovaná hostovaná síť, kdy se zařízení může připojit skrze speciálně vytvořenou síť.

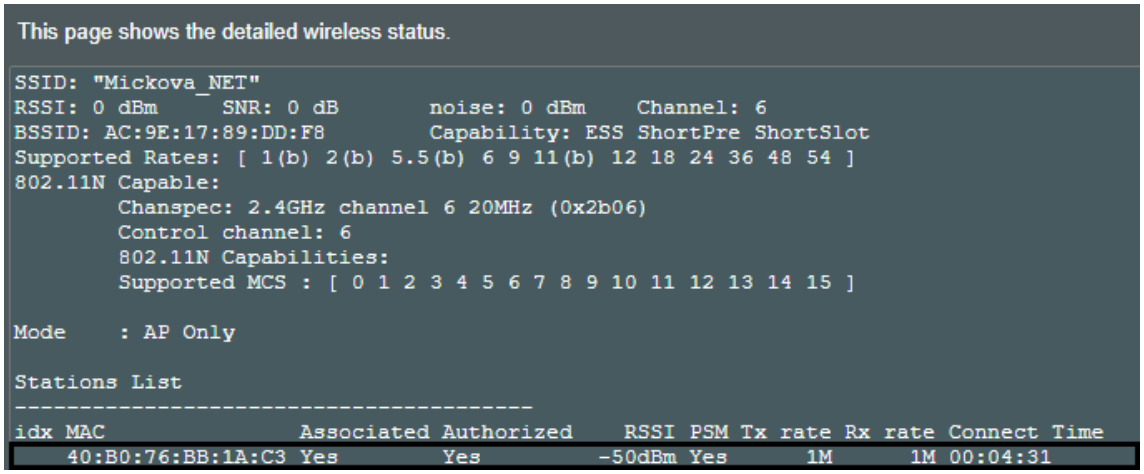
Bezpečnost a aktualizace v segmentu síťových tiskáren, kamer či dalšího „smart“ příslušenství se v síti odvíjí poměrně individuálně. Nicméně pravidla tu platí v obecné rovině naprosto stejně jako u jakýchkoliv jiných zařízení. Například

u takové monitorovací kamery je rozhodně žádoucí poskytovat konektivitu a provádět filtrování, obzvláště když kamera podporuje možnosti jako je vzdálený aktivní monitoring. Tato zařízení mohou být cílem útočníků a hackerů stejně jako běžný počítač nebo notebook.

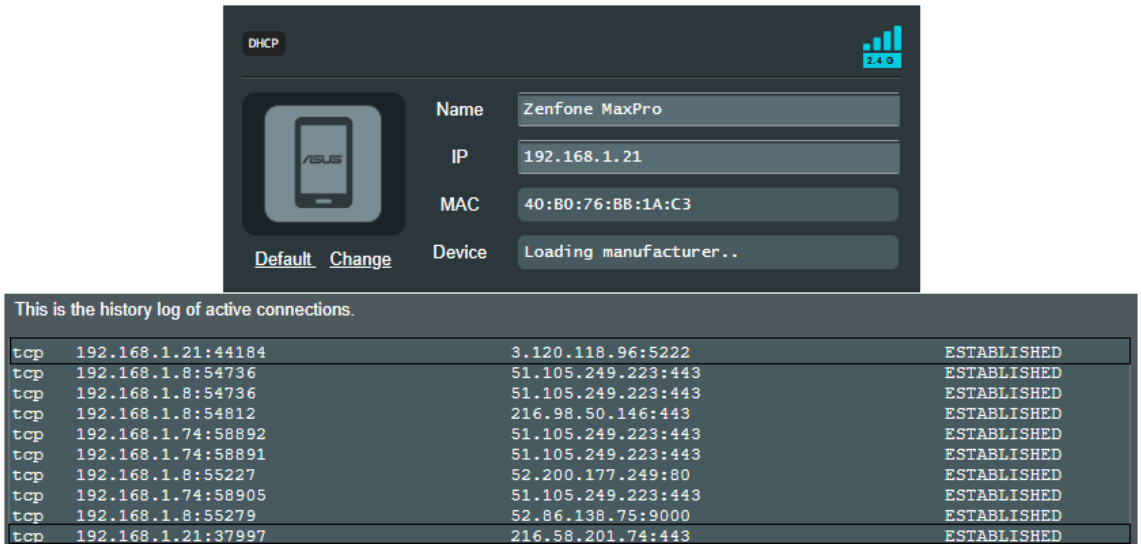
5 Testování a výsledky

5.1 Test konektivity a připojení k síti

První test se věnoval bezdrátovému zabezpečení. Konkrétně šlo o připojení zcela nového zařízení do Wi-Fi sítě skrze hlavní, nehostovanou síť, která vyžadovala standardní autentifikaci s metodou WPA2-Personal. Pro účely testu byly využity logy routeru a také síťové nástroje, kterými RT-N12 disponuje. Jak lze vidět v logu bezdrátové činnosti na Obrázek 28, zařízení bylo úspěšně připojeno a identifikováno. Záznam MAC adresy souhlasí s MAC adresou zařízení a v polích „Associated“ a „Authorized“ se nachází hodnota „yes“. V logu aktivních připojení v síti na Obrázek 29 si lze také dle příslušně přiřazené IP adresy zařízení povšimnout, že se toto spojení nachází ve stavu „Established“ – navázáno. Celý proces tedy skončil úspěchem.



