Bezpečnost bezdrátových sítí

Bc. Jakub Karlík

Diplomová práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jakub Karlík**
Osobní číslo:	**A14430**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnost bezdrátových sítí**
Téma anglicky:	**Wireless Network Security**

Zásady pro vypracování:

1. **Popište bezdrátovou technologii standardu IEEE 802.11.**
2. **Uveďte přehled modifikací 802.11 s ohledem na parametry (rychlost, modulace, frekvence).**
3. **Zpracujte přehled způsobů zabezpečení bezdrátové sítě IEEE 802.11.**
4. **Sestavte a vyhodnoťte anketu založenou na zjištění povědomí uživatelů o bezpečnosti bezdrátových sítí.**
5. **Proveďte prolomení zabezpečení WEP a porovnejte časovou náročnost prolomení hesla.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **PETROWSKI, Thorsten. Bezpečí na internetu: pro všechny. Vyd. 1. Liberec: Dialog, 2014, 243 s. Tajemství (Dialog). ISBN 978-80-7424-066-9.**
2. **OREBAUGH, Angela. Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí. Vyd. 1. Brno: Computer Press, 2008, 444 s. ISBN 978-80-251-2048-4.**
3. **KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.**
4. **HOLT, Alan a Chi-Yu HUANG. 802.11 wireless networks: security and analysis. New York: Springer, c2010, xxi, 212 p. ISBN 978-1-84996-274-2.**
5. **HAINES, Brad a Tim KRAMER. Seven deadliest wireless technologies attacks. Boston: Syngress/Elsevier, c2010, xvi, 122 p. ISBN 978-1-59749-541-7.**
6. **LUKÁŠ, Luděk a kol. Bezpečnostní technologie, systémy a management V. 1. vyd. Zlín: VeRBuM, 2015, 368 s. ISBN 978-80-87500-67-5.**

Vedoucí diplomové práce: **Ing. Jiří Korbel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **5. února 2016**

Termín odevzdání diplomové práce: **16. května 2016**

Ve Zlíně dne 5. února 2016

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 1.5.2016

.....
podpis diplomanta

ABSTRAKT

Předkládaná diplomová práce je zaměřena na bezpečnost bezdrátových sítí, konkrétně na sítě standardu IEEE 802.11. Pro lepší pochopení dané problematiky jsou zde objasněny základní pojmy a princip činnosti. Dále se práce věnuje a popisuje jednotlivé modifikace standardu IEEE 802.11 se zaměřením na rychlost, modulace a využívané frekvence. V neposlední řadě práce obsahuje přehled způsobů zabezpečení. Praktická část se zabývá vytvořením ankety, založené na zjištění povědomí uživatelů o bezpečnosti bezdrátových sítí a následně jejím vyhodnocením. Závěr praktické části je věnován praktické ukázce prolomení zabezpečení WEP, zároveň s porovnáním časové náročnosti na získání hesla.

Klíčová slova: Wi-Fi, IEEE 802.11, bezdrátová síť, zabezpečení.

ABSTRACT

This diploma thesis is focused on the security of wireless networks, specifically networks IEEE 802.11. For a better understanding of the issues are clarified the basic terms and principles of operation. Further, the thesis describes the modification of the standard IEEE 802.11 focusing on speed, modulations and used frequency. Furthermore, the thesis contains overview of kinds of the security. The practical part deals with the creation of the survey, based on finding users' awareness of wireless security and then its evaluation. Conclusion of the practical part is devoted to practical demonstration of breaking WEP security, and also comparing time required to obtain a password.

Keywords: Wi-Fi, IEEE 802.11, wireless network, security.

Chtěl bych poděkovat všem osobám, které při mně po celou dobu stály a pomáhaly mi s vypracováním diplomové práce. Především to byl vedoucí mé diplomové práce pan Ing. Jiří Korbel, Ph.D., který mi byl po celou dobu oporou a veškeré mé náměty se mnou konzultoval. Zároveň bych mu chtěl také poděkovat za jeho odborné rady a připomínky v průběhu psaní této diplomové práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Bezdrátové Wi-Fi sítě se staly téměř neoddělitelnou součástí života. Obklopují společnost téměř na každém rohu a jejich počet neustále narůstá. Spousta lidí vlastní nejedno zařízení, které umožňuje připojení k bezdrátové síti pomocí Wi-Fi. I přes spoustu bezesporných výhod je nutné se na tuto technologii zaměřit i z pohledu bezpečnosti, jelikož pomocí těchto sítí se šíří mnohdy obrovské množství informací a dat, které mohou být následně lehce zneužitelné. Z toho důvodu je potřeba znát alespoň základní metody, jak tyto sítě zabezpečit a vyhnout se tak možným rizikům.

Nejvyšší hrozby číhají na veřejných sítích, na které se může připojit téměř kdokoliv. Problém je zde ten, že kdykoliv může být připojen i případný útočník. Tento typ sítí je i přesto velice oblíbený, jelikož jeho bezplatné užívání je poskytováno mnoha společnostmi, mezi které patří především kavárny, obchodní centra či restaurace. Nejlepší je se však takovým sítím vyvarovat a používat výhradně domácí sítě, které jsou většinou lépe zabezpečeny, a nemůže se k nim připojit každý.

V diplomové práci jsou uvedeny základní informace o standardu IEEE 802.11, ze kterého vychází samotná činnost a princip fungování Wi-Fi. V práci jsou také popsány jednotlivé modifikace standardu IEEE 802.11 se zaměřením na jejich přenosové rychlosti, modulace a využívané frekvence. Důležitou částí je také popis jednotlivých metod zabezpečení. Znalost těchto metod by měla být samozřejmostí pro ty, kteří si budují vlastní domácí Wi-Fi síť.

V praktické části je vytvořena anketa, která se zaměřuje na zjištění povědomí uživatelů o bezpečnosti bezdrátových Wi-Fi sítí. Tato anketa je následně vyhodnocena a výsledky zobrazeny ve formě grafů. V další části je provedena také praktická realizace útoku na Wi-Fi síť se zabezpečením WEP. Hlavním cílem je získání hesla, které slouží pro přístup do sítě. Zhodnocena je také časová náročnost na získání hesla.

Cílem diplomové práce je poukázat na zranitelnost těchto sítí a popsat metody, které slouží k jejímu zabezpečení. Na základě výsledků ankety tak bude možné zhodnotit chování uživatelů na bezdrátových Wi-Fi sítích a jejich znalosti týkající se jednotlivých metod zabezpečení. Útokem na vytvořenou Wi-Fi síť je poukázáno na její zranitelnost.

I. TEORETICKÁ ČÁST

1 HISTORIE

Využití bezdrátových technologií, které primárně slouží k datovým přenosům, nemá až tak dlouhou historii, jak by se mohlo na první pohled zdát. Bezdrátový přenos byl dlouhou dobu používán pouze jako nouzové řešení a to především tam, kde nebylo možné vybudovat běžnou kabelovou infrastrukturu. Například v rozsáhlých areálech a budovách nebo v historických objektech. Postupem času si bezdrátový přenos našel i další uplatnění. Tím byly bezdrátové pokladny, které se využívaly především v nákupních centrech, kdy zákazníci mohli v jednotlivých obchodech platit kartami. Hlavním problémem byly neexistující standardy. Tento problém vedl k tomu, že vznikalo velké množství protokolů, které byly velmi pomalé, a vznikala zařízení, která byla drahá a vzájemně nekompatibilní. Bezpečnost těchto přenosů vyplývala ze znalosti použitých protokolů a vzhledem k tomu, že většina společností si vytvořila vlastní protokoly, tak bezpečnost byla zajištěna pouze přísným utajením použitého řešení. [2]

Důležitý milník nastal v roce 1985, kdy Federal Communications Commission uvolnila frekvenční pásmo pro bezdrátové sítě LAN, určené pro průmyslové, vědecké a lékařské účely. V roce 1990 se objevila technologie, která využívala frekvenční pásmo 900 MHz a dosahovala maximální rychlosti až 1 Mb/s. Běžné kabelové připojení v té době dosahovalo rychlosti až 10 Mb/s. Vzhledem k tomu, že v 90. letech neustále narůstaly požadavky uživatelů na jejich mobilitu a docházelo k rozšiřování mobilních sítí, které následně využívaly datové služby UMTS a GPRS, bylo jasné, že pro rozšíření a plnohodnotné fungování musejí vzniknout nějaké normy a standardy. Proto vznikl v roce 1990 projekt IEEE 802.11, který byl schválen až v roce 1997. [1, 3]

Původní specifikace 802.11 podporovala rychlost 1 až 2 Mb/s. Neustále však docházelo k pozvolnému vylepšování a to po všech směrech. Hlavní změny se objevily o 2 roky později v roce 1999, kdy byly představeny dva doplňky 802.11a (až 54 Mb/s) a 802.11b (až 11Mb/s), které podporovaly vyšší rychlost. Také došlo k představení šifrování WEP, které mělo zajistit bezpečnou komunikaci. V roce 1999 vznikla také aliance WECA, která se od roku 2002 nazývá Wi-Fi Alliance, která v současné době zajišťuje testování výrobků různých společností, založených na standardu 802.11 a zajišťuje tak vzájemnou kompatibilitu mezi jednotlivými zařízeními. V následujících letech docházelo k neustálému zlepšování a vzniku nových standardů, modulací a šifrovacích metod. [1, 2]

2 BEZDRÁTOVÁ SÍŤ WI-FI

Základní příčinou vzniku bezdrátových sítí byla snaha rozšířit technologii LAN o možnost přenosu dat prostřednictvím rádiových vln tzv. Wireless LAN. To se povedlo a dalo by se říci, že předčilo původní očekávání. Wireless LAN je standard 802.11, který vznikl díky organizaci IEEE (Institut pro elektrotechnické a elektronické inženýry). Ta vydává závazné standardy, které říkají, jak mezi sebou jednotlivá zařízení komunikují. Samotný název Wi-Fi, který je dnes všeobecně znám, je využitím několika standardů, které jsou součástí obecného standardu 802.11. Za tímto názvem také stojí organizace Wi-Fi Alliance, která se stará o vzájemnou kompatibilitu jednotlivých výrobků, ale o ní více v podkapitole Wi-Fi Alliance. [4]

Jak je již výše zmíněno, tak tato bezdrátová technologie předčila veškerá původní očekávání a během pár let tak došlo k masovému rozšíření ve společnosti. V současné době by se dalo říci, že Wi-Fi je v moderním světě součástí téměř každého člověka. Ve větších městech se nachází téměř na každém rohu a to díky různým společnostem (restaurace, kavárny, instituce…), které nabízí ve svých prostorech bezplatné připojení. Stačí mít mobilní telefon, notebook nebo jakékoliv jiné zařízení, využívající bezdrátovou Wi-Fi technologii, a během pár chvil je možné naleznout a připojit se na bezplatnou Wi-Fi síť. Wi-Fi je využívána milióny lidí po celém světě a neslouží pouze pro připojení k internetu bez kabelu, ale i k vytváření bezdrátových sítí, jak v domácnostech, tak i na pracovištích. Avšak přes bezesporný počet těchto výhod, má Wi-Fi i svá úskalí. Jedním z těchto úskalí je bezpečnost těchto sítí. Mnoho lidí si ani neuvědomuje, do jaké sítě se připojují a jsou hlavně rádi, že mají internet zdarma. Avšak ne pokaždé musí být toto připojení bezpečné a vzhledem k tomu, že Wi-Fi se šíří pomocí elektromagnetických vln, tak je velice obtížné zjistit, kdo se na síti pohybuje. [4]

2.1 Wi-Fi Alliance

Na počátku vzniku standardu IEEE 802.11 jednotlivé výrobky mnohdy měly problémy se vzájemnou komunikací a spoluprací s výrobky jiných značek. To bylo především dáno tím, že neexistovaly žádné všeobecné postupy, jak testovat tato zařízení a zjistit tak, jestli vyhovuje veškerým standardům. Proto v roce 1999 vznikla organizace WECA, která měla za úkol zajistit řízení této bezdrátové technologie bez ohledu na výrobce. WECA začala tuto technologii označovat jako Wi-Fi, což je název, který je dnes velmi široce užíván v kavár-

nách, restauracích a je velice dobře znám. V roce 2002 se WECA přejmenovala na Wi-Fi Alliance. [4]

Wi-Fi Alliance je nezisková organizace, která však není zcela neutrální, jelikož mezi členy této aliance jsou jednotliví výrobci zařízení standardu IEEE 802.11. V současné době sdružuje více než 600 společností. Hlavním důvodem vzniku této aliance je zajištění kompatibility jednotlivých výrobků a to bez ohledu na výrobce, avšak podílí se i na zavádění nových doplňků a bezpečnostních mechanismů. Wi-Fi Alliance vytvořila vlastní testovací laboratoře, kde dochází k testování těchto výrobků. Od roku 2000 začala produkty, které prošly testováním a splňují veškerá kritéria, certifikovat. V současné době došlo k udělení certifikátu u více než 25 000 výrobků. Dnes zakoupená zařízení nesoucí certifikát Wi-Fi, znamenají jistotu, že budou fungovat s jakýmkoliv jiným zařízením, které vlastní také tento certifikát. [4, 5]

Obr. 1. Certifikát Wi-Fi [6]

2.2 Základní komponenty bezdrátové sítě

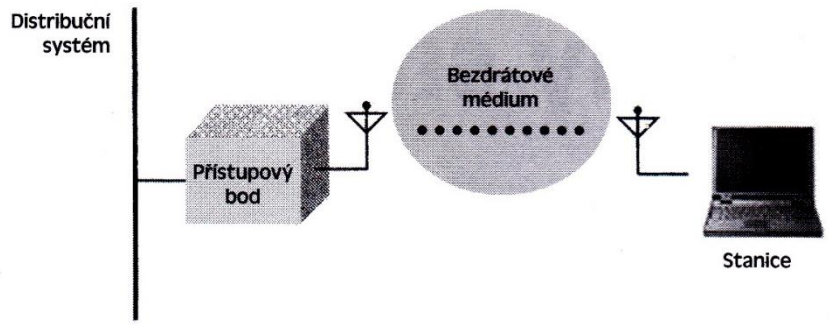
Bezdrátová Wi-Fi síť, která se dnes nachází ve většině domácností, se skládá ze čtyř hlavních komponentů:

Distribuční systém – v případě využití více přístupových bodů, které spolu tvoří jakoukoliv síť, musí být zajištěna jejich vzájemná komunikace. K tomu slouží právě distribuční systém, který zajišťuje správné směrování datového toku. Distribučním médiem je páteřní síť, která se využívá právě pro přenos dat mezi jednotlivými přístupovými body. Jako nejčastější volba páteřní sítě je využíván Ethernet. [7]

Přístupový bod – jedná se o zařízení, sloužící nejčastěji k převodu z kabelové sítě na síť bezdrátovou, a nachází se v téměř každé domácnosti, využívající Wi-Fi technologii. K tomuto zařízení se následně připojují jednotlivé přístroje. Přístupový bod neboli access point neslouží pouze k převodu signálů, ale zajišťuje i spoustu dalších funkcí. Mezi hlavní funkce patří ty, které zajišťují bezpečnost domácí sítě. [7]

Bezdrátový přenos – ačkoliv nejčastěji používanou přenosovou cestou je kabel, po kterém proudí veškerá data, u standardu IEEE 802.11 tento přenos zajišťují rádiové vlny, které přemisťují data od stanice k přístupovému bodu a k dalším zařízením. Tyto rádiové vlny využívají nejčastěji frekvenční pásma 2,4 GHz a 5 GHz, ale o těch více v kapitole Využívané frekvence. [7]

Stanice – hlavním účelem bezdrátových sítí je přenos dat mezi různými stanicemi. Proto jsou hlavní součástí celého systému a bez nich by bezdrátový přenos neměl ani žádný smysl. Těmito stanicemi se rozumí jakékoliv zařízení např.: počítač, notebook, mobilní telefon atd. [7]



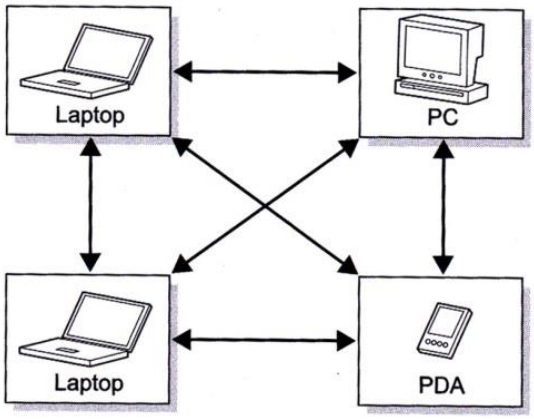
Obr. 2. Komponenty bezdrátové sítě [7]

2.3 Topologie bezdrátových sítí

Existuje několik způsobů, jak spolu mohou jednotlivá zařízení komunikovat při využití WLAN. Každý síťový adaptér obsahuje přijímač, vysílač a anténu, které slouží k bezdrátovému přenosu dat. Zařízení spolu mohou komunikovat přes přístupový bod, který vytváří síť a zařízení jsou do ní připojené nebo pomocí přímého spojení.

2.3.1 Síť Ad-Hoc

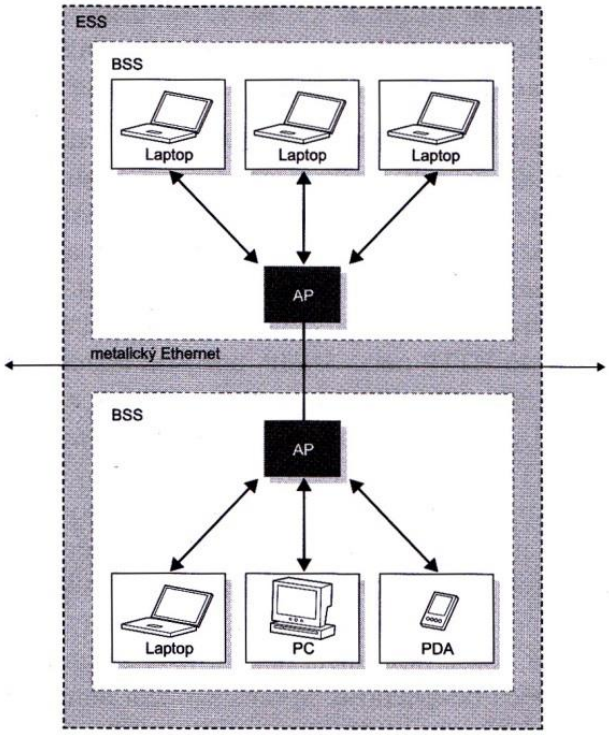
Ad-Hoc sítě fungují v režimu Independent Basic Service Set a často jsou nazývány jako nezávislé. V této síti spolu zařízení neboli stanice komunikují přímo mezi sebou a nepotřebují žádného prostředníka např.: přístupový bod. Tato metoda je nejjednodušší variantou sítě, která je závislá především na vzdálenosti jednotlivých zařízení, jelikož musejí být ve vzájemném rádiovém dosahu. Proto je vhodná především pro dočasné zasíťování dvou nebo více stanic. Využívá se hlavně pro krátkodobé spojení za účelem přenosu dat a vzájemné komunikace. Nejčastěji je tento typ tvořen mezi zařízeními, které jsou spolu v místnosti. [2, 8]



Obr. 3. Ad-Hoc [2]

2.3.2 Síť infrastruktura

Oproti sítím Ad-Hoc zde neprobíhá přímá komunikace mezi stanicemi, ale dochází k využití prostředníka a to přístupového bodu. Infrastruktura obsahuje alespoň jeden tento přístupový bod, který vytváří bezdrátovou buňku. K té se připojují jednotlivá zařízení, ta již nekomunikují vzájemně, ale právě přes tento uzel. Přístupový bod může být připojen k metalické infrastruktuře např.: pomocí ethernetu a zajistit tak přístup k Internetu pro veškeré stanice. [2]



Obr. 4. Infrastruktura [2]

Pokud dochází k využití jednoho přístupového bodu, ke kterému se připojují bezdrátové stanice, tak se jedná o Basic Service Set. Avšak pokud je využíváno více těchto bezdrátových stanic a tedy i více BSS, které jsou vzájemně propojeny nějakým distribučním systémem, jedná se o Extended Service Set, který nejčastěji slouží pro rozšíření bezdrátové sítě na velké ploše. [2, 8]

2.3.3 Přemostění sítí

Vzhledem k tomu, že přístupový bod dokáže pracovat v různých režimech, tak dochází k možnostem i jeho dalšího využití. K těmto přístupovým bodům se nemusejí připojovat pouze stanice jako notebooky, telefony atd., ale i další přístupové body, které následně tvoří tzv. přemostění. Níže jsou popsány ty nejznámější metody propojení.

Point to Point Bridge

Dochází k bezdrátovému propojení dvou sítí. Propojení se děje pomocí konfigurace MAC adres na obou spárovaných přístupových bodech. Tato metoda je odolná proti snaze proniknout do tohoto spoje, a to právě díky konfiguraci MAC adres. [19]

Point to Multipoint Bridge

Jedná se o obdobu Point to Point, avšak s tím rozdílem, že dochází k propojení více než dvou sítí. Problémy zde občas mohou nastat, pokud dojde k propojení jednotlivých zařízení, která nepocházejí od stejného výrobce.

