Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Analýza bezpečnostních mechanismů Wi-Fi sítí

Bakalářská práce

Michal Prokeš

Školitel: Ing. Petr Břehovský

České Budějovice 2012

Bibliografické údaje:

Prokeš Michal, 2012: Analýza bezpečnostních mechanismů Wi-Fi sítí.
[Analysis of Wi-Fi network security mechanisms. Bc. Thesis, in Czech.] - 57 p.
Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Annotation:

The goal of this thesis is to analyze the most commonly used mechanisms for secure operation of computer networks and Wi-Fi transmitters. The analysis will be a real testing of different methods and at the end will be made an overview and comparison of individual tests. In addition, the power output of each device will be also tested, depending on the security methods.

Anotace**:**

Úkolem této bakalářské práce je analyzovat nejčastěji používané mechanismy pro zabezpečení provozu počítačových sítí a Wi-Fi vysílačů. Analýza bude probíhat reálným testováním jednotlivých metod, na jehož konci bude zpracovaný přehled a porovnání jednotlivých testů. Dále se také bude testovat potřebný výkon jednotlivých zařízení v závislosti na zabezpečovacích metodách.

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

23. dubna 2012

Podpis

Poděkování

Rád bych poděkoval svému školiteli Ing. Petru Břehovskému za odborné vedení této práce, za cenné rady, připomínky a poskytnutí podkladů pro tvorbu. Také bych rád poděkoval p. Ing. Jaroslavu Kothánkovi, Ph.D. za rady a konzultace v oblasti legislativních aspektů této práce, rodině a všem, kteří mi během studia jakkoliv pomohli.

Seznam obrázků

Seznam grafů

1. Úvod

Rozvoj počítačových sítí a bezdrátových technologií nám v dnešní době umožňuje přistupovat k internetu téměř odkudkoliv. Přes internet posíláme důležité dokumenty, provádíme citlivé operace (například obsluhujeme bankovní účty) a komunikujeme se všemi lidmi z našeho okolí.

Několik posledních let se v České republice velice rychle rozvíjí trend poskytování bezdrátového připojení k internetu, který umožňuje ve volně šiřitelných frekvencích 2,4Ghz a 5Ghz nabídnout velice zajímavou alternativu k ostatním druhům kabelového připojení. V odlehlých městech, obcích a vesnicích dokáže bezdrátové připojení nabídnout stejné, ne-li lepší podmínky, než někteří poskytovatelé internetu ve větších městech. Právě díky tomuto faktu jsou bezdrátové sítě velice oblíbené. Zásadní problematikou ale je zabezpečení takové sítě, která musí odolat útokům z vnějšího prostředí a zároveň ochránit uživatelská data proti odchytu a odposlechu uvnitř sítě.

Cílem této práce je na základě praktického testování popsat, analyzovat a vyhodnotit nejlepší možné řešení pro zabezpečení bezdrátových sítí a to jak v rozsahu většího poskytovatele internetu, tak na úrovni malé lokální sítě. Testování bude probíhat na nejčastěji používaných zařízeních, která jsou v dnešní době dostupná.

2. Výběr komponent

Výběr komponent je pro tuto práci velice důležitý. Jednotlivá zařízení musí poskytnout dostatečný výkon, aby bylo možno vyzkoušet jednotlivé metody popsané dále, včetně jejich možných kombinací. Pokud bude některé zařízení během testování na hranici svého možného výkonu, mohou být výsledky tímto faktem zkreslené. Pro dostatečné množství informací o dostupných zařízeních a jejich četnosti prodeje, bylo dotázáno několik společností, které se zabývají distribucí a prodejem Wi-Fi zařízení pro volně šiřitelné frekvence 2,4 a 5Ghz. Jak je patrné z elektronické korespondence[1], všechny společnosti se shodují na tom, že díky cenové dostupnosti jsou v dnešní době nejoblíbenější produkty od firem Mikrotik, Ubiquiti a TP-Link.

Pro zjištění podrobnějších informací o využívání těchto zařízení byla kontaktována společnost, která se zabývá přímo poskytováním bezdrátového připojení k internetu. Z elektronické korespondence[2] je tedy vidět, že zařízení jsou opravdu velice rozšířená a mají své uplatnění.

Pro potřeby testování byla vybrána následující zařízení:

- RouterBoard RB800 (v určitých fázích testování bylo zařízení doplněno o miniPCI Wi-Fi kartu CM9)
- Ubiquiti NanoStation M5
- Ubiquiti NanoStation 5
- Ubiquiti NanoStation 5 Loco
- Ubiquiti Bullet 5

RouterBoard RB800

Jedno z nejvýkonnějších zařízení od Litevské firmy Mikrotik, které disponuje následujícími vlastnostmi[3]:

- Procesor PowerPC 800Mhz
- Operační paměť 256MB DDR2
- 3x nezávislé gigabit ethernet porty
- 4x nezávislé miniPCI porty umožňující připojení podporovaných bezdrátových karet

[1] Příloha č. 1: Elektronická korespondence se společnostmi i4wifi a.s a Aspa a.s.
[2] Příloha č. 2: Elektronická korespondence se společností Inet4 s.r.o.
[3] Převzato z oficiálních stránek společnosti MikrotTik. Zdroj: http://routerboard.com/RB800

- Operační systém RouterOS

Toto zařízení je možné obsluhovat několika způsoby. Pro jednodušší konfiguraci je možné využít základní webovou administraci, která je v továrním nastavení vždy dostupná na adrese "http://ip_zarizeni:80/webfig". Pro potřeby složitější konfigurace je možné využití Secure Shell protokolu, který je dostupný na IP adrese zařízení, na portu 22. Je však poměrně nepřehledný a vyžaduje dobrou znalost práce s terminálem a také stromové struktury systému. Jako nejoptimálnější řešení se tedy jeví možnost obsluhy přes program WinBox, který umožňuje připojení k jakémukoliv zařízení s operačním systémem RouterOS a je obsažen ve všech zařízeních RouterBoard. Tento program umožňuje v přehledném grafickém rozhraní[4] správu a konfiguraci systému. Během testování však bylo objeveno několik drobností, které je možné nastavit pouze přes příkazový terminál systému nebo přes Secure Shell protokol. Toto řešení se také ukázalo jako poměrně nebezpečné v určitých variantách konfigurace.

Zařízení Ubiquiti

Zařízení od tohoto výrobce jsou oblíbená především díky jejich velice příznivé pořizovací ceně, jednoúčelovému využití, snadné montáži a především díky jednoduché konfiguraci, která je dostupná přes webové rozhraní na IP adrese zařízení. Po přihlášení do zařízení se zobrazí velice jednoduché a přehledné prostředí, které umožňuje v několika krocích nastavit zařízení do plně funkčního stavu. Díky tomu se snižují i náklady na udržení odbornosti koncových techniků instalačních firem, neboť konfigurace těchto zařízení vyžaduje pouze základní znalosti počítačových sítí a Wi-Fi technologií.

Zařízení TP-Link

Bezdrátové prvky od společnosti TP-Link jsou svým charakterem a možnostmi určeny spíše pro využití v domácnosti. Plní zde roli hlavně jako domácí Access Pointy a zařízení pro routování a překlad adres (NAT). Pro tuto práci tedy nebudou využity.

2.1 Zařízení pro tvorbu přístupového bodu (Access Pointu)

Možností tohoto operačního módu disponují všechna zařízení a také se všechna zařízení v určitých částech jako Access Point používají.

[4] Příloha č. 3: Grafické rozhraní programu WinBox pro konfiguraci zařízení Mikrotik

Použití RouterBoardu RB800 jako přístupového bodu:

K tomu aby mohlo být toto zařízení využito jako přístupový bod, je nutné osadit ho bezdrátovými miniPCI kartami (lze připojit až čtyři). Tím vznikne možnost vytvoření až čtyř oddělených vysílacích bodů, které je možné nastavit na vysílací frekvence 2,4Ghz nebo 5Ghz.

Ke konfiguraci zařízení bude použit program WinBox. Po jeho otevření se zobrazí okno[5], ve kterém je možné zadání IP adresy zařízení, uživatelského jména, hesla, možnost přidání názvu zařízení a jeho uložení do seznamu. Bezprostředně vedle řádku pro zadání adresy se nachází tlačítko, po jehož kliknutí se rozbalí dialogové okno[6], ve kterém jsou zobrazena všechna zařízení se systémem RouterOS, která se nacházejí ve stejné síti jako počítač. Kromě fyzické MAC adresy jsou v tomto okně také zobrazené informace o verzi systému. Výhodou tohoto programu je také fakt, že dokáže se zařízením, které je ve stejné podsíti, komunikovat pouze prostřednictvím MAC adresy. V továrním nastavení jsou všechna zařízení dodávána bez přednastavené IP adresy a díky tomu je jistota, že nově přidané zařízení nebude kolidovat s čímkoliv jiným v síti. Po vybrání testovacího zařízení je potřeba vyplnit uživatelské jméno a heslo (v továrním nastavení žádné není) a poté je možné připojení k zařízení. V úvodním okně[7] otevřené konfigurace je vidět přehledné menu na levé straně. Pro nastavení bezdrátové miniPCI karty do módu AP je nutné otevřít záložku Wireless. Pokud je do zařízení vložena podporovaná karta, bude vidět v okně aplikace nový interface s názvem wlan1. Po rozkliknutí tohoto rozhraní se otevře okno s několika záložkami, ve kterých je možné upravit parametry bezdrátové sítě. Pro tuto práci bude důležitá pouze záložka Wireless, ve které se nastavují vysílací parametry sítě:

- Mode - operační mód karty. Možnosti nastavení - AP bridge, Station, Station bridge, Station pseudobridge, atd. Pro tuto práci bude potřeba pouze mód AP bridge
- Band - zde se nastavuje vysílací frekvence karty. Je možné nastavit jak pásmo 2Ghz (2Ghz-B, 2Ghz-B/G, 2Ghz-only-G) tak i pásmo 5Ghz (5Ghz-A, v novějších kartách také možnost 5Ghz-N). Pro tuto práci bude použit pouze mód 5Ghz-A.
- Frequency - konkrétní frekvence v jednotkách Mhz, ve které bude síť vysílat. Možnost výběru těchto frekvencí je vždy omezena daným státem, ve kterém zařízení funguje. Důvodem tohoto omezení je fakt, že každý stát využívá určité frekvence pro své vlastní účely - například meteorologické radary, vojenské radary atd. V současné době

[5] Příloha č. 4 – Úvodní okno programu WinBox po jeho otevření
[6] Příloha č. 5 – Okno programu WinBox s otevřeným dialogovým oknem a nalezeným zařízením
[7] Příloha č. 3 – Úvodní okno programu WinBox po připojení do zařízení

vysílají v České republice dva meteoradary[8] pásmu 5Ghz. Jeden v oblasti Skalky u Protivanova na frekvenci 5645 MHz a druhý v oblasti Brdy-Praha na frekvenci 5630 Mhz. Pro tuto práci byla po analýze prostředí vybrána frekvence 5520 Mhz.

- SSID - název sítě, který se bude zobrazovat při skenování sítí. Pro tuto práci byl zvolen název "test_bak".
- Security Profile - Slouží k zabezpečení sítě metodami WEP, WPA, Radius a EAP. Pro aplikaci některé z těchto metod je nutné vytvořit profil, ve kterém bude uvedený typ zabezpečení a jeho přesné nastavení. Profily se vytváří v úvodním okně Wireless, na poslední záložce Security Profiles. Zde je z továrního nastavení vytvořen profil "default", který však žádnou metodu neobsahuje. Pokud je tedy zvolen, bude síť vidět jako otevřená. Pro účely této práce byly vytvořeny tři profily, pro zabezpečení WEP, WPA-PSK (s časem aktualizace klíče TKIP 0:30) a WPA2-AES.
- Frequency mode - nastavení vysílacího výkonu karty a zohlednění země, ve které se zařízení nachází. V případě zvolení položky "manual txpower" má uživatel možnost nastavit zařízení libovolnou frekvenci a libovolný výkon karty, bez ohledu na platnou legislativu. Odpovědnost za provoz pak přebírá provozovatel zařízení. Pokud bude zvoleno "regulatory domain" budou volitelné frekvence a maximální výkon karty automaticky upravené dle platné legislativy daného státu. Vzhledem k minimální zarušenosti prostředí a potřeby minimálního výkonu karty byla pro tuto práci vybrána možnost "regulatory domain".
- Country - stát nebo oblast, ve které se zařízení nachází. V tomto případě "czech republic".
- Antenna Gain - výkon vysílací karty v jednotkách dBi. Pokud je ve Frequency mode zvolena možnost "regulatory domain", lze nastavit pouze rozsah určený pro daný region. V případě zvolení "manual txpower" je možné nastavit až maximální možný výkon, který vždy záleží na daném typu karty. V případě že je vyplněný údaj nula, vysílá zařízení nejvyšším možným povoleným výkonem. Vzhledem k tomu, že testování probíhalo ve vnitřních podmínkách na vzdálenosti maximálně několika metrů s přímou viditelností přijímačů na vysílač, bylo možné stažení vysílacího výkonu na úplné minimum, tedy 1dBi.

Předcházející údaje by měly dostačovat pro tvorbu Access Pointu v zařízení RB800. V případě, že je vysílač tvořen v oblasti, která je více zarušená nebo je v okolí větší množství bezdrátových sítí, může být nápomocna funkce všech zařízení se systémem RouterOS, která

[8] Podrobnosti o jednotlivých meteorologických stanicích v České republice. Zdroj: http://portal.chmi.cz

se jmenuje Frequency Usage. Nachází se v okně nastavení bezdrátových rozhraní. Po jejím otevření a spuštění tlačítkem Scan se zobrazí tabulka všech použitelných frekvencí a jejich využívanost v daném prostoru[9]. Pro zjištění okolních sítí je také možno použít funkce Scan, která zobrazí všechny dostupné sítě, včetně jejich frekvence a dalších doplňujících informací.

Použití zařízení NanoStation jako přístupového bodu

Uplatnění tohoto zařízení v konfiguraci Access Point je především na větších vysílacích bodech, kde je potřeba pokrýt rozsáhlejší oblast nebo poskytnout připojení většímu počtu uživatelů. Vzhledem k omezeným možnostem RouterBoardů v počtu možných bezdrátových sítí, figuruje zde toto zařízení pouze jako drátový router, který je doplněn o několik zařízení NanoStation v režimu AP.

Od distribuce prvních modelů těchto zařízení byla konfigurace možná pouze přes webový prohlížeč (oficiálně podporovaný je pouze Internet Explorer, ostatní prohlížeče nemusí fungovat korektně). Z továrního nastavení je ve všech zařízeních nastavená IP adresa 192.168.1.20 a webová administrace je dostupná na portu 80. Do jednotky je tedy možné přihlášení na adrese http://192.168.1.20/. Po zadání adresy vyzve prohlížeč k vyplnění přihlašovacích údajů, které jsou v základním nastavení "ubnt" (jak uživatelské jméno, tak heslo). Po přihlášení se zobrazí přehledová stránka[10], kde jsou vidět podrobnější informace o zařízení. Mezi nejdůležitější patří:

- Base Station SSID - Název sítě, ke které je zařízení připojeno nebo s jakým názvem vysílá (v závislosti na konfiguraci)
- TX a RX Rate - Maximální teoretická rychlost přenosu, která je ovlivněná použitou technologií (802.11a - 54Mbit/s, 802.11n - 300Mbit/s). Nejvyšší rychlost je vždy určena nejpomalejším zařízením, které je k vysílači připojené.
- Frequency, Channel - Frekvence, na které zařízení operuje. V módu klient se jedná o frekvenci vysílače, v režimu AP se jedná o frekvenci nastavenou v tomto zařízení. Zobrazený kanál je pouze numerickým vyjádřením dané frekvence.
- Antenna - Vzhledem k tomu, že všechna zařízení NanoStation v sobě mají integrovanou anténu, je možná změna polarizace antény pouze softwarově. V tomto řádku je zobrazeno aktuální nastavení polarizace.

[9] Příloha č. 6: Výsledky měření pomocí metody Frequency Usage
[10] Příloha č. 7: Úvodní stránka po přihlášení do zařízení NanoStation

- Transmit CCQ[11] - Hodnota v procentech, která zobrazuje, jak efektivně je využita maximální teoretická rychlost spoje.

Oproti původním zařízením NanoStation, jsou nové modely řady NanoStation M vylepšené o několik funkcí. Mezi ty nejzajímavější patří:

- Podpora standardu 802.11n v obou pásmech 2,4Ghz i 5Ghz. Díky dobré implementaci tohoto standardu je teoretická přenosová kapacita mezi zařízeními až 300Mbit/s. Vzhledem k faktu, že zařízení obsahuje pouze 100Mbit/s ethernetový port, je reálná rychlost průtoku dat limitována právě tímto prvkem. Avšak reálné testy ukazují[12], že při správné konfiguraci není problém dosáhnout reálného průtoku dat mezi zařízeními i 80Mbit/s fullduplex.
- Technologie AirMAX - TDMA[13] - Systém, který nachází využití především ve velice zarušených oblastech. Jeho princip je založen na rozdělení zařízení do priorit, podle kvality připojení k vysílači. Pokud bude na jeden Access Point připojeno několik zařízení s vynikajícím signálem a dobrou hodnotou CCQ, technologie AirMAX se postará o to, aby je nebrzdili klienti s horším signálem nebo propustností dat.
- Přístup přes zabezpečené Secure Shell rozhraní - Stejně jako je možné přistupovat do zařízení se systémem RouterOS přes protokol SSH, je tato možnost dostupná i v novějších NanoStationech ze série N. Systém je zde také členěn do stromové struktury, jeho rozdělení však více odpovídá webové administraci a díky tomu je přehlednější a jednodušší na ovládání.

Díky těmto vlastnostem nacházejí NanoStationy čím dál tím větší uplatnění jako zařízení pro oba konce přenosu, tedy jak pro vysílač AP, tak pro koncové klienty.