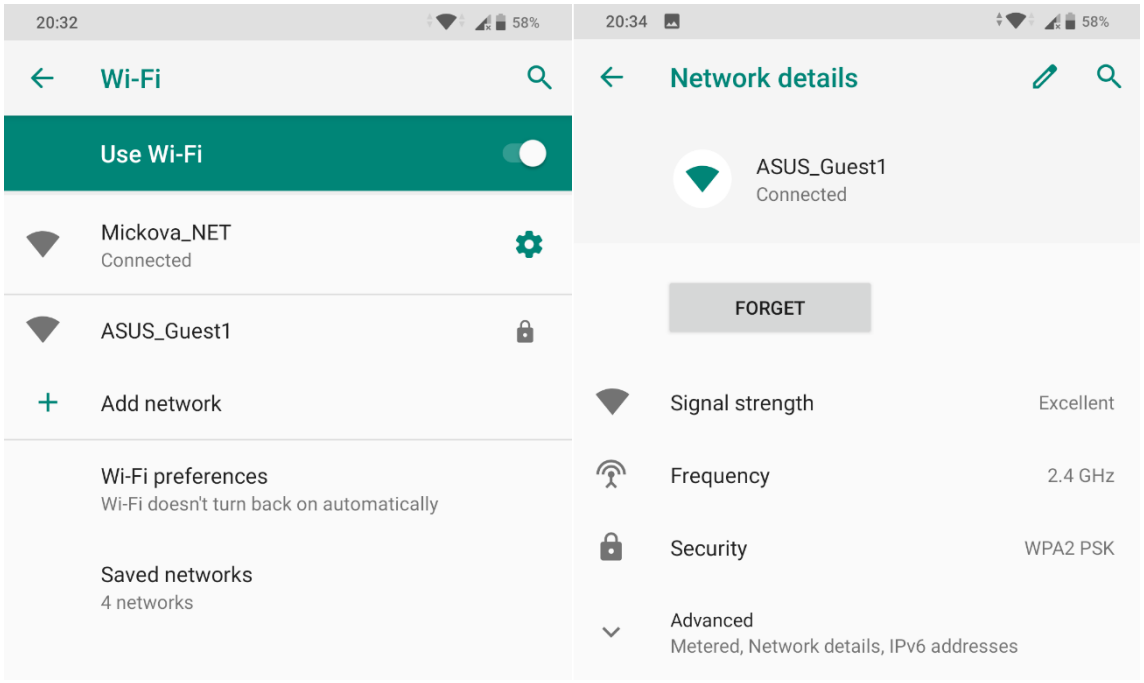
Obrázek 28 *Log bezdrátových připojení, zdroj: Autor*



Obrázek 29 *Informační okno zařízení (nahoře) a log aktivních připojení (dole), zdroj: Autor*

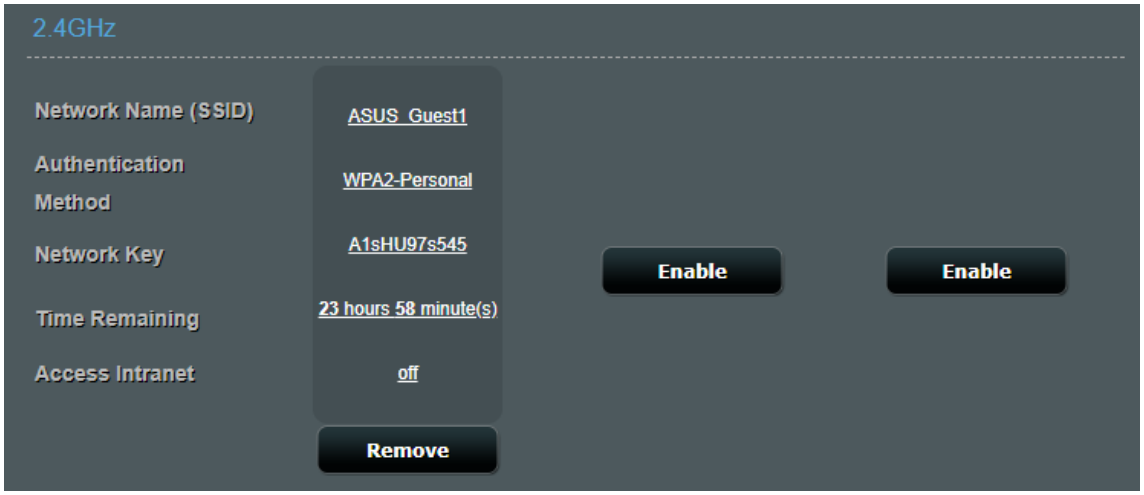
Test se dále zaměřoval také na hostovanou síť. Testovací zařízení se tentokrát připojovalo do vytvořené oddělené sítě pro hosty. Pro spoustu uživatelů je rozhodujícím faktorem, proč sáhnout po hostované síti, to, že hosté k ní připojení se ve výchozím stavu nedostanou k intranetu[19]. Zabezpečení a připojení probíhá principiálně velmi obdobně jako u připojení ke klasické primární Wi-Fi síti. Jak znázorňuje Obrázek 30, host se připojuje k příslušné SSID hostované sítě, zde konkrétně tedy k „ASUS_Guest1“, v kombinaci s poskytnutým síťovým klíčem, viz také Obrázek 31.