Repeater

Tento režim se využívá v případě, kdy je zapotřebí rozšířit signál bezdrátové sítě do dalších prostorů a zlepšit tak celkové pokrytí. Avšak ne každý přístupový bod nabízí tuto funkci repeater a proto je vhodné před koupí si zjistit veškeré informace.

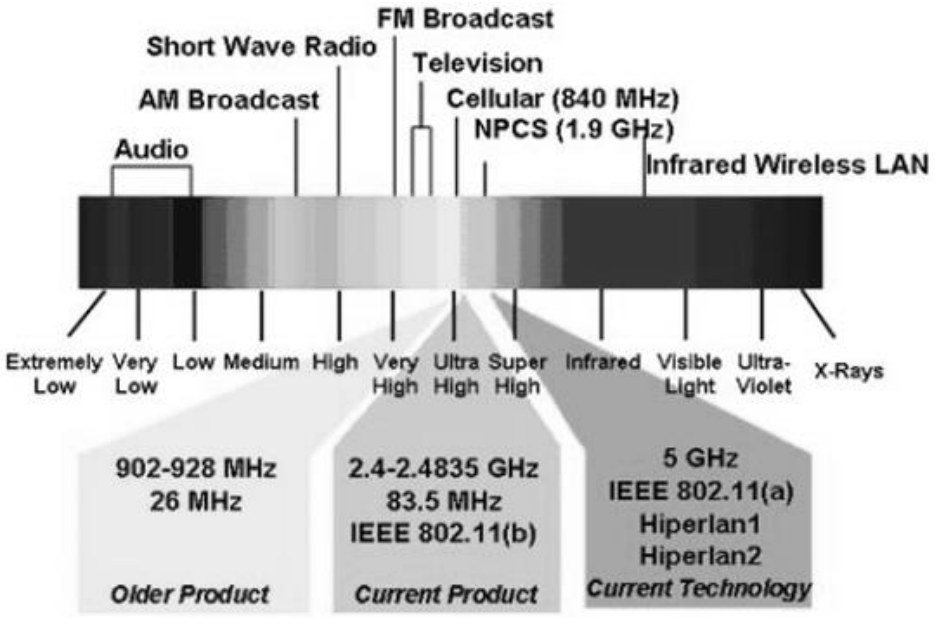
2.4 Využívané frekvence

Každý bezdrátový signál, který je vysílán se nazývá rádiové vysílání. Přístroje, které zajišťují příjem, a vysílání se staly součástí našeho každodenního života. Jedná se o rádia, mobilní telefony a spousty jiných zařízení. Avšak rádiové spektrum nabízí omezený počet frekvencí a následně dochází ke kolizím ve vysílání mezi jednotlivými přístroji. Proto je zapotřebí těmto kolizím předcházet, a to se děje díky snaze regulace a vymezení pásem pro určité přístroje. Samotnou regulaci zajišťuje vláda a mezinárodní dohody. [4]

Standard IEEE 802.11 využívá spektra, která jsou vyhrazená pro nelicencované a tedy i pro soukromé využití. V Evropě, USA a jiných zemích se používají odlišná frekvenční pásma, avšak v České republice to jsou následující pásma:

- 2400 – 2483,5 MHz;
- 5,15 – 5,35 GHz (pouze uvnitř budov);
- 5,470 – 5,725 GHz;
- 5,725 – 5,845 GHz (pouze zařízení s malým výkonem). [9]

I přes snahu regulovat tyto pásma tak, aby nedocházelo ke kolizím, tak bohužel je na světě tolik přístrojů, že zkrátka nelze zajistit, aby nedocházelo k vzájemnému rušení. V těchto pásmech pracuje např.: bluetooth, které se také využívá pro bezdrátové propojení a přenos dat. Zajímavostí je, že v pásmu 2,4 GHz pracuje i mikrovlnná trouba, která však pracuje cca s tisíckrát vyšším výkonem než WLAN. [8]



Obr. 5. Frekvenční spektrum [10]

2.4.1 Kanály

Využívaná spektra jsou rozdělena do jednotlivých kanálů, po kterých jednotlivá zařízení vzájemně komunikují. V pásmu 2,4 GHz je k dispozici 13 kanálů, navzájem se překrývajících, kde celková šířka má velikost 82 MHz. Při využití šířky pásma 20 MHz, ve výsledku vzniknou pouze 3 kanály, které se nepřekrývají. Jedná se o kanály 1, 6 a 11. V případě, využití šířky 40 MHz, vzniknou pouze 2 kanály, které se navzájem nebudou rušit, a to 1 a 9. Nevýhodou je velké rušení i od ostatních zařízení, jako jsou bluetooth nebo velký problém nastává ve městech, kde se v panelových domech nachází velké množství přístupových bodů a je mnohdy nemožné najít volný kanál, a předejít tak rušení. [7, 11]

Tab. 1. Kanály v pásmu 2,4 GHz [11]

Kanál	1	2	3	4	5	6	7	8	9	10	11	12	13
Start [MHz]	2401	2404	2411	2416	2421	2426	2431	2436	2441	2446	2451	2456	2461
Finish [MHz]	2423	2428	2433	2438	2443	2448	2453	2458	2463	2468	2473	2478	2483

Oproti pásmu 2,4 GHz má pásmo 5GHz frekvenční rozsah velikosti 520 MHz. Tím vzniká 19 nepřekrývajících se kanálů se šířkou 20 MHz. Další výhodou pásma 5 GHz je menší rušení a tím pádem vyšší rychlost přenosu dat. Bohužel toto pásmo je více náchylné na překážky a proto má i menší dosah. [11]

Tab. 2. Kanály v pásmu 5 GHz [11]

Kanál	**36**	**40**	**44**	**48**	**52**	**56**	**60**	**64**	**100**	**104**	**108**	**112**	**116**
Frekvence [MHz]	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580
Kanál	**120**	**124**	**128**	**132**	**136**	**140**							
Frekvence [MHz]	5600	5620	5640	5660	5680	5700							

3 STANDARD IEEE 802.11

Dnes by Wi-Fi nemohla fungovat bez dodržování určitých podmínek a pravidel. Dříve, kdy neexistovaly žádné standardy, a bezdrátový přenos byl zajištěn jen díky vlastní konfiguraci zařízení, bylo nevýhodou, že tato zařízení nebyla vzájemně kompatibilní se systémy od jiných výrobců a přenosy byly velmi pomalé. Proto v roce 1997 byla schválena první specifikace IEEE 802.11, která využívala modulace FHSS a DSSS, kde rychlost dosahovala 1 – 2 Mb/s. Od té doby dochází k neustálému rozšiřování tohoto standardu 802.11 pomocí doplňků, kde je kladen důraz především na rychlost a zabezpečení. [2]

Tab. 3. Standard IEEE 802.11

Standard	Rok vydání	Využívané pásmo [GHz]	Maximální rychlost [Mb/s]	Modulace
Původní IEEE 802.11	1997	2,4	1-2	FHSS/DSSS

Standard tedy říká, jak zařízení mezi sebou využívají volná spektra a jakým způsobem spolu komunikují. Níže v jednotlivých podkapitolách jsou popsány nejdůležitější doplňky.

802.11a

Tento doplněk byl schválen v roce 1999 a vyčnívá tím, že pracuje v pásmu 5 GHz. Tímto je zajištěno především menší rušení od okolních zdrojů, avšak nevýhodou je jeho vyšší náchylnost přechodu přes překážky. Doplněk není také zpětně kompatibilní s doplňkem 802.11b, ale toho se dá i v některých případech využít, jelikož se vzájemně neruší, a tak je možné provozovat tyto dva systémy současně. Rychlost zde může dosahovat až 54 Mb/s a je zde využívána modulace OFDM. [2, 4]

Tab. 4. Standard IEEE 802.11a

Standard	Rok vydání	Využívané pásmo [GHz]	Maximální rychlost [Mb/s]	Modulace
802.11a	1999	5	54	OFDM

802.11b

Před pár lety se jednalo o nejrozšířenější doplněk standardu 802.11. Ale vzhledem k jeho maximální dosažitelné rychlosti až 11 Mb/s, dnes nedostačuje a bývá nahrazován především novějšími doplňky jako 802.11g, n a ac, které jsou mnohem rychlejší. Nevýhodou je také velké rušení, které je v pásmu 2,4 GHz a také nižší rychlost, vznikající při slabém signálu. Doplněk vznikl taktéž v roce 1999 a je zde využita modulace DSSS. [2, 4]

Tab. 5. Standard IEEE 802.11b

Standard	Rok vydání	Využívané pásmo [GHz]	Maximální rychlost [Mb/s]	Modulace
802.11b	1999	2,4	11	DSSS

802.11c

Tento doplněk se věnuje přemosťování bezdrátových zařízení tzv. bridge. Přidává požadavky na přemosťování MAC, která je součástí linkové vrstvy. [12]

802.11d

Doplněk 802.11d bývá nazýván také jako harmonizační, jelikož zde dochází k přizpůsobení požadavků v různých zemích, kde nejsou povolena zařízení využívající některé doplňky 802.11. Dochází zde ke změnám ve využívaných frekvencích, výkonech a propustnosti signálu. [12]

802.11e

Zaměřuje se na zlepšení MAC, kde rozšiřuje podporu a kvalitu služeb (QoS). Využívá se pro aplikace, které jsou citlivé na zpoždění jako např.: videohovory a přenosy videa a hlasu. [12]

802.11g

Tento doplněk je obdobou doplňku 802.11a, avšak s tím rozdílem, že pracuje v pásmu 2,4 GHz a je zpětně kompatibilní s doplňkem 802.11b. 802.11g je postaven na podobném základě jako 802.11b, ale došlo ke změně modulace z DSSS na OFDM. Vznikl v roce 2003 a jeho maximální rychlost je stejná jako u 802.11a, tedy až 54 Mb/s. [4]

Tab. 6. Standard IEEE 802.11g

Standard	Rok vydání	Využívané pásmo [GHz]	Maximální rychlost [Mb/s]	Modulace
802.11g	2003	2,4	54	OFDM

802.11h

Doplněk zlepšuje řízení vysílacího výkonu, výběru kanálu a doplňuje 802.11a tak, aby byl navržen s ohledem k evropským podmínkám a aby bylo možné jeho využití jak pro vnitřní, tak i pro vnější komunikaci v pásmu 5 GHz. [12]

802.11i

Zabývá se zlepšením zabezpečení IEEE 802.11. Zavádí šifrování AES, přístup pomocí PSK atd. [2]

802.11n

Jedná se o doplněk, v dnešní době hojně využívaný, především z důvodu vysoké rychlosti, a to až 600 Mb/s. To je dáno díky využití technologie MIMO (Multiple Input Multiple Output), která používá více vysílacích a přijímacích antén a také kanálem se šířkou 40 MHz. 802.11n využívá ke své činnosti obě volná pásma 2,4 GHz a 5 GHz. [12]

Tab. 7. Standard IEEE 802.11n

Standard	Rok vydání	Využívané pásmo [GHz]	Maximální rychlost [Mb/s]	Modulace
802.11n	2009	2,4/5	600	OFDM (MIMO)

802.11ac

Jedná se o první doplněk, který nabízí rychlost přesahující 1 Gb/s. Byl schválen v roce 2013 a většina nových produktů již tento doplněk obsahuje. Hlavní snahou zde bylo dosáhnout co nejvyšší rychlosti, což se povedlo díky šířce kanálu, která je 80 MHz nebo 160 MHz, práci v pásmu 5 GHz a také pomocí modulace OFDM. Je zde využita i technologie MIMO, která obsahuje až 8 prostorových kanálů. [13]

Tab. 8. Standard IEEE 802.11ac

Standard	Rok vydání	Využívané pásmo [GHz]	Maximální rychlost [Mb/s]	Modulace
802.11ac	2013	5	1350	OFDM (MIMO)

4 POKRYTÍ, PŘENOSOVÁ RYCHLOST A MODULACE

Při budování domácí nebo rozsáhlejší podnikové sítě existuje obrovské množství metod a způsobů, jak tuto síť vytvořit. Před začátkem je dobré si uvědomit, o jakou síť se bude jednat, jak bude rozsáhlá, jaké rychlosti se zde bude dosahovat a na tomto základě je vhodné volit další možnosti, jako je volba vhodného standardu a s ním spojených spousta dalších parametrů. Tato kapitola je věnována možnostem pokrytí a způsobům, jak zajistit správný dosah přenášeného signálu, dále je zde podkapitola, zabývající se přenosovými rychlostmi, a to především z pohledu různých vlivů, ovlivňujících rychlost. Závěrem jsou zde popsány jednotlivé typy modulací, které jsou využívány jednotlivými standardy.

4.1 Pokrytí

Téměř v každé domácnosti je problém s tím, že v různých místnostech je různý dosah signálu. Může se stát, že signál bude slabý nebo dokonce žádný. Existují ale zařízení a metody, které pomohou tento problém vyřešit.

Jednou z těchto možností je využití Wi-Fi repeateru. Jedná se o jednoduché zařízení, které je schopno přijmout signál a následně ho vyslat dále. Repeater neboli opakovač se umisťuje tam, kde je ještě nějaký signál, repeater ho přijme a zesílený ho pošle zase dál. Jedná se o poměrně levné a jednoduché zařízení, které v současné době vyniká zejména svou snadnou instalací. Avšak použití tohoto řešení s sebou nese jisté nevýhody. Jednou z nich je, že se výsledná rychlost sníží na polovinu. To je dáno tím, že většina repeaterů využívá pouze jedno rádiové rozhraní, které nejprve signál příjme a následně ho přes to samé rozhraní odešle. Existují však repeatery, které obsahují i více rádiových rozhraní, ale jejich cena je vyšší, avšak za tento příplatek lze získat zařízení, se kterým zůstane rychlost neměnná. Další nevýhodou je, že zařízení se musí umístit tam, kde je ještě dostačující signál, v opačném případě by se výsledná rychlost ještě snížila.

Obdobou repeateru je systém WDS. Dochází zde k využití dvou Wi-Fi routerů, které musejí tuto funkci podporovat. Routery se mezi sebou musejí vzájemně nakonfigurovat. Tato metoda je o něco lepší, jelikož WDS protokol zajišťuje, že veškeré počítače a zařízení na něj připojeny vystupují pod svou vlastní MAC adresou a nedochází tak ke zbytečným kolizím (problém některých repeaterů). Tato metoda ale neřeší veškeré problémy repeateru, jelikož i zde musíme druhý router mít v dosahu signálu vysílaného z routeru prvního a i

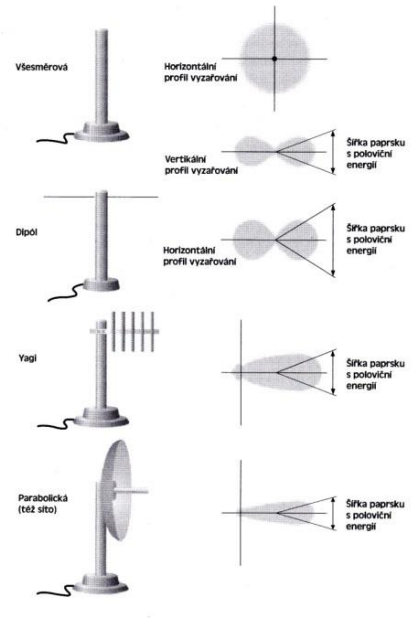
zde dochází ke snížení rychlosti za druhým routerem. Tedy pouze v případě, pokud router neobsahuje více rádiových rozhraní.

Další metodou, jak rozšířit pokrytí sítě je využití tzv. plnohodnotného Wi-Fi systému. Tento způsob je zřejmě jednou z nejlepších možností, jelikož zde nedochází ke snížení rychlosti a lze ho využít na delší vzdálenosti. Podobně jako u WDS systému jsou potřeba dva Wi-Fi routery, které jsou ale vzájemně propojeny kabelem. Je nutné na druhém Wi-Fi routeru nastavit jiný kanál, aby nedocházelo k rušení. Mezi hlavní nevýhodu zde patří nutnost použití kabelu, který propojuje jednotlivé Wi-Fi routery. Avšak ne vždy se nabízí možnost v daném prostředí tento kabel využít.

V současné době existuje mnoho podobných produktů a metod pro rozšíření pokrytí. Je nutné si před koupí nějakého zařízení uvědomit veškeré funkce, které budou po systému vyžadovány.

4.1.1 Antény

Šíření bezdrátového signálu by se nemohlo obejít bez antén, které slouží pro příjem a vysílání signálu. Pro pokrytí většiny domácností a uvnitř budov stačí využít antény, které jsou součástí přístupových bodů tzv. pendreky. Pokud bude signál nedostačující, tak lze využít některou z výše popsaných metod pro rozšíření pokrytí. I když je Wi-Fi primárně určena právě pro výstavbu sítě uvnitř budov, tak stále častěji dochází k bezdrátovému propojení budov i na větší vzdálenosti nebo dokonce k distribuci internetového připojení. V takových případech je jasné, že běžné antény, dodávané výrobcem jsou nedostačující a proto je potřeba využít externí antény. [7, 19]



Obr. 6. Typy antén [7]

Všesměrové antény

Nejčastěji používaným typem jsou všesměrové antény. Ty šíří signál do všech stran, jejich úhel vykrytí je tedy 360°. Nalézají se ve většině domácností, jelikož tento typ je běžnou součástí přístupových bodů. Na základě její vyřazovací charakteristiky je vhodné její umístění do středu bytu, abychom zajistili co největší a rovnoměrné pokrytí. [2, 7]

Sektorové antény

Dalším typem jsou antény sektorové, které najdou své využití tam, kde je potřeba zajistit pokrytí pouze v určitých místech, a tím i zabránit vysílání signálu do jiných částí. Antény jsou tedy vyráběny s vyřazovací charakteristikou pod určitými úhly, nejčastěji však pod úhlem 90°. [7]

Směrové antény

Dalo by se říci, že směrové antény jsou podkapitolou antén sektorových, jelikož zde dochází k šíření signálu také pod určitým úhlem. Tento úhel je většinou kolem 30°. Na základě tohoto úhlu je jasné, že tento typ antén neslouží většinou k pokrytí nějakého většího počtu uživatelů. Signál je soustředěn do jednoho bodu a je schopný dozářit na větší vzdálenost. Využívají se zde antény parabolické nebo typu Yagi. [7]

4.2 Přenosová rychlost

Přenosová rychlost je hlavním parametrem a není se také čemu divit. Avšak většina si určitě všimla, že výrobci udávané teoretické rychlosti jsou s praxí úplně někde jinde. Všeobecně je rozdíl mezi udávanou teoretickou maximální rychlostí a rychlostí v praxi třetinový. Pro dosažení co nejvyšších rychlostí, tak asi vždy bude lepší použít staré, ale stále spolehlivé kabelové spojení, avšak je to vynahrazeno cenou našeho pohodlí. Důvodů tohoto radikálního snížení je spousta a proto jsou níže popsány ty nejdůležitější z nich, na které se může zaměřit i běžný uživatel a částečně si tak může pomoci k vyšším rychlostem.

Standard

Základní volbou je výběr standardu. Standardy mají různé parametry a s tím jsou spojeny samozřejmě jisté výhody i nevýhody. Vzhledem k tomu, že prioritou je zajistit co nejvyšší rychlost, tak se předpokládá, že se využije některý z novějších standardů např.: 802.11ac. Ale je dobré si také uvědomit, jakou přenosovou rychlost poskytovatel internetu dodává, jelikož pokud je rychlost cca do 50 Mb/s, tak postačí i některé starší standardy. S volbou standardu je také spjata volba koupě přístupového bodu. Zde je nutné si uvědomit, že tato investice nemusí být sice levnou záležitostí, ale kvalitní přístupový bod zajistí dlouhá léta provozu bez dalších potřebných investic. Proto je vhodné se při koupi zaměřit na standardy, které obsahuje, a také na počet antén při využití technologie MIMO, díky které lze dosahovat dnešních vysokých rychlostí. Více o této technologii níže.

Frekvenční pásma

Jak je již výše uvedeno, tak tato bezdrátová technologie využívá bezlicenční pásma a to na frekvencích 2,4 GHz a 5 GHz. Jsou standardy, které fungují na jednom z těchto dvou pásem nebo dokáží pracovat na obou, a proto pří výběru standardu je nutné se zaměřit i na tyto parametry. Při volbě standardu využívající pásmo 2,4 GHz, se musí počítat mnohdy s velkým rušením od jiných zařízení. Je to především dáno tím, že tyto pásma jsou určena pro volné využití a proto mnoho výrobců vyrábí svá zařízení právě na těchto frekvencích. Proto je vhodnější mnohdy použít pásmo 5 GHz, které není tolik rušené, ale mezi jeho slabiny patří špatný přechod přes překážky. Avšak nové standardy využívají více právě tohoto 5 GHz pásma, jelikož není tak přeplněné a především lze na něm dosahovat vyšších rychlostí, což je rozhodně větší argument proti tomu, že se signál hůře šíří. Při výběru frekvence je tedy dobré si nejprve vyhodnotit stav svého okolí a zjistit, jestli se zde nachází nějaké

velké rušení od jiných zdrojů nebo si uvědomit, jaké překážky by mohly šíření signálu narušit.