Nastavení zařízení NanoStation do módu Access Point je o poznání jednodušší než u zařízení RouterBoard. Pokud se nebude uvažovat problematika IP adresace zařízení, nachází se veškeré potřebné nastavení v záložce Wireless[14]. Popsání všech potřebných parametrů je uvedeno výše u zařízení RouterBoard, proto v této části budou popsány pouze body, které je nutné nastavit pro správnou funkci. Část Basic Wireless Settings:

- Wireless mode - Access Point

[11] Definice hodnoty a její funkce: http://wiki.mikrotik.com/wiki/Manual:Wireless_FAQ
[12] Příloha č. 8: Měření rychlosti mezi zařízeními NanoStation M5
[13] Definice a přesný popis fungování technologie AirMax: http://i4wifi.blog.cz/1102/tipy-ubiquiti-jak-pracuje-airmax
[14] Příloha č. 9: Možnosti nastavení bezdrátové části zařízení NanoStation

- ESSID - název vysílané sítě
- Country code - Czech republic
- IEEE 802.11 Mode - A (pro 802.11a - 54Mbit/s v pásmu 5GHz) nebo N (pro 802.11n - 300Mbit/s v pásmu 5Ghz i 2,4Ghz)
- Channel Spectrum Width - šířka vysílaného kanálu. Snížením může dojít k menšímu rušení s ostatními sítěmi, ale také ke snížení teoretické rychlosti komunikace mezi vysílačem a klientem
- Output Power - Vysílací výkon bezdrátové karty

Část Wireless security:

V této části se nastavuje zabezpečení bezdrátové sítě technologiemi WEP, WPA a WPA2. Oproti zařízení RouterBoard zde neexistuje možnost přípravy všech metod a jejich postupná záměna. Při každé změně je potřeba přenastavit tuto část konfigurace a zařízení restartovat.

2.2 Zařízení pro tvorbu klientského zařízení

Z vybraných zařízení pro tento účel vyhovuje celá produktová řada výrobce Ubiquiti. Díky tomu, že všechna zařízení obsahují stejný operační systém AirOS, je konfigurace jednotná. Pro nastavení do klientského režimu je nutné pouze přihlášení na IP adresu zařízení a v záložce Wireless nastavení Wireless mode do režimu Station. Pokud síť, na kterou se bude zařízení připojovat, obsahuje nějaký typ zabezpečení, je ho potřeba vyplnit v části Wireless Security. V určité části praktického testování bude využita i metoda NAT (Network Address Translation)[15]. Tato možnost se nastavuje v záložce Network, kde je potřeba přepnutí možnosti Network Mode z režimu Bridge do režimu Router. Tato změna nám umožní zadat do zařízení dvě IP adresy - WAN a LAN. První adresa označená jako WAN bude nastavena na bezdrátovou kartu a díky tomu bude viditelná z vnější části sítě. Adresa označená jako LAN bude tvořit bránu pro počítače umístěné za zařízením. Povolením funkce Enable NAT začne zařízení automaticky překládat adresy z vnitřní sítě (LAN) do vnější sítě (WAN).

[15] Definice Network Address Translation: http://www.farpost.net/glossary/nat.php

3. Metody zabezpečení

V této části budou popsány a zhodnoceny všechny zabezpečovací metody a mechanismy, které se budou vyskytovat v praktickém testování. Vzhledem k faktu, že cílem této práce je analýza zabezpečení sítí internetových poskytovatelů a lokálních Wi-Fi, budou vypuštěna některá řešení, která nacházejí své uplatnění spíše v oblasti větších firem a institucí (například zabezpečení WPA s ověřování identity přes RADIUS server).

Použité metody a technologie se dají rozdělit do dvou kategorií podle typu určení - Aktivní a Pasivní. Aktivní metody jsou určené k tomu, aby útočníkovi z vnějšího prostředí zabránili v průniku do sítě. K tomuto typu zabezpečení patří:

- WEP
- WPA
- WPA2
- IP filter
- MAC filter

Druhým typem jsou metody pasivní, které jsou určené pro (v ideálním případě) znemožnění odchytu dat útočníkem, který se již nachází uvnitř sítě. Pokud nelze zabránit přímému odchytu dat, měly by tyto metody minimálně zkomplikovat útočníkovi orientaci v dané síti. Mezi tyto metody patří:

- Skrytí názvu sítě SSID
- Subnetting - rozdělení větší sítě do několika menších podsítí
- Úprava firewallu pro izolaci klientů mezi sebou
- Statické DHCP

3.1 WEP (Wired Equivalent Privacy)

Jedná se o první známý a rozšířený typ zabezpečení bezdrátových sítí. Tento standard byl schválen v roce 1997 jako součást původního standardu IEEE 802.11. Jak již překlad anglického názvu napovídá, cílem tohoto zabezpečení bylo poskytnout uživatelům stejnou úroveň bezpečnosti, jako kdyby šlo o klasickou ethernetovou síť. Postupem času se však začaly objevovat nedostatky tohoto šifrování a v roce 2001 bylo poprvé prolomeno. Od té doby bylo zveřejněno několik programů a zaručených postupů, které umožňují uživatelům (i bez jakékoliv znalosti bezdrátových sítí) velice jednoduchým způsobem prolomit toto zabezpečení. V dnešní době se tedy tento standard již nepovažuje za bezpečný.

WEP funguje na symetrickém principu, kdy se pro šifrování a dešifrování používá stejný algoritmus i totožný statický klíč (nejčastější a nejslabší 40ti bitový) a klienti jej využívají spolu se svou adresou MAC pro autentizaci vůči přístupovému bodu. Ve skutečnosti se tedy ověřuje totožnost síťové karty, nikoli samotného uživatele. Autentizace ve WEP pracuje pouze jednostranně, nikoli vzájemně. Šifrování přenášených dat se provádí 64-bitovým klíčem, který je složen z uživatelského klíče a dynamicky se měnícího vektoru IV (Initialization Vector) o délce 24 bitů. Ten se posílá v otevřené formě a mění se s každým paketem, takže výsledná šifra je jedinečná pro každý jednotlivý paket. WEP používá šifrovací algoritmus RC4. V závislosti na výrobci může nabízet silnější zabezpečení ve formě 128- bitového šifrování (sdílený klíč má délku 104 bitů, vektor poté 24 bitů)[16].

Prolomení zabezpečení WEP

Jak již bylo napsáno dříve, manuálů, programů nebo dokonce i video návodů jak prolomit tuto formu zabezpečení je k dispozici nepřeberné množství. Je tedy zbytečné v této práci reálný test provádět a bude zde pouze teoreticky popsána jedna z možných variant.

Základem úspěšného testu je správná volba bezdrátové karty v počítači, na kterém bude test probíhat. Výběr je důležitý především proto, že je ve většině případů nutná instalace speciálně upravených ovladačů dané karty, které ji dokážou přepnout do takzvaného "promiskuitního" módu, který umožňuje pasivní odposlech dat mezi vysílačem a již připojeným klientem. Také je nutný výběr správného vysílače - k němu musí být připojeni uživatelé, kteří v době testu síť aktivně využívají. Pokud je vše připravené, může dojít k instalaci programu na odchyt klíčů. Mezi nejznámější patří AirCrack[17], WEPCrack[18] nebo AirSnort[19]. Podstata těchto programů spočívá v tom, že jsou odchytávány pakety mezi vysílačem a připojenými klienty. Pokud je nashromážděno dostatečné množství dat, program z nich dokáže hledaný klíč poskládat, a to na základě znalostí o problémech s inicializačním vektorem. Potřebné množství vždy záleží na bitové délce klíče, tedy jestli je 64bitový (40bit klíč + 24bit inicializační vektor) nebo 128bit (104bit klíč + 24bit IV). Pokud je klíč delší, je nutné odchycení většího počtu paketů.

---

[16] Základní charakteristika WEP. Zdroj: http://support.netgear.com/app/answers/detail/a_id/1141/~/what-is-wep-encryption-for-wireless-networks%3F

[17] AirCrack je OpenSource software určený pro audit bezdrátových sítí. Zdroj: http://www.aircrack-ng.org/index.html

[18] WEPCrack je OpenSource program určený k prolamování klíčů zabezpečení WEP. Zdroj: http://wepcrack.sourceforge.net/

[19] AirSnort je OpenSource program určený pro obnovu zapomenutých WEP klíču. Zdroj: http://airsnort.shmoo.com/

Budoucnost WEP

Mohlo by se zdát, že po prolomení tohoto zabezpečení nebude důvod ho nadále používat nebo vyvíjet, a že všechny snahy budou směřovat na vývoj nových standardů a technologií. K tomu také ve větší míře došlo, nicméně se našlo několik výrobců, kteří se pokusili o jeho záchranu. Vznikla tak dvě řešení, která nesou označení WEPplus a WEP2. Jejich snahou je především rozšíření bitové délky inicializačního vektoru, což byl největší problém původní technologie WEP. Ani jedna tato metoda však problém nevyřešila, nicméně díky delšímu inicializačnímu vektoru zabere útočníkovi mnohem více času prolomení klíče a potřebuje k tomu mnohem více dat. Oba tyto systémy se však ve větší míře nerozšířily a to hlavně kvůli faktu, že je možné je použít pouze v sítích, kde jsou podporovány všemi zařízeními.

3.2 WPA (Wi-Fi Protected Access)

Tento standard byl uveden v říjnu roku 2002, jako reakce na prolomení technologie WEP. Vzhledem k tomu, že všechna zařízení té doby hardwarově podporovala pouze zabezpečení WEP a šifrování RC4, měla být první verze WPA pouze aktualizací předcházející technologie, aby ji bylo možné po aktualizaci softwaru používat i na stávajících zařízeních. Z tohoto důvodu je základem také šifrování pomocí RC4, nicméně slabiny technologie WEP jsou zde ošetřeny technologií TKIP (Temporal Key Integrity Protokol). Jedná se o dynamickou správu šifrovaných klíčů, které se díky takzvanému supplicantu[20] dynamicky mění nejen na začátku komunikace, ale v celém jejím průběhu. Autentizace do sítě chráněné pomocí WPA je zajišťována takzvaným PSK (Pre-Shared Key) nebo pomocí autentizačního serveru RADIUS. Klíč PSK slouží jako heslo, které je vyžadováno při každém přihlášení do sítě. Pro korektní funkci musí být tyto klíče uloženy ve všech zařízeních, které se do sítě připojují.

Mohlo by se zdát, že WPA vyřešilo všechny nedostatky původního WEP a že ho lze bez obav a problémů použít na všech zařízeních. V dnešní době je však prolomeno i toto zabezpečení a to skrze technologii TKIP. Původně demonstrovaná metoda útoku vyžadovala cca 15 minut[21], japonští odborníci ovšem přišli na způsob, jak toto zabezpečení prolomit

[20] Informace o WPA supplicantu a podporované síťové karty: http://hostap.epitest.fi/wpa_supplicant/
[21] Zdroj: http://securityworld.cz/aktuality/Sifrovani-WPA-lze-prolomit-nejen-hrubou-silou-1345

během několika desítek vteřin[22]. Objevují se také první implementace, které dovolují tuto metodu použít i na běžně dostupném softwaru AirDump[23].

3.3 WPA2 (Wi-Fi Protected Access)

Z předcházející kapitoly byla vypuštěna část o budoucnosti standardu WPA, neboť je jím právě standard WPA2. Ten byl schválen v červnu roku 2004[24] a byl prvním standardem, který plně vyhovuje normě IEEE 802.11i[25]. Toto zabezpečení je navrženo pro nová zařízení a díky tomu není nutná kompatibilita se šifrovacím algoritmem RC4. WPA2 tak používá mimo jiné úplně nový typ šifrování, takzvanou blokovou šifru AES[26] (Advaced Encrytion Standard). Délka šifry zde začíná na 128 bitech a končí až na 265 bitech.

Tento typ zabezpečení se v dnešní době považuje za nejbezpečnější, neboť zatím nebyl objeven způsob, kterým by bylo možné tento standard prolomit (platí pouze pro WPA-AES, nikoliv TKIP). Jedinou šancí, jak se do takové sítě dostat, je možnost použití slovníkového útoku. Tato metoda je obecně možná pro všechny typy zabezpečení, které jsou založeny na klíči či hesle. Pomocí něj se uživatel snaží odhadnout heslo jeho opakovaným zadáváním bez jakýchkoliv podkladů či znalostí tak dlouho, dokud se do sítě nedostane (neboli stylem pokus/omyl).

Dle již dříve zmíněné normy IEEE 802.11i je zaručeno, že všechna (v dnešní době dostupná) zařízení mají možnost zabezpečení WPA2-AES. Tuto skutečnost dokládá fakt, že všechna zařízení, která jsou certifikována pro bezpečný provoz Wi-Fi sítí, nemohou certifikací projít, pokud tento standard neobsahují[27].

3.4 IP Filter

Tento způsob ochrany sítě není žádnou organizací certifikován, ani není uznáván za platnou technologii. Jde tedy spíše o metodu zabezpečení, která využívá možností firewallu a povoluje nebo naopak blokuje cestu paketům, které zařízením procházejí. Pro správné fungování IP filtru je nutné ve firewallu vytvořit sadu pravidel, ve které jsou postupně povolovány průchody paketů vybraných IP adres, které mají být sítí propuštěny dále. Na

---

[22] Zdroj: http://www.computerworlduk.com/news/networking/16351/how-to-hack-wpa-wireless-security-in-one-minute/
[23] http://airdump.cz/tkiptun-ng-prvni-implementace-utoku-na-wpa-tkip/
[24] Definice standardu WPA2. Zroj: http://standards.ieee.org/findstds/interps/802.11i-2004.html
[25] Definice normy 802.11i. Zdroj: http://standards.ieee.org/findstds/interps/802.11i-2004.html
[26] Specifikace šifrování AES Zdroj: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[27] Certifikace zařízení pro Wi-Fi. Zdroj: http://www.wi-fi.org/knowledge-center/white-papers/state-wi-fi®-security-wi-fi-certified™-wpa2™-delivers-advanced

konci tohoto seznamu musí být aktivní pravidlo, které bude zahazovat ostatní pakety, které tomuto filtru nevyhovují. Příklad aktivního IP filteru vypsaného přes terminál zařízení RouterBoard pro tři IP adresy - 10.0.0.1, 10.0.0.2 a 10.0.0.3:

```
[admin@test_bak] /ip firewall filter> print
Flags: X - disabled, I - invalid, D - dynamic
0   chain=forward action=accept src-address=10.0.0.1 in-interface=ether2
1   chain=forward action=accept src-address=10.0.0.2 in-interface=ether2
2   chain=forward action=accept src-address=10.0.0.3 in-interface=ether2
3   chain=forward action=drop src-address=10.0.0.0/24 in-interface=ether2
[admin@test_bak] /ip firewall filter>
```

Fungování této metody je následující - Zařízení, ve kterém je IP filter spuštěný, analyzuje každý příchozí paket. Při této analýze je z paketu zjištěna zdrojová IP adresa (tedy IP adresa zařízení, ze kterého byl paket odeslán) a ta je porovnána s IP adresami uvedenými ve filtru. Pokud vyhovuje některé z uvedených adres, je paket propuštěn sítí dále. Pokud tomu tak není, vztahuje se pro něj poslední pravidlo v seznamu a paket je zařízením nenávratně zahozen. Menší nevýhodou tohoto řešení oproti standardům WEP a WPA je fakt, že tato metoda v sobě neobsahuje autentizační mechanismus. Pokud je tedy na Access Pointu aplikován pouze IP filter, není útočníkovi jakkoliv zabráněno v připojení do sítě.

Prolomení IP filtru

Jak vyplývá z popisu této metody, její prolomení není téměř žádný problém. Útočník však musí vědět, že je IP filter v dané síti využíván. Pokud se o tomto faktu přesvědčí a není v síti použita jiná forma zabezpečení, stačí se připojit k síti (což by při absenci WEP a WPA neměl být problém), odchytit určité množství paketů a získat z nich zdrojové IP adresy. Čím více je paketů odchyceno, tím více je získáno IP adres z dané sítě a tím větší je pravděpodobnost, že bude vybrána adresa, která v dané chvíli nebude aktivní a nebude docházet ke kolizím. Útočníkovi pak stačí nastavení vybrané IP adresy do svého zařízení a tím získá plný přístup do sítě.

3.5 MAC Filter

Tato metoda vychází ze stejného principu jako IP filter, místo IP adresy se však získává zdrojová MAC (Media Access Control) adresa. Tato adresa se také někdy nazývá

fyzickou a jedná se o určitý druh identifikátoru. Ten by měl být jedinečný pro každou vyrobenou síťovou kartu a je jí přiřazen a nastaven při výrobě. Jeho délka je 48 bitů a nejčastěji se zapisuje jako šestice hexadecimálních dvojciferných čísel. Tvorba těchto adres je rozdělena na dvě poloviny. První část má vždy přidělenou výrobce hardware a musí ji použít u všech síťových karet a zařízení, které vyrobí. Druhá část adresy je náhodně vygenerována, ale musí být zajištěno, aby se nikdy neopakovala. Jako celek by pak měla tato fyzická adresa jednoznačně určit zařízení v síti. Z pohledu bezpečnosti bylo možné důvěřovat této adrese jako jedinečné a nezaměnitelné. Příklad MAC filtru vypsaného přes terminál systému RouterOS:

```
[admin@test_bak] /ip firewall filter> print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=forward action=accept in-interface=ether2 src-mac-address=00:15:6D:F6:3E:1E
 1   chain=forward action=accept in-interface=ether2 src-mac-address=00:0C:42:D0:D0:FD
 2   chain=forward action=accept in-interface=ether2 src-mac-address=11:22:33:44:55:AA
 3   chain=forward action=drop in-interface=ether2
[admin@test_bak] /ip firewall filter>
```

Prolomení MAC Filtru

Tato metoda se jeví jako sofistikovanější než kontrola zdrojových IP adres. Bezpečnost by zde měla být na první pohled výrazně lepší, neboť MAC adresa je pro každé zařízení jedinečná a je nastavena při jeho výrobě. Problém je však v tom, že tuto fyzickou adresu je možné softwarově přepsat. Pokud tedy bude mít síťová karta v počítači fyzickou MAC adresu 00:15:6D:F6:3E:1E, není problém ji softwarově upravit na 00:0C:42:D0:D0:FD. K tomuto kroku dokonce není potřeba zvláštních programů nebo ovladačů a je ho možné provést přímo v systému Windows - doplněním nepravé adresy do Správce zařízení[28] nebo úpravou registrů systému[29]. Tato metoda je tedy pro útočníka poněkud komplikovanější a vyžaduje více znalostí než IP filter. Jako samostatný prvek však neposkytuje dostatečnou ochranu sítě ani dat, které jí protékají.

3.6 Skrytí názvu sítě SSID

[28] Příloha č. 10: Softwarová úprava MAC adresy počítače v části Správce zařízení

Touto funkcí disponují v dnešní době téměř všechna zařízení, která dokáží fungovat jako Access Point. Po její aktivaci přestane být název sítě viděn mezi ostatními.