[19] Intranet je častý název počítačové sítě v organizacích, firmách a různých institucích. Této síti se říká vnitřní síť, protože bývá většinou nastavena tak, aby se k ní nedostal nikdo z vnějšku, resp. z Internetu



Obrázek 30 *Připojení k hostované síti ASUS_Guest1, zdroj: Autor*

V sekci hostované sítě routeru lze pak kdykoliv v průběhu spravovat a měnit i její nastavení, což je vidět na Obrázek 31 s aktuálním nastavením a úrovní bezpečnosti.



Obrázek 31 *Hostovaná síť s aktuálním nastavením, zdroj: Autor*

V logu bezdrátové činnosti na Obrázek 32 je opět vidět záznam zařízení po úspěšné autentifikaci. Jedna věc se však liší, a to je „idx“ neboli index. Router totiž už záznam o komunikaci s tímto zařízením má a indexaci zahajuje vždy od nuly. Jednička na záznamu tedy značí, že zařízení už v minulosti bylo k síti připojeno,

avšak skrze jiné připojení. Příznaky autentifikace jsou opět vyjádřeny hodnotou „yes“ a potvrzují tak úspěšné připojení do hostitelské sítě.

```
Stations List
-----------------------------------------
idx MAC               Associated Authorized    RSSI PSM Tx rate Rx rate Connect Time
1   40:B0:76:BB:1A:C3 Yes        Yes         -48dBm Yes      1M      1M 01:51:29
```

Obrázek 32 *Záznam zařízení připojeného v hostované síti se změnou indexu, zdroj: Autor*

5.2 Test síťového provozu na úrovni aplikační vrstvy

Druhý test se věnoval šifrování v síťovém provozu na úrovni vrchních vrstev TCP/IP modelu, resp. na úrovni aplikační vrstvy. Tento test byl demonstrován na webových stránkách s podporou zabezpečeného připojení (HTTPS protokol), kde se přihlašovalo za pomocí uživatelského jména a hesla k uživatelskému účtu.