Výběr kanálu

Pro výběr frekvence, o které je psáno výše, může pomoci další parametr a tím je vhodný výběr kanálu, na kterém bude komunikace probíhat. Této problematice je věnována celá podkapitola výše viz Kanály. Ve městech a především v panelových domech je téměř nemožné najít vhodný volný kanál, aby nebyl rušen. Existuje ale rychlá a levná metoda, jak zjistit, které kanály jsou již využity např.: sousedy, a které jsou ještě volné. K tomu postačí notebook nebo chytrý mobilní telefon, do kterého lze stáhnout bezplatné aplikace, zabývající se analýzou Wi-Fi sítě. Po spuštění je vhodné si s tímto programem projít celý byt a sledovat sílu signálu a kanály ostatních vysílačů, následně dojde k vyhodnocení a zobrazení kanálu, který by byl nejvhodnější.

Síla signálu

Sílu signálu lze korigovat především dvěma způsoby. Jedním z nich je výkon, který lze částečně nastavit na přístupovém bodu, avšak tyto možnosti jsou omezeny, jelikož tyto parametry jsou pro jednotlivé regiony předem dány. V USA jsou tyto limity o něco vyšší než v Evropě, ale při použití vyšších limitů, než těch schválených v dané zemi hrozí získání vysoké pokuty. V České republice se o tyto věci stará Český telekomunikační úřad.

Druhým způsobem, jak dosáhnout co nejlepšího signálu je využití tzv. vícecestného šíření signálu, tedy technologie MIMO. Dochází zde k využití více přijímacích a vysílacích antén a díky tomu lze u novějších standardů dosáhnout co nejvyšší rychlosti. Při koupi nového přístupového bodu je nutné se zaměřit kromě ostatních věcí i na počet těchto antén.

Využití MIMO technologie

Pomocí modulace OFDM lze dosáhnout přenosové rychlosti až 54 Mb/s. Avšak v současné době rychlosti přesahují 100 Mb/s nebo existují doplňky, kde rychlost může být až 1,3 Gb/s. Je tedy jasné, že samotná modulace OFDM by takových rychlostí nikdy nedosáhla, avšak pokud se využije technologie MIMO, tak není žádný problém dosáhnout již zmíněných rychlostí. Tuto technologii lze použít současně ve spojení s OFDM. [1]

Pod pojmem MIMO si lze obecně představit přenos signálu pomocí více přenosových kanálů mezi přijímačem a vysílačem. Principem je, že vysílač a přijímač obsahují více přijímacích a vysílacích antén, které jsou od sebe mírně vzdálené. Přitom každá anténa vyžadu-

je přítomnost vlastního modulátoru a kodéru na straně vysílače a obdobný způsob je i na straně přijímače. Jednotlivé vysílané a přijímané signály je nutné od sebe rozlišit, a to se děje pomocí kódování specifickými kódy, kde nejjednodušší je zavedení časového offsetu mezi signály. [1, 15]

Dělení technologie MIMO vychází především z počtu použitých antén, kde značení 1T1R znamená jednu anténu na vysílači a jednu na přijímači, další možnosti jsou:

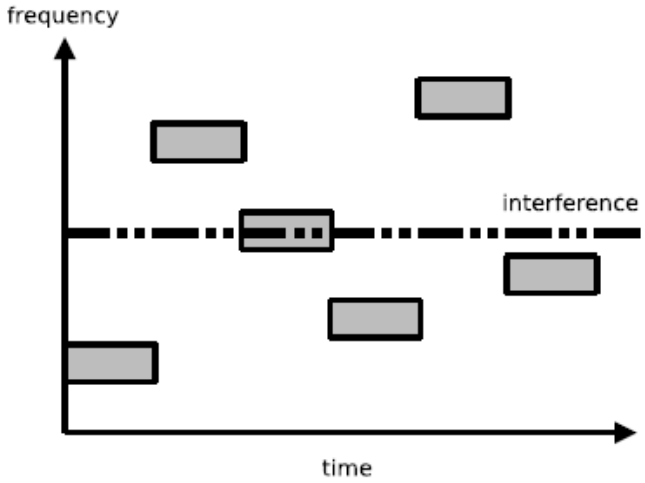
- 2T2R;
- 3T3R;
- 4T4R;
- 8T8R. [15]

4.3 Modulace

Je jasné, že signál, který je využíván k přenosu dat u standardu 802.11 a jeho doplňků musí splňovat dané parametry a kritéria. Pro přenos signálu se využívají různé modulace, které jsou součástí fyzické vrstvy modelu OSI pro standard 802.11. Veškeré tyto metody využívají rozprostřeného spektra. To znamená, že signál, který je přenášen se rozptýlí po širokém obsahu frekvencí. Využitím rozprostřeného spektra je zajištěna i částečná bezpečnost přenášených informací, vzhledem k tomu, že jednotlivé signály se hůře detekují a mnohdy vypadají pouze jako šum. [2]

4.3.1 FHSS

FHSS neboli metoda frekvenčních proskoků má vojenský původ. Jedná se o metodu, která byla patentována již v roce 1942 pod názvem Bezpečný komunikační systém. Úkolem bylo rádiové ovládání torpéd a zároveň zajištění proti rušení ze strany nepřítele. Princip je takový, že frekvenční šířka je rozdělena do 79 kanálů, kde každý kanál má šířku 1 MHz. Vysílač následně skáče v náhodném pořadí po jednotlivých pásmech, kde vysílá vždy krátký datový proud. Posloupnost bitů je kódována frekvenční modulací. Maximální čas působení na jednom kanálu může být 400 ms. Tato metoda byla využita u původní specifikace standardu 802.11, avšak dnes se již nevyužívá a to především kvůli nízké přenosové rychlosti 1 Mb/s. [2, 3]



Obr. 7. Proskoky po jednotlivých kanálech [1]

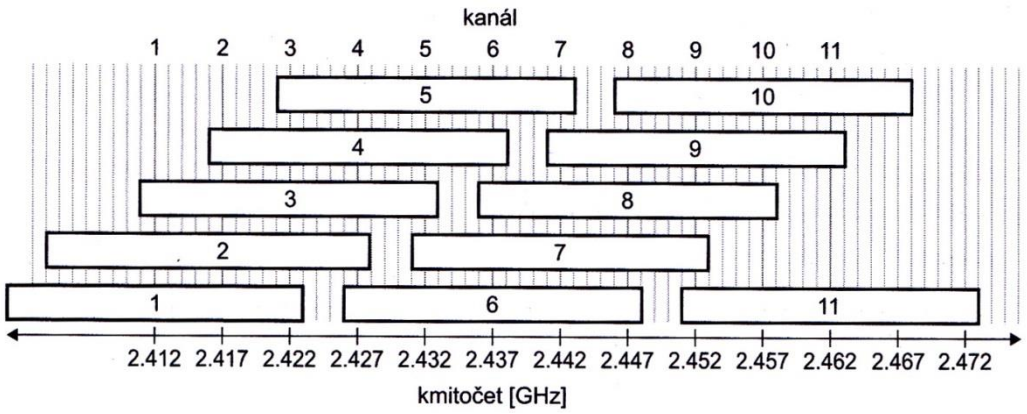
4.3.2 DSSS

Oproti metodě FHSS je zde vyšší maximální rychlost (u 802.11b až 11 Mb/s) a přenos dat je zajištěn v jednom pásmu, který má šířku 22MHz. Jednotlivé bity, které nesou výslednou informaci, jsou kódovány do přenosového kódu tzv. chipping code. To znamená, že každý bit je vyjádřen několika bity, u standardu 802.11 je to 11 bitů. Tím je zajištěna vysoká spolehlivost přenosu dat, jelikož při částečném poškození zprávy je možné rekonstruovat původní zprávu. Využívá se zde funkce XOR, kde jsou použity vstupní bity (zpráva) a generovaný kód, výsledkem je přenosový kód, který je bezdrátově vysílán. Přijímač tato data přijme a pomocí funkce XOR získá původní zprávu. [2]

Tab. 9. Princip DSSS

Data	**1**	**0**	**1**	**0**
Generovaný kód	10101100010	10101100010	10101100010	10101100010
Signál	01010011101	10101100010	01010011101	10101100010

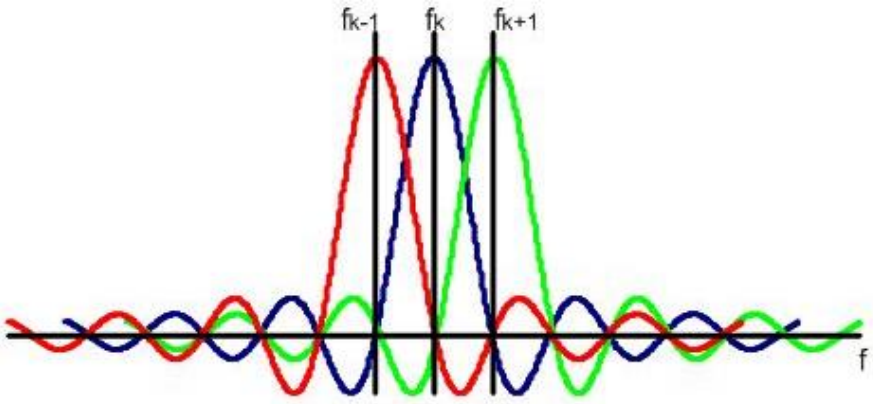
Vzhledem k tomu, že metoda DSSS využívá šířku pásma o velikosti 22 MHz a pracuje v povoleném pásmu 2,4 GHz (82 MHz), tak je jasné, že pokud se má předejít vzájemnému rušení, tak se mohou použít pouze 3 nepřekrývající se kanály. Ale metoda DSSS využívá 11 kanálů, proto se vzájemně překrývají a dochází k rušení. [2]



Obr. 8. Možnosti využití kanálů u DSSS [2]

4.3.3 OFDM

Tato metoda se řadí mezi jednu z nejvýkonnějších, ale zároveň nejkomplikovanějších metod, které využíváme ve standardu 802.11. Tato metoda spočívá v tom, že celé pásmo je rozděleno na desítky až tisíce nosných kmitočtů tzv. subkanálů, které mají od sebe rovnoměrný odstup a jsou přenášeny velice těsně od sebe, tím je zajištěno co největší využití spektra. Zpráva, která je přenášena, je tedy roztrhána a přenášena pomocí již zmíněných nosných kmitočtů. Tyto nosné kmitočty jsou následně modulovány robustními modulacemi (QPSK, 16QAM, 64QAM) a jsou navíc vzájemně ortogonální, to znamená, že jejich skalární součin je nulový (maximum každé nosné se střetává s ostatními nosnými, které právě prochází nulou). Na těchto subkanálech se nepřenášejí pouze data ale i pilotní nosné, které jsou použity pro synchronizaci a k úpravě deformovaných signálů. [3, 7, 14]

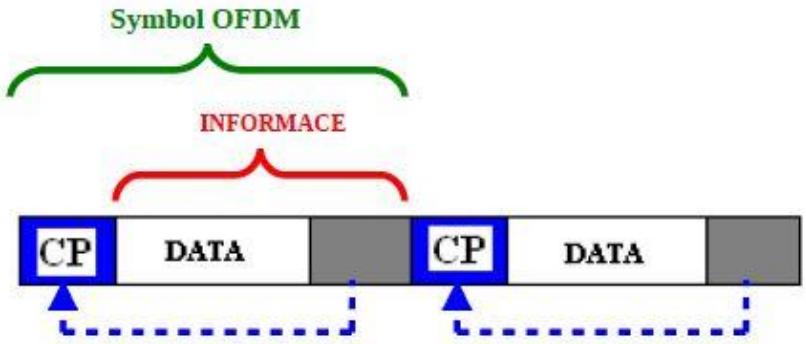


Obr. 9. Subkanály OFDM [14]

Data se v každém subkanálu přenášejí relativně pomalu, avšak ve výsledku dochází k součtu všech subkanálů a přenosová rychlost může být až 54 Mb/s. Proto se dnes nejběžněji využívá tato metoda pro nové doplňky standardu 802.11, kde je potřeba zajistit především co nejvyšší přenosovou rychlost. Výhodou je, že OFDM je dobře přizpůsobivé podmínkám a nevyžaduje frekvenční kanály o pevně dané šířce. To je dáno tím, že jednotlivé nosné jsou na sobě nezávislé. [7]

Cyklická předpona

Metoda OFDM využívá cyklickou předponu, aby zabránila interferenci. Tato předpona navíc tvoří interval mezi sousedními symboly. Cyklickou předponu tvoří daný počet posledních vzorků daného symbolu, které jsou zkopírovány a následně přeneseny na začátek symbolu. Případné rušení následně nemá vliv přenášenou informaci. [14]



Obr. 10. Cyklický prefix u OFDM [14]

5 ZABEZPEČENÍ WI-FI

I přesto, že bezdrátové sítě mají spoustu výhod a současný život bez nich by byl pro většinu obyvatel moderního světa nepředstavitelný, mají tyto sítě bezesporu i své nevýhody. Jednou z hlavních nevýhod je, že není úplně možné přesně omezit prostor, kterým se signál šíří. Tato nevýhoda je také i výhodou těchto sítí, jelikož právě bezdrátové šíření signálu je samotným principem Wi-Fi. Počet těchto bezdrátových sítí neustále narůstá a obklopují společnost téměř na každém kroku, a tak je velmi důležité zaměřit se i na jejich bezpečnost, jelikož provozování těchto sítí s sebou přináší i jistá bezpečnostní rizika. Hlavním důvodem, proč zajistit bezpečnost těchto sítí, je znemožnit útočníkovi dostat se do této sítě a následně mu alespoň ztížit přístup ke komunikaci a souborům. [4, 16, 20]

V případě domácích bezdrátových sítí, je bezpečnost závislá především na našem nastavení a konfiguraci. Ale bezdrátové sítě dnes bezplatně a komukoliv poskytují různí provozovatelé kaváren, restaurací a jsou tedy na každém rohu. Zde jsou mnohem větší bezpečnostní rizika, jelikož na těchto sítích se může pohybovat téměř kdokoliv a pro útočníka je tedy mnohem snadnější dostat se ke komunikaci a datům. Proto je dobré se nejlépe vyvarovat těmto veřejným sítím nebo se alespoň nepřipojovat k důležitým účtům, jako jsou např.: bankovní, emailové atd. [16, 20]

5.1 Přístup do sítě

Důležitou součástí zajištění bezpečnosti sítě je zajištění přístupu do ní neboli autentizace. Tam, kde jsou pouze kabelové sítě, není až tak složité zamezit přístupu těm nesprávným osobám. V případě sítí bezdrátových, kde se člověk může připojit takřka z kteréhokoliv místa, kde se nachází dostatečné pokrytí, je zajištění přístupu o něco složitější. Pro přístup do bezdrátové sítě se využívají převážně 3 následující metody. [7, 8]

Autentizace otevřená

Tato metoda, nazývaná také jako open-systém, je nejjednodušší mechanismus, díky kterému je možné se do bezdrátové sítě přihlásit. Princip je snadný a spočívá v tom, že klient přístupovému bodu pošle žádost na autentizaci spolu se svými údaji. Přístupový bod následně odpoví a klientovi je umožněn přístup do sítě. Tato metoda spočívá v tom, že klientovi je vždy umožněn přístup, pokud mu tedy není přístup předem zakázán. Navíc se zde nepoužívá žádné heslo, a proto své využití najde především u bezplatných veřejných sítí jako např.: restaurace, kavárny, obchodní domy. [7]

Autentizace se sdíleným/před sdíleným klíčem

Autentizace se sdíleným klíčem se využívá především za využití bezpečnostního protokolu WEP. Autentizace probíhá pomocí sdíleného klíče. Hlavním rozdílem oproti otevřené autentizaci je, že pro přístup do sítě je důležitá znalost WEP klíče. Vzájemná komunikace mezi klientem a přístupovým bodem je následující. [7]

- Klient zašle požadavek o autentizaci přístupovému bodu.
- Přístupový bod zpět zašle nezašifrovaný a náhodně vygenerovaný řetězec.
- Klient již zmíněný nezašifrovaný řetězec přijme a díky WEP klíči, který musí znát, tento řetězec zašifruje a následně odešle zase zpět.
- Přístupový bod přijme zašifrovaný řetězec od klienta a vzhledem k tomu, že také zná WEP klíč, tak porovná, jestli je přijatý řetězec správný.
- Na základě předchozího srovnání přístupový bod klientovi oznámí, jestli byla autentizace úspěšná a přiřadí klienta do sítě či ne. [7]

Nevýhodou je, že WEP využívá statický klíč, který se po celou dobu relace nemění a proto je pro případného útočníka snadné během krátké chvíle tuto síť zcela ovládnout. Proto je autentizace s před sdíleným klíčem více odolná a nazývá se Pre-Shader Key neboli PSK. Komunikace mezi klientem a přístupovým bodem je zde obdobná, avšak hlavní změnou je zde využití protokolu TKIP, který zajišťuje, že klíč již není statický, ale neustále se dynamicky mění. Pro zajištění přístupu do sítě klient a přístupový bod využijí předem zvolený klíč, jako u první metody, avšak následně dochází ke generování a využívání dočasných klíčů. Tím má případný útočník ztížené podmínky pro zjištění klíče. [7]

IEEE 802.1x

Lze vidět, že předchozí dvě metody nezaručují zrovna vysoký stupeň zabezpečení, i když pro většinu domácností mohou být plně dostačující. Jelikož standard IEEE 802.11 a jeho doplňky nenabízí další možnosti řešení přístupu, je potřeba využít jiný standard. Jedná se o bezpečnostní standard IEEE 802.1x, který zahrnuje další metodu autentizace. Největší výhodou je možnost jednoznačného určení uživatele, který se do sítě plánuje připojit, a také zde dochází k ověřování přístupového bodu, a tím je zajištěno, že útočník se nemůže vydávat za případný falešný přístupový bod. Oproti předchozím metodám, kde komunikace probíhala pouze mezi klientem a přístupovým bodem, tak se zde navíc využívá činnosti autorizačního serveru (radius). Ten implementuje funkce Authentication Authorization, accounting, tedy AAA. [7, 19]

Autentizace: slouží k jednoznačnému určení uživatele (klienta), který se snaží připojit do systému.

Autorizace: navazuje většinou ihned na autentizaci. Dochází zde k ověření veškerých oprávnění uživatele vstupujícího do systému. Na základě nastavených oprávnění jsou mu povoleny vykonávat příslušné akce.

Účtování: zajišťuje monitorování a používání různých služeb. Je možné uživatele např.: omezit v délce připojení v síti.

Postup, jakým se klient přihlašuje do sítě je následující.

- Klient odešle přístupovému bodu požadavek se žádostí vstupu do sítě.
- Přístupový bod obratem pošle dotaz na totožnost.
- Klient odpoví a zašle identifikační údaje (přihlašovací jméno a heslo) autorizačnímu serveru (radius). Komunikace probíhá přes přístupový bod.
- Autorizační server si získané identifikační údaje porovná se svou databází a odešle zprávu o povolení nebo zakázání přístupu klientovi.
- V případě povoleného přístupu je klient autentizován. [7]

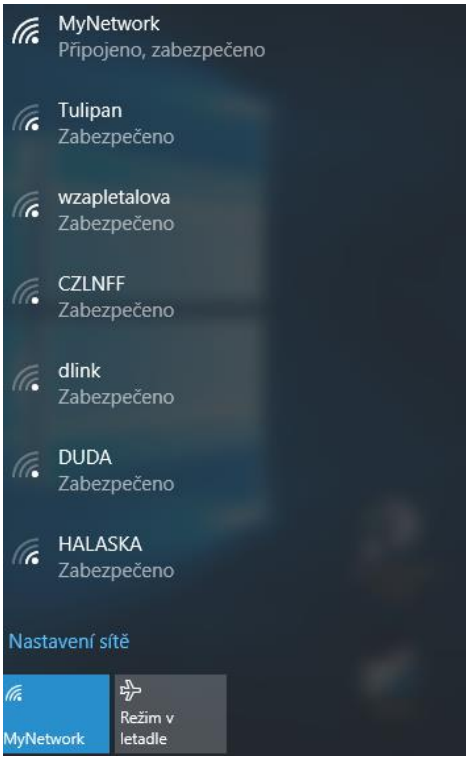
5.2 Metody zabezpečení

Jak je již výše zmíněno, tak útoky na bezdrátové sítě mohou být velmi časté a snadné, navíc se uživatel o nich nemusí mnohdy ani dozvědět. V případě tvorby vlastní domácí sítě existuje spousta metod, jak zajistit její bezpečnost. V následujících podkapitolách jsou popsány ty nejznámější z nich.

5.2.1 SSID

Service Set Identifier neboli SSID je název bezdrátové sítě, který je běžně vysílán do prostoru. Kdokoliv je v dosahu této sítě, tak ve výpisu dostupných bezdrátových sítí ji může spatřit. Ve městech nebo panelových domech je možné vidět obrovské množství těchto identifikátorů. Pro případného útočníka je tedy velice snadné si vybrat bezdrátovou síť, na kterou bude chtít svůj útok směrovat. Nejhorší variantou je, pokud jako název sítě je zvoleno jméno nebo příjmení majitele. Útočník v tomto případě přímo ví, o koho se jedná a komu příslušná síť patří. Existuje zde však jednoduché řešení, jak se tomu vyvarovat. Tím je vypnutí vysílání identifikátoru. Toto vypnutí se provádí v nastavení Wi-Fi routeru. Následně se daná síť již nebude nikomu poblíž zobrazovat ve výpisu. To ale neznamená, že

případný útočník nemůže zjistit dostupnost dané sítě, avšak určitý krok k bezpečnosti to je. Vypnutím tohoto vysílání se také trochu zkomplikuje připojování nových zařízení do této sítě, jelikož ji neuvidí v seznamu. Při připojování nového uživatele je tedy nutné název sítě zadat ručně. [16]



Obr. 11. Vysílání SSID

5.2.2 Změna hesla přístupového bodu

Veškeré nastavení, kterým jsou prováděny změny v bezdrátových sítích, se nastavují ve Wi-Fi routeru. Přístup do tohoto zařízení je nejčastěji chráněn heslem nebo přihlašovacím jménem a heslem. V případě, že se útočník již dostal do sítě, bylo by vhodné mu zabránit, aby se nezmocnil i celého routeru. Wi-Fi routery používají univerzální přihlašovací údaje do těchto zařízení, které jsou běžně známé a není žádný velký problém je zjistit. A proto ihned po zakoupení a nastavení routeru se doporučuje změnit tyto údaje.