Při nastavení zařízení do režimu vysílače se začne vysílat takzvaný beacon. Jeho obsahem je mimo jiné i název sítě - SSID. Tento beacon slouží jako identifikátor sítě a díky němu je zařízeními v okolí rozpoznána. Pokud je tedy na vysílači aktivována možnost Hide SSID, síť sice vysílá své beacony, ty ale neobsahují informace o názvu a tím je docíleno jejího skrytí. Pokud se pak chce uživatel k vysílači připojit, musí ručně vyplnit všechny údaje (název, heslo WEP nebo WPA, popř. i vysílací frekvence). Jestliže jsou vyplněny správně, zařízení se automaticky připojí. Pokud nejsou, síť je nadále pro běžného uživatele neviditelná.

Prolomení skrytého SSID

Nástrojů pro rozkrytí skrytého názvu sítě je dostupných spoustu (například Karma nebo airbase-ng), stejně tak jako návodů jak postupovat. Zjištění SSID by se dalo přirovnat z odchytu WEP klíče. Bezdrátová karta se opět přepne do tzv. promiskuitního módu a odposlouchává pakety z okolí. U této metody vyvstává problém ve chvíli, kdy se k vysílači připojí oprávněný klient. V tom okamžiku dojde k výměně informací mezi ním a vysílačem. Mezi tyto informace patří i ESSID[30], po jehož odchytu je možné díky výše zmíněným programům zjistit SSID.

3.7 Subnetting

V tomto případě se jedná pouze o využití výhod, které plynou z možností rozdělení sítí ve formátu IPv4. V případě připojení více klientů k jednomu vysílacímu bodu může být využito většího rozsahu IP adres. Příklad nastavení - vysílač bude mít nastavenou IP adresu 192.168.1.1 s maskou 255.255.255.0 a všechna zařízení připojená k tomuto vysílači budou mít adresu z rozsahu 192.168.1.2 - 192.168.1.254 se stejnou maskou. Výhodou tohoto způsobu je větší přehlednost sítě a její snazší správa, nevýhodou je však viditelnost všech zařízení mezi sebou v rámci stejné podsítě (192.168.1.0/24). Metoda subbnetigu využívá možnosti dělení sítě. Celý rozsah 192.168.1.0/24 je rozdělen na několik menších celků, nejčastěji pouze pro dvě použitelné IP adresy, aby bylo možné jednu nastavit na vysílač a druhou klientovi. Výsledek tedy bude takový, že z jedné sítě získáme několik menších podsítí:

[29] Příloha č. 11: Softwarová úprava MAC adresy počítače v části Registry systému

- Původní rozsah - 192.168.1.0/24
- Nové rozsahy - 192.168.1.0/30, 192.168.1.4/30, 192.168.1.8/30, atd.

Po aplikaci subnettingu tedy bude na vysílači nastaveno více IP adres, každá z jiného rozsahu a každá bude reprezentovat bránu (default gateway) pro jiné zařízení v síti. Tímto je zajištěno oddělení klientů v síti na úrovni IP adres. Po správném nastavení firewallu je pak možný zákaz komunikace mezi jednotlivými subnety a tím dojde k celkové izolaci uživatelů od svého okolí.

3.8 Úprava firewallu pro izolaci klientů

Pokud byla aplikována metoda subnettingu uvedená výše, je možné jednotlivé klienty navzájem izolovat pomocí firewallu. Tato funkce přichází do úvahy pouze v případě, je v sítí zapnuté dynamické routování, neboť to automaticky tvoří routy mezi všemi známými sítěmi. Pokud je v síti zapnuté jen statické routování (což u sítí na úrovni poskytovatele internetu s větším počtem uživatelů není únosné) je možné ručně vytvořit routy pouze mezi sítěmi, do kterých uživatel může nebo musí mít přístup.

Ve firewallu tedy musí být vytvořené pravidlo které specifikuje, z jaké IP adresy se klient do sítě dostává a na jakou jinou IP adresu (nebo adresy, popřípadě subnety) má přístup. Za tímto pravidlem pak vždy musí být pravidlo "drop", které zajistí zahození paketů při nesplnění předchozího pravidla. Tato kombinace pravidel pak musí být vytvořena pro každou IP adresu síti. Příklad firewallu vypsaného přes konzoli systému RouterOS:

```
[admin@test_bak] /ip firewall filter> print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=forward action=accept src-address=10.0.0.2 dst-address=10.0.0.0/30
1   chain=forward action=drop src-address=10.0.0.2
2   chain=forward action=accept src-address=10.0.0.6 dst-address=10.0.0.4/30
3   chain=forward action=drop src-address=10.0.0.6
4   chain=forward action=accept src-address=10.0.0.10 dst-address=10.0.0.8/30
5   chain=forward action=drop src-address=10.0.0.10
[admin@test_bak] /ip firewall filter>
```

[30]Definice pojmu ESSID: http://wiki.airdump.cz/ESSID

V tomto příkladu je firewall nastaven tak, že se každý klient, který má vlastní subnet (IP adresy klientů jsou 10.0.0.2, 10.0.0.6 a 10.0.0.10) dostane pouze na IP adresy ze stejného síťového rozsahu (dst-address=10.0.0.x/30). Pokud je potřeba přidělit více rozsahů nebo rozsah a více konkrétních IP adres, je potřeba vytvořit tzv. destination address list (v systému dst-add-list). Příklad address listu, který se jmenuje "accessible" a umožní přístup do subnetu 10.0.0.0/30 a na IP adresu 192.168.1.20:

```
[admin@test_bak] /ip firewall address-list> print
Flags: X - disabled, D - dynamic
 #   LIST                                                ADDRESS
 0   accessible                                           10.0.0.0/30
 1   accessible                                           192.168.1.20
[admin@test_bak] /ip firewall address-list>
```

Přiřazení listu "accessible" k IP adrese 10.0.0.2:

```
[admin@test_bak] /ip firewall filter> print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=forward action=accept src-address=10.0.0.2 dst-address-list=accessible
 1   chain=forward action=drop src-address=10.0.0.2
 2   chain=forward action=accept src-address=10.0.0.3 dst-address=10.0.0.1
 3   chain=forward action=drop src-address=10.0.0.3
 4   chain=forward action=accept src-address=10.0.0.4 dst-address=10.0.0.1
 5   chain=forward action=drop src-address=10.0.0.4
[admin@test_bak] /ip firewall filter>
```

3.9 Statické DHCP

DHCP[31] neboli Dynamic Host Configuration Protocol je služba běžící v síti, která zajišťuje automatické přidělení IP adresy klientům, kteří si o ni zažádají. Při konfiguraci v systému RouterOS je vždy potřeba při tvorbě serveru nastavit Address Pool na hodnotu Static only. Díky tomu budou adresy z DHCP přidělovány pouze zařízením, jejichž IP se nacházejí v sekci Leases a mají hodnotu Static. Příklad sekce Leases vypsané přes terminál

[31] Definice a popis DHCP: http://www.abclinuxu.cz/slovnik/dhcp

systému RouterOS:

```
[admin@test_bak] /ip dhcp-server lease> print
Flags: X - disabled, R - radius, D - dynamic, B - blocked
 #   ADDRESS         MAC-ADDRESS       HOST-NAME       SERVER          STATUS
 0 D 192.168.1.103   10:93:E9:33:DA:9D Michals-iPad    (unknown)       bound
 1   192.168.1.104   0C:60:76:56:A2:37  Michal-NTB      (unknown)       bound
 2 D 172.16.0.253    00:1A:92:BB:1A:E8 Michal-Mac-Pro  (unknown)       bound
 7 D 172.16.0.251    00:15:6D:D6:B9:23 UBNT            (unknown)       bound
[admin@test_bak] /ip dhcp-server lease>
```

Z tohoto výpisu je vidět, že IP adresu ze správně nastaveného DHCP serveru dostane pouze zařízení Michal-NTB, neboť jako jediné nemá atribut Flag - D (dynamic) a jeho hodnota je tedy statická.

Hodnocení metod zabezpečení:

Pokud by měly být metody aktivního zabezpečení zhodnocené na základě úrovně bezpečnosti, kde bude hodnotícím kritériem obtížnost a časová náročnost jejich prolomení, vypadal by žebříček následovně (metody jsou řazené od nejbezpečnější):

1. WPA2-AES

2. WPA-TKIP

3. WEP

4. Mac Filter

5. IP Filter

Rozdíly mezi WPA-TKIP a WEP jsou, co se časové náročnosti týká, velice sporné. Toto uspořádání bylo vybráno na základě dostupnosti nástrojů, kterých je pro prolomení zabezpečení WEP o poznání více

4. Příprava praktického testování

V této části práce bude provedena příprava na testování jednotlivých metod uvedených výše. Na základě získaných údajů o prodejnosti zařízení budou vytvořeny všechny možné konfigurace, které připadají v úvahu. Na nich poté budou testovány konkrétní metody zabezpečení a jejich kombinace.

4.1 Vytvoření testovacího souboru

Testování bude probíhat stahováním určitého souboru, jehož název je t.zip, velikost 2,5GB a jedná se o balík náhodně vygenerovaných dat. Pro vytvoření tohoto souboru byl použit program Random Data File Creator[32], který vygeneroval soubor t.bin. Soubor však byl přejmenován na koncovkou .zip, neboť se bude z počítače získávat přes http server, jehož roli bude plnit program Microsoft ISS[33]. Tento systém podporuje pouze koncovky známých typů souborů a se souborem t.bin nefungoval. Přejmenováním na t.zip se soubor zpřístupnil.

4.2 Příprava zařízení

K testování budou použita zařízení, která jsou uvedena v kapitole 2. Některá z nich budou v určitých konfiguracích plnit různé funkce. Ze získaných informací[34] lze odvodit čtyři možné topologie sítě. Celkově je pak lze rozdělit na dvě základní skupiny, které budou v této práci pojmenovány jako I. a II. Základní rozdíl mezi těmito dvěma skupinami je ve funkci zařízení RouterBoard RB800. Zatímco bude ve skupině I. obohaceno o bezdrátovou síťovou kartu CM9 a bude tvořit router s vysílacím bodem dohromady (vhodné především pro menší vysílací body, řešení tzv. vše v jednom) ve variantě II. bude figurovat jako čistě kabelový router s podružným zařízením NanoStation v režimu AP bridge (řešení pro větší vysílače). Ve všech čtyřech topologiích bude server s uloženým testovacím souborem připojen za zařízením RouterBoard a propojení mezi nimi bude realizováno přímým spojením (kabelem CAT6 o délce 2m) o rychlosti 1Gbit/s. Na opačném konci topologie se budou nacházet zařízení UBNT NanoStation 5, 5 Loco a Bullet. Ta budou připojena (přes dodávané PoE splittery) k počítačům síťovým rozhraním o rychlosti 100Mbit/s. Krátký přehled počítačů, na kterých se bude provádět stahování souborů a měření:

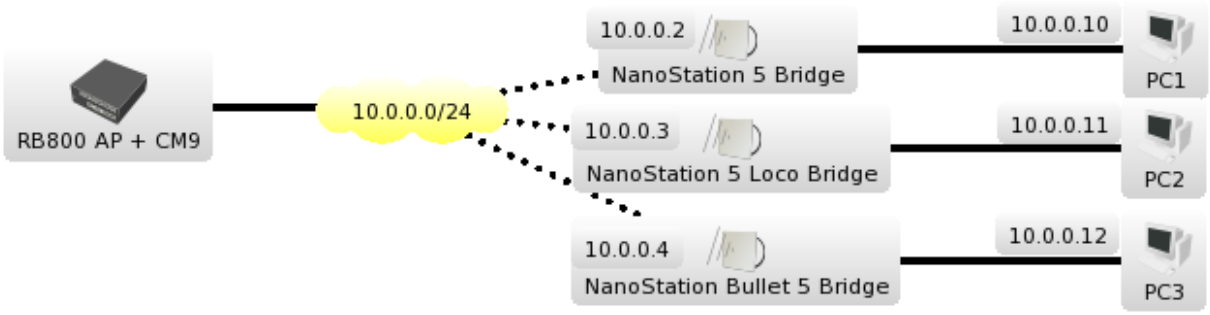
[32] Random File Data Creator je freeware aplikace pro tvorbu souborů z náhodně vygenerovaných dat. Zdroj: http://www.bertel.de/software/rdfc/index-en.html

[33] Microsoft IIS je komerční webový server dostupný v serverových edicích systému Windows. Zdroj: http://www.iis.net/

1. Notebook HP Pavilion dv6-1230-ec, AMD Athlon X2 2,1Ghz, 3GB ramm, 320GB HDD, Windows 7 Professional
2. Intel Core2Duo 2Ghz, 2GB ramm, 500GB HDD, MacOS X 10.7.1 Lion
3. HTPC AsRock 330ion, DualCore Intel Atom 1,6Ghz, 2GB ramm, 250GB HDD, Windows 7 Home Premium

Topologie I. A

Základní konfigurace, ve které figuruje zařízení RB800 jako vysílač s routerem dohromady a zařízení připojená za ním se nacházejí v režimu bridge. Bez jakékoliv modifikace tedy přeposílají pakety z bezdrátového rozhraní na ethernet a naopak. V této topologii se všechny prvky, jak klientské zařízení NanoStation tak i koncové počítače, nacházejí ve stejné podsíti, konkrétně 10.0.0.0/24, kde je vysílač reprezentován IP adresou 10.0.0.1. Obrázek reprezentující tuto topologii:

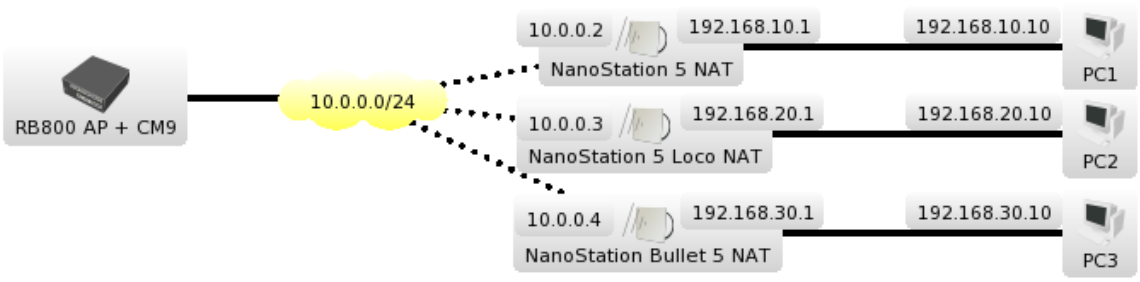


Obrázek č. 1: Topologie I. A vykreslena programem The Dude

Topologie I. B

Jediný, ale podstatný rozdíl, kterým se liší tato topologie od předcházející, je nastavení klientských zařízení NanoStation. V této konfiguraci se nachází v režimu NAT a tím pádem obsahují dvě IP adresy, mezi kterými musí probíhat překlad. Koncové počítače jsou tak každý ve vlastní podsíti a vidí pouze svou bránu (default gateway) kterou zde tvoří klientské zařízení. Obrázek topologie:

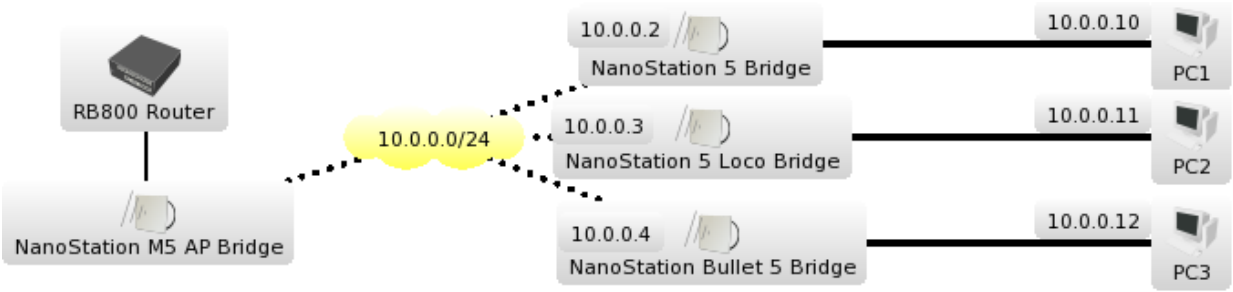
[34] Příloha č. 1: Elektronická korespondence se společnostmi i4wifi a.s a Aspa a.s.



Obrázek č. 2: Topologie I. B vykreslena programem The Dude

Topologie II. A

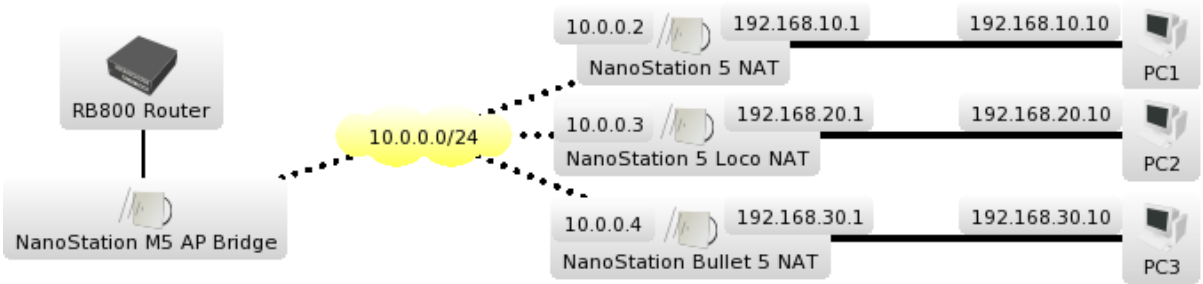
V druhé skupině je zařízení RB800 konfigurováno bez bezdrátové karty CM9, ale s podružným zařízením NanoStation M5, které je nastaveno do módu AP bridge. Chová se tedy jako vysílač, který pouze propouští veškerou komunikaci mezi připojeným klientem a RouterBoardem. V první verzi této konfigurace jsou klientská zařízení opět nastavena do módu bridge. Obrázek topologie:



Obrázek č. 3: Topologie II. A vykreslena programem The Dude

Topologie II. B

V poslední konfiguraci je RouterBoard opět v kombinaci s NanoStation M5 v módu AP bridge. Oproti předcházející konfiguraci jsou zde klientská zařízení nastavena do režimu NAT. Obrázek topologie:



Obrázek č. 3: Topologie II. B vykreslena programem The Dude

4.3 Příprava sítě

Pro objektivní výsledky měření je nutná řádná příprava, umístění a konfigurace zařízení. Testování probíhalo ve vnitřních podmínkách, v místnosti 5 x 7m. Všechna zařízení byla nastavena na frekvenci 5Ghz a bylo ověřeno nulové rušení v celé místnosti. Testu tohoto rušení bylo docíleno RouterBoardem s bezdrátovou miniPCI kartou CM9. V každém místě místnosti, kde bylo umístěno klientské zařízení, byl nejdříve umístěn RouterBoard a bylo provedeno Frequency Usage skenování, které vždy ukázalo nulové rušení[35]. Dále bylo potřeba zajistit správné uchycení antén kvůli signálu a polarizaci. Vzhledem k nulovému rušení od okolních sítí mohla být použita vertikální polarizace, ve které běžně fungují všesměrové antény a která vždy bývá největším zdrojem rušení. Uchycení antén bylo nutné zajistit kolmo k podlaze místnosti, aby nedošlo k pře-polarizování antény a tím ke snížení kvality spoje. K zafixování zařízení byla použita část výložníku, který se jako celek používá pro rozšíření místa na stožárech. Přišroubováním k dřevěnému podstavci bylo docíleno stabilních držáků, na které byly jednotlivé antény přichyceny. Dále bylo potřeba vyladit samotnou síť. Na plánku[36] je vidět umístění jednotlivých prvků v místnosti. Snahou bylo vytvořit co největší rozestupy mezi klientskými zařazeními, aby nedocházelo k vzájemnému rušení. Bylo také nutné upravit vysílací výkon, neboť všechna zařízení jsou primárně určena pro venkovní použití a pro vzdálenosti na několik stovek metrů. Přes oficiálním testem proběhlo několik cvičných stahování testovacího souboru, při kterém byla sledována kvalita přenosu, údaje o signálu, kvalitě připojení, teoretické rychlosti a CCQ. Po každém stahování byly upraveny vysílací výkony zařízení a test proběhl znovu. Po několika pokusech bylo zjištěno, že díky minimálním vzdálenostem stačí ke kvalitnímu přenosu minimální výkon zařízení a všechny klientské antény byly upraveny na vysílací výkon 1dBi. I při takto nízkém výkonu byly signály všech zařízení v ideálním rozsahu -51/-53 při maximální teoretické přenosové rychlosti a 100% CCQ.