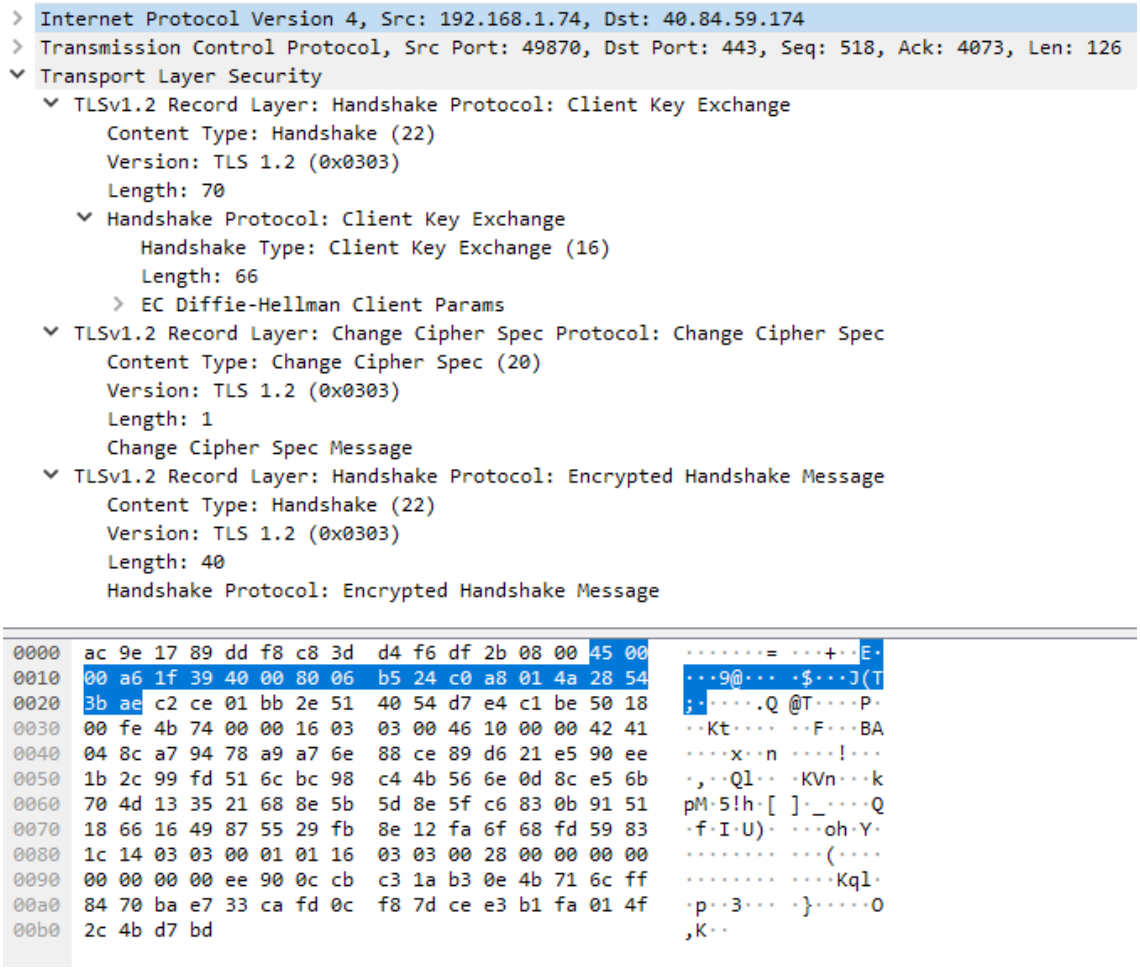
Pro účely testování zde byl využit síťový nástroj a analyzátor, Wireshark. Na Obrázek 33 se nachází tabulkový rozpis TCP konverzace celkem o 10 paketech (událostech). Co je zde nejdůležitější jsou samozřejmě sloupce „Source“ a „Destination“, které značí odkud kam probíhala komunikace, dále také „Protocol“ vyjadřující používaný komunikační protokol a v poslední řadě „Info“ sloupec, kde se nacházejí informace k jednotlivým paketům.

Source	Destination	Protocol	Length	Info
192.168.1.74	40.84.59.174	TCP	66	49870 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
40.84.59.174	192.168.1.74	TCP	66	443 → 49870 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
192.168.1.74	40.84.59.174	TCP	54	49870 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
192.168.1.74	40.84.59.174	TLSv1.2	571	Client Hello
40.84.59.174	192.168.1.74	TCP	2974	443 → 49870 [ACK] Seq=1 Ack=518 Win=262656 Len=2920 [TCP segment of a reassembled PDU]
192.168.1.74	40.84.59.174	TCP	54	49870 → 443 [ACK] Seq=518 Ack=2921 Win=66048 Len=0
40.84.59.174	192.168.1.74	TLSv1.2	1206	Server Hello, Certificate, Server Key Exchange, Server Hello Done
192.168.1.74	40.84.59.174	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
40.84.59.174	192.168.1.74	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
192.168.1.74	40.84.59.174	TCP	54	49870 → 443 [ACK] Seq=644 Ack=4124 Win=65024 Len=0

Obrázek 33 *Analýza TCP konverzace, zdroj: Autor*

V celém záznamu konverzace lze vidět několik typů tzv. „handshake messages“. Ty značí způsob komunikace, kterým se obě komunikující strany dorozumívají. Na čtvrtém řádku lze vidět např. „Client Hello“, na šestém „Server Hello“ atd. Co je však zde směrodatnou informací je sedmý až devátý paket – tedy především informace „Server key Exchange, Client key Exchange“ a hlavně informace „Encrypted Handshake Message“ podaná z obou stran účastníků komunikace, tj. počítačem s dynamicky přidělenou IP adresou v lokální síti (192.168.1.74) a webovou stránkou, s kterou probíhá komunikace (40.84.59.174). „Handshake proces“ skončil z obou stran úspěšně, viz opět Obrázek 33.

Při pohledu do detailního výpisu jednoho z paketů, kde proběhlo zašifrování přenášených informací, vidíme v TLS protokolu[20] další důkazy. Záznamy jsou opět šifrované, což je patrné i z níže viditelných segmentů dat.