Obr. 12. Přihlášení do nastaveni Wi-Fi routeru

5.2.3 Omezení počtu IP adres

IP adresa je číselné značení, které identifikuje příslušné zařízení v síti. Aby se cizí zařízení nepřipojovala do sítě, tak právě pomocí těchto adres je možné omezit jejich připojení. Jednou z možností je omezení IP adres, které automaticky přiřazuje DHCP server. V nastavení lze nadefinovat maximální počet automaticky přiřazovaných IP adres. Tím se zajistí, že se do sítě nepřipojí vyšší počet zařízení, než který je nastaven. [16]

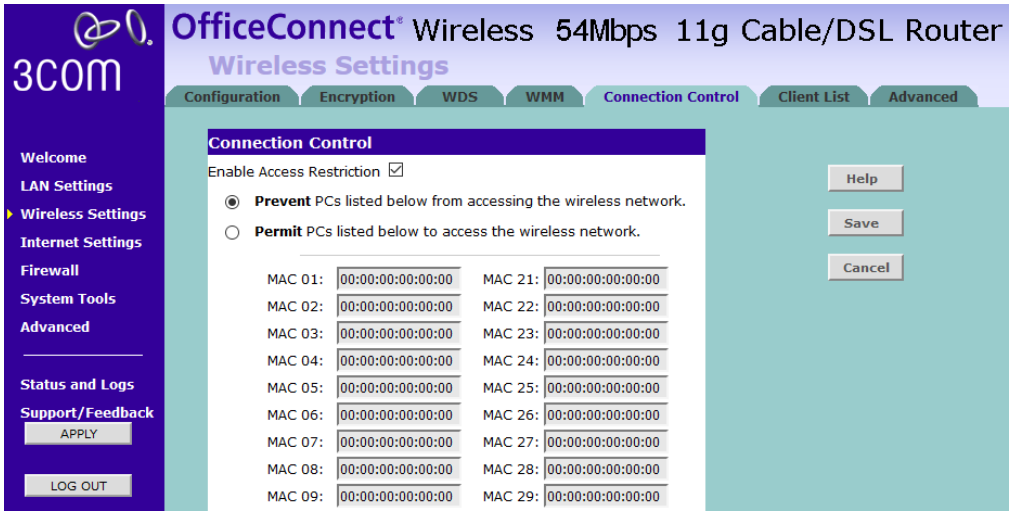
Kontrola DHCP záznamu

I přes veškeré snahy zabezpečit bezdrátovou Wi-Fi síť je vhodné jednou za čas zkontrolovat záznam DHCP protokolu, který se nachází také v nastavení Wi-Fi routeru. V tomto záznamu je seznam všech zařízení, které se do sítě připojily a to včetně přidělených IP adres a MAC adres. Pokud se do sítě nepřipojuje velké množství zařízení, tak by mělo být snadné rozpoznat jednotlivé zařízení a zjistit tak, jestli se zde nenachází nějaké neznámé. V takovém případě lze takovému nechtěnému uživateli omezit přístup do sítě. [16]

5.2.4 Filtrování MAC adres

Obdobou IP adres jsou MAC adresy a díky nim je možné bezpečnost zajistit jejich filtrováním. MAC adresa je jedinečné sériové číslo, které se skládá z kombinace dvanácti hexadecimálních číslic nebo písmen, které jsou uspořádány po dvojicích vždy s dvojtečkou mezi každou dvojicí. První 3 dvojice vyjadřují výrobce a další 3 dvojice jsou identifikátorem daného zařízení přiřazeného výrobcem. Tímto způsobem je označen každý síťový produkt. Tohoto značení se využívá právě i u zabezpečení bezdrátových sítí. Wi-Fi router umožňuje filtrování připojovaných zařízení na základě MAC adres. Nejprve je nutné zjistit adresu zařízení, které se chce do sítě připojit a následně ho nakonfigurovat do seznamu

MAC adres, kterým je umožněn přístup do sítě. Pokud ale útočník dokáže zjistit tuto adresu, která má umožněný přístup, tak je schopen ji v dnešní době podvrhnout a připojit se tak do sítě i s jiným zařízením. Naskýtá se také možnost zcela opačná, a to zadání MAC adres zařízení, které nebudou do sítě připuštěny. [16, 18]



Obr. 13. Možnost nastavení přístupu podle MAC adres

5.2.5 Zajištění správného dosahu vysílání

Každý by chtěl mít co nejlépe pokrytý svůj dům, byt nebo dokonce i zahradu signálem Wi-Fi, aby se mohl odkudkoliv a bezstarostně připojit. To bývá nejčastějším problémem, jelikož mnoho lidí si neuvědomuje, že vysílaný signál je často vysílán mnohem dál, než jsou hranice našeho pozemku. To je nejčastější příčinou toho, že případný útočník se snadno dostane k vysílané síti. Jednou z nejjednodušších metod, jak zajistit, aby bezdrátová síť nebyla šířena tam, kde by neměla, je umístit přístupový bod co nejvíce do středu bytu nebo domu. Signál by se měl rozprostřít po domě a měl by co nejméně přesahovat za naše hranice. Následně je dobré si např.: s mobilním telefonem projít okolí svého obydlí a zjistit tak, jak daleko sahá bezdrátová síť. [17]

RF stínění

I přesto, že omezení šíření Wi-Fi signálu není vůbec jednoduché, tak je mnohdy zapotřebí zajistit, aby vysílaný signál neopouštěl hranice domu nebo pokoje. Naštěstí existují metody, které umožňují zastavení tohoto šíření. Všeobecně se využití této metody nazývá radio-

frekvenční stínění. Hlavním problémem bezdrátových sítí je ten, že útočník zachytí vysílání a následně se může pokoušet o jednotlivé útoky. Jednotlivé metody, zajišťující omezení šíření elektromagnetických vln, však nejsou levnou záležitostí. Proto se využívají spíše tam, kde hrozí vyšší riziko útoku a s tím spojené odcizení důležitých informací jako např.: ve firmách, státních organizacích. Avšak radiofrekvenční stínění neslouží pouze pro zajištění bezpečnosti, ale také pro odstranění rušení z jiných zdrojů, vysílajících na stejných frekvencích. Stínění si najde své využití také v nemocnicích, kde slouží především k tomu, aby nebyly rušeny přístroje, které zajišťují životní funkce pacientů. [17]

Pro správnou funkci stínění se zde využívají oxidy železa a hliníku, které na určitých frekvencích rezonují, a tím je zabráněno průchodu rádiových vln. Díky těmto materiálům lze zajistit stínění pouze na určitých frekvencích a umožnit tak cestu jiným potřebným signálům. Mezi využívané stínící metody patří tapety, fólie do oken a nátěry na zdi. [17]

Obr. 14. Stínící tapeta [17]

5.2.6 Šifrování

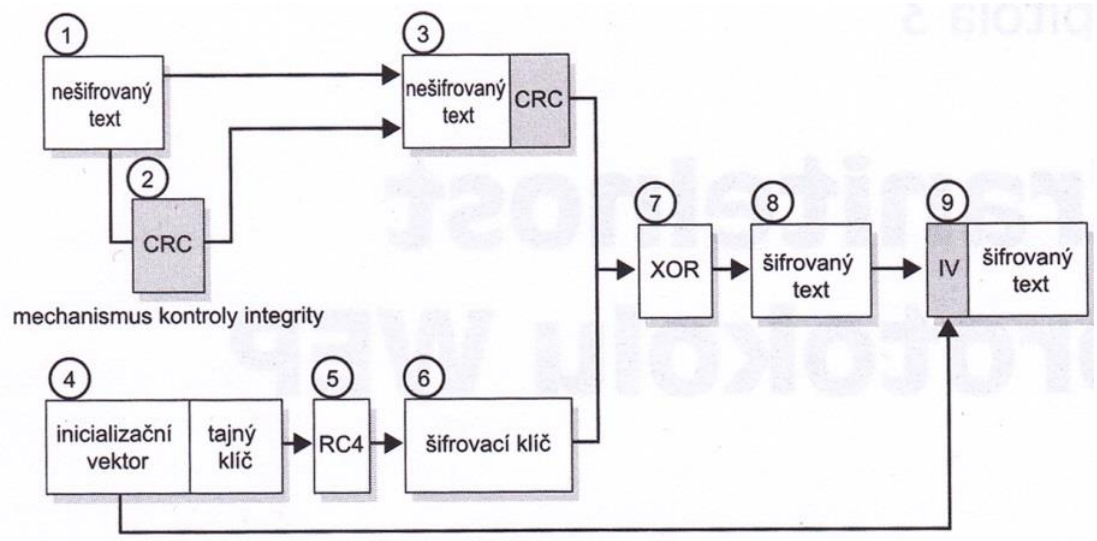
Aby v bezdrátových sítích nebylo možné jednoduše zjistit komunikaci, která probíhá mezi jednotlivými zařízeními a přístupovými body, tak se využívá tzv. šifrování těchto zpráv. Jedná se o úplný základ bezpečnosti bezdrátové komunikace, jelikož by nebylo vhodné, kdyby se přihlašovací údaje a další zprávy přenášely bez jakéhokoliv šifrování. V takovém případě by pro případného útočníka nebyl žádný problém tyto údaje zjistit a následně je zneužít v jeho prospěch. Šifrování je proces, kdy se zpráva v podobě otevřeného textu převádí do jiné podoby, kterou lze následně přečíst jen díky určité znalosti např. klíče. Jednot-

livé metody šifrování jsou dány protokoly, které jsou určeny právě pro šifrování bezdrátových sítí. V následujících podkapitolách jsou popsány ty nejdůležitější protokoly. [21]

WEP

Protokol WEP je již v dnešní době na ústupu, a to zejména proto, že tato metoda zabezpečení byla již dávno prolomena. Pokud se útočník bude chtít dostat do takto zabezpečené sítě, tak mu to v horším případě zabere jen pár desítek minut. Jelikož v praktické části bude provedena realizace útoku na síť s tímto zabezpečením, tak protokolu WEP zde bude věnována větší část a bude popsán samotný princip. [2, 7]

Celý proces začíná nezašifrovanou zprávou, která se má odeslat. Z této zprávy neboli textu se nejprve provede cyklický redundantní součet, tedy CRC. Tento kontrolní součet se přikládá k přenášené zprávě, aby bylo možné po přijetí zjistit, jestli je zpráva původní a nebylo s ní manipulováno. V dalším kroku dojde ke spojení inicializačního vektoru a tajného klíče. Tato kombinace následně vstoupí do generátoru pseudonáhodných čísel RC4, kde výsledkem bude šifrovací klíč. Poté se provede logický součet XOR z textu spolu s kontrolním součtem a šifrovacím klíčem. Výsledkem je šifrovaný text, před který se pouze připojí nezašifrovaná hodnota inicializačního vektoru a takto se výsledek odešle. Připojený inicializační vektor se přenáší nezašifrovaný, jelikož je potřebný k následnému dešifrování. [2]



Obr. 15. Šifrováni protokolem WEP [2]

Problém protokolu WEP

Hlavní roli zde hraje již výše zmíněný inicializační vektor (IV). Samotný protokol WEP nijak nespecifikuje, jak se má tento vektor generovat, ale jeho hodnota spolu s kombinací tajného klíče slouží k inicializaci generátoru RC4. Inicializační vektor je 24 bitová hodnota, kde jeho hlavním úkolem je zajistit pokaždé jinou hodnotu generátoru RC4. Základním požadavkem šifry RC4 je však ten, že se za žádných okolností nesmí nikdy opakovat inicializační hodnota. Avšak zde nastává ten hlavní problém. Jelikož délka inicializačního vektoru je 24 bitů, tak je jasné, že při dnešních vysokých rychlostech se veškeré možné hodnoty inicializačního vektoru vyčerpají. Protože WEP tedy nespecifikuje jak se má tento inicializační vektor generovat, tak dochází k porušení základní podmínky šifry RC4 a hodnoty inicializačních vektorů se začnou opakovat. Tento problém se nazývá kolize inicializačního vektoru, čehož využívají případní útočníci, kteří veškerý přenos odposlouchávají a jelikož se inicializační vektor přenáší nezašifrovaný, tak tuto kolizi lehce zjistí a může provést nějaký z útoků. I když výrobci používají 64bitový WEP, 128bitový WEP atd., tak stejně se přenáší vždy nezašifrovaný inicializační vektor o velikosti 24 bitů, což tedy neřeší ten hlavní problém. [2, 20]

WPA

Protokol WPA je nástupcem protokolu WEP, který napravuje jeho největší chyby a problémy, díky kterým se WEP dnes již nedoporučuje využívat. Veškeré změny provedeny v tomto protokolu vycházejí ze standardu IEEE 802.11i.

První důležitou změnou je autentizace pomocí využití standardu IEEE 802.1x nebo PSK. Obě tyto metody jsou popsány výše, viz kapitola Přístup do sítě. Avšak pro domácí použití se využívá převážně metoda PSK, která je založena na tom, že na veškerých připojovaných zařízeních a přístupovém bodě se nastaví tzv. hlavní klíč, který slouží pro přístup do sítě. Tak tomu je i u protokolu WEP, avšak hlavní změnou je, že tento hlavní klíč se zde použije pouze jednou a dále jsou využívány pouze jeho odvozené hodnoty. Tak je tedy zajištěna jistota, že tento klíč nikdy nebude použit dvakrát, kdežto u WEP se používá neustále dokola. Tato metoda se nazývá dynamická změna klíče. [2]

Toho by však nebylo možné dosáhnout bez využití šifrování pomocí protokolu TKIP (Temporal Key Integrity Protocol). Právě díky němu je možné provádět dynamickou změnu klíče. Tento protokol řeší ale i další nedostatky WEPu. I když stále využívá šifru RC4, která u protokolu WEP působila problémy, používá její důkladnější inicializaci a díky to-

mu již není možné, aby došlo ke kolizi inicializačního vektoru, který byl hlavník důsledkem útoků na protokol WEP. Samotná hodnota inicializačního vektoru byla zdvojnásobena na 48 bitů. V neposlední řadě došlo k lepšímu zajištění integrity přenášených dat. Zde byla metoda CRC nahrazena metodou MIC, která zajišťuje data proti úmyslným změnám při přenosu. [2]

WPA2

Nástup protokolu WPA byl pouze rychlou odezvou a náhradou za ne zrovna bezpečný a také již prolomený WEP. Z toho důvodu WPA využívá některé funkce, které jsou součástí standardu 802.11i, který v době příchodu WPA nebyl ještě zcela hotový. Avšak WPA2, dalo by se říci, je celý plnohodnotný standard 802.11i. Hlavní a důležitou změnou je, že WPA 2 již nevyužívá šifrovací metodu RC4, ale AES, který pracuje s bloky o velikosti 128 bitů a proto se řadí do blokových šifer. Kdežto šifrovací metoda RC4 se řadila mezi proudové šifry, kde docházelo ke XORování každého bitu zvlášť. [2, 21]

II. PRAKTICKÁ ČÁST

6 ANKETA A JEJÍ VYHODNOCENÍ

Tato kapitola se bude zabývat vytvořením ankety, zaměřené na zjištění povědomí respondentů o bezpečnosti Wi-Fi sítí. Výsledky zde budou následně zpracovány a vyhodnoceny.

6.1 Charakteristika a tvorba ankety

Jako první bylo potřeba zvolit způsob, jakým byli jednotliví respondenti dotazováni. Byla zvolena metoda internetového (elektronického) dotazování. Tento způsob je v současné době velice oblíbený a rozšířený. Mezi jeho největší výhody patří nízké náklady, rychlost dotazování a jednoduché zpracování dat, jelikož veškerá data jsou ukládána v elektronické podobě.

Dalším úkolem bylo zapotřebí zvolit internetový portál, přes který byla anketa vytvořena. Portálů nabízejících tuto službu je spousta, avšak byl zvolen portál Google Forms neboli formuláře google. Google Forms je zcela zdarma a nabízí možnost vytvoření anket a následnou možnost analýzy dat, které se ukládají v elektronické podobě. Následně došlo k vytvoření ankety, která obsahuje následující typy otázek.

- Otevřené otázky: tento typ otázek nabízí respondentovi odpovědět na otázky svým vlastním způsobem a není nijak omezen předem vytvořenými odpověďmi.
- Uzavřené otázky: v takovém případě má respondent předem vytvořené varianty odpovědí, ze kterých si vybírá.

Anketa je rozdělena na jednotlivé části, které se zabývají vždy určitou problematikou. Díky využití Google Forms byla anketa sestavena tak, aby respondent na základě rozhodovacích otázek vždy odpovídal pouze na otázky, které je schopen odpovědět. Anketa je složena celkem ze tří hlavních částí.

- První část se zabývá zjištěním základních informací o respondentech (otázky 1-3).
- Další část je věnována pouze uživatelům, kteří mají doma Wi-Fi router. Zde dochází ke zjištění, jestli jednotliví uživatelé vědí, jakým způsobem je zabezpečen (otázky 6-10).
- Poslední část je věnována službám, které uživatelé využívají na různých typech sítí (otázky 11-18).
- Zbytek otázek slouží pro zjištění, jestli respondent je schopen odpovědět na následující části. V případě, že není, tak v závislosti na typu otázky je anketa ukončena nebo přejde na další části (otázky 4, 5).

Po vytvoření ankety bylo nutné zajistit její rozšíření mezi respondenty. Proto byla anketa rozeslána studijním oddělením mezi studenty a následně byla šířena pomocí emailu mezi další známé. Anketa také byla zveřejněna na facebookových skupinách, které se zabývají vzájemným vyplňováním dotazníků a anket. Díky těmto možnostem byl zajištěn dostatečný počet respondentů pro vyhodnocení ankety.

6.2 Cíl ankety a základní informace

Hlavním cílem ankety je zjistit všeobecné povědomí uživatelů o bezpečnosti bezdrátových Wi-Fi sítí. Dochází zde také ke zjištění, jestli uživatelé vědí, jakým způsobem je zabezpečen jejich Wi-Fi router. V neposlední řadě je cílem ankety zjistit, jaké služby uživatelé nejčastěji využívají a co na jednotlivých typech sítí dělají.

Termín realizace: 28. 4. 2015 – 17. 3. 2016.

Počet otázek: 19.

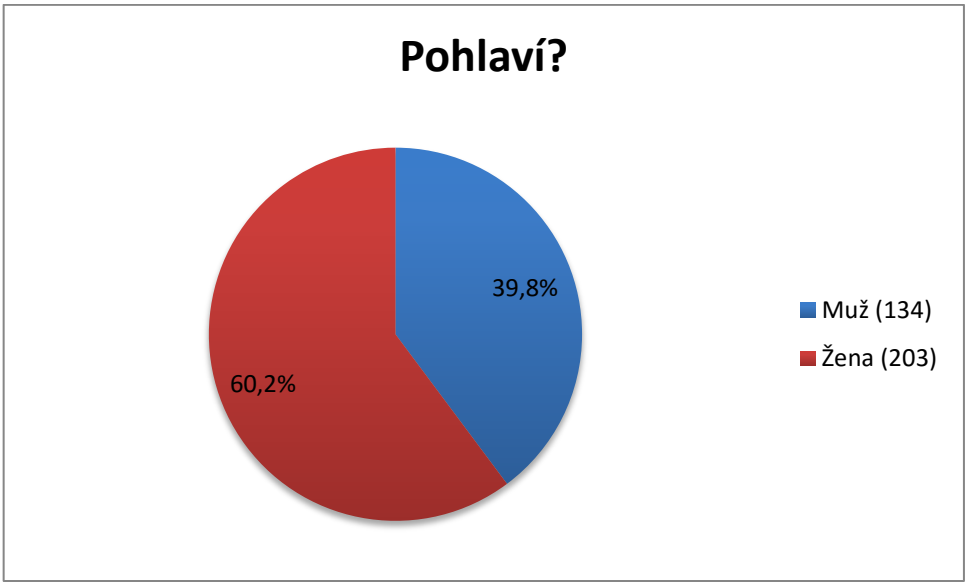
Celkový počet respondentů: 337.

6.3 Vyhodnocení ankety

Na základě získaných odpovědí od jednotlivých respondentů, byla výsledná data zpracována a vyobrazena pomocí grafů, které jsou popsány níže.