4.4 Příprava testování

Po vyladění sítě bylo nutné stanovit postupy a cíle měření. Během cvičného stahování souboru bylo rozhodnuto, že postup bude následující: na každé topologii se nejdříve provede stažení souboru bez jakéhokoliv zabezpečení. Tím budou získány výchozí údaje pro porovnání se všemi dalšími druhy ochrany sítě. Dále se bude provádět testování

[35] Příloha č. 6: Výsledky měření zarušená prostředí pomocí metody Frequency Usage v zařízení MikroTik

metod na základě jejich teoretické náročnosti na systém. Postupně tedy měly být vyzkoušeny metody v tomto pořadí - IP filter, MAC filter, WEP, WPA-TKIP, WPA2-EAP. Během prvního testování se však ukázalo, že metody IP filteru a MAC filteru mají na systém úplně stejný vliv a nároky, proto budou ve všech výsledcích uvedeny pouze testy IP filteru.

Dále bylo potřeba stanovit metody zaznamenávání údajů ze zařízení a koncových počítačů. Z RouterBoardu měly být získávány údaje o vytížení procesoru a o celkovém průtoku dat. K tomuto účelu měl být původně využit systém grafů, který operační systém RouterOS nabízí. Po bližším prozkoumání konfigurace grafového rozhraní však bylo zjištěno, že nejkratší možný interval pro zaznamenávání údajů je 5 minut. Tato možnost bohužel platila jak pro grafy vytížení CPU tak pro grafy sledující průtok dat jednotlivými síťovými rozhraními. Kvůli tomuto problému se tedy systémové grafy nedají použít a bylo nutné všechny údaje a změny systému zaznamenávat ručně a poté vyhodnotit. Dále bylo také zjištěno, že u zařízení NanoStation (všechny druhy) nelze jakýmkoliv způsobem zjistit vytížení procesoru. Jediný údaj, který tak bylo možné určit byl průtok dat, který je dán rychlostí stahování na počítači za zařízením. Na všech počítačích pak byla sledována rychlost stahování testovacího souboru a po celou dobu byla sledována a zaznamenávána odezva na vysílací bod (příkazem ping ip_adresa_brány s parametrem -l 1024).

[36] Příloha č. 12: Půdorys testovací místnosti včetně rozmístění jednotlivých prvků

5. Praktické testování

Jednotlivé topologie zde budou prezentovány ve stejném pořadí, v jakém byly uvedeny výše, tedy I. A, I. B, II. A a II. B.

5.1 Topologie I. A

Nejdříve bylo provedeno měření bez jakéhokoliv zabezpečení. Zde by měly být výsledky nejoptimálnější a to se také potvrdilo. Při stahování souboru z jednoho počítače bylo dosaženo průměrné rychlosti 25Mbit/s s odchylkou -+ 200kbit/s. Vytížení CPU zařízení RouterBoard se v tomto případě pohybovalo mezi 37-46%. Při postupném přidávání počítačů se neměnila rychlost průtoku dat ani vytížení CPU a rychlost stahování se rozložila rovnoměrně mezi všechny tři počítače.

Shrnutí - Topologie I. A - bez zabezpečení

Připojení 1 PC - Průtok 25,1Mbit/s -+ 200kbit/s Vytížení CPU RB - 37-45%

Připojení 2 PC - Průtok 25Mbit/s -+ 200kbit/s Vytížení CPU RB - 37-45%

Připojení 3 PC - Průtok 25Mbit/s -+ 200kbit/s Vytížení CPU RB - 39-46%

Latence na vysílač (v tomto případě IP adresa 10.0.0.1):

PC1 53-80ms PC2 56-90ms PC3 59-70ms

5.1.1 IP Filter

Po aplikaci této metody lze očekávat zvýšení zatížení CPU, kvůli kontrole zdrojových IP adres u všech paketů. Toto očekávání se testováním potvrdilo. Je zde také vidět mírný pokles celkového průtoku při aktivitě všech tří počítačů.

Shrnutí - Topologie I. A - IP Filter

Připojení 1 PC Průtok 25Mbit/s -+ 300kbit/s Vytížení CPU RB - 39-45%

Připojení 2 PC Průtok 24,8Mbit/s -+300kbit/s Vytížení CPU RB - 41-46%

Připojení 3 PC Průtok 24,5Mbit/s -+ 500kbit/s Vytížení CPU RB - 44-50%

Latence na vysílač (v tomto případě IP adresa 10.0.0.1):

PC1 58-82ms PC2 61-92ms PC3 61-81ms

5.1.2 WEP - Wired Equivalent Privacy

U tohoto zabezpečení se očekává zvýšená zátěž procesoru, která by mohla při

připojení více klientů vést až ke snížení datové propustnosti.

Shrnutí - Topologie I. A - WEP

Připojení 1 PC Průtok - 22,3Mbit/s -+500Kbit/s Vytížení CPU RB - 36-47%
Připojení 2 PC Průtok - 22,0Mbit/s -+ 500Kbit/s Vytížení CPU RB - 41-47%
Připojení 3 PC Průtok - 21,5Mbit/s -+ 450Kbit/s Vytížení CPU RB - 41-50%
Latence na vysílač (v tomto případě IP adresa 10.0.0.1):
PC1 59-109ms PC2 58-117ms PC3 59-108ms

Z výsledků je patrné, že pokles průtoku dat je značný, stejně tak jako odchylky, ve kterých se rychlost pohybuje. Také se poněkud zvýšila odezva na vysílač, která už se může v těchto hodnotách negativně projevit při souběžném používání sítě pro běžné úkony. Nárůst zátěže procesoru u této metody není oproti předpokladům nikterak výrazný.

5.1.3 WPA-PSK TKIP (update key 30s)

Pokročilejší metoda zabezpečení, u které se předpokládá ještě větší zátěž procesoru a snížení průtoku dat než u metody WEP. Díky časté změně dynamických klíčů by se také měla zvýšit režie síťového provozu.

Shrnutí - Topologie I. A - WPA-PSK + TKIP

Připojení 1 PC Průtok - 21,5Mbit/s -+ 300Kbit/s Vytížení CPU RB - 44 - 50%
Připojení 2 PC Průtok - 21Mbit/s -+ 400Kbit/s Vytížení CPU RB - 46 - 51%
Připojení 3 PC Průtok - 21Mbit/s -+600Kbit/s Vytížení CPU RB - 55 - 60%
Latence na vysílač (v tomto případě IP adresa 10.0.0.1):
PC1 70-140ms PC2 100-130ms PC3 90-140ms
V tomto měření je úbytek datové propustnosti ještě zřejmější než u předchozích metod. Pokud by mělo dojít k porovnání, metoda WPA potřebuje k obsloužení tří připojených klientů o téměř 20% více výkonu než síť bez zabezpečení. Časové odezvy se ještě zvyšují a zvyšuje se také rozptyl datové propustnosti, který dosahoval až 600kbit/s.

5.1.4 WPA-PSK TKIP (update key 30s) + IP filter

Toto měření se bude objevovat u všech topologií a bude reprezentovat vylepšené zabezpečení WPA obohacené o IP filter. Tato metoda by měla nést rysy WPA a vytížení CPU by mělo být ještě vyšší díky filteru.

Shrnutí - Topologie I. A - WPA-PSK (TKIP) + IP filter

Připojení 1 PC Průtok - 21,3Mbit/s -+300kbit/s Vytížení CPU RB - 48 - 56%

Připojení 2 PC Průtok - 21Mbit/s -+ 400Mbit/s Vytížení CPU RB - 51 - 57%

Připojení 3 PC Průtok - 21Mbit/s -+600kbit/s Vytížení CPU RB - 57- 62%

Latence na vysílač (v tomto případě IP adresa 10.0.0.1):

PC1 72-156ms PC2 80-154ms PC3 71-150ms

Měřením se tedy potvrdila původní domněnka - je zřejmá zvýšená zátěž procesoru a oproti předchozí metodě poněkud vzrostly i odezvy na vysílač. Pokud vezmeme v úvahu fakt, že jsou k vysílači připojeni pouze tři klienti a u této hodnoty je strop přenosu 21Mbit/s a vytížení procesoru zařízení 60%, je tato možnost naprosto nepoužitelná pro připojení více klientů.

5.1.5 WPA2-AES

Předpokládané chování tohoto typu zabezpečení nelze odvodit z žádného z předchozích měření, neboť se jedná o zcela jiný typ algoritmu a bude záležet na kvalitě implementace v daném zařízení.

Shrnutí - Topologie I. A - WPA2-AES

Připojení 1PC Průtok - 22,4Mbit/s -+400kbit/s Vytížení CPU RB - 42 - 46%

Připojení 2PC Průtok - 22Mbit/s -+ 350Kbit/s Vytížení CPU RB - 54 - 60%

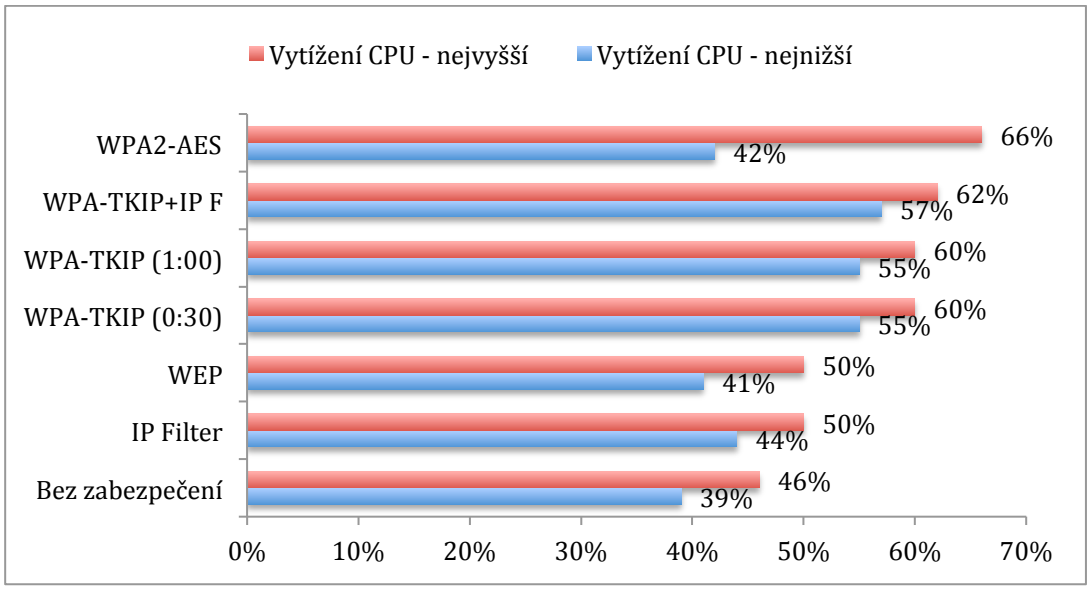
Připojení 3PC Průtok - 22Mbit/s -+400kbit/s Vytížení CPU RB - 59 - 66%

Latence na vysílač (v tomto případě IP adresa 10.0.0.1):

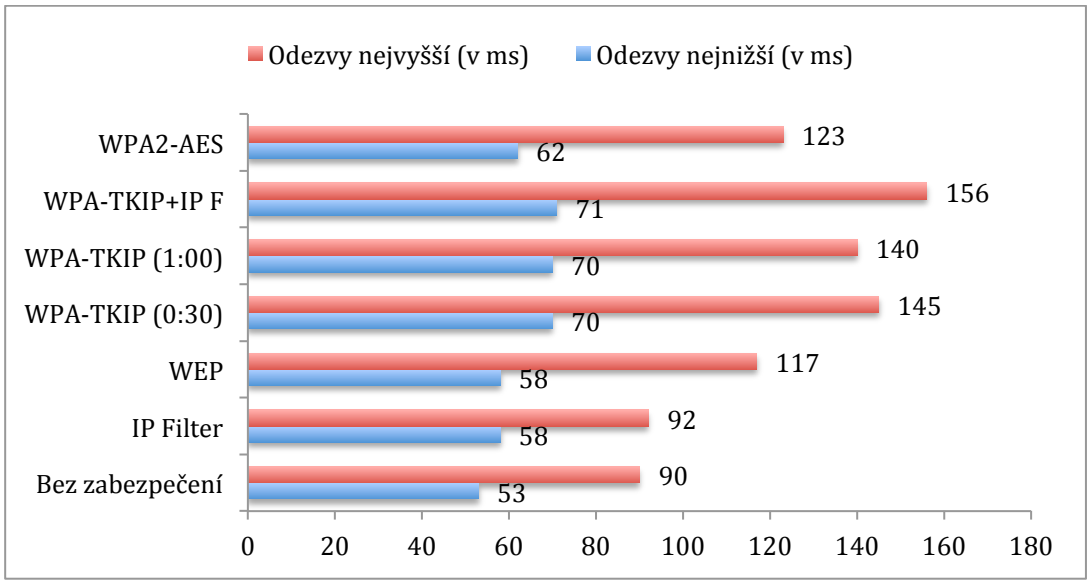
PC1 63-114ms PC2 67-117ms PC3 62-123ms

Z výsledků měření vyplývá, že je standard WPA2-AES v určitých směrech lépe implementován než WEP a WPA. Při tomto zabezpečení je dosahováno mnohem lepší datové propustnosti, nicméně se zvýšilo vytížení procesoru, které je zde nejvyšší ze všech naměřených hodnot. Také se zde objevuje značná nestabilita odezvy na vysílač.

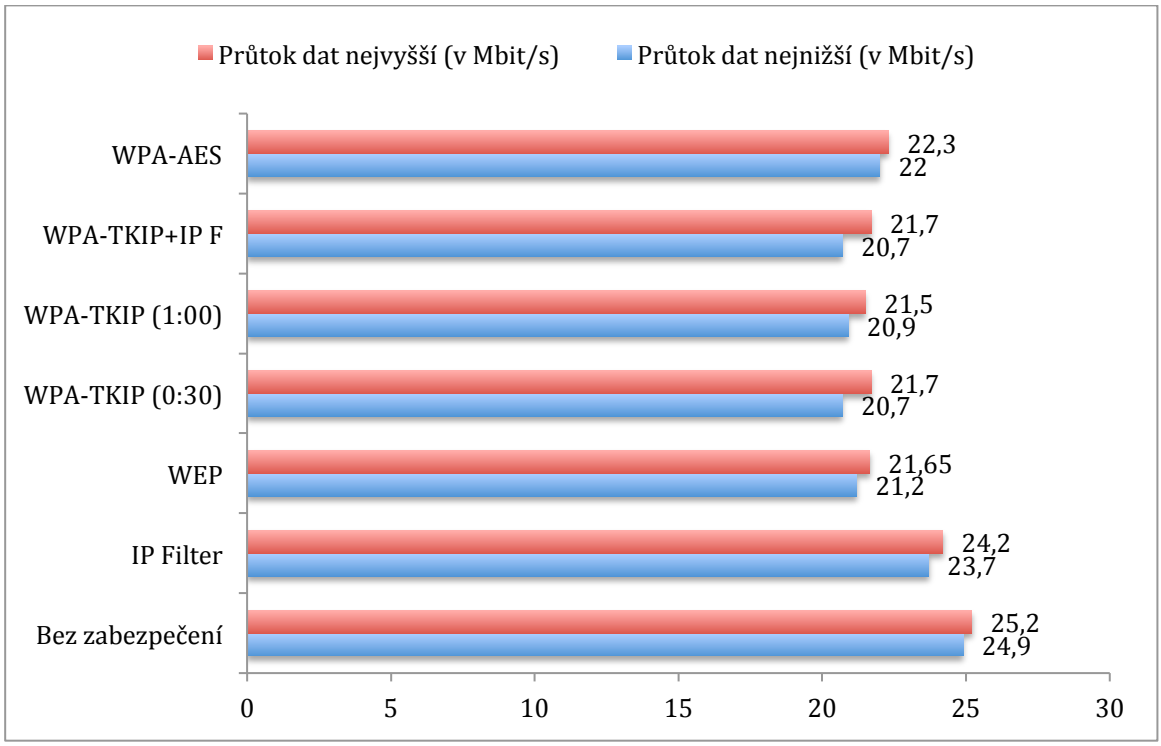
5.1.6 Shrnutí v grafech



Graf č. 1: Naměřené hodnoty vytížení CPU u topologie I. A



Graf č. 2: Naměřené hodnoty odezvy na vysílač u topologie I. A



Graf č. 2: Naměřené hodnoty průtoku dat u topologie I. A

5.2 Topologie I. B

Jak již bylo napsáno dříve, rozdíl od předchozí topologie je v nastavení klientských zařízení. Ta jsou v této části nastavena do režimu NAT. U této konfigurace se předpokládá snížení průtoku klientskými zařízeními a rozdíly by tedy měli být patrné především u hodnot, které jsou zaznamenány při stahování z jednoho počítače. Po připojení ostatních strojů se předpokládá plné vytížení vysílače a zde by rozdíly neměly být patrné.