Obrázek 34 *Detailní pohled do TLS protokolu, zdroj: Autor*

5.3 Penetrační test a analýza z vnějšího prostředí

Dalším zajímavým testem byl penetrační test. Díky dispozici veřejné WAN IP[21] adresy se podařilo nasimulovat sérii útoků a penetračních testů z vnějšího reálného světa. Vše probíhalo za pomocí webové aplikace a online nástroje Intruder.

[20] TLS protokol je vylepšenu verzí dříve používaného SSL protokolu. Tyto protokoly pomáhají zajišťovat bezpečnost komunikace mezi dvěma klienty v síti.

[21] Veřejná IP adresa přináší oproti klasické, hojněji používané, privátní IP adrese celou řadu výhod, ale také nebezpečí. Zřizuje se například kvůli zastoupení role serveru nebo obecně k jakémukoliv poskytování síťového provozu do vnějšího světa. Je však o to snadnějším cílem pro síťové útoky a infiltraci jakéhokoliv nebezpečí do sítě.

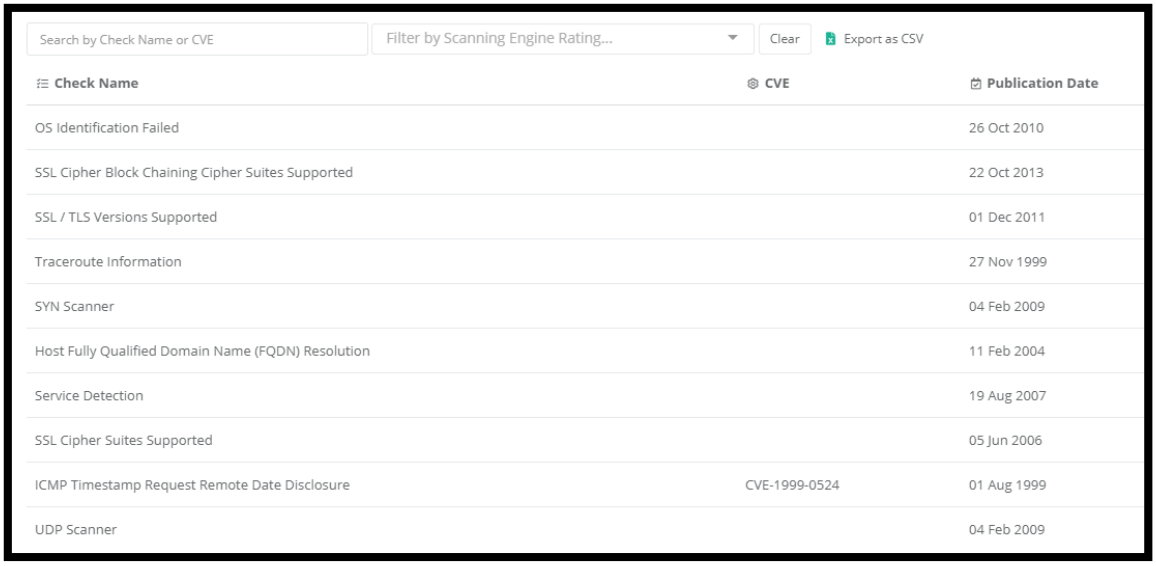
Jedná se o britský projekt, vyvinutý za účelem ochrany proti internetovým útokům a kriminalitě, který uvítají z dlouhodobého hlediska hlavně firmy a bezpečnostní společnosti.

Skenování spolu s testem zabralo bezmála dvě hodiny čistého času. Součástí bylo hledání běžných bezpečnostních chyb, chyb v konfiguraci routeru, chybějících bezpečnostních záplat, aplikačních bugů či prostorů k útoku včetně slabin v šifrování.

Jak znázorňuje Obrázek 35, výsledky dopadly velmi obstojně. Bylo zkontrolováno bezmála deset tisíc zranitelných objektů či položek, kde žádný nebyl vyhodnocen jako problémový na úrovni vnějšího nebezpečí.

Obrázek 35 *Základní přehled síťového skenu v Intruderu, zdroj: Autor*

Za „Noise“ kategorií pak stojí čistě informativní záležitosti, které byly Intruderem odfiltrovány, protože nepředstavují žádné hrozby po stránce bezpečnosti. Jedná se zpravidla o nějaké běžící služby na pozadí, viz tabulkový výpis na Obrázek 36.



Obrázek 36 *Detailní výpis odfiltrovaných „noise“ položek, zdroj: Autor*

Avšak Intruder přeci jen odhalil problém, i když je pouze jeden. Tím problémem jsou porty protokolů a aplikací. V kombinaci s veřejnou IP adresou představují jakékoliv otevřené porty pro komunikaci v síti velké nebezpečí. Jak je vidět na Obrázek 37, Intruder našel potenciální hrozbu v otevřeném portu na síti, konkrétně se zde jedná o port příslušící herní platformě Steam, který je vyhrazený na různé vysílací služby této platformy. V praxi nastává problém v momentě, kdy může například někdo takto v síti s veřejnou IP adresou oskenovat právě otevřené porty a zjistit, které jsou otevřené pro komunikaci. Proto je dobré vždy myslet na tato rizika a povolovat v takové síti dlouhodobě komunikaci jen tam, kde je to opravdu nezbytně nutné a využívané.