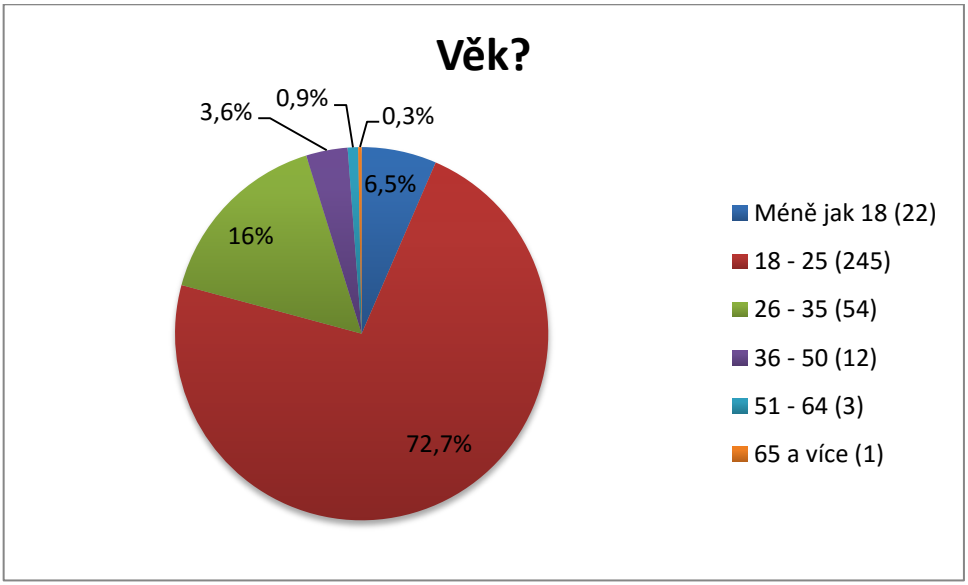
Charakteristika respondentů

Mezi respondenty, kteří odpověděli na anketu, patří ženy i muži. Avšak o něco vyšší zastoupení zde mají ženy (60,2 %), to je zapříčiněno především tím, že byly více ochotné odpovědět na tuto anketu. Avšak rozdíl není až tak markantní. Tento poměr lze vidět na níže uvedeném grafu (Graf 1. Respondenti dle pohlaví).



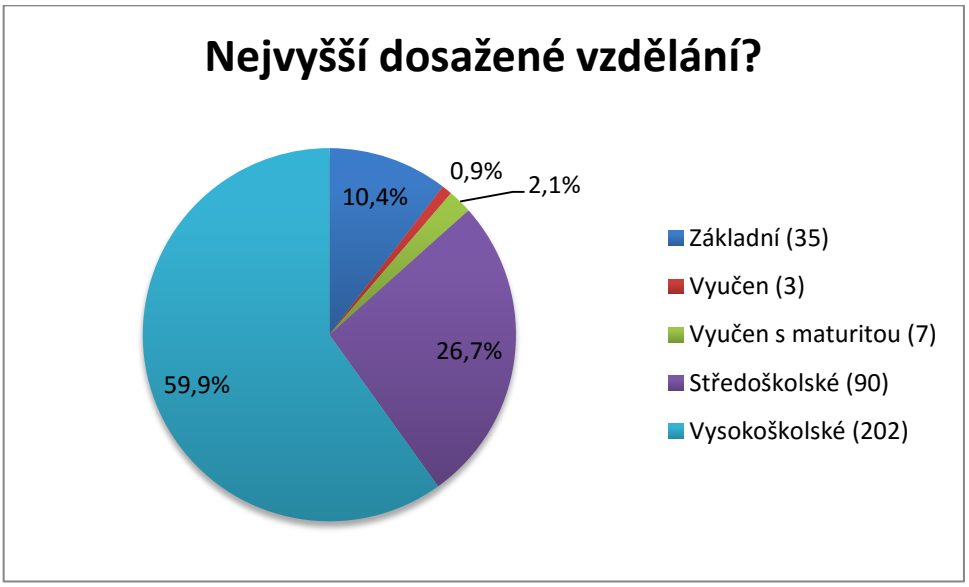
Graf 1. Respondenti dle pohlaví

Dalším sledovaným údajem byl věk respondentů, odpovídajících na anketu. Zde viditelně má největší zastoupení věková kategorie 18 – 25 let (72,7 %), což je dáno tím, že anketu vyplňovali především studenti vysokých škol. Mezi další, ale již méně zastoupenou věkovou kategorii patří respondenti ve věku 25 – 35 let (16 %). Zbytek respondentů, patřících do jiných věkových kategorií, je zde zastoupen již minimálně. Výsledky lze vidět v následujícím grafu (Graf 2. Věk respondentů).



Graf 2. Věk respondentů

Posledním sledovaným údajem týkajícím se charakteristiky respondentů je zjištění jejich nejvyššího dosaženého vzdělání (Graf 3. Nejvyšší dosažené vzdělání respondentů). Zde mají nejvyšší zastoupení respondenti s vysokoškolským vzděláním (59,9 %), rovněž je to dáno tím, že anketu vyplňovali studenti vysokých škol, kteří již mají dokončené minimálně bakalářské vzdělání. Mezi další početnou skupinu patří respondenti se středoškolským vzděláním (26,7 %) a následně to jsou respondenti se základním vzděláním (10,4 %).



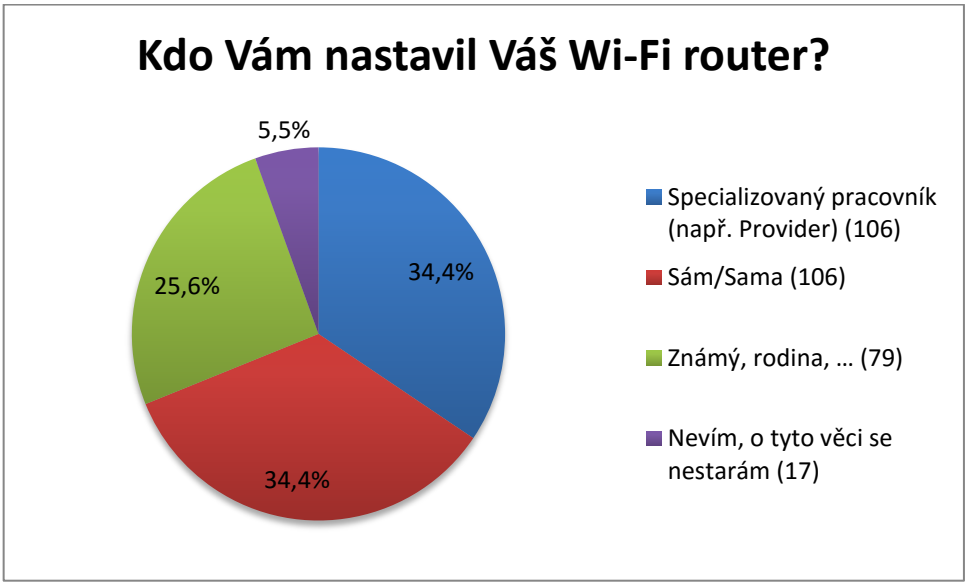
Graf 3. Nejvyšší dosažené vzdělání respondentů

Závěrem této části, týkající se charakteristiky respondentů, byla otázka, která měla za úkol zjistit, jestli respondenti využívají připojení pomocí Wi-Fi. V případě, respondentů nevyužívajících tuto technologii, by bylo pro ně zbytečné pokračovat v této anketě, a proto byla pro ně anketa ukončena. Z celkového počtu respondentů 337, ukončilo anketu na základě této otázky 16 respondentů.

Zabezpečení Wi-Fi routeru

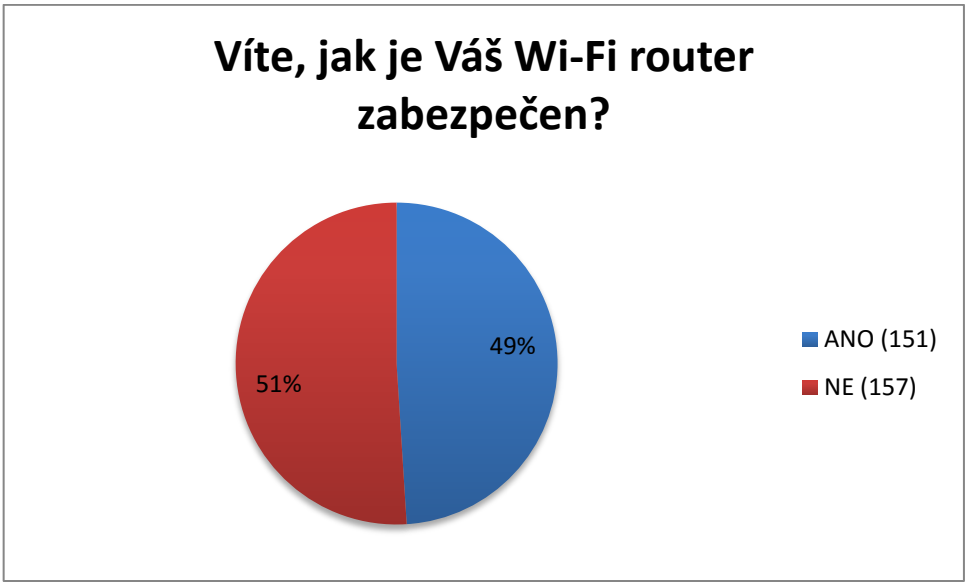
Následující část byla zaměřena na otázky ohledně zabezpečení domácího Wi-Fi routeru. Avšak ne všichni mají doma vlastní Wi-Fi router, z toho důvodu tato část začala otázkou, zjišťující, jestli respondenti vlastní Wi-Fi router. Z výsledků této otázky bylo zjištěno, že 96 % respondentů má Wi-Fi router, což bylo 308 z 321 respondentů. Ti tedy pokračovali v této části. Zbytek respondentů byl přesměrován na další část ankety.

Samotná část této ankety začala otázkou, která měla za úkol zjistit, kdo respondentům neboli uživatelům provádí nebo provedl nastavení Wi-Fi rotueru. Výsledný graf (Graf 4. Nastavení Wi-Fi routeru), popisující výsledek této otázky je níže. Z výsledků lze vyčíst, že Wi-Fi router si nejčastěji nastavují uživatelé sami (34,4 %) nebo tuto práci nechají na specializovaném pracovníkovi (34,4 %). Další skupinou jsou uživatelé, kterým toto nastavení provedl někdo známý nebo někdo z rodiny (25,6 %). Pouhých 5,5 % respondentů uvedlo, že neví nebo se o tyto věci nestarají.



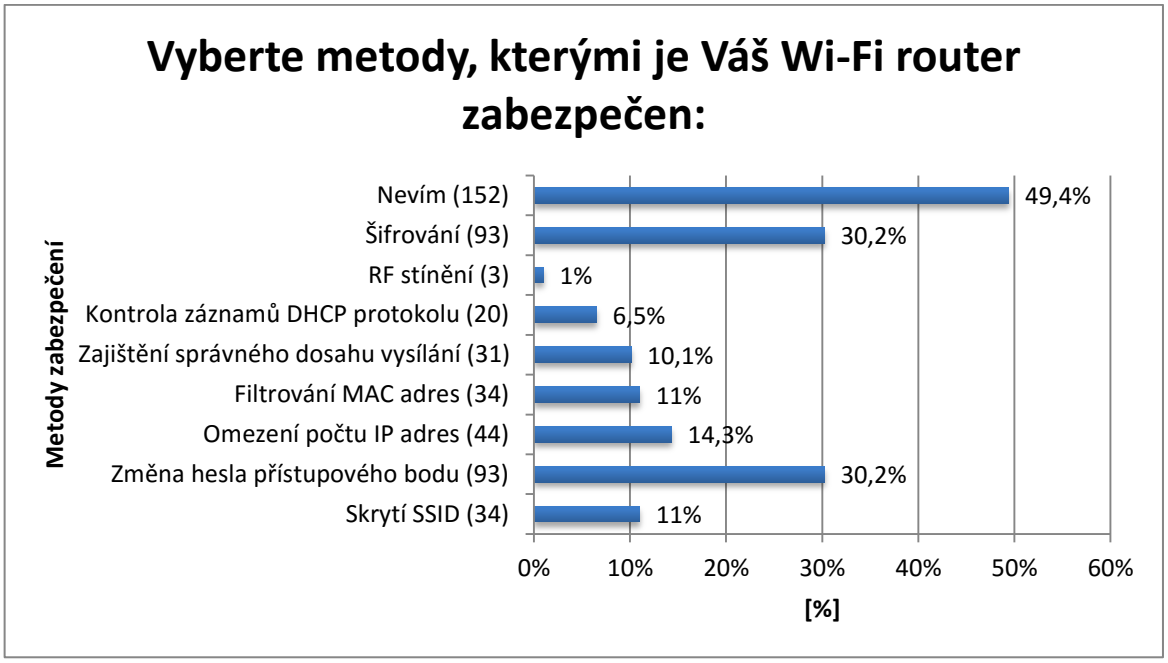
Graf 4. Nastavení Wi-Fi routeru

Následovala otázka, která zjišťovala, jestli uživatelé vědí, jak je jejich Wi-Fi router zabezpečen. Zde už byly výsledky o něco zajímavější, jelikož odpovědi byly téměř ve shodném poměru. Celých 51 % respondentů uvedlo, že nevědí, jak je jejich Wi-Fi router zabezpečen. Z toho plyne, že pokud je jejich Wi-Fi router špatně zabezpečen a oni o tom nevědí, tak mohou být nejvíce ohroženou skupinou. Výsledky jsou uvedeny v následujícím grafu (Graf 5. Zjištění povědomí o zabezpečení Wi-Fi routeru).



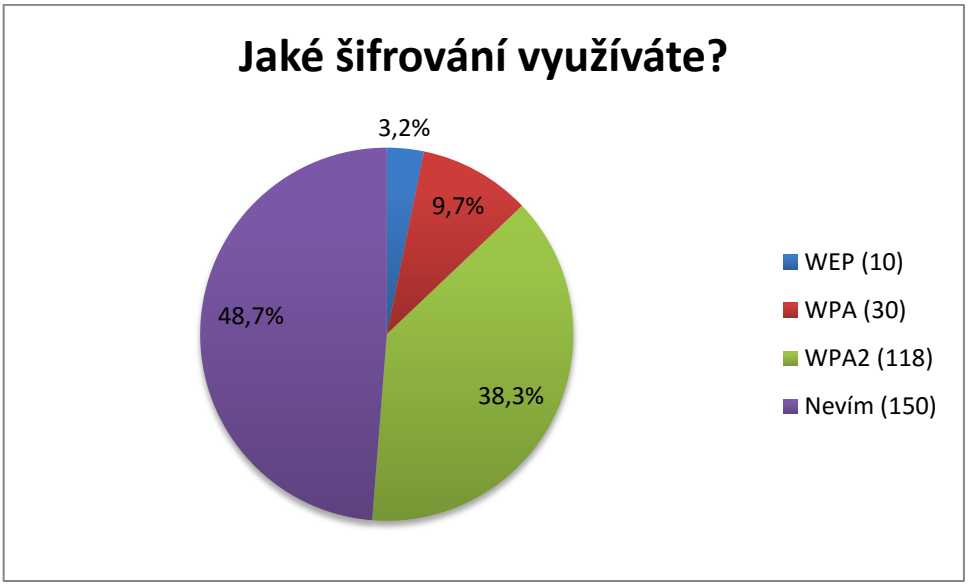
Graf 5. Zjištění povědomí o zabezpečení Wi-Fi routeru

Následovala otázka: Vyberte metody, kterými je Váš Wi-Fi router zabezpečen. Tato otázka byla zaměřena více do hloubky samotného problému. Respondenti zde měli vybrat jednotlivé metody, které využívají u zabezpečení jejich Wi-Fi routeru. Celých 49,4 % respondentů nevědí, jakými metodami je jejich Wi-Fi router zabezpečen, což se však shoduje s předchozí otázkou, kdy 51 % uvedlo, že nevědí, jak je jejich Wi-Fi router zabezpečen. Zbytek, který věděl, jaké zabezpečení využívají, uvedl, že nejvíce využívanou metodou je použití šifrování (30,2 %), což je naprostý základ zabezpečení. Stejný počet také využívá možnost změny hesla samotného přístupového bodu, což patří také mezi první kroky, které jsou nutné udělat pro správné zabezpečení. Následovali odpovědi, které zahrnují zbytek možností zabezpečení, avšak zcela nejnižší zastoupení má metoda RF stínění, která je však poměrně finančně náročnější a také se ani běžně nevyužívá v domácích podmínkách. Podrobnější výsledky jsou vyobrazeny v následujícím grafu (Graf 6. Využívané metody zabezpečení Wi-Fi routeru).



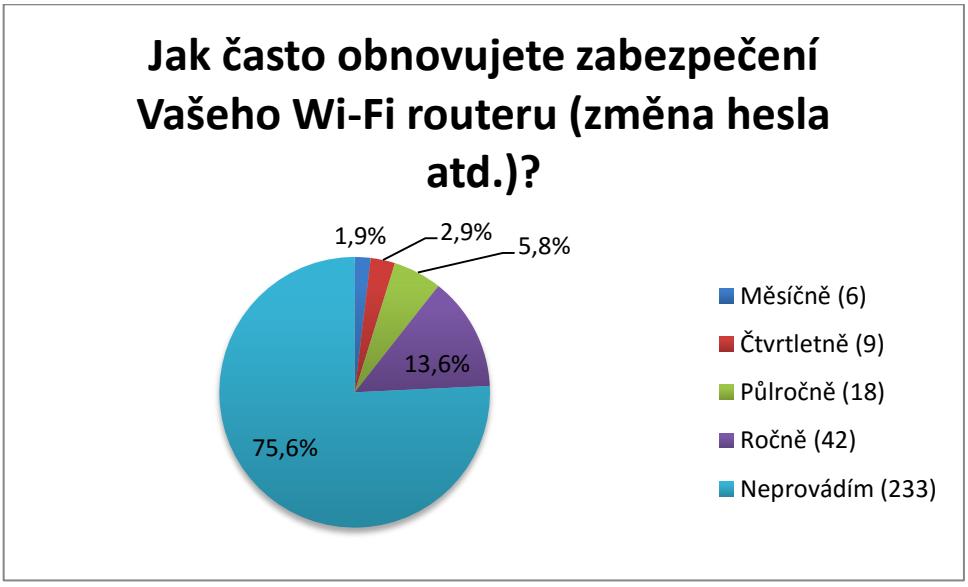
Graf 6. Využívané metody zabezpečení Wi-Fi routeru

Jak je již výše zmíněno, tak šifrování je, dalo by se říci, samotným základem pro zabezpečení Wi-Fi routeru a také samotné komunikace. Proto následující otázka měla za úkol zjistit, jaký typ šifrování využívají, jelikož jak je psáno již v teoretické části, tak ne všechny metody jsou dnes bezpečné. Nejvíce nebezpečnou možností je dnes WEP, tuto odpověď zvolilo pouze 3,2 % respondentů, avšak lze vidět, že stále jsou uživatelé využívající tuto možnost, která se v současné době nedoporučuje. O něco lepším typem zabezpečení je využití šifrování pomocí WPA, tuto odpověď zvolilo 9,7 % respondentů. Nejlepší možností, jak zabezpečit Wi-Fi router je však volba WPA2, tuto možnost zvolilo nejvíce respondentů z těch, kteří věděli, jaké šifrování využívají.



Graf 7. Využívaná metoda šifrování

Závěrem této části byla otázka, zaměřena na dobu obnovování zabezpečení Wi-Fi routeru. Většina respondentů (75,6 %) uvedla, že obnovu zabezpečení neprovádí vůbec. To je dáno zřejmě tím, že někteří nevědí, jak je jejich Wi-Fi router zabezpečen, natož aby prováděli změny. Pouze 13,6 % uživatelů provádí nějaké změny alespoň 1x za rok. Zbytek respondentů jsou spíše výjimky. Ti provádějí obnovu zabezpečení s kratším intervalem než je jednou za půl roku, což je samozřejmě v současné době vhodné. Výsledky jsou zobrazeny v následujícím grafu (Graf 8. Doba obnovení zabezpečení).

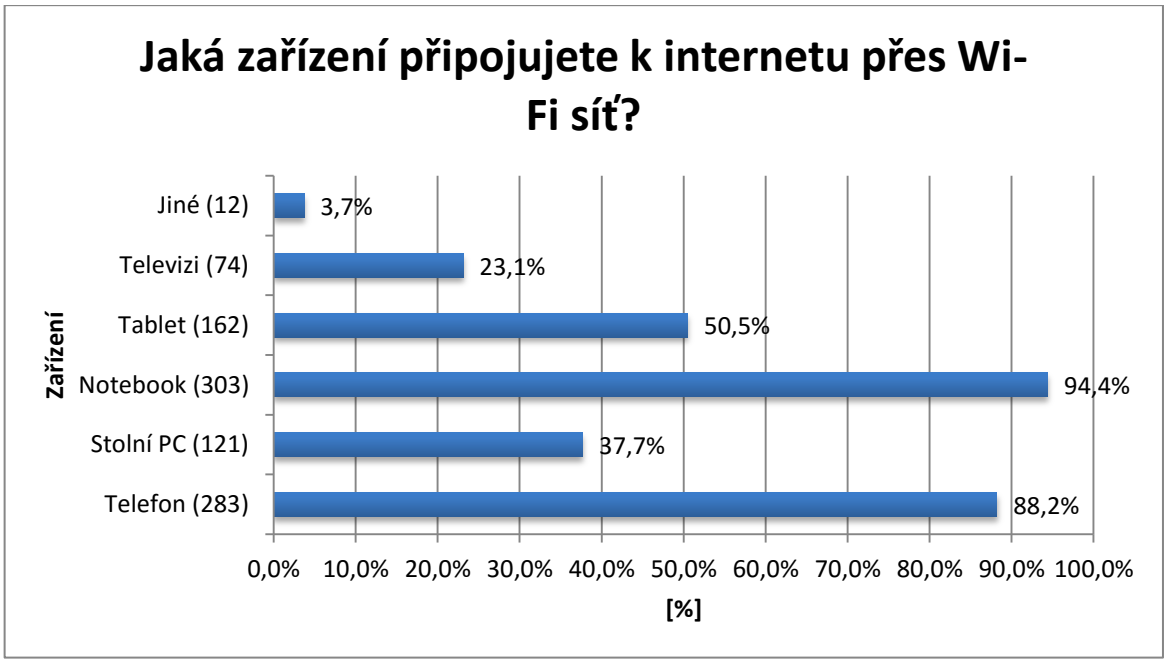


Graf 8. Doba obnovení zabezpečení

Využívané služby na Wi-Fi sítích

Další a zároveň poslední část ankety se zabývala zjištěním, co jednotliví uživatelé na Wi-Fi sítích dělají a jaké služby využívají. Na tuto část celkem odpovědělo 321 respondentů.