Opět se bude vycházet z původního měření bez jakéhokoliv zabezpečení. Už to by mělo potvrdit původní domněnku.

Shrnutí - Topologie I. B - Bez zabezpečení

Připojení 1 PC Průtok - 21,3Mbit/s -+ 300Kbit/s Zatížení CPU RB - 31 - 33%

Připojení 2 PC Průtok - 25Mbit/s +- 300Kbit/s Zatížení CPU RB - 37 - 45%

Připojení 3 PC Průtok - 25Mbit/s +-300Kbit/s Zatížení CPU RB - 39 - 46%

Latence na vysílač (v tomto případě IP adresa 10.0.0.1):

PC1 60-94ms PC2 67-102ms PC3 63-88ms

V tomto měření se opět potvrdil předpoklad a u stahování z jednoho počítače je vidět snížení průtoku zařízením RouterBoard o více jak 3,5Mbit/s. Po započatém stahování ze dvou a více

zařízení bylo dosaženo přenosového stropu bezdrátové karty CM9 a proto už zde rozdíly nejsou vidět.

5.2.1 IP Filter

Zde by měli být výsledky stejné jako u předcházející konfigurace, neboť by režim NAT na klientských zařízeních neměl mít vliv na funkci firewallu.

Shrnutí - Topologie I.B - IP Filter

Připojení 1 PC	Průtok - 21Mbit/s -+ 300Kbit/s	Zatížení CPU RB - 34 - 40%
Připojení 2 PC	Průtok - 24,8Mbit/s -+300kbit/s	Vytížení CPU RB - 41 - 46%
Připojení 3 PC	Průtok - 24,5Mbit/s -+ 500kbit/s	Vytížení CPU RB - 44 - 50%

Latence na vysílač (IP adresa 10.0.0.1):

PC1	60-94ms	PC2	73-114ms	PC3	66-102ms

Zde z výsledků vyplývá, že byla naplněna předpověď a nedošlo k žádné anomálii.

5.2.2 WEP

V této topologii by mohlo být zajímavé sledovat chování klientských zařízení, která zde budou muset obsloužit jak překlad adres NAT, tak i zabezpečení bezdrátové sítě pomocí WEP. Může se zde tedy ještě více snížit průtok jednotlivých klientů.

Shrnutí - Topologie I. B - WEP

Připojení 1PC	Průtok - 19,3Mbit/s -+ 300kbit/s	Vytížení CPU RB - 31 - 39%
Připojení 2PC	Průtok - 22Mbit/s -+ 300kbit/s	Vytížení CPU RB - 41 - 47%
Připojení 3PC	Průtok - 21,5Mbit/s -+ 450Kbit/s	Vytížení CPU RB - 41 - 50%

Latence na vysílač (IP adresa 10.0.0.1):

PC1	61-112ms	PC2	63-120ms	PC3	64-114ms

Zde je vidět, že při stahování souboru z jednoho počítače se ještě více snížil průtok dat a je tedy patrné, že klientské zařízení nedokáže výkonem obsloužit šifrování sítě pomocí metody WEP a zároveň překlad adres NAT.

5.2.3 WPA-PSK (TKIP update 30s)

Stejně jako u předcházejícího měření, i zde lze očekávat snížení průtoku dat při

připojení prvního počítače. Toto snížení může být ještě výraznější než u metody WEP.

Shrnutí - Topologie I. B - WPA-PSK (TKIP update 30s)

Připojení 1PC Průtok - 18,6Mbit/s -+ 400kbit/s Vytížení CPU RB - 36 - 40%

Připojení 2PC Průtok - 21,2Mbit/s -+ 600kbit/s Vytížení CPU RB - 53 - 57%

Připojení 3PC Průtok - 21,3Mbit/s -+ 1Mbit/s Vytížení CPU RB - 54 - 60%

Latence na vysílač (IP adresa 10.0.0.1):

PC1 80 - 170ms PC2 100-168ms PC3 94 - 163ms

Původní domněnka se zde potvrdila a je patrné, že nároky na všechna zařízení jsou zde ještě vyšší než u ostatních typů zabezpečení. Potvrdilo se také snížení průtoku při aktivitě jediného počítače a to v průměru o více jak 0,5Mbit/s. Zajímavostí však je velice značný rozptyl datové propustnosti, který zde byl naměřen až 1Mbit/s. Také jsou zde zatím nejvyšší naměřené hodnoty u odezvy na vysílač, které jsou za hranicí normální použitelnosti.

5.2.4 WPA-PSK TKIP (update key 30s) + IP filter

Předpoklady u této kombinace jsou stejné jako v předchozí topologii. Lze tedy očekávat stejné chování jako při zabezpečení WPA-PSK, u vytížení CPU by však měly být vyšší hodnoty a vše by mělo být ovlivněno nastavením NATu na klientských zařízení.

Shrnutí - Topologie I. B - WPA-PSK (TKIP) + IP filter

Připojení 1PC Průtok - 18,6Mbit/s -+ 400kbit/s Vytížení CPU RB - 38 - 42%

Připojení 2PC Průtok - 21,2Mbit/s -+ 600kbit/s Vytížení CPU RB - 56 - 62%

Připojení 3PC Průtok - 21,1Mbit/s -+ 1Mbit/s Vytížení CPU RB - 57 - 64%

Latence na vysílač (IP adresa 10.0.0.1):

PC1 81 - 168ms PC2 102-174ms PC3 96 - 172ms

Z výsledků měření je patrné, že vše odpovídá předpokladu.

5.2.5 WPA2-EAP

Pokud by byly zohledněny výsledky měření této metody u topologie I. A a bylo by přihlédnuto k faktu, který se zatím potvrdil u všech metod v topologii I. B, mělo by pouze dojít ke snížení datové propustnosti u připojení jednoho PC.

Shrnutí - Topologie I. B - WPA2-AES

Připojení 1PC Průtok - 18,5Mbit/s -+400kbit/s Vytížení CPU RB - 38 - 43%

Připojení 2PC Průtok - 22Mbit/s -+ 400Kbit/s Vytížení CPU RB - 55 - 62%

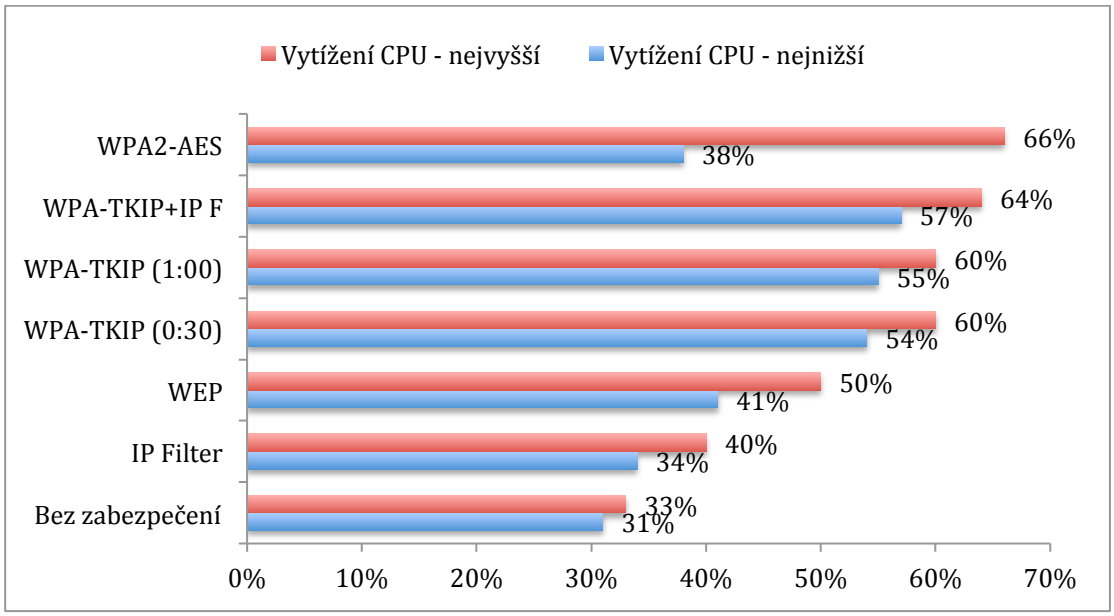
Připojení 3PC Průtok - 22Mbit/s -+500kbit/s Vytížení CPU RB - 59 - 66%

Latence na vysílač (IP adresa 10.0.0.1):

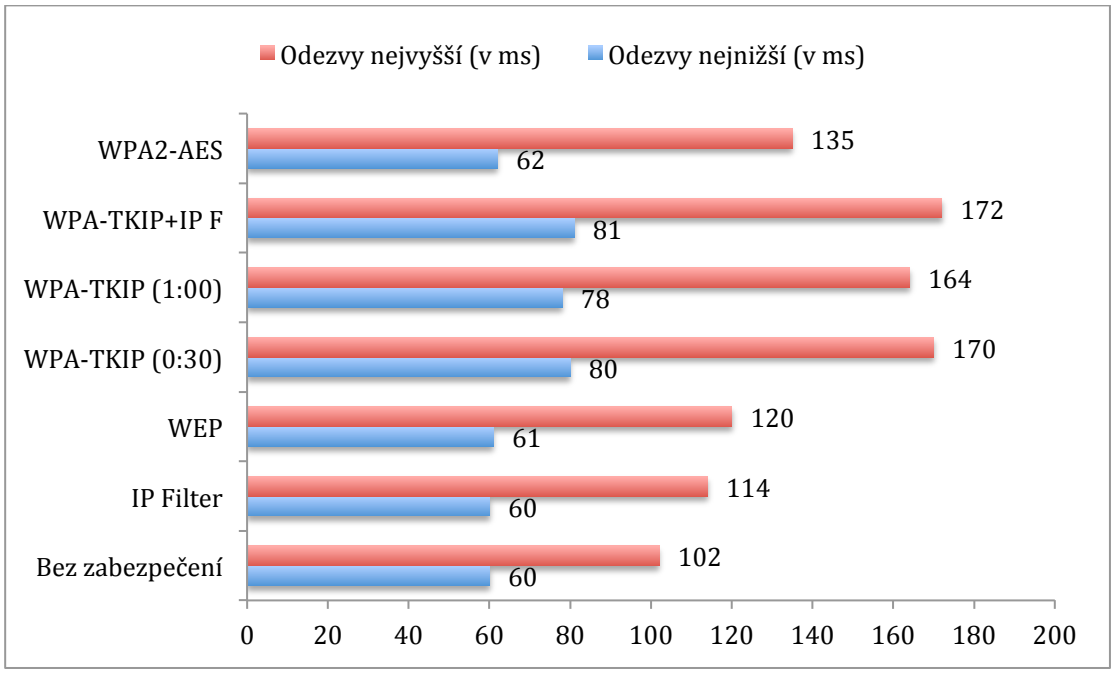
PC1 63-125ms PC2 67-131ms PC3 62-135ms

Výsledky naplnily očekávání. Za povšimnutí zde stojí skutečnost, že při kombinaci NATu s metodou WPA2-AES byl naměřen nejmenší průtok při připojení jednoho počítače.

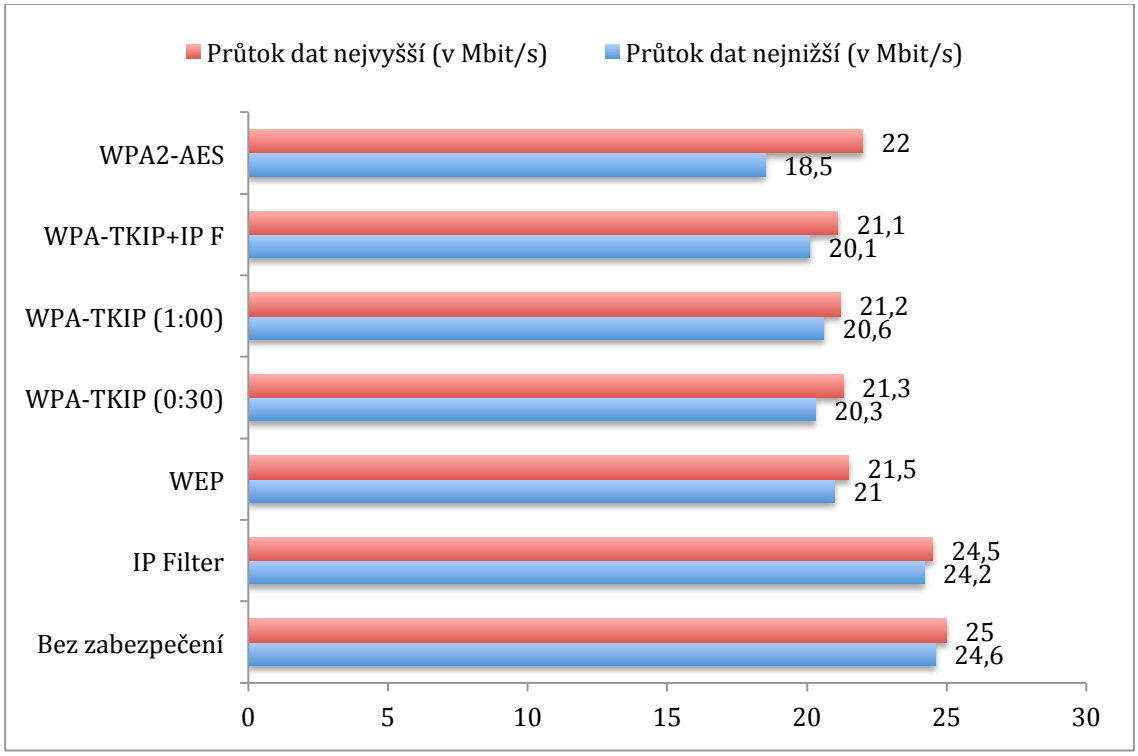
5.2.6 Shrnutí v grafech



Graf č. 4: Naměřené hodnoty vytížení CPU u topologie I.B



Graf č. 5: Naměřené hodnoty odezvy na vysílač u topologie I.B



Graf č. 6: Naměřené hodnoty průtoku dat u topologie I.B

5.3 Topologie II. A

U této konfigurace bude zařízení RB800 figurovat pouze jako drátový router, který bude zajišťovat pouze IP nebo MAC filter. Mezi ním a NanoStationy koncových klientů bude figurovat zařízení NanoStation M5, které bude v módu AP bridge, čímž bude tvořit

vysílací bod a všechna data jím budou procházet v nezměněné formě. U této topologie bude zajímavé sledovat především chování NanoStationu M5, který bude v určitých fázích zajišťovat zabezpečení sítě pomocí WEP, WPA a WPA2. Díky rozšíření sítě o pomocný vysílač by také mělo dojít k rozložení potřebného výkonu zařízení, což by mělo mít za následek snížení vytížení CPU u RouterBoardu. Jak již bylo zmíněno dříve, u zařízení NanoStation bohužel nelze jakkoliv sledovat vytížení systému a vše lze tedy pouze odhadovat. Jako u každé topologie, i zde bude nejdříve provedeno měření bez jakéhokoliv zabezpečení.

Shrnutí - Topologie II. A - Bez zabezpečení

Připojení 1PC	Průtok - 23Mbit/s +- 200Kbit/s	Vytížení CPU RB - 18 - 21%
Připojení 2PC	Průtok - 23Mbit/s +- 300Kbit/s	Vytížení CPU RB - 19 - 24%
Připojení 3PC	Průtok - 25Mbit/s +-300Kbit/s	Vytížení CPU RB - 21 - 25%

Latence na vysílač (IP adresa 10.0.0.1):

PC1	53-80ms	PC2	56-90ms	PC3	59-70ms

Oproti topologiím I. je zde vidět celkově menší datová propustnost, ovšem také značné snížení vytížení CPU u zařízení RouterBoard, které je menší až o jednu polovinu.

5.3.1 IP filter

Pokud bychom měli u této metody vycházet z výsledků předchozího měření, jediný rozdíl by zde měl být ve vytížení CPU RouterBoardu, které by mělo být vyšší.

Shrnutí - Topologie II. A - IP Filter

Připojení 1PC	Průtok - 23Mbit/s +- 200Kbit/s	Vytížení CPU RB - 22 - 25%
Připojení 2PC	Průtok - 23Mbit/s +- 300Kbit/s	Vytížení CPU RB - 23 - 29%
Připojení 3PC	Průtok - 25Mbit/s +-300Kbit/s	Vytížení CPU RB - 40 - 44%

Latence na vysílač (IP adresa 10.0.0.1):

PC1	74-155ms	PC2	82-152ms	PC3	73-151ms

Předpoklady se zde potvrdily. Je zde ovšem patrný značný nárůst hodnot u odezvy na vysílač, který se dá porovnat s hodnotami u topologie I. se zabezpečením WPA-PSK a opět je nelze považovat za použitelné.

5.3.2 WEP

Zde dochází k zatím netestované situaci a to k aplikaci zabezpečení na vysílacím zařízení NanoStation. Nelze zde tedy dopředu odhadnout, jak se celá síť bude chovat.

Shrnutí - Topologie II. A - WEP

Připojení 1PC	Průtok - 4,7Mbit/s +-100Kbit/s	Vytížení CPU RB - 5 - 11%
Připojení 2PC	Průtok - 4,9Mbit/s +-100Kbit/s	Vytížení CPU RB - 5 - 11%
Připojení 3PC	Průtok - 4,9Mbit/s +- 100Kbit/s	Vytížení CPU RB - 5 - 11%

Latence na vysílač (IP adresa 10.0.0.1):

PC1	1320-1360ms	PC2	1318-1357ms	PC3	1327-1373ms

Jak je patrné z výsledků, dochází zde k velice zásadnímu problému. Pokud se porovnají tyto výsledky s údaji získanými v topologii I. A je pravděpodobné, že problém vzniká v zařízení NanoStation M5, které nestačí výkonem. Také velice vzrostly odezvy na vysílač, které jsou v hodnotách naprosto nepoužitelných pro správné fungování sítě. Toto zabezpečení tedy nelze v žádném případě použít pro tento typ topologie.

5.3.3 WPA-PSK TKIP

Pokud by k předpokladům tohoto měření měly být zohledněny výsledky předcházejícího a opravdu by byl problém v nedostatečném výkonu zařízení NanoStation M5, pak by tento typ zabezpečení měl působit ještě větší potíže. Také stojí za zmínku fakt, že oproti zařízení RouterBoard zde nelze nastavit čas změny klíče a tato hodnota je pevně definována v systému.