Obrázek 37 *Výpis síťových služeb v Intruderu, zdroj: Autor*

5.4 Doporučení a shrnutí

Zvolením prostředí běžné domácí sítě společně s využitým hardwarem, představením jeho funkcionalit a konfigurace, se podařilo poukázat na celou škálu bezpečnostních prvků, které hrají zásadní roli v bezpečnosti malých a domácích sítí. Router, který zde slouží jako jediným a hlavním síťovým prvkem, byl podroben

detailnímu rozboru zejména po softwarové stránce, kde bylo zjištěno, jak si uživatel může správnou konfigurací a vynucením určitých nastavení pomoci ochránit svoji síť od potenciálních síťových útoků nebo neoprávněného přístupu k rozhraní routeru z vnější sítě. Bohužel u velké části domácích síťových zařízení však končí hranice možností ochrany právě v závislosti na omezení softwaru a aplikačních součástí. Typicky se volbou správných položek a tlačítek májí nastavit či aktivovat další ochranné prvky. Alternativou by bylo použití Open WRT prostředí, k tomu je ale třeba odborné znalosti převyšující běžného uživatele, což nebyl záměr této práce.

Další možnosti, jak zvýšit bezpečnost a ochranu, odhalily právě výše provedené testy. Díky takovým testům se totiž v síti naleznou další slabiny, které mohou být daleko závažnější. Zde například odhalil penetrační test, že se na síti, jež je dostupná pod veřejnou IP adresou, nachází otevřený port, příslušící určité službě nebo aplikaci. Jakmile by kdokoliv zjistil, že se tato síť nachází pod veřejnou IP adresou, už zde vzniká problém kritických následků. Port se tedy podařilo odhalit a bezpečně vypnout.

Pokud domácí routery nabízejí dodatečné součásti jako nějaký zjednodušený integrovaný firewall, možnosti vytvářet hostovanou síť nebo třeba správu monitorovacích funkcí, vyplatí se tyto funkcionality využívat. Obzvláště pak v sítích, kde je velký provoz, neboť dále diverzifikují a chrání síť.

Stejně tak jako u jakýchkoliv síťových aktivních prvků, kde se čas od času mohou objevovat důležité aktualizace na firmware, tak i na koncových zařízeních je rozhodně žádoucí provádět pravidelné aktualizace, a to nejen samotných součástí operačních systému a celkových zařízení, ale také firmware hardwarových komponent a nainstalovaného programového vybavení. Díky tomu se zvyšuje odolnost každého zařízení v síti. Pokud totiž už dojde k tomu, že se dostane nějaká část nežádoucího kódu nebo softwaru do sítě, může se alespoň zamezit dalšímu šíření a jednotlivá zařízení zůstávají také více chráněna. K tomu je potřeba, aby se uživatelé ke svým zařízením hlásili pod účty uživatelů, aby škodlivý kód nemohl převzít kontrolu.

6 Závěr

Problematika zabezpečení v síti a online světě je nesmírně důležitou oblastí, kde narůstají nároky a míra nebezpečí každým dnem. Cílem práce bylo nejen vyzdvihnout důležitost bezpečnosti a popsat principy počítačové sítě se souvisejícími hrozbami, ale také představit návrh, jak může takový příklad zabezpečení domácí počítačové sítě vypadat.

Návrh proběhl na domácím routeru ASUS RT-N12D1, který se stará o provoz typické domácí sítě, jejíž lokalita je víceméně hned v centru města. Představeno bylo zabezpečení bezdrátového přenosu a Wi-Fi sítě se zaměřením na nejdůležitější nastavení včetně firewallu. Díky možnostem tohoto routeru byly také představeny funkcionality jako hostovaná síť nebo rodičovský režim, které zabezpečení sítě ještě více vyzdvihnou. Router nabídl jako bonus selekci síťových a diagnostických nástrojů, implementovaných přímo do ovládacího rozhraní routeru, které byly nápomocné při testovací části. V testovací části bylo provedeno několik specifických druhů testů včetně simulace reálného penetračního testu z vnějšího prostředí.