Smyslem první otázky této části byla snaha zjistit, jaké zařízení uživatelé nejčastěji připojují k bezdrátovým Wi-Fi sítím. Nikoho však nepřekvapí, že nejvyšší počet respondentů připojuje k bezdrátovým sítím notebook (94,4 %) a mobilní telefon (88,2 %). Následuje tablet (50,5 %) a stolní počítače (37,7 %). Mírným překvapením je však počet uživatelů, kteří připojují k bezdrátové sítí televizory, jedná se o 23,1 % uživatelů. Jedná se však o trend, který je v současné době stále oblíbenější. Podrobnější výsledky jsou v následujícím grafu (Graf 9. Zařízení připojované k Wi-Fi).

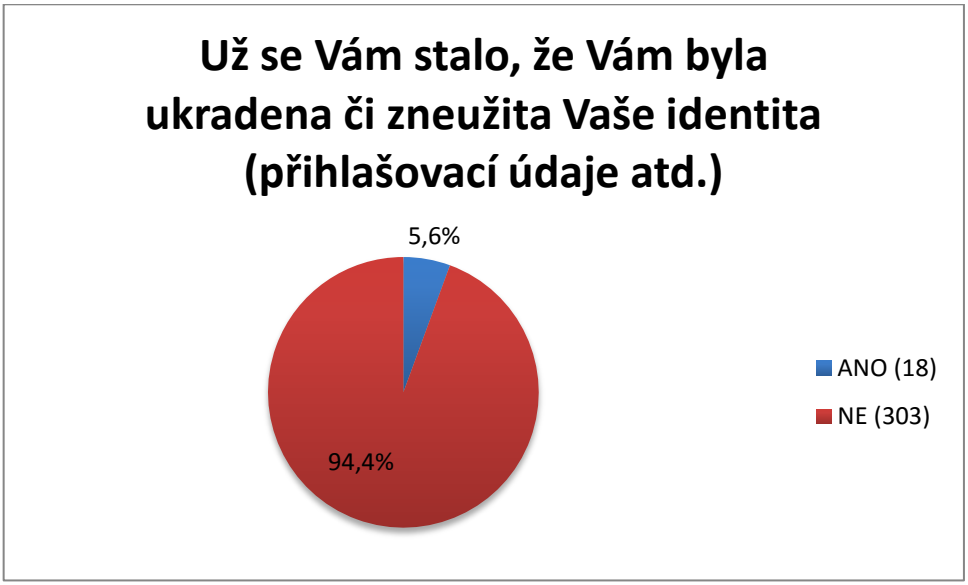


Graf 9. Zařízení připojované k Wi-Fi

Jelikož je celá práce zaměřena na zabezpečení bezdrátových Wi-Fi sítí, tak následující otázka měla za úkol zjistit, jestli uživatelé mají povědomí nebo jestli už slyšeli o nějakých hrozbách, které mohou na těchto sítích hrozit. Překvapivě se ukázalo, že většina respondentů (61,7 %) neslyšela o těchto hrozbách. Pouhých 123 (38,3 %) respondentů o hrozbách slyšelo. Avšak je nutné, aby uživatelé věděli, jaká rizika jsou ve spojení s bezdrátovými Wi-Fi sítěmi, aby těmto rizikům mohli předcházet.

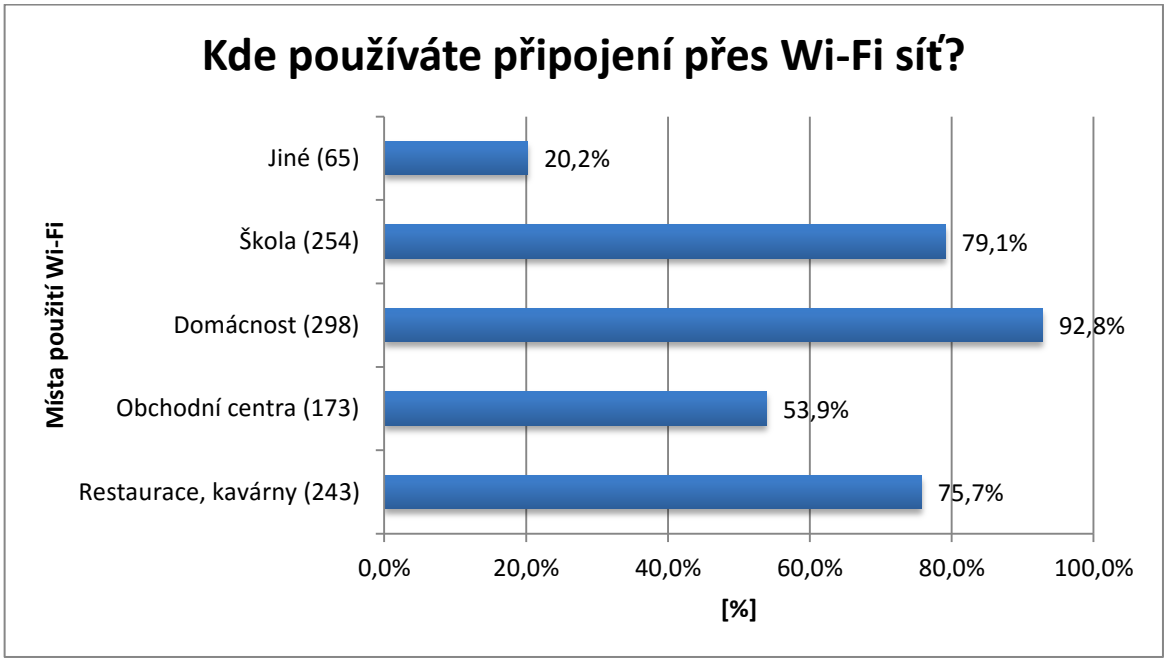
Graf 10. Znalost hrozeb

Jelikož není příliš složité dostat se do bezdrátových sítí, a už vůbec ne do veřejných bezdrátových sítí, tak většina útočníků se snaží získat důležité informace, které by mohli následně zneužít. Na to byla zaměřena další otázka, která zjišťovala, jestli někomu z respondentů již byla ukradena a následně zneužita jeho identita. Celých 5,6 % odpovědělo, že ano, avšak toto číslo může být ve výsledku ještě vyšší, jelikož někteří uživatele se o zneužití identity nemusí ani dozvědět.



Graf 11. Ztráta identity

Nejvíce nebezpečné sítě jsou ty mimo domov a především veřejné hotspoty. Na to byla zaměřena tato otázka, která zjišťovala, kde se všude uživatelé připojují. Z výsledků zle vyčíst, že nejvíce se uživatelé připojují k domácím sítím (92,8 %), avšak hned za ní následovali školní sítě (79,1 %), následně restaurace a kavárny (75,7 %) a také obchodní centra (53,9 %). Poslední dvě možnosti připojení jsou zřejmě nejnebezpečnější, jelikož na těchto sítích se může pohybovat kdokoliv a nikdy nevíme, jestli se na síti nepohybuje případný útočník.



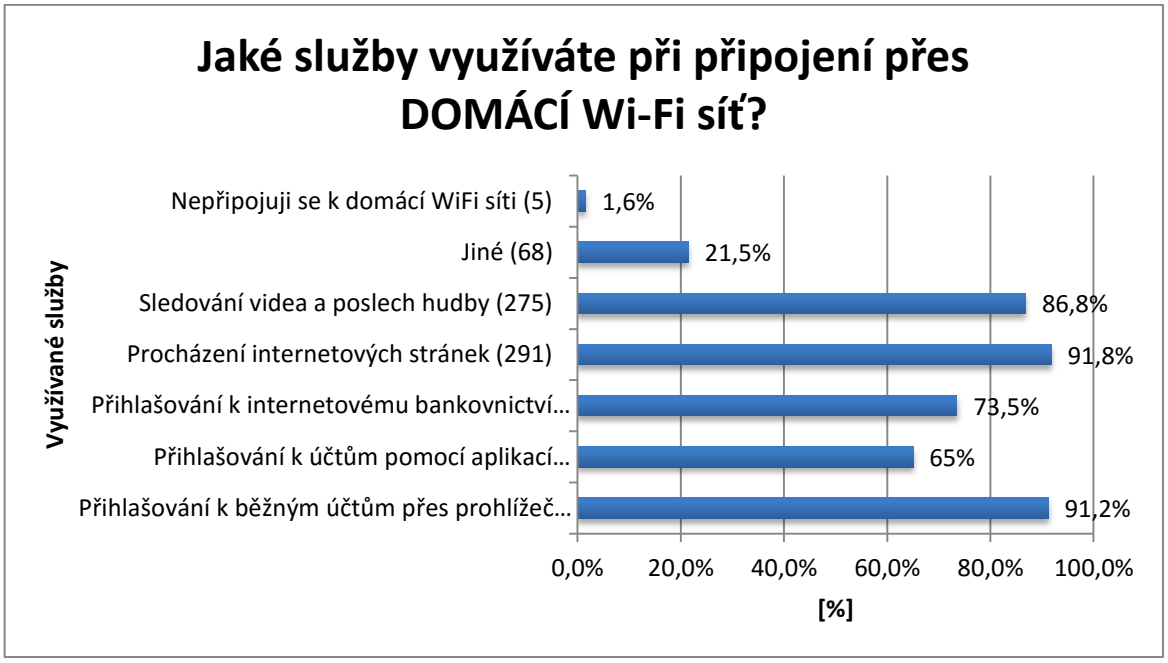
Graf 12. Místa využívání Wi-Fi

Jelikož je velký rozdíl, jestli se uživatelé připojují doma nebo na jiných a veřejných sítích, tak bylo důležité zjistit, jestli sledují, jak jsou jednotlivé sítě, ke kterým se připojují, zabezpečeny. Převažující většina (60,7 %) uvedla, že toto nesledují. Je to dáno zřejmě tím, jak z předchozích otázek plyne, že většina lidí neví, jak má vypadat správné zabezpečení.

Graf 13. Kontrola připojení

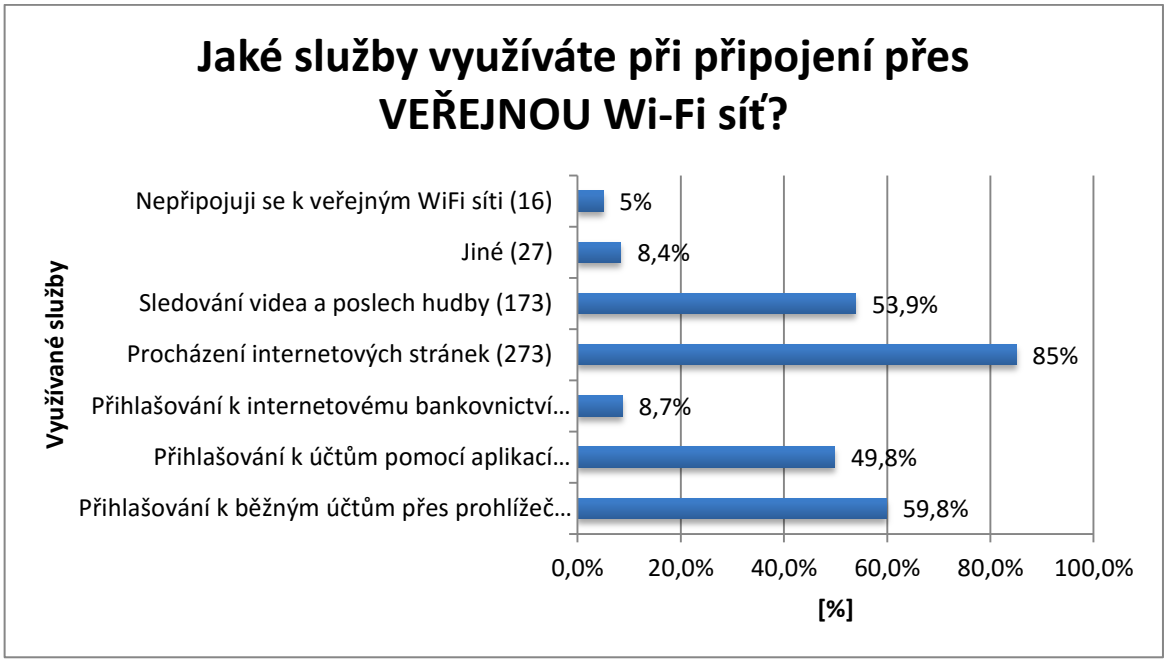
Závěrečné dvě otázky se snaží zjistit, co uživatelé na bezdrátových Wi-Fi sítích dělají a jaké služby nejčastěji využívají. Hlavní snahou bylo také zjistit, jestli uživatelé využívají rozdílné služby v závislosti, jestli jsou připojeni na domácích Wi-Fi sítích nebo na veřejných Wi-Fi sítích. Výsledný rozdíl je docela viditelný.

Na domácích Wi-Fi sítích uživatelé využívají rovnoměrně veškeré služby, drobné rozdíly jsou pouze v tom, jestli k přihlašování k účtům využívají přímo aplikace k tomu určené nebo webový prohlížeč. To je dáno především závislostí, jestli se uživatel přihlašuje přes telefon a tablet, kde se většinou využívají právě aplikace, nebo přes počítač nebo notebook kde se využívá více prohlížeč. Samozřejmě nejvíce lidé využívají internetový prohlížeč k procházení webu (91,8 %), přihlašovaní k různým účtům (91,2 %) a také sledují videa nebo poslouchají hudbu. Je dobré se také zaměřit na přihlašování k internetovému bankovnictví, to dělá na domácí síti téměř 73,5 % uživatelů.



Graf 14. Služby využívané na domácí Wi-Fi síti

V případě využívaných služeb na veřejných sítích jsou výsledky jiné. Uživatelé stále využívají nejvíce tento typ sítí k procházení webových stránek (85 %), avšak co se týče připojování k různým typům účtů, tak jsou zde respondenti poněkud opatrnější a těchto služeb zde využívá o téměř 30 % méně uživatelů. V případě nejrizikovějšího účtu, a to tedy internetového bankovnictví, kleslo jeho využívání na veřejných sítích téměř o 65 % na 8,7 %. Lze tedy usoudit, že uživatelé si uvědomují možnosti hrozeb a jsou tedy opatrnější.



Graf 15. Služby využívané na veřejných Wi-Fi sítích

6.4 Závěrečné zhodnocení výsledků

Anketa měla za úkol zjistit celkové povědomí uživatelů o bezpečnosti na bezdrátových Wi-Fi sítích. Vzhledem k dostatečnému počtu respondentů, bylo možné zjistit veškeré potřebné informace a díky nim bylo možné zpracovat jednotlivé výsledky.

První část ankety se zabývala zjištěním základních charakteristik respondentů. Jednalo se o pohlaví, věk a nejvyšší dosažené vzdělání. Ze zpracovaných výsledků je jasně vidět, že anketu vyplňoval především vysoký počet studentů s nejčastěji dokončeným vysokoškolským vzděláním. Bylo to dáno tím, že anketa byla primárně rozeslána mezi studenty. Avšak anketu vyplnily i jiné věkové kategorie a respondenti s jiným než jen vysokoškolským vzděláním. To bylo díky tomu, že anketa byla vyvěšena na různých skupinách, kde mohl na anketu odpovídat kdokoliv.

Po charakteristických otázkách respondentů následovala rozhodovací otázka, která zjišťovala, jestli respondenti využívají připojení pomocí Wi-Fi sítě. Nebylo tedy žádným překvapením, že valná většina tento typ připojení využívá a proto pokračovali dále v anketě v dalších otázkách.

Další část se zabývala zjištěním, na jaké úrovní mají respondenti zabezpečen jejich domácí Wi-Fi router, a jak se v jednotlivých metodách orientují. Ze zpracovaných výsledků je

možno vidět, že více jak polovina respondentů neví, jak je jejich Wi-Fi router zabezpečen, z toho plyne, že tím pádem si většina uživatelů ani neuvědomuje, jaké rizika jim na síti hrozí. Avšak je i spousta takových, kteří tomu nerozumí a raději svěřili veškeré bezpečnostní nastavení do rukou známých nebo specializovaných pracovníků. Uživatelé, kteří věděli, jak je jejich Wi-Fi router zabezpečen, tak v mnoha případech volili pro zabezpečení routeru pouze ty základní metody jeho zabezpečení.

Poslední část se zabývala zjištěním, jaká zařízení respondenti nejčastěji připojují k Wi-Fi sítím a také co na různých typech sítí dělají a jaké využívají služby. Nejvíce respondentů k Wi-Fi sítím připojuje notebooky, mobilní telefony a tablety. Mírným překvapením bylo, že téměř každý čtvrtý respondent připojuje k Wi-Fi televizory. Vzhledem k rozšířenosti Wi-Fi sítí, lze z výsledků vidět, že lidé se připojují opravdu všude. Samozřejmě nejvíce lidí využívá domácího připojení, ale také mezi velice rozšířená místa patří restaurace, kavárny, školy a v neposlední řadě také obchodní centra. Přesto, že většina uživatelů nesleduje, o jaké připojení se jedná a jak je zabezpečeno, tak si nejspíše uvědomují, že jim může něco na určitých typech sítí hrozit. Jelikož z výsledků plynou znatelné rozdíly v tom, co lidé dělají na domácích Wi-Fi sítích a co na veřejných.

7 PROLOMENÍ ZABEZPEČENÍ WEP

V této kapitole bude provedena praktická realizace útoku na bezdrátovou Wi-Fi síť se zabezpečením WEP. Cílem bude získat heslo, které slouží pro přístup do sítě. Součástí tohoto útoku bude vyhodnocení časové náročnosti na získání hesla.

7.1 Potřebné vybavení

Pro realizaci útoku na bezdrátovou síť bylo použito následující vybavení.

HP ProBook 4545s

Útok na bezdrátovou síť byl proveden z notebooku HP ProBook 4545s.

Tab. 10. Konfigurace HP ProBook 4545s

Název	HP ProBook 4545s (H5K12EA#BCM)
Instalovaný procesor	AMD A4-4300M (2.50/3.00 GHz, 1 MB LLC, Dual-Core)
RAM (MB)	4096 DDR3-1600 (1x4096)
HDD (GB)	500 (Hitachi HTS545050A7E380, 5400rpm, 8MB cache)
DVD	DVD SuperMulti DL (hp DVDRAM UJ8D1)
LCD	15,6" TFT (matný)
LCD rozlišení	HD (1366 x 768)
Video	AMD Radeon HD7420G
LAN	10/100/1000 (Realtek RTL8168/8111 PCIe Gigabit Ethernet)
Wi-Fi	Ralink RT3290 802.11bgn (a/b/g/n)
Zvuková karta	IDT HD Audio
Polohovací zařízení	touchpad (Synaptics)
Software	Windows 10 (64bit, CZ)
Baterie/výdrž	Li-Ion 47 Wh / 7h 27min
Rozhraní	2x audio IN/OUT, SD/MMC/MS, 2x USB 3.0, 2x USB 2.0, VGA, HDMI
Rozměry	373 x 255 x 30-35 mm
Hmotnost (kg)	2,59

Obr. 16. HP ProBook 4545s

Wi-Fi router TP-Link TL-WR543G

Wi-Fi router byl použit pro vytvoření bezdrátové Wi-Fi sítě se zabezpečením WEP. Na tuto síť byly následně prováděny útoky.

Tab. 11. TP-Link TL-WR543G

Název	TP-Link TL-WR543G
Maximální rychlost	54 Mb/s
LAN	4 ×
WAN	1×
Počet antén	1×
Zisk antény	5 dBi
Další parametry	Odnímatelná anténa
Funkce	Router, Klient
Standardy	802.11b (2,4 GHz), 802.11g (2,4 GHz)

Obr. 17. TP-Link TL-WR543G

Wi-Fi USB adaptér TP-Link TL-WN722N

Vzhledem k tomu, že Wi-Fi karta v notebooku neumožňuje přepnutí do monitorovacího režimu, tak bylo nutné použít tento Wi-Fi USB adaptér, který tuto funkci umožňuje. Jedná se o bezdrátový Wi-Fi adaptér, který se připojuje do USB portu v počítači nebo notebooku.