Shrnutí - Topologie II. A - WPA-PSK TKIP

Připojení 1PC	Průtok - 4,5Mbit/s +-100Kbit/s	Vytížení CPU RB - 4 - 9%
Připojení 2PC	Průtok - 4,4Mbit/s +-100Kbit/s	Vytížení CPU RB - 4 - 9%
Připojení 3PC	Průtok - 4,4Mbit/s +-100Kbit/s	Vytížení CPU RB - 4 - 9%

Latence na vysílač (IP adresa 10.0.0.1):

PC1	1004-1054ms	PC2	1008-1039ms	PC3	1011-1043ms

Výsledky potvrzují předpoklad. Došlo zde k ještě většímu snížení datového průtoku, ikdyž se o několik stovek milisekund snížila odezva na vysílač. Toto řešení však také není v žádném případě použitelné.

5.3.4 WPA-PSK TKIP + IP Filter

V předcházejícím testu bylo prokázáno, že v této topologii není zabezpečení WPA-PSK použitelné, proto se zde toto testování objevuje pouze pro úplnost.

Shrnutí - Topologie II. A - WPA-PSK TKIP + IP Filter

Připojení 1PC	Průtok - 4,5Mbit/s +-100Kbit/s	Vytížení CPU RB - 6 - 10%
Připojení 2PC	Průtok - 4,4Mbit/s +-100Kbit/s	Vytížení CPU RB - 6 - 10%
Připojení 3PC	Průtok - 4,4Mbit/s +-100Kbit/s	Vytížení CPU RB - 6 - 10%

Latence na vysílač (IP adresa 10.0.0.1):

PC1	1002-1057ms	PC2	1008-1036ms	PC3	1006-1048ms

5.3.5 WPA2-AES

U tohoto měření bude velice záležet na implementaci standardu WPA2-AES v zařízení NanoStation M5. Jak již bylo napsáno dříve, toto zabezpečení vychází z jiného algoritmu než všechny předcházející metody a proto z jejich výsledků nelze vycházet.

Shrnutí - Topologie II. A - WPA2-AES

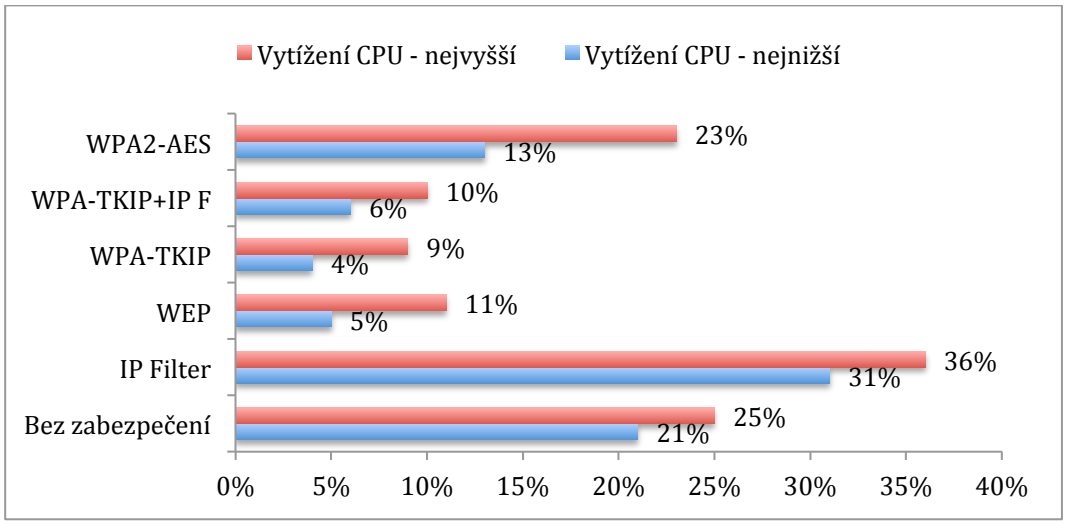
Připojení 1PC	Průtok - 17Mbit/s -+400kbit/s	Vytížení CPU RB - 17 - 23%
Připojení 2PC	Průtok - 8,3Mbit/s -+ 200Kbit/s	Vytížení CPU RB - 13 - 20%
Připojení 3PC	Průtok - 8,3Mbit/s -+200kbit/s	Vytížení CPU RB - 13 - 20%

Latence na vysílač (IP adresa 10.0.0.1):

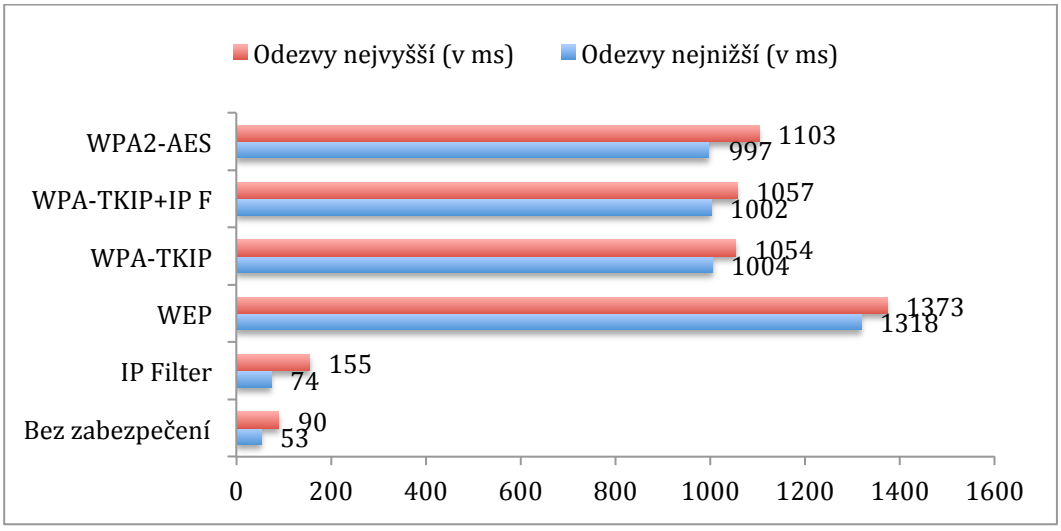
PC1	1010-1103ms	PC2	1003-1089ms	PC3	997-1096ms

U tohoto standardu je vidět mnohem lepší funkčnost než u metod WEP a WPA, nicméně po připojení více než jednoho počítače došlo opět k zásadnímu snížení průtoku dat a k nárůstu odezvy na vysílač.

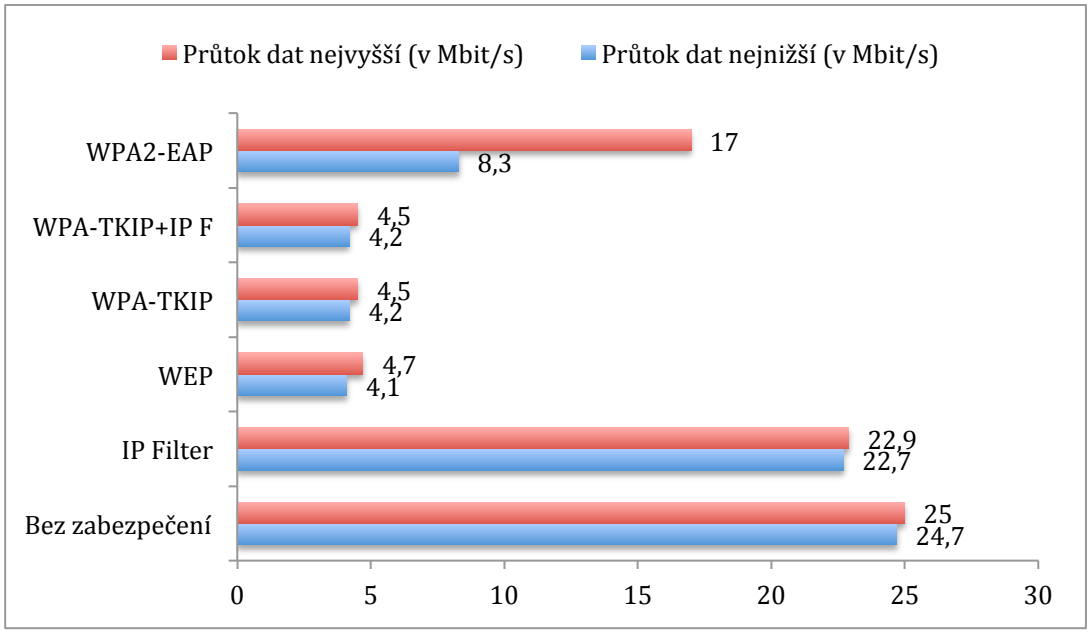
5.3.6 Shrnutí v grafu



Graf č. 7: Naměřené hodnoty vytížení CPU u topologie II.A



Graf č. 8: Naměřené hodnoty odezvy na vysílač u topologie II.A



Graf č. 9: Naměřené hodnoty průtoku dat u topologie II.A

5.4 Topologie II. B

Tato topologie vychází jako kombinace všech předchozích a proto zde není nutné každou variantu zabezpečení komentovat. Vždy tedy budou zobrazeny pouze výsledky měření a okomentovány budou pouze v případě, že by se v nich vyskytla zajímavost nebo anomálie.

Výsledky testování bez jakéhokoliv zabezpečení:

Shrnutí - Topologie II. B - Bez zabezpečení

Připojení 1PC	Průtok - 20,5Mbit/s +- 300Kbit/s	Vytížení CPU RB - 17 - 22%
Připojení 2PC	Průtok - 25Mbit/s +- 400Kbit/s	Vytížení CPU RB - 19-24%
Připojení 3PC	Průtok - 25Mbit/s +-400Kbit/s	Vytížení CPU > 22-27%

Latence na vysílač (IP adresa 10.0.0.1):

PC1	63-104ms	PC2	67-102ms	PC3	63-88ms

5.4.1 IP Filter

Shrnutí - Topologie II. B - IP Filter

Připojení 1PC	Průtok - 23Mbit/s +- 200Kbit/s	Vytížení CPU RB - 22 - 25%
Připojení 2PC	Průtok - 23Mbit/s +- 300Kbit/s	Vytížení CPU RB - 23 - 29%
Připojení 3PC	Průtok - 25Mbit/s +-300Kbit/s	Vytížení CPU RB - 40 - 44%

Latence na vysílač (IP adresa 10.0.0.1):

PC1	74-155ms	PC2	82-152ms	PC3	73-151ms

5.4.2 WEP

Shrnutí - Topologie II. B - WEP

Připojení 1PC	Průtok - 4,7Mbit/s +- 100Kbit/s	Vytížení CPU RB - 5 - 11%
Připojení 2PC	Průtok - 4,9Mbit/s +- 100Kbit/s	Vytížení CPU RB - 5 - 11%
Připojení 3PC	Průtok - 5,1Mbit/s +- 100Kbit/s	Vytížení CPU RB - 5 - 11%

Latence na vysílač (IP adresa 10.0.0.1):

PC1	1324-1376ms	PC2	1323-1367ms	PC3	1331-1378ms

5.4.3 WPA-PSK TKIP

Shrnutí - Topologie II. B - WPA-PSK TKIP

Připojení 1PC Průtok - 4,8Mbit/s +- 100Kbit/s Vytížení CPU RB - 4 - 9%

Připojení 2PC Průtok - 4,7Mbit/s +- 100Kbit/s Vytížení CPU RB - 4 - 9%

Připojení 3PC Průtok - 4,8Mbit/s +- 100kbit/s Vytížení CPU RB - 4 - 9%

Latence na vysílač (IP adresa 10.0.0.1):

PC1 1002-1049ms PC2 997-1146ms PC3 1014-1065ms

5.4.4 WPA-PSK TKIP + IP Filter

Shrnutí - Topologie II. B - WPA-PSK TKIP + IP Filter

Připojení 1PC Průtok - 4,5Mbit/s +- 100Kbit/s Vytížení CPU RB - 6 - 10%

Připojení 2PC Průtok - 4,4Mbit/s +-100Kbit/s Vytížení CPU RB - 6 - 10%

Připojení 3PC Průtok - 4,4Mbit/s +-100Kbit/s Vytížení CPU RB - 6 - 10%

Latence na vysílač (IP adresa 10.0.0.1):

PC1 1003-1054ms PC2 1000-1146ms PC3 1014-1065ms

5.4.5 WPA2-EAP

Shrnutí - Topologie II. B - WPA2-AES

Připojení 1PC Průtok - 15,7Mbit/s -+400kbit/s Vytížení CPU RB - 16 - 20%

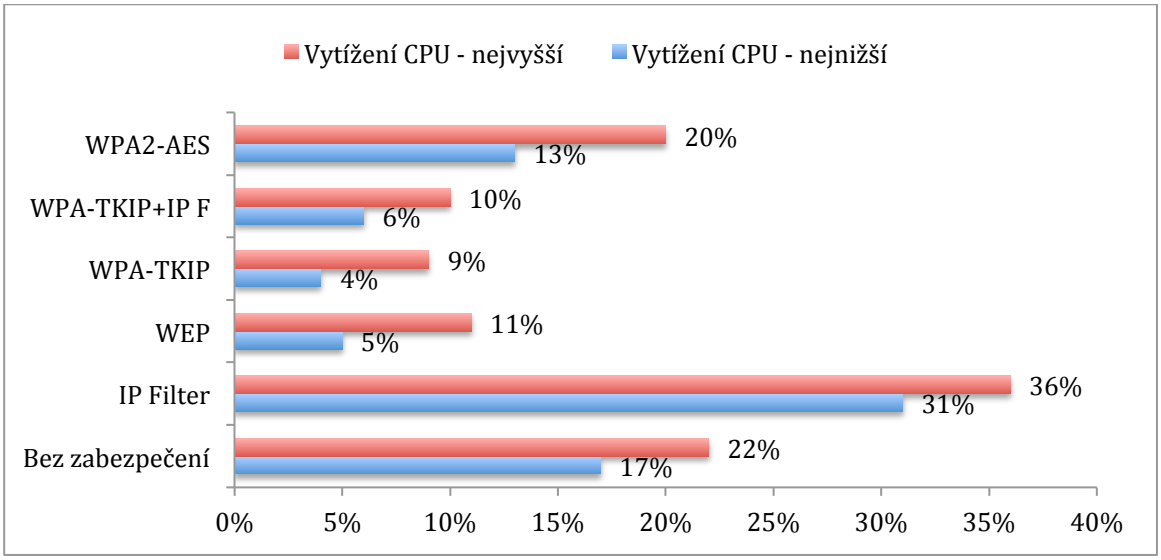
Připojení 2PC Průtok - 8,3Mbit/s -+ 200Kbit/s Vytížení CPU RB - 13 - 17%

Připojení 3PC Průtok - 8,3Mbit/s -+200kbit/s Vytížení CPU RB - 13 - 17%

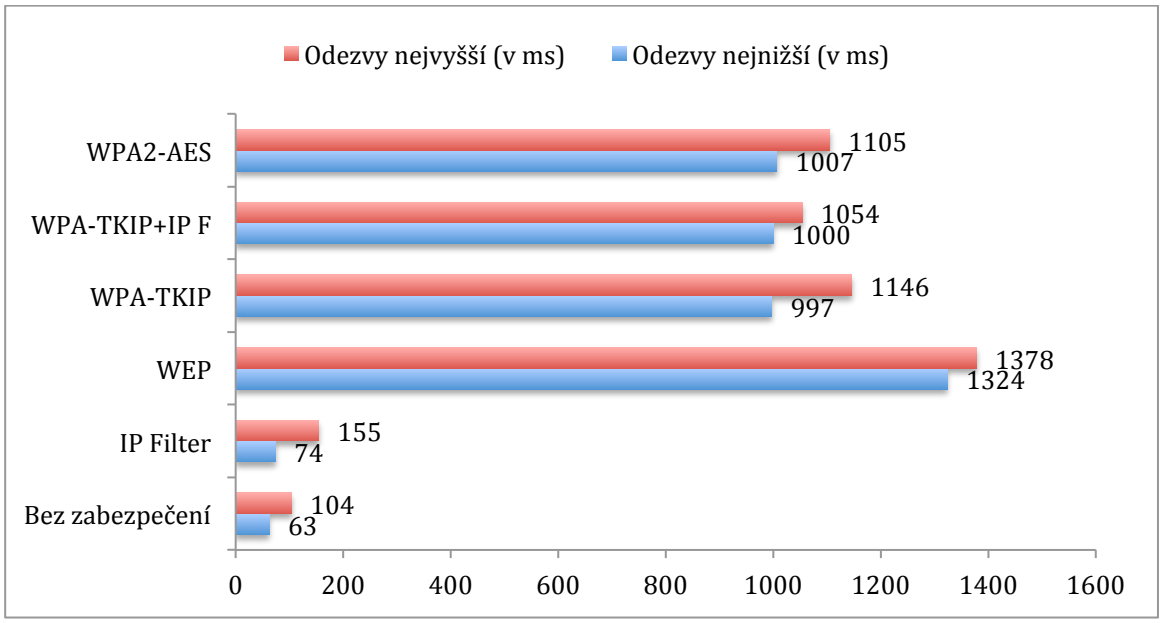
Latence na vysílač (IP adresa 10.0.0.1):

PC1 1007-1070ms PC2 1012-1105ms PC3 1009-1088ms

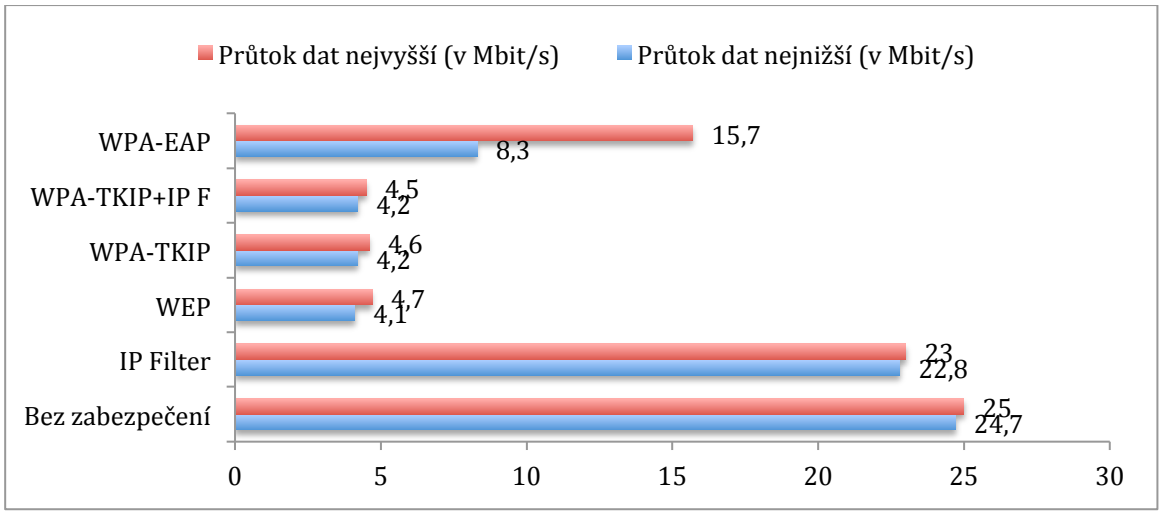
5.4.6 Shrnutí v grafu



Graf č. 10: Naměřené hodnoty vytížení CPU u topologie II. B



Graf č. 11: Naměřené hodnoty odezvy na vysílač u topologie II. B



Graf č. 12: Naměřené hodnoty průtoku dat u topologie II. B

6. Závěr - Souhrn z pohledu bezpečnosti

Z výsledků testování plyne několik závěrů. Pokud by se zohlednily údaje poskytnuté společností Inet4 o počtech uživatelů na jeden vysílač, je jasné, že rozsáhlejší vysílací body lokálních internetových poskytovatelů nelze nikdy dostatečně zabezpečit. Na vysílačích s větším počtem uživatelů nelze kromě IP a MAC filtru aplikovat žádnou z metod aktivního zabezpečení a nelze tak aktivní formou zabránit průniku do sítě. Jedinou možností tak zůstává aplikace všech pasivních metod, které sice nezvyšují vytíženost zařízení, ale také síť aktivně neochrání. Dojde pouze ke zkomplikování situace útočníkovi, kterému zabere delší čas orientace v síti. Tyto pasivní metody však samy o sobě dokážou chránit před útoky uvnitř sítě, neboť při správně konfiguraci všech zmíněných metod a při použití NATu nemá vnitřní útočník šanci identifikovat své okolí.