Tato práce je pouze zlomek toho, za čím se skrývá skutečná míra zabezpečení a internetové bezpečnosti. Je to neustálý boj mezi těmi, kteří vymýšlejí nové technologie a přicházejí s novými řešeními, a těmi, kteří pracují od prvního dne na jejich znehodnocení a prolomení. Člověk může mít síť zabezpečenou tou nejlepší technologií na trhu v nákladech, které si mnozí ani neumí představit, ani to však není stoprocentní jistotou. Odposlech, zachytávání dat v síti nebo kybernetické útoky se dějí pravidelně po celém světě, proto by nikdo neměl brát zabezpečení v síti na lehkou váhu. Je až děsivé vědět, jak jednoduchým způsobem může běžný uživatel na Internetu přijít svojí nedbalostí a neopatrností úplně o všechno.

7 Seznam použité literatury

[1] Co je to počítačová síť. Internet a jeho služby [online]. [cit. 2020-01-09]. Dostupné z: http://ijs.8u.cz/index.php/pocitacove-site/co-je-to-pocitacova-sit

[2] Počítačová síť (Computer network). Managementmania.com [online]. 2016 [cit. 2019-06-16]. Dostupné z: https://managementmania.com/cs/pocitacova-sit

[3] 802.11 – Wi-Fi wireless standards and facts. Air802.com [online]. [cit. 2020-08-07]. Dostupné z: https://www.air802.com/files/802-11-WiFi-Wireless-Standards-and-Facts.pdf

[4] LANs, WANs and Other Area Networks. Lifewire.com [online]. 2019 [cit. 2020-01-10]. Dostupné z: https://www.lifewire.com/lans-wans-and-other-area-networks-817376

[5] Aktivní síťové prvky (Active Networking Hardware). Managementmania.com [online]. 2017 [cit. 2020-01-30]. Dostupné z: https://managementmania.com/cs/aktivni-sitove-prvky

[6] Pasivní síťové prvky (Passive Networking Components). Managementmania.com [online]. 2018 [cit. 2020-01-30]. Dostupné z: https://managementmania.com/cs/pasivni-sitove-prvky

[7] Aktivní síťové prvky. Internet a jeho služby [online]. [cit. 2020-01-30]. Dostupné z: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=18&Itemid=123

[8] Cyber security basics. BlumShapiro.com [online]. 2019 [cit. 2020-07-21]. Dostupné z: https://www.blumshapiro.com/insights/cyber-security-basics-cyber-attacks-cyber-threats-ct-ma-ri/

[9] The Most Common Types Of Network Vulnerabilities. Purplesec.us [online]. 2020 [cit. 2020-07-21]. Dostupné z: https://purplesec.us/common-network-vulnerabilities/

[10] What is a Wireless router? Cisco.com [online]. [cit. 2020-08-03]. Dostupné z: https://www.cisco.com/c/en/us/products/wireless/wireless-router.html#~q-a

[11] How to choose the best Wi-Fi router. Windowscentral.com [online]. 2020 [cit. 2020-08-03]. Dostupné z: https://www.windowscentral.com/how-to-choose-best-router

[12] What is a Denial-of-Service (DoS) attack? Cloudflare.com [online]. [cit. 2020-07-21]. Dostupné z: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

[13] What is a Brute-Force attack? Lifewire.com [online]. 2020 [cit. 2020-08-07]. Dostupné z: https://www.lifewire.com/what-is-a-brute-force-attack-4684687

[14] What is a computer firewall | Hotspot shield. Hotspotshield.com [online]. [cit. 2020-08-07]. Dostupné z: https://www.hotspotshield.com/resources/what-is-a-computer-firewall/

[15] Personal Cloud Storage – MS OneDrive. Microsoft.com [online]. [cit. 2020-07-22]. Dostupné z: https://www.microsoft.com/en-ww/microsoft-365/onedrive/online-cloud-storage
[16] Rozdělení počítačových sítí. Internet a jeho služby [online]. [cit. 2020-01-30]. Dostupné z: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=5&Itemid=112
[17] RT-N12 D1| ASUS Global. Asus.com [online]. [cit. 2020-06-10]. Dostupné z: https://www.asus.com/Networking/RTN12_D1/overview/
[18] ASUSWRT | ČR. Asus.com [online]. [cit. 2020-06-10]. Dostupné z: https://www.asus.com/cz/ASUSWRT/
[19] What is Firmware? Lifewire.com [online]. 2020 [cit. 2020-07-10]. Dostupné z: https://www.lifewire.com/what-is-firmware-2625881
[20] FUP. DSL.cz [online]. [cit. 2020-07-15]. Dostupné z: https://www.dsl.cz/slovnik/fup
[21] Autentizace, ověření, identifikace. Managementmania.com [online]. 2018 [cit. 2020-07-16]. Dostupné z: https://managementmania.com/cs/autentizace-identifikace
[22] JOHNSON, Allan. 31 Days Before your CCNA Exam [eKniha]. Cisco Press, 2020 [cit. 2020-08-04]. ISBN 978-0-13-596408-8. Dostupné z: https://www.ciscopress.com/store
[23] MOHTADI, Hamed a Alireza RAHIMI. Advances in Computer Science: an International Journal: New attacks on Wi-Fi Protected Setup [eKniha]. 2015 [cit. 2020-08-06]. ISSN 2322-5157. Dostupné z: http://www.acsij.org/acsij/article/view/67
[24] 3 Types of backup. Iosafe.com [online]. [cit. 2020-11-01]. Dostupné z: https://iosafe.com/data-protection-topics/3-types-of-backup/
[25] About Firewalls. Indiana university: Knowledge base [online]. 2020 [cit. 2020-11-06]. Dostupné z: https://kb.iu.edu/d/aoru
[26] Types of Firewall Explained with Functions and Features. Computernetworkingnotes.com [online]. 2020 [cit. 2020-11-06]. Dostupné z: https://www.computernetworkingnotes.com/ccna-study-guide/types-of-firewall-explained-with-functions-and-features.html