Tab. 12. TP-Link TL-WN722N

Název	TP-Link TL-WN722N
Podporované standardy	IEEE 802,11n IEEE 802,11g IEEE 802,11b
Přenosové rychlosti	11n: až 150 Mb/s 11g: až 54 Mb/s 11b: až 11 Mb/s
Frekvenční rozsah	2,4 - 2,4835 GHz
Bezdrátový vysílací výkon	20 dBm
Podporované pracovní módy	Ad-Hoc Infrastructure
Bezpečnost	WEP, WPA/ WPA2, WPA-PSK/ WPA2-PSK (TKIP/AES), filtrování MAC
Rozhraní	USB 2.0
Rozměry	93,5 x 26 x 11 mm

Obr. 18. TP-Link TL-WN722N

Linux BackTrack 5R3

Linuxová distribuce BackTrack slouží především k penetračnímu testování a pomáhá tak posuzovat zranitelnost jednotlivých systémů. Součástí této distribuce je spousta nástrojů, které slouží právě pro jednotlivé možnosti zjištění rizik. Tato linuxová distribuce v žádném případě neslouží k tomu, aby se s ní škodilo, ale výhradně k penetračnímu testování a zjišťování slabin v systému. Výhodou této distribuce je, že není nutné ji instalovat, ale lze ji nabootovat jako LiveDVD nebo přes USB flash disk.

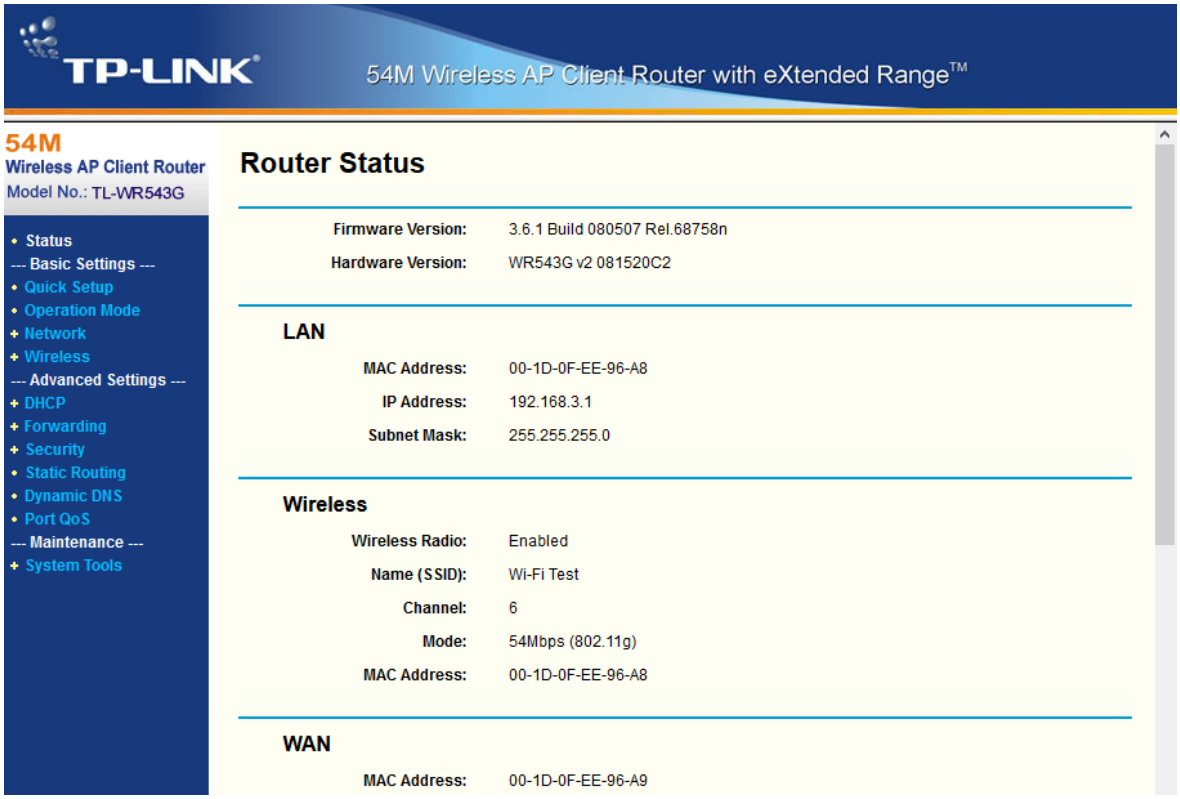
Obr. 19. Linux BackTrack 5R3

7.2 Vytvoření sítě

Pro vytvoření sítě byl použit Wi-Fi router TP-LINK TL-WR543G, který umožňuje využít zabezpečení WEP s možností délky klíče 64 bitů, 128 bitů a 152 bitů. Pro realizaci útoku byly využity první dvě délky klíčů, jelikož použitý USB Wi-Fi adaptér nepodporuje délku klíče 152 bitů. Každá délka klíče byla využita dvakrát v závislosti na složitosti hesla.

Vstup do nastavení Wi-Fi routeru

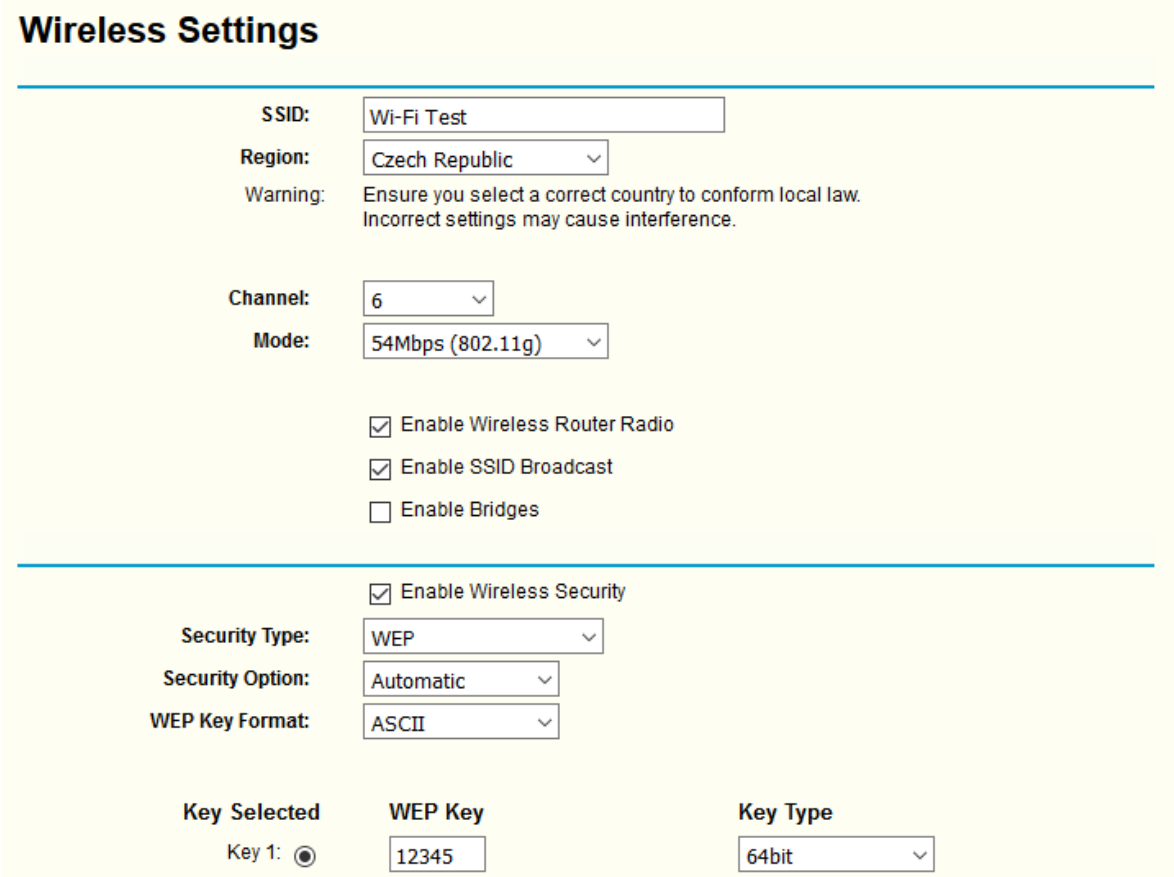
Jako první bylo potřeba se dostat do samotného nastavení Wi-Fi routeru, aby bylo možné dále zprovoznit a nastavit bezdrátovou síť. Přes webový prohlížeč byla do řádku adres vložena IP adresa routeru, kde po zadání přihlašovacích údajů byl umožněn vstup do nastavení Wi-Fi routeru.



Obr. 20. Úvodní obrazovka Wi-Fi routeru

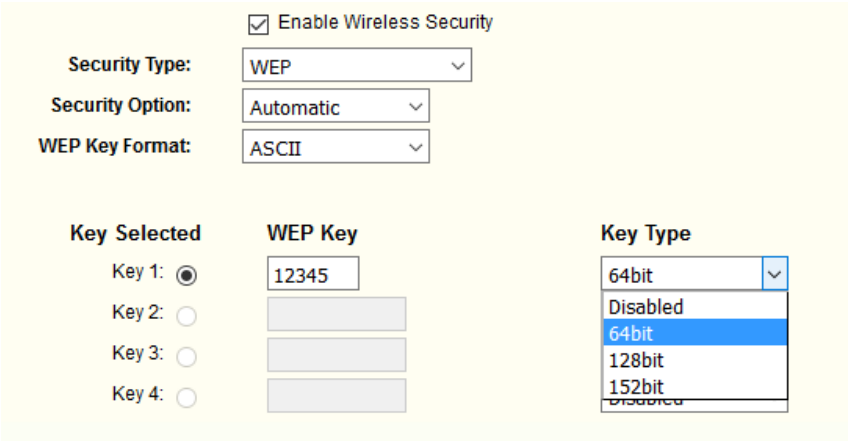
Nastavení bezdrátové sítě

Nyní bylo zapotřebí zprovoznit a nastavit parametry bezdrátové sítě. Z úvodní obrazovky se přes položku Wireless přešlo do samotného nastavení bezdrátové sítě, kde jako první došlo k jejímu pojmenování pomocí SSID. Jako název sítě byl zvolen Wi-Fi Test. V dalším kroku bylo možné nastavit kanál, na kterém síť bude provozována a mód sítě. Tyto parametry zůstaly nezměněny, jelikož nemají vliv na cíl této práce. Jako typ zabezpečení byl vybrán WEP a formát klíče byl zvolen v ASCII kódu.



Obr. 21. Nastavení bezdrátového sítě

Co se týče samotného hesla neboli klíče, tak pro první pokus byla zvolena délka klíče 64 bitů a klíč byl: 12345. Pro zjištění časové náročnosti na prolomení klíče se jeho délka a náročnost postupně měnila. Ostatní nastavení zůstalo neměnné.



Obr. 22. Nastavení zabezpečení bezdrátové sítě

7.3 Útok na bezdrátovou síť

Pro samotný útok na vytvořenou bezdrátovou síť byla využita Linuxová distribuce Back-Track ve verzi 5R3.

Změna MAC adresy zařízení

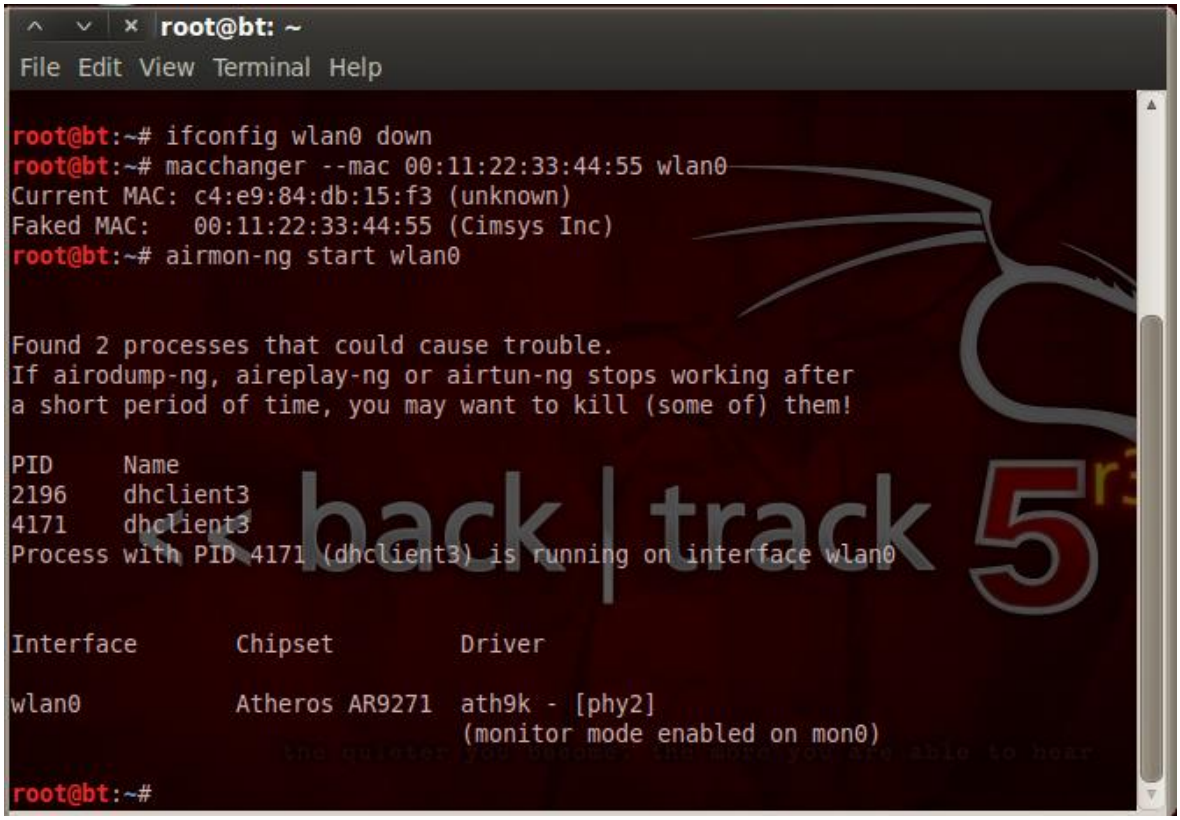
Nejprve bylo nutné zjistit název síťového zařízení, přes které byl útok prováděn. Pomocí příkazu ***iwconfig*** došlo k výpisu těchto rozhraní. Aby bylo možné změnit původní MAC adresu, bylo zapotřebí nejprve vypnout připojené síťové rozhraní pomocí příkazu ***ifconfig wlan0 down***. Následně bylo možné změnit původní MAC adresu na jakoukoli jinou. Pro lepší pochopení byla zvolena adresa 00:11:22:33:44:55 přes příkaz ***macchanger --mac 00:11:22:33:44:55 wlan0.***

Obr. 23. Změna MAC adresy

Monitorovací režim a výběr cíle pro útok

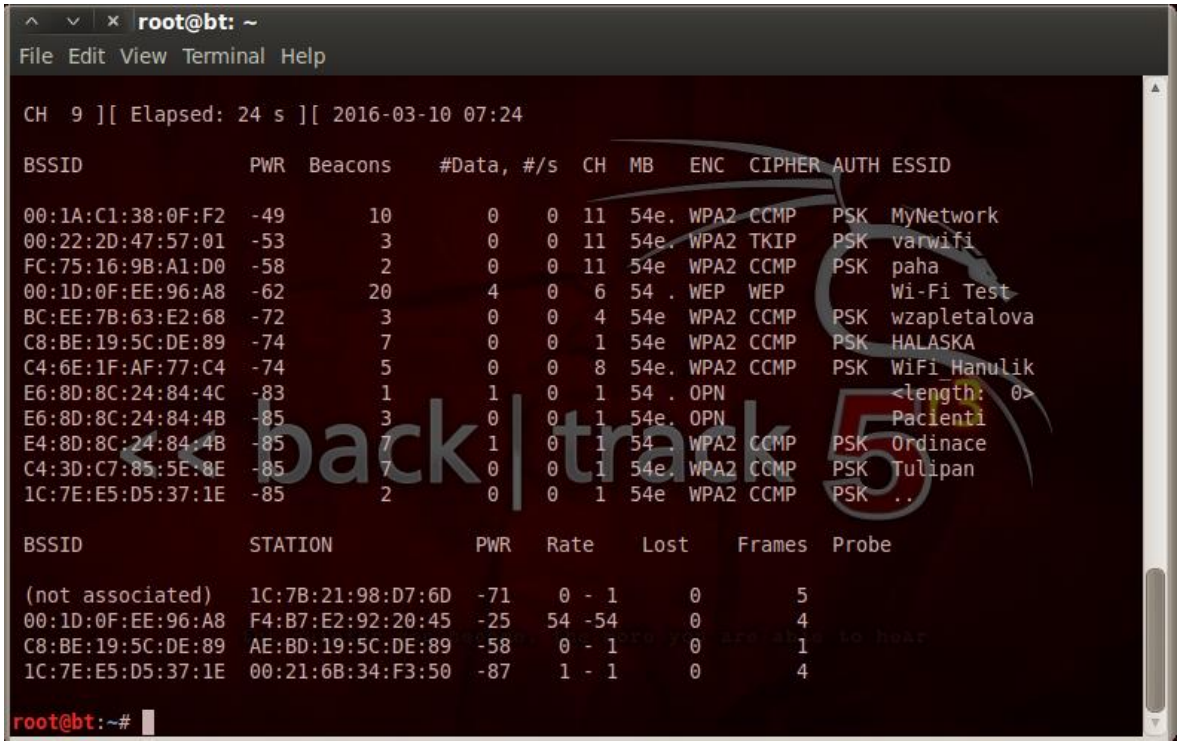
Součástí distribuce BackTrack je software airodump-ng, který umožňuje zjistit a sledovat provoz bezdrátových sítí v dosahu. Nejprve však bylo nutné přepnout síťové zařízení do

monitorovacího režimu. To se stalo díky příkazu ***airmon-ng start wlan0*** a softwaru airmon-ng, který je taktéž součástí distribuce BackTrack. Jak je možné vidět na obrázku (Obr. 24. Zapnutí monitorovacího režimu), došlo k vytvoření virtuálního zařízení mon0.



Obr. 24. Zapnutí monitorovacího režimu

Po přepnutí síťového rozhraní do monitorovacího režimu bylo možné zobrazit veškeré bezdrátové sítě v dosahu pomocí příkazu ***airodump-ng mon0***. Z výpisu je možné vidět jednotlivé sítě, kanály, na kterých pracují a především typ zabezpečení. Jako čtvrtou je možné vidět uměle vytvořenou síť Wi-Fi Test, na kterou byl útok proveden.



Obr. 25. Výpis dostupných bezdrátových sítí

Spuštění monitorování a zachytávání inicializačních vektorů

Po výběru sítě, na který byl útok prováděn, bylo zahájeno zachytávání a ukládání paketů, které jsou důležité pro následné rozluštění hesla. K tomu sloužil příkaz ***airodump-ng --ivs -w test –c 6 --bssid 00:1D:0F:EE:96:A8 mon0***, kde:

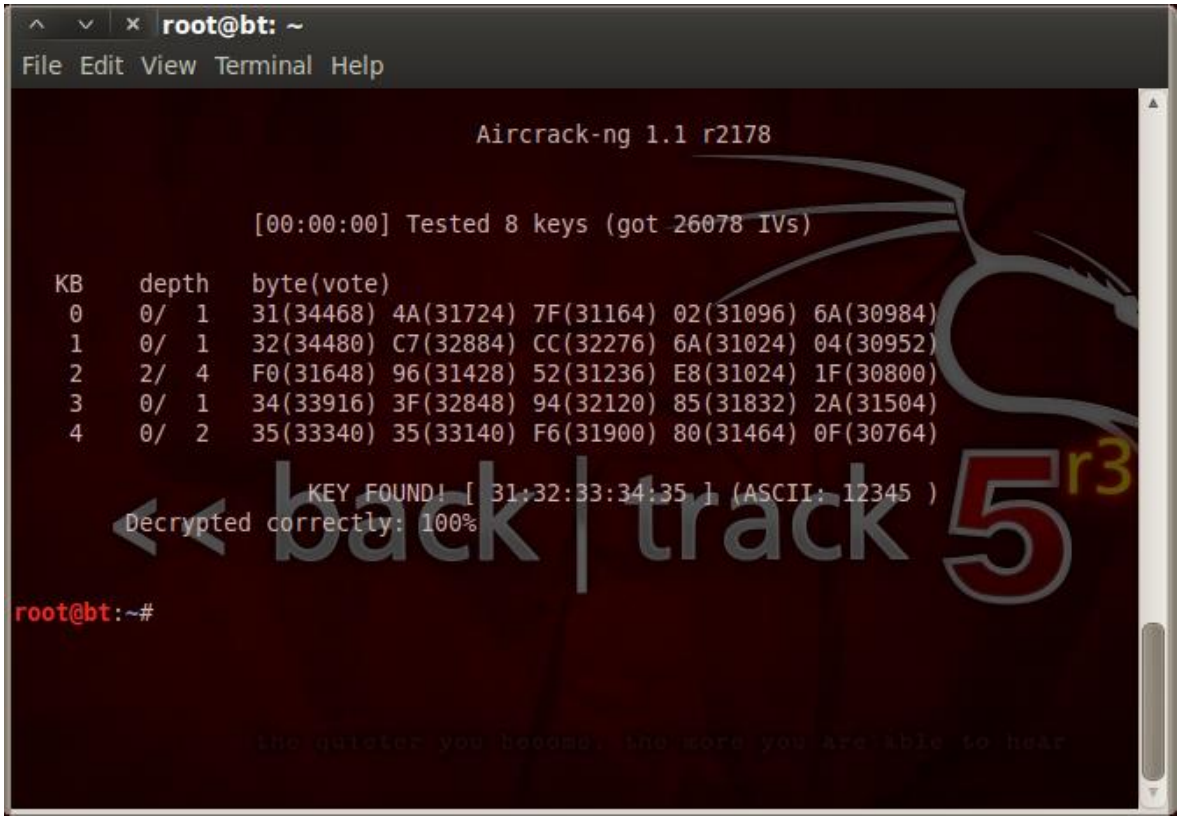
- --ivs je parametr sloužící pro zaznamenávání pouze inicializačních vektorů (IV),
- -w test je název souboru, do kterého se jednotlivé IV zapisují,
- -c je parametr, který definuje kanál, které dané zařízení využívá (v tomto případě jde o kanál číslo 6),
- --bssid parametr zajištující, že se budou zapisovat pouze IV vysílané z daného zařízení pod MAC adresou 00:1D:0F:EE:96:A8 (MAC adresa testovacího Wi-Fi routeru),
- mon0 je pouze určení rozhraní, které bude provádět zaznamenávání.