6.1 Zabezpečení jednotlivých topologií

V této části lze řešení rozdělit do dvou částí podle typu topologií. U konfigurace I. A a I. B je situace plně závislá na počtu uživatelů a službách, jaké jim budou poskytovány (rychlost připojení, VoIP, internetová TV, atd.). U vysílače menšího typu, který by měl být těmito topologiemi reprezentován, lze do určitého počtu připojených klientů uvažovat i o zabezpečení WEP nebo WPA. V kombinaci se všemi pasivními metodami a s použitím NATu pak lze dosáhnout relativně dobře zabezpečené sítě, kterou by mohl být problém prolomit a získat z ní nějaká data.

U topologií II. A a II. B je situace poněkud složitější. Pokud se budou brát v úvahu počty připojených klientů udávané společností Inet4, je použití metod WEP a WPA naprosto nemožné. V tomto případě lze uvažovat pouze o užití IP/MAC filteru (nebo jejich kombinaci), jehož náročnost se však také stupňuje s počtem připojených klientů. U těchto konfigurací je naprosto nezbytné využití alespoň pasivních metod zabezpečení, které alespoň trochu snižují pravděpodobnost úspěšného odchytu dat v síti.

6.2 Zabezpečení menší bezdrátové sítě

Pokud by měly být výsledky měření aplikovány pro výstavbu menší (lokální) bezdrátové sítě například pro objekt sídla společnosti (nebudeme uvažovat použití WPA v kombinaci s RADIUS serverem) nebo pro domácnost, je zde více aspektů, které musí být zhodnoceny. Kromě počtu uživatelů, který je zde ovšem také důležitý, je nutné prověřit rizikovost okolního prostředí a charakter přenášených dat. Pokud bude síť nutně disponovat

velkým vyzařovacím výkonem, který by mohl být zachycen v širokém, hustě osídleném okolí, je nutné počítat s vyšší pravděpodobností útoku na síť. Dále je potřeba zhodnotit typ dat, který je sítí přenášen. Pokud se jedná síť, kde je Wi-Fi používána pouze pro přenos online TV, je zde kladen důraz především na přenosovou kapacitu sítě a nemusí být perfektně zabezpečena. Naopak v síti s vyšší citlivostí přenášených dat by měly být eliminovány větší datové přenosy bezdrátovou částí sítě a důraz by měl být kladen především na bezpečnost. Pokud bude sítí protékat menší množství dat, bude možné ji dobře zabezpečit i při větším množství uživatelů.

6.3 Bezpečnost v praxi

Pro větší hodnotu této práce a zobecnění údajů dodaných společností Inet4 s.r.o., byl proveden průzkum bezdrátových sítí v Českých Budějovicích. Ten probíhal ze střechy objektu, z níž je vidět větší část města, včetně přilehlých aglomerací. Na obrázku[37], kterým je otisk obrazovky z konfigurace zařízení NanoStation, je vidět seznam nalezených sítí. Z legislativních důvodů byly překryty přesné názvy sítí a některé další údaje. Nicméně je zde vidět, že drtivá většina sítí poskytovatelů internetu (jsou označeny numerickými hodnotami, jiné číslo, jiný poskytovatel) neobsahují žádné zabezpečení.

[37] Příloha č. 13: Zjištěné sítě v Českých Budějovicích a nejbližším okolí

7. Bibliografie

1. Specifikace zařízení Mikrotik RB800 [online]. [cit. 2012-04-10]. Dostupné z: http://routerboard.com/RB800

2. Seznam meteorologických stanic ČR [online]. [cit. 2012-04-10]. Dostupné z: http://portal.chmi.cz

3. Definice CCQ [online]. [cit. 2012-04-10]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:Wireless_FAQ

4. Definice AirMax. [cit. 2012-04-10]. Dostupné z: http://i4wifi.blog.cz/1102/tipy-ubiquiti-jak-pracuje-airmax

5. Definice NAT. [cit. 2012-04-10]. Dostupné z: http://www.farpost.net/glossary/nat.php

6. Definice WEP. [cit. 2012-04-10]. Dostupné z: http://support.netgear.com/app/answers/detail/a_id/1141/~/what-is-wep-encryption-for-wireless-networks%3F

7. Definice standardu WPA2 . [cit. 2012-04-10]. Dostupné z: http://standards.ieee.org/findstds/interps/802.11i-2004.html

8. Certifikace Wi-Fi zařízení . [cit. 2012-04-10]. Dostupné z: http://www.wi-fi.org/knowledge-center/white-papers/state-wi-fi®-security-wi-fi-certified™-wpa2™-delivers-advanced

9. Definice pojmu ESSID. [cit. 2012-04-10]. Dostupné z: http://wiki.airdump.cz/ESSID

10. Definice a popis DHCP. [cit. 2012-04-10]. Dostupné z: http://www.abclinuxu.cz/slovnik/dhcp

8. Seznam příloh

Příloha č. 1: Elektronická korespondence se společnostmi i4wifi a.s a Aspa a.s.

I4wifi a.s.:

Vážený pane Prokeši,

Naše firma se na trhu vyskytuje od roku 2007 a již od samotného počátku jsme jedním z největších distributorů Wi-Fi zařízení v České republice. V prodejnosti zařízení u naší firmy jednoznačně dominují zařízení od firmy Ubiquiti, Mikrotik a TP-link. Z Vaší zprávy je patrné, že máte zájem především o zařízení používaná poskytovateli bezdrátového internetového připojení. Mezi ta se již od samotného začátku řadí celá produktová řada společnosti Ubiquiti a také zařízení od firmy MikroTik. Díky našemu firemnímu blogu a zpětné odezvě od našich stálých zákazníků Vám můžeme říci, že zařízení Ubiquity jsou velice oblíbená jako klientské prvky a to především pro jejich bezporuchovost, snadnou montáž i nastavení. Poslední dobou (hlavně od uvedení zařízení Ubiquiti řady M s podporou AirMaxu) se používají i jako vysílací nebo point-to-point body. Zařízení Mikrotik jsou pak používána jako routery a nebo menší vysílače a jejich největší výhodou je systém RouterOS. Zařízení TP-link jsou používána pouze jako routery a access pointy do domácností a malých organizací.

Přeji hodně štěstí při psaní bakalářské práce,

S pozdravem

Michal Štepánek,

Obchodně technické oddělení i4wifi a.s.

```
From: Michal Prokeš [mailto:prokes@tz-mont.cz]
Sent: Wednesday, March 22, 2012 11:00 AM
To: 'sales@i4wifi.cz'
Subject: Podklady pro bakalářskou práci

Vážená společnosti,

Obracím se na Vás s prosbou o spolupráci pro mou bakalářskou práci.
Jmenuji se Michal Prokeš, jsem studentem třetího ročníku Aplikované
informatiky na Přírodovědecké fakultě Jihočeské univerzity a právě pracuji
na bakalářské práci s názvem Analýza bezpečnostních mechanizmů Wi-Fi sítí.
Cílem této práce bude testování zabezpečovacích metod na nejčastěji
prodávaných zařízeních pro Wi-Fi a to jak v rozsahu menších (lokálních)
bezdrátových sítí, tak na i sítích poskytující bezdrátové připojení
k internetu. Rád bych Vás proto poprosil o údaje o prodejnosti zařízení,
popřípadě pokud by bylo možné jejich rozdělení do kategorií podle
využitelnosti (poskytovatelé/domácnosti).

Mockrát děkuji,

S pozdravem


Michal Prokeš
```

Příloha č. 1: Elektronická korespondence se společnostmi i4wifi a.s a Aspa a.s.

Aspa a.s.:

Dobrý den,

Na základě sumarizace našich realizovaných objednávek Vám můžeme sdělit, že mezi nejprodávanější zařízení v oblasti Wi-Fi patří zařízení od společností Ubiquiti, Mikrotik a TP-Link

S pozdravem

Jiří Kučera,

Obchodní oddělení

Aspa a.s.

From: Michal Prokeš [mailto:prokes@tz-mont.cz]
Sent: Wednesday, March 22, 2012 11:20 AM
To: 'hardware@aspa.cz'
Subject: Podklady pro bakalářskou práci

Vážená společnosti,

Obracím se na Vás s prosbou o spolupráci pro mou bakalářskou práci. Jmenuji se Michal Prokeš, jsem studentem třetího ročníku Aplikované informatiky na Přírodovědecké fakultě Jihočeské univerzity a právě pracuji na bakalářské práci s názvem Analýza bezpečnostních mechanizmů Wi-Fi sítí. Cílem této práce bude testování zabezpečovacích metod na nejčastěji prodávaných zařízeních pro Wi-Fi a to jak v rozsahu menších (lokálních) bezdrátových sítí, tak na i sítích poskytující bezdrátové připojení k internetu. Rád bych Vás proto poprosil o údaje o prodejnosti zařízení, popřípadě pokud by bylo možné jejich rozdělení do kategorií podle využitelnosti (poskytovatelé/domácnosti).

Mockrát děkuji,

S pozdravem

Michal Prokeš

Příloha č. 2: Elektronická korespondence se společností Inet4 s.r.o.

Dobrý den,

Co se týká zařízení, můžeme Vám potvrdit informace od níže uvedených společností. Všechny tyto produkty používáme a v praxi se nám velice osvědčili. Zařízení Mikrotik se používají především na vysílací body a důležité páteřní uzle sítě, zatímco zařízení Ubiquiti jsou výborným klientským zařízením. Od vydání NanoStationu M5 je používáme i na vysílače, protože mají mnohem větší propustnost než AP stavěná pouze na MikroTiku. Použité metody zabezpečení Vám z důvodu naší firemní politiky sdělit nemohu, nicméně průměrný počet uživatelů na jednom vysílači je v naší síti okolo 10-15ti, v závislosti na lokalitě a velikosti vysílače.

S pozdravem

Tomáš Rychlík

Hlavní technik

Inet4 s.r.o.

From: Michal Prokeš [mailto:prokes@tz-mont.cz]
Sent: Thursday, March 23, 2012 15:20 PM
To: 'info@inet4.cz'
Subject: Podklady pro bakalářskou práci

Vážená společnosti,

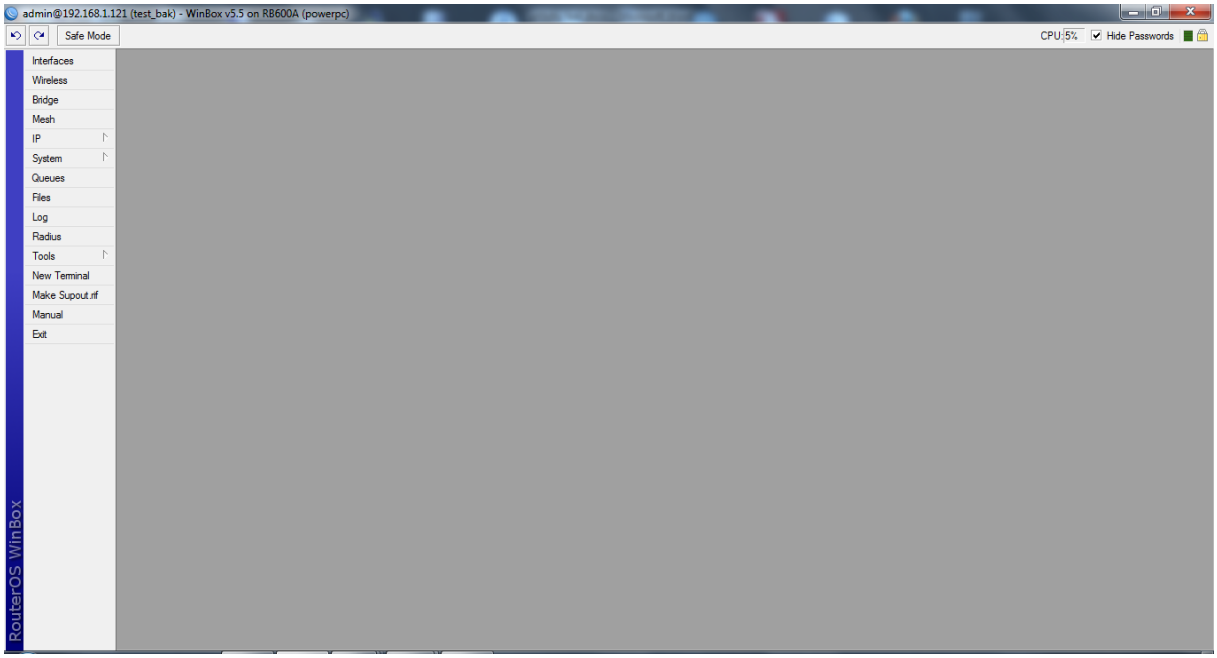
Obracím se na Vás s prosbou o spolupráci pro mou bakalářskou práci. Jmenuji se Michal Prokeš, jsem studentem třetího ročníku Aplikované informatiky na Přírodovědecké fakultě Jihočeské univerzity a právě pracuji na bakalářské práci s názvem Analýza bezpečnostních mechanizmů Wi-Fi sítí. Cílem této práce bude testování zabezpečovacích metod na nejčastěji prodávaných zařízeních pro Wi-Fi a to jak v rozsahu menších (lokálních) bezdrátových sítí, tak na i sítích poskytující bezdrátové připojení k internetu. Již jsem oslovil společnosti i4wifi a.s. a Aspa a.s., kteří jsou jedni z největších dodavatelů Wi-Fi zařízení v České republice. Obě tyto společnosti se shodly na tom, že mezi nepoužívanější zařízení patří produkty firem Mikrotik, Ubiquiti a TP-Link. Rád bych se Vás proto zeptal, zda tato zařízení ve Vaší síti používáte, popřípadě v jakém rozsahu. Pokud by to bylo možné, rád bych se také informoval o typu zabezpečení, které v síti používáte a kolik máte průměrně připojených klientů na vysílač.

Mockrát děkuji,

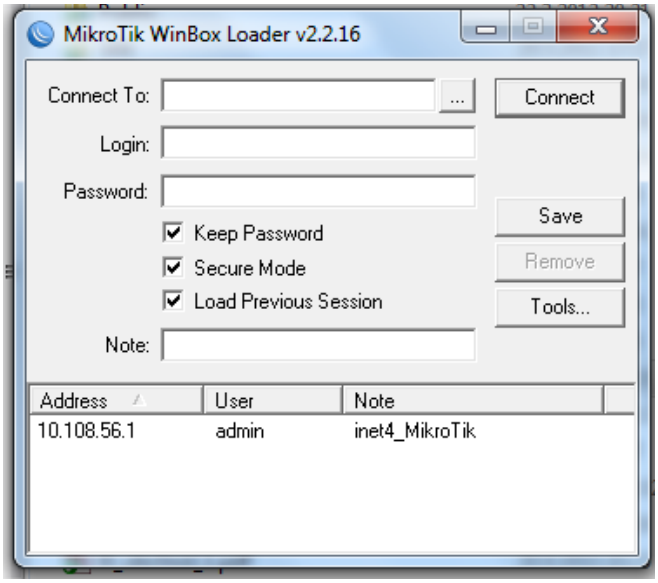
S pozdravem

Michal Prokeš

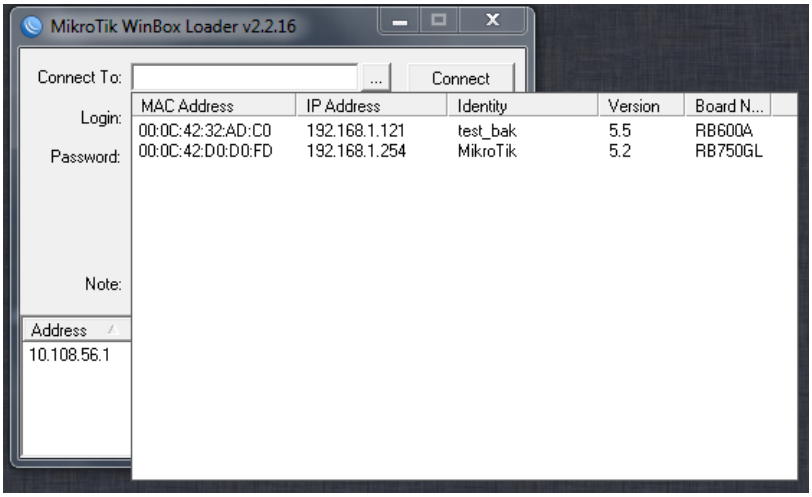
Příloha č. 3: Příloha č. 3: Grafické rozhraní programu WinBox pro konfiguraci zařízení Mikrotik