8 Seznam zdrojů obrázků

Obrázek [2] Ilustrace PC sítě. Sobonpipe.com [online]. 2018 [cit. 2019-06-16]. Dostupné z: http://www.sobonpipe.com/what-are-computer-networks/

Obrázek [3] LAN & WAN Scheme. Wikipedia.org [online]. 2011 [cit. 2020-01-10]. Dostupné z: https://en.wikipedia.org/wiki/Wide_area_network

Obrázek [4] What is computer networking. Learncomputernetworking.blogspot.com [online]. [cit. 2020-01-30]. Dostupné z: https://learncomputernetworking.blogspot.com/p/network-cables.html

Obrázek [5] Fyzická a logická topologie. Cnt4all.com [online]. 2015 [cit. 2019-06-16]. Dostupné z: http://www.cnt4all.com/2016/10/09-data-link-layer-logical-vs-physical.html

Obrázek [6] & [7] NIC & UTP. Amazon.com [online]. 2019 [cit. 2020-01-10]. Dostupné z: https://www.amazon.com/

Obrázek [8] Scheme of token ring. Digital Guide [online]. 2018 [cit. 2020-01-10]. Dostupné z: https://www.ionos.co.uk/digitalguide/server/know-how/token-ring/

Obrázek [9] Netgear Nighthawk smart Wi-Fi router. Netgear.com [online]. [cit. 2020-08-07]. Dostupné z: https://www.netgear.com/home/products/networking/wifi-routers/R6700.aspx

Obrázek [12] Brute-force attack. Passcape.com [online]. [cit. 2020-08-07]. Dostupné z: https://www.passcape.com/bruteforce_attack

Obrázek [13] Firewalls, Firewalls, Firewalls. BangITsolutions.com [online]. 2018 [cit. 2020-07-17]. Dostupné z: https://bangitsolutions.com/firewall/

Obrázek [14] Diferenční – rozdílová záloha. Acronis.cz [online]. [cit. 2020-11-01]. Dostupné z: https://www.acronis.cz/kb/diferencialni-zaloha/

Obrázek [25] [Adaptive QoS] Introduction of Traffic Monitor. ASUS Support [online]. 2018 [cit. 2020-07-14]. Dostupné z: https://www.asus.com/support/FAQ/114483/

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor:	**Viktor Míčka**
Studium:	I1700112
Studijní program:	B1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název bakalářské práce:	**Zabezpečení malé domácí sítě**
Název bakalářské práce AJ:	Home network security

Cíl, metody, literatura, předpoklady:

Cíl práce: Prozkoumat možnosti zabezpečení domácí sítě a navrhnout zabezpečení pro konkrétní síť.

Osnova:

- Úvod
- Počítačová síť a její prvky
- Zabezpečení
- Návrh zabezpečení
- Testování a výsledky
- Závěr

KLEMENT, Milan. *Úvod do problematiky počítačových sítí. Olomouc: Univerzita Palackého v Olomouci, 2015, 64 s. Studijní opora. ISBN 978-80-244-4570-0.*

RAMO, Joshua Cooper. Sedmý smysl: návod na přežití v době sítí. Přeložil Mojmír MOLÁČEK. Brno: BizBooks, 2017, 320 s. ISBN 978-80-265-0674-4.

CARROLL, Brandon. Bezdrátové sítě Cisco: autorizovaný výukový průvodce : [samostudium]. Brno: Computer Press, 2011, 478 s. ISBN 978-80-251-2884-8.

DOLNÍK, Bystrík. Ochrana počítačových sietí. Košice: Technická univerzita v Košiciach, 2012, 1 CD-ROM (83 s.). ISBN 978-80-553-1075-6.

Garantující pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	Ing. Pavel Blažek, Ph.D.
Datum zadání závěrečné práce:	21.10.2018