Obr. 26. Monitorování zvolené sítě

Po provedení příkazu popsaného výše je spuštěno zachytávání komunikace, které lze vidět na obrázku (Obr. 26. Monitorování zvolené sítě). Nejdůležitější je sloupeček #Data, který udává počet zachycených inicializačních vektorů.

Zjištění klíče

Po zachycení dostatečného množství IV byl zahájen pokus o zjištění klíče. To se dělo v nově otevřeném příkazovém řádku, kde pomocí příkazu ***aircrack-ng test-01.ivs*** bylo zahájeno luštění klíče. Celý proces luštění netrval ani vteřinu a klíč byl úspěšně zjištěn.



Obr. 27. Zjištění WEP klíče

7.4 Výsledky a jejich zhodnocení

Jak je možné vidět, tak zjištění klíče a vlastně prolomení tohoto typu zabezpečení není vůbec složité a díky správným nástrojům a postupům lze tento útok provést v relativně krátkém čase. Je nutné dodat, že pro zachycení inicializačních vektorů je zapotřebí, aby na síti byl nějaký provoz. V opačném případě, kdy by nedocházelo k žádné komunikaci, by nebylo možné nasbírat dostatečné množství inicializačních vektorů a následně by nebylo možné ani zahájit luštění klíče.

Pro tuto realizaci byl provoz na síti zajištěn stahováním objemného souboru, kde průměrná rychlost stahování byla 20,7 Mb/s. Dalo by se říci, že takový případ by byl pro útočníka zcela ideální, avšak je nutné počítat s tím, že pokud bude uživatel sítě pouze procházet internetové stránky a občas si přečte email, tak toto zachytávání může trvat klidně i celý den.

Dalším důležitým parametrem je počet zachycených inicializačních vektorů. Pokud dojde k zachycení malého počtu, tak klíč nemusí být rozluštěn, avšak nejde nikdy s jistotou říci,

jaký počet zachycených IV je dostačující. Navíc se zvyšující se délkou klíče roste také počet potřebných zachycených IV. Pro tuto realizaci a měření byly zvoleny následující minimální hodnoty potřebných IV, které jsou plně dostačující pro zjištění klíče.

Tab. 13. Délky klíčů a počet IV

Délka klíče [bit]	Počet potřebných IV
64	25 000
128	100 000

Pro zjištění časových závislostí prolomení klíče byl útok na síť opakován a to se změnou délky klíčů a složitosti jednotlivých klíčů. Naměřené hodnoty jsou uvedeny v následující tabulce.

Tab. 14. Naměřené hodnoty

Délka klíče [bit]	Klíč	Počet stažených IV	Otestovaných klíčů	Čas pro stažení potřebného množství IV [min:s]	Čas prolomení [min:s]	Čas celkem [min:s]
64	12345	26078	8	00:45	00:00	00:45
64	@H=1j	25715	467	00:52	00:01	00:53
128	0123456789012	100960	1454131	03.24	00:03	03:27
128	A@9=*w-V/<P?+	101322	20545	02:53	00:01	02:54

Z tabulky (Tab. 14. Naměřené hodnoty) jde vidět, že celkový čas útoku na síť je závislý především na použité délce klíče. To je dáno tím, že čím je větší délka klíče, tím je potřeba zajistit více inicializačních vektorů. Avšak hlavní roli zde nehraje čas samotného prolomení a získání klíče, ale potřebný čas pro stažení potřebného množství inicializačních vektorů. Tento čas je závislý na provozu, který se odehrává na síti, avšak pro toto měření byl použit a zajištěn téměř konstantní provoz po celou dobu útoků. Z naměřených hodnot vyplývá, že složitost hesla nemá téměř žádný vliv na celkový čas prolomení. Je to dáno tím,

že pro samotné rozluštění klíče není zapotřebí nijak extra výkonný počítač a tento útok se dá v současné době realizovat téměř na každém počítači. Čas prolomení je tedy závislý na dostatečném počtu stažených inicializačních vektorů a následně na počtu otestovaných klíčů. Čím více klíčů je potřeba otestovat, tím více času to zabere, i když naměřené hodnoty prolomení klíče jsou spíše zanedbatelné. V neposlední řadě zde hraje roli také štěstí, které se naskýtá při sledování inicializačních vektorů, jelikož pokud dochází k častým kolizím IV, tak mnohdy stačí i menší množství jejich zachycení, než bylo pro toto měření zvoleno, avšak tyto kolize jsou zcela náhodné a nelze je předem ovlivnit.

ZÁVĚR

První kapitola diplomové práce je věnována historii vzniku bezdrátových sítí. Počátky a postupný vývoj byly základem pro vznik bezdrátových Wi-Fi sítí, jaké jsou známy dnes. Jsou zde popsány milníky, které měly základní vliv na vývoj a také jsou v práci zmíněny první způsoby uplatnění bezdrátových sítí. I přesto, že začátky nebyly vůbec jednoduché, tak v současné době jsou tyto sítě díky vyspělým technologiím na dobré úrovni a jsou běžnou součástí každodenního moderního života.

Další kapitola se zabývá základním popisem bezdrátové technologie Wi-Fi. Vzhledem k tomu, že Wi-Fi síť je v současné době velice oblíbená a rozšířená, tak je důležité znát základní pojmy a princip činnosti. Vzhledem k tomu, že pod pojmem bezdrátových sítí je možné si dnes představit mnoho různých technologií, je dobré vědět, kde se vzal samotný název a technologie Wi-Fi, které se diplomová práce primárně věnuje. V práci byly zmíněny i základní topologie sítí, což jsou způsoby propojení, které jsou důležité při vytváření sítí. Poslední část této kapitoly byla věnována frekvencím, které jsou vyčleněny a využívány právě bezdrátovou Wi-Fi technologií.

Jak už ze samotné historie vyplývá, tak hlavní překážkou plnohodnotného fungování této bezdrátové sítě byla neexistence všeobecných pravidel, které by stanovovaly základní způsob činnosti. Avšak dnes správnou činnost zajišťují standardy, které musejí být dodržovány. Těmto standardům a jejich doplňkům se věnovala právě třetí kapitola, kde byly popsány jednotlivé doplňky se zaměřením na rychlost, modulace a využívané frekvence.

Čtvrtá kapitola se blíže zabývala metodami pokrytí, možnostmi zlepšení a rozšíření signálu. Také více popisovala přenosové rychlosti a především hlavní vlivy, které mohou výslednou rychlost razantně ovlivnit. V neposlední řadě se kapitola více věnovala modulacím, které slouží k přenosu dat a jsou využívány jednotlivými doplňky standardů.

I přes bezesporné množství výhod má bezdrátová Wi-Fi technologie i své nevýhody. Největším úskalím je bezpečnost těchto sítí. Právě bezpečnosti byla věnována poslední kapitola teoretické části, která se skládala ze dvou podkapitol. První podkapitola se zabývala možnostmi přístupu do sítě včetně popisu komunikace mezi klientem a přístupovým bodem. Druhá podkapitola byla věnována jednotlivým způsobům zabezpečení, které byly postupně popsány.

Hlavní snahou diplomové práce bylo zjistit informace o povědomí uživatelů o bezpečnosti této bezdrátové Wi-Fi technologie a také zhodnotit jejich chování a znalosti. Proto byla vytvořena anketa, která byla rozeslána mezi jednotlivé uživatele a také umístěna na různých stránkách tak, aby na ni mohli respondenti odpovídat. Na základě získaných informací byly zpracovány výsledky a následně popsány a prezentovány v praktické části.

Součástí praktické části byla také praktická ukázka prolomení konkrétní metody zabezpečení. Jednalo se o zabezpečení pomocí šifrovacího protokolu WEP, kde cílem bylo získat heslo do sítě. Získání hesla bylo opakováno se změnou složitosti hesla a délky klíče. Výsledkem také bylo zhodnocení časové náročnosti na získání hesla.

SEZNAM POUŽITÉ LITERATURY

[1] HOLT, Alan a Chi-Yu HUANG. 802.11 wireless networks: security and analysis. New York: Springer, c2010, xxi, 212 p. ISBN 978-1-84996-274-2.

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

[3] KÁLLAY, Fedor a Peter PENIAK. *Počítačové sítě a jejich aplikace: LAN / MAN / WAN*. 2. aktualiz. vyd. Praha: Grada, 2003, 356 s. ISBN 80-247-0545-1.

[4] DAVIS, Harold. *Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě: není zapotřebí žádných předchozích zkušeností!*. 1. vyd. Praha: Grada, 2006, 334 s. Průvodce (Grada). ISBN 80-247-1421-3.

[5] Who We Are . *WiFi Alliance.* [online]. 2016 [cit. 2016-01-27]. Dostupné z: *http://www.wi-fi.org/who-we-are*

[6] Certification. *WiFi Alliance.* [online]. 2016 [cit. 2016-01-27]. Dostupné z: *http://www.wi-fi.org/certification*

[7] ZANDL, Patrick. *Bezdrátové sítě WiFi: praktický průvodce : jak vybrat hardware a anténu, realizace a bezpečnost sítí WiFi, podpora WiFi v operačních systémech*. Vyd. 1. Brno: Computer Press, 2003, x, 190 s. ISBN 80-7226-632-2.

[8] KÖHRE, Thomas. *Stavíme si bezdrátovou síť Wi-Fi*. Vyd. 1. Brno: Computer Press, 2004, 294 s. ISBN 80-251-0391-9.

[9] Využívání vymezených rádiových kmitočtů. *Český telekomunikační úřad* [online]. 2016 [cit. 2016-02-02]. Dostupné z: http://www.ctu.cz/vyuzivani-vymezenych-radiovych-kmitoctu

[10] Základní přehled standardů IEEE 802.11. *Eprin* [online]. 2009 [cit. 2016-02-02]. Dostupné z: http://www.eprin.cz/zakladni-prehled.html

[11] PROKOP, Mirek. Wi-Fi: Jak si zajistit velké pokrytí, rychlost a silný signál: Wi-Fi standardy, nastavení kanálů, rozšíření rozsahu. *Živě.cz* [online]. 2014 [cit.

2016-02-02]. Dostupné z: http://www.zive.cz/clanky/wi-fi-jak-si-zajistit-velke-pokryti-a-silny-signal/sc-3-a-172347/default.aspx

[12] Přehled standardů IEEE 802.11. *Blog o internetovém připojení, wifi, antény, VoIP, Mikrotik návod manuál.* [online]. 2.1.2008 [cit. 2016-02-12]. Dostupné z: *http://mb.optimax.cz/2008/01/02/wirelless/prehled-standardu-ieee-80211/*

[13] Moderní WiFi, standard 802.11ac. *VAHAL*. [online]. 1.6.2015 [cit. 2016-02-12]. Dostupné z: *http://www.vahal.cz/o-firme/clanky/moderni-wifi-standard-802-11ac.html*

[14] OTÝPKA, Miloslav. OFDM - ortogonální multiplex s frekvenčním dělením. *Coptel: Internetový portál* [online]. Coptel, 2010 [cit. 2016-02-18]. Dostupné z: http://coptel.coptkm.cz/index.php?action=2&doc=7981&docGroup=147&cmd=0&instance=1

[15] PROKOP, Mirek. Wi-Fi: Jak si zajistit velké pokrytí, rychlost a silný signál. *Živě.cz* [online]. Živě.cz, 2014 [cit. 2016-02-18]. Dostupné z: http://www.zive.cz/clanky/wi-fi-jak-si-zajistit-velke-pokryti-a-silny-signal/sc-3-a-172347/default.aspx

[16] PETROWSKI, Thorsten. *Bezpečí na internetu: pro všechny*. Vyd. 1. Liberec: Dialog, 2014, 243 s. Tajemství (Dialog). ISBN 978-80-7424-066-9.

[17] LEXA, Jaroslav. Tapety blokující Wi-Fi signál. *PC TUNING* [online]. 2012 [cit. 2016-03-07]. Dostupné z: http://pctuning.tyden.cz/index.php?option=com_content&view=article&id=24054&catid=1&Itemid=57

[18] OREBAUGH, Angela. *Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí*. Vyd. 1. Brno: Computer Press, 2008, 444 s. ISBN 978-80-251-2048-4.

[19] KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488s. ISBN 978-80-251-2236-5.

[20] HAINES, Brad a Tim KRAMER. Seven deadliest wireless technologies attacks. Boston: Syngress/Elsevier, c2010, xvi, 122 p. ISBN 978-1-59749-541-7.

[21] LUKÁŠ, Luděk a kol. *Bezpečnostní technologie, systémy a management V*. 1. vydání. Zlín: Radim Bačuvčík - VeRBuM, 2015, 368 s. ISBN 978-80-87500-67-5.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
BSS	Basic Service Set
CRC	Cyclic Redundancy Check
DSSS	Direct Sequence Spread Spectrum
ESS	Extended Service Set
FHSS	Frequency Hopping Spread Spectrum
GPRS	General Packet Radio Service
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
MAC	Media Access Control
MIMO	Multiple-input multiple-output
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PSK	Pre Shared Key
QAM	Quadrature Amplitude Modulation
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
UMTS	Universal Mobile Telecommunication System
USB	Universal Serial Bus
WDS	Wireless Distribution System
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity

WLAN Wireless Local Area Network

WPA Wi-Fi Protected Access

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: ANKETA

1. ***Pohlaví?***

- Muž
- Žena

2. ***Věk?***

- Méně jak 18
- 18-25
- 26-35
- 36-50
- 51-64
- 65 a více

3. ***Nejvyšší dosažené vzdělání?***

- Základní
- Vyučen
- Vyučen s maturitou
- Středoškolské
- Vysokoškolské

4. ***Využíváte připojení pomocí Wi-Fi?***

- ANO *(pokračování následující otázkou číslo 5)*
- NE *(konec ankety)*

5. ***Máte doma Wi-Fi router?***

- ANO *(pokračování následující otázkou číslo 6)*
- NE *(pokračování otázkou číslo 11)*

6. ***Kdo Vám nastavil Váš Wi-Fi router?***

- Specializovaný pracovník (např. Provider)

- Sám/Sama
- Známý, rodina, …
- Nevím, o tyto věci se nestarám

7. Víte, jak je Váš Wi-Fi router zabezpečen?

- ANO
- NE

8. Vyberte metody, kterými je Váš Wi-Fi router zabezpečen:

- Skryti SSID
- Změna hesla přístupového bodu
- Omezení počtu IP adres
- Filtrování MAC adres
- Zajištění správného dosahu vysílání
- Kontrola záznamů DHCP protokolu
- RF stínění
- Šifrování
- Nevím

9. Jaké šifrování využíváte?

- WEP
- WPA
- WPA2
- Nevím

10. Jak často obnovujete zabezpečení Vašeho Wi-Fi routeru (změna hesla atd.)?

- Měsíčně
- Čtvrtletně
- Půlročně
- Ročně
- Neprovádím

11. Jaká zařízení připojujete k internetu přes Wi-Fi síť?

- Telefon
- Stolní PC
- Notebook
- Tablet
- Televizi
- Jiné

12. Slyšel/a jste někdy o nějakých hrozbách, které mohou hrozit při připojení přes Wi-Fi?

- ANO
- NE

13. V případě, že jste slyšel/a o nějakých hrozbách, napište prosím, o jaké hrozby se jednalo:

14. Už se Vám stalo, že Vám byla ukradena či zneužita Vaše identita (přihlašovací údaje atd.)?

- ANO
- NE

15. Kde používáte připojení přes Wi-Fi síť?

- Restaurace, kavárny
- Obchodní centra
- Domácnost
- Škola
- Jiné

16. Pokud se připojujete mimo domov, sledujete, o jaké připojení se jedná a jaké má zabezpečení?

- ANO

- NE

17. Jaké služby využíváte při připojení přes DOMÁCÍ Wi-Fi síť?

- Přihlašování k běžným účtům přes prohlížeč (facebook, email ...)
- Přihlašování k účtům pomocí aplikací (facebook, email...)
- Přihlašování k internetovému bankovnictví
- Procházení internetových stránek
- Sledování videa a poslech hudby
- Jiné
- Nepřipojuji se k domácí Wi-Fi síti

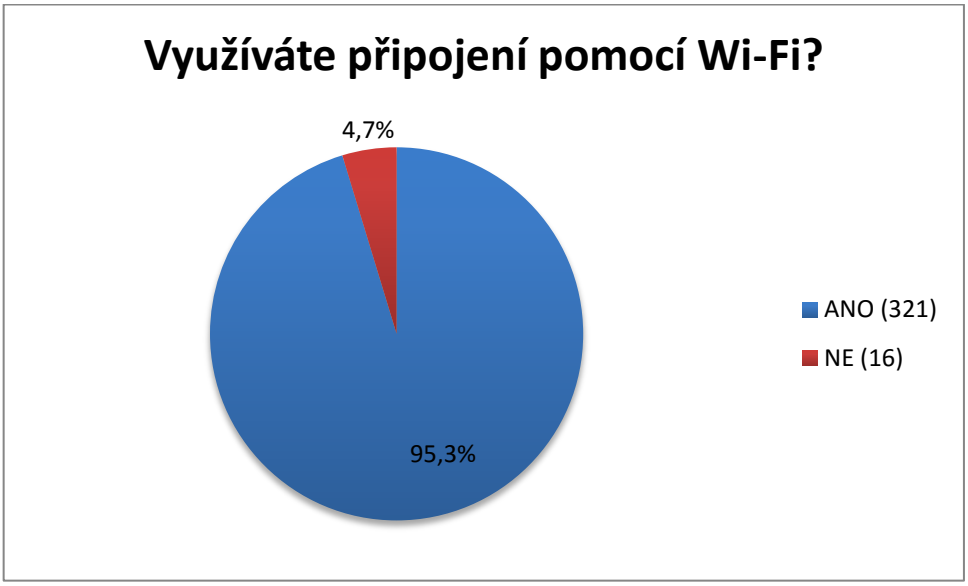
18. Jaké služby využíváte při připojení přes VEŘEJNOU Wi-Fi síť?

- Přihlašování k běžným účtům přes prohlížeč (facebook, email ...)
- Přihlašování k účtům pomocí aplikací (facebook, email...)
- Přihlašování k internetovému bankovnictví
- Procházení internetových stránek
- Sledování videa a poslech hudby
- Jiné
- Nepřipojuji se k veřejným Wi-Fi sítím

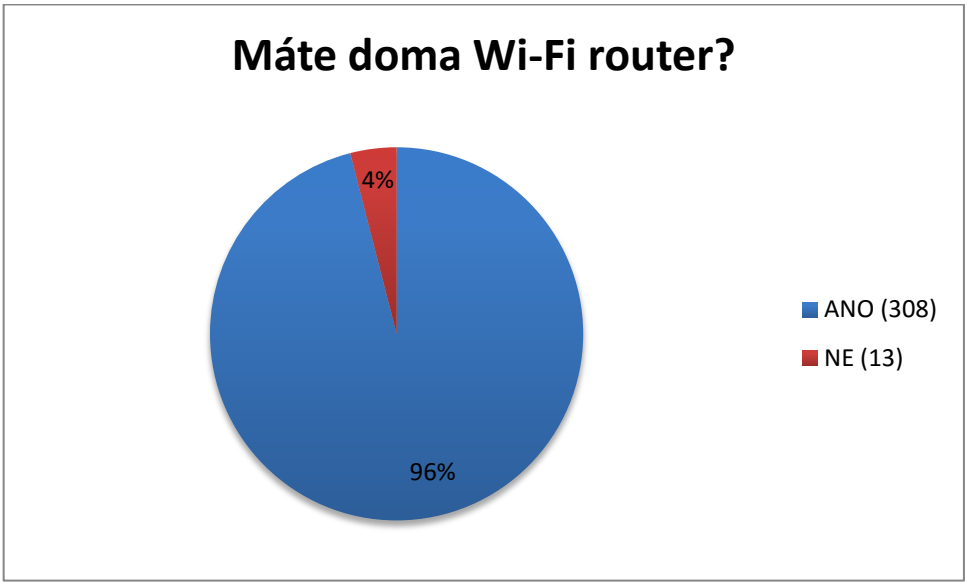
19. Máte nějaké připomínky k této anketě nebo se chcete podělit o nějakou vlastní zkušenost?

PŘÍLOHA P II: NEVYUŽITÉ GRAFY

Níže jsou uvedeny grafy, které nebyly použity v praktické části.



P II. Graf 16. Uživatelé využívající Wi-Fi připojení



P II. Graf 17. Uživatelé mající doma Wi-Fi router