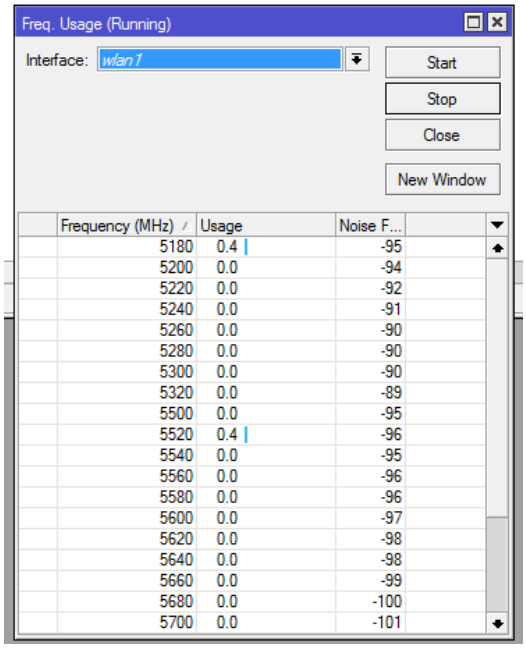
Příloha č. 4: Úvodní obrazovka programu WinBox



Příloha č. 5: Okno programu WinBox s otevřeným dialogovým oknem a nalezeným zařízením

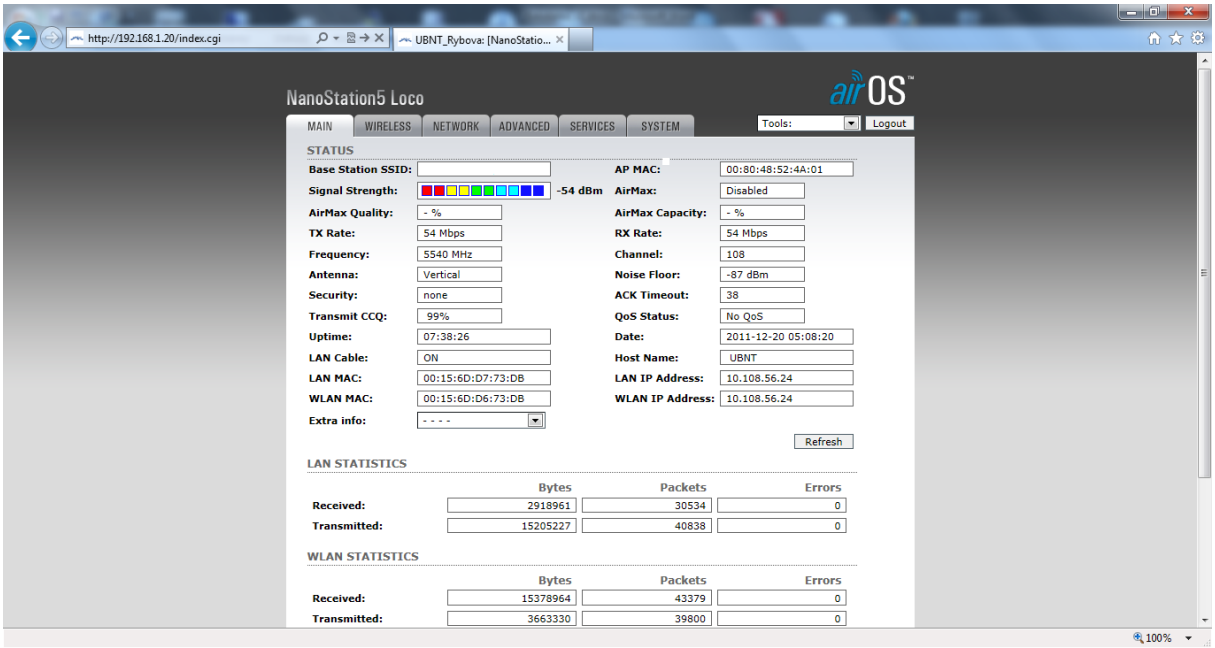


Příloha č. 6: Výsledky měření pomocí metody Frequency Usage

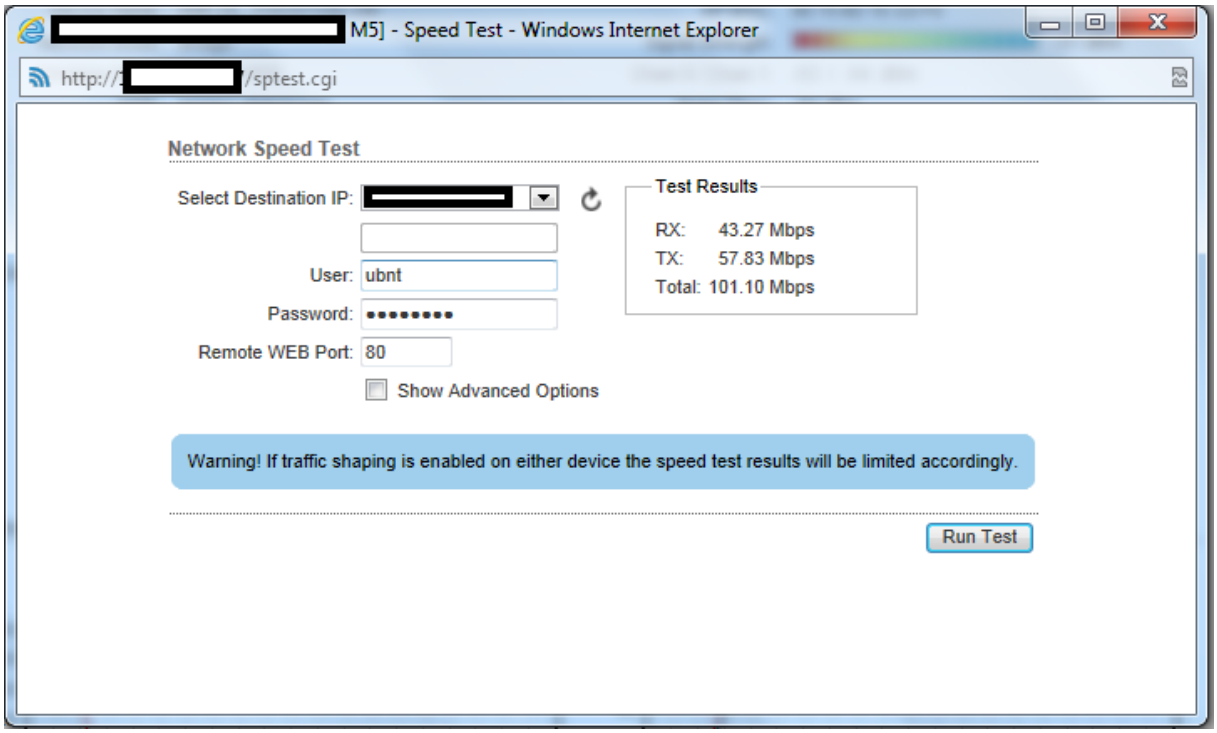


Frequency (MHz)	Usage	Noise F...
5180	0.4	-95
5200	0.0	-94
5220	0.0	-92
5240	0.0	-91
5260	0.0	-90
5280	0.0	-90
5300	0.0	-90
5320	0.0	-89
5500	0.0	-95
5520	0.4	-96
5540	0.0	-95
5560	0.0	-96
5580	0.0	-96
5600	0.0	-97
5620	0.0	-98
5640	0.0	-98
5660	0.0	-99
5680	0.0	-100
5700	0.0	-101

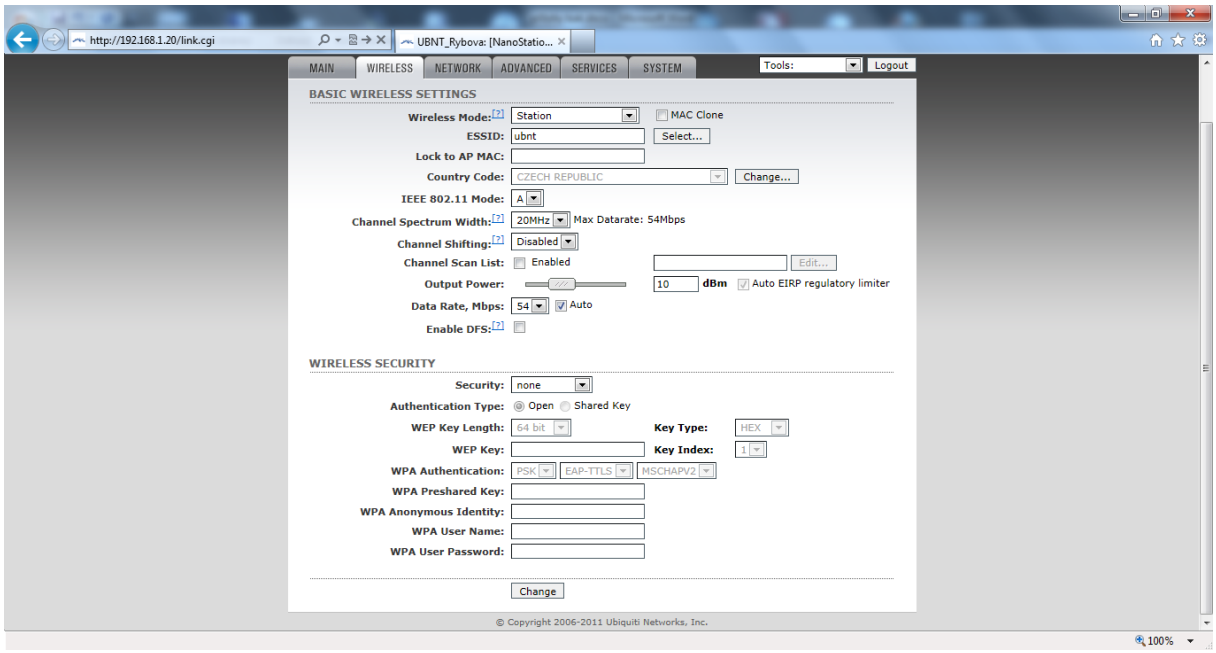
Příloha č. 7: Úvodní stránka po přihlášení do zařízení NanoStation



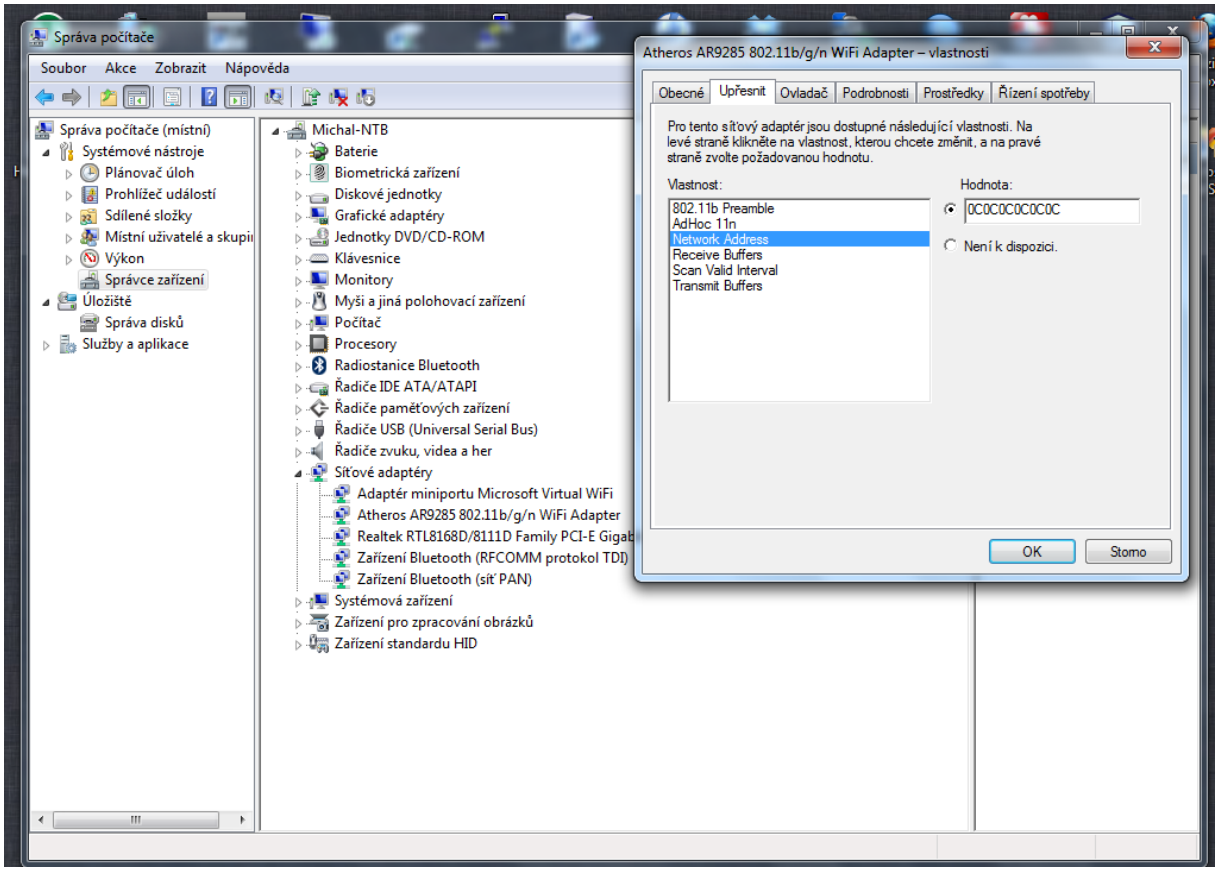
Příloha č. 8: Měření rychlosti mezi zařízeními NanoStation M5



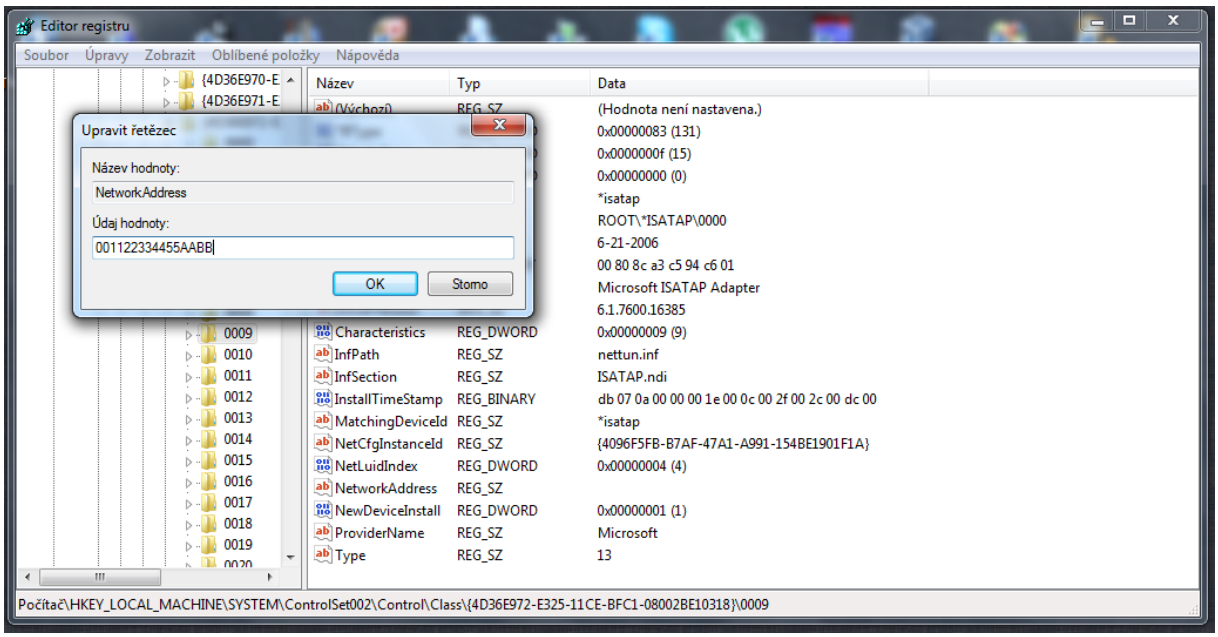
Příloha č. 9: Možnosti nastavení bezdrátové části zařízení NanoStation



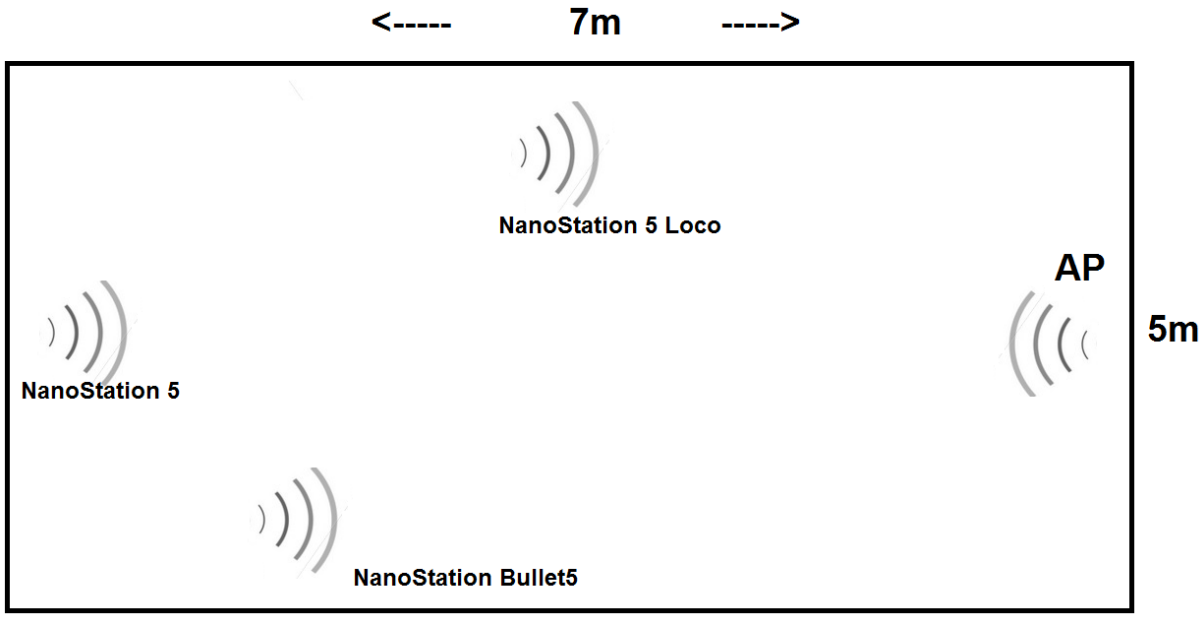
Příloha č. 10: Softwarová úprava MAC adresy počítače v části Správce zařízení



Příloha č. 11: Softwarová úprava MAC adresy počítače v části Registry systému



Příloha č. 12: Půdorys testovací místnosti včetně rozmístění jednotlivých prvků



Příloha č. 13: Zjištěné sítě v Českých Budějovicích a nejbližším okolí