Sem vložte zadání Vaší práce.

České vysoké učení technické v Praze
Fakulta informačních technologií
Katedra počítačových systémů

Diplomová práce

Vylepšení bezdrátové síťové infrastruktury

Bc. Jaroslav Pouzar

Vedoucí práce: Ing. Viktor Černý

4. května 2015

Poděkování

Chtěl bych poděkovat vedoucímu práce za poskytnutí cenných a praktických rad a za zapůjčení spektrálního analyzéru. Rovněž bych chtěl poděkovat vedení střední školy, v jejímž prostředí tato práce vznikala a zejména pak správci sítě za důvěru ve mě vloženou při rekonfiguraci síťových zařízení a implementaci navržených úprav.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, avšak pouze k nevýdělečným účelům. Toto oprávnění je časově, teritoriálně i množstevně neomezené.

V Praze dne 4. května 2015 .....

Odkaz na tuto práci

Pouzar, Jaroslav. *Vylepšení bezdrátové síťové infrastruktury.* Diplomová práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2015.

Abstrakt

Podstatou této práce je analyzovat již existující bezdrátovou síť, posoudit její kvality a následně navrhnout a implementovat možná vylepšení. Důraz je přitom kladen nejenom na zlepšení dostupnosti a kvality služby ve školním areálu, ale i na zvýšení úrovně zabezpečení sítě a zlepšení možností dohledu a správy síťových zařízení. Výsledné řešení nabídne uživatelům možnost připojení k bezdrátové síti s šifrovaným přenosem dat a centrální autentizací integrovanou do stávající autentizační a autorizační infrastruktury.

Klíčová slova wifi, bezdrátová síť, RADIUS, MikroTik, RouterBOARD, optimalizace

Abstract

The purpose of this thesis is to analyze an existing wireless network, measure its quality and suggest possible improvements and then implement these where appropriate. Improvements are not limited to wireless performance and coverage only but they also focus on other areas such as encryption, monitoring and network devices management. Final implemented solution offers a possibility for users to connect to a broadcasted wireless network with encrypted data transfer and central authentication mechanism which is integrated to a current authentication and authorization infrastructure.

Keywords wifi, wireless network, RADIUS, MikroTik, RouterBOARD, optimization

Obsah

Seznam obrázků

Seznam tabulek

Úvod

O škole
Tato diplomová práce se věnuje bezdrátové počítačové síti na střední a vyšší odborné škole s oficiálním názvem „Střední zdravotnická škola a Vyšší odborná škola zdravotnická, České Budějovice, Husova 3“ – dále v textu uváděna jen jako „škola“. Tuto školu v aktuálním školním ročníku 2014/2015 navštěvuje přibližně 520 žáků a působí zde celkem dohromady 73 pedagogických a nepedagogických zaměstnanců[1].

Struktura práce
Strukturu této diplomová práce tvoří teoretická a praktická část. Nejprve se v první (teoretické) části zabývám popisem komunikačních principů bezdrátových sítí určených pro použití v budovách a dále se pak zaobírám rozborem a popisem charakteristik a jevů, jež mají z různých pohledů vliv na kvalitu a výkon bezdrátových sítí. V další části práce (praktické) se pak věnuji analýze konkrétní existující sítě a navrhuji její možná vylepšení a to s velkým ohledem na možné finanční náklady a technické možnosti stávajících prvků síťové infrastruktury. Vybraná možná vylepšení následně realizuji, přičemž podstatná část práce se věnuje právě implementaci navržených úprav a následnému měření a testování jejich vlivu. Je nutné uvést, že v průběhu řešení práce bylo takřka vždy nutné řešit a implementovat současně několik záležitostí z různých oblastí, jejichž problematiku jsem se ale pro účely lepší přehlednosti a struktury práce rozhodl rozdělit na několik částí – např. implementace VLAN, úprava adresních rozsahů IP sítě, migrace DHCP služby atd. Závěr tohoto dokumentu je věnovaný zhodnocení efektů a přínosů realizovaných změn a nastínění dalších problematik k řešení.

Tématu analýzy, modifikací a úprav bezdrátových sítí se věnují i některé specializované společnosti a poskytují tyto služby na komerční bázi. Po prozkou-

mání produktových nabídek několika takových společností je nutné konstatovat, že se i přes podporu ze strany katedry počítačových systémů při fakultě informačních technologií a katedry počítačů při fakultě elektrotechnické nemohu srovnávat použitým vybavením se společnostmi přímo specializovanými na tuto problematiku. Příkladem je deklarované analyzování více než 600 metrik bezdrátové sítě v několikaměsíčním období společností 7Signal[2].

Význam a použití školní bezdrátové sítě
Žáci školy mají možnost připojit se k internetu prostřednictvím těchto prostředků:

- 4 terminálové stanice ve školní knihovně během její provozní doby
- počítače v učebně výpočetní techniky
- bezdrátová síť

Z uvedeného stručného výčtu plyne, že školní bezdrátová síť je na této škole pro žáky nejvýznamnějším způsobem připojení k internetu. Bezdrátová síť byla na škole vybudována během letních prázdnin v roce 2011 a v nezměněné podobě funguje dosud. Význam přítomnosti možnosti připojení k internetu během denní výuky resp. o přestávkých podporuje i průzkum provedený ČSÚ v březnu 2015 v ČR v němž se uvádí, že „téměř všichni studenti starší 16let používají internet, pouze 3 studenti z tisícovky internet nepoužívají“[3]. Připojení k internetu se tak stává čím dál více neodloučitelným prvkem života dnešních školáků.

Vzhledem k tomu, že je tato práce velmi silně implmentačně zaměřena, tak bych ještě na závěr úvodní části rád upozornil na obsah přiloženého datového nosiče, kde přikládám nákresy, výstupy z měření, konfigurace, vytvořené skripty, logy, snímky z implementace, dokumentaci některých postupů, snímky obrazovek nebo jejich výřezy, vlastní pořízené fotografie a další související materiály, na které se v textu práce odkazuji.

Většina analytických a implementačních prací na stávající bezdrátové síti probíhala za běžného provozu školy s vyjímkou několika zásadních konfiguračních kroků a v práci popsaného syntetického testu se zapůjčenými školními laptopy.

Kapitola 1

Analýza problematiky a prostředí

1.1 Teoretická část

1.1.1 Komunikační standardy a teorie komunikace

Komunikační standardy
Nejznámější a celosvětově nejrozšířenější sadou komunikačních standardů pro připojení standardních uživatelských zařízení jakými jsou např. mobilní telefony, tablety, přenosné počítače k počítačové síti resp. internetu pomocí bezdrátových technologií je rodina standardů s názvem IEEE 802.11. V takto označené skupině nalezneme sadu protokolů jednak těch, jenž se zabývají přístupem ke sdílenému médiu a rovněž také těch, jenž specifikují operace a využití samotné fyzické vrstvy. Struktura uvedeného názvu se skládá ze zkratky instituce zajišťující sdružení vědců a inženýrů ve vybraných oblastech elektroniky, telekomunikací a počítačů. Tato instituce se sídlem v USA vznikla sloučením 2 organizací 1.ledna 1963 a jejím záměrem je sdružovat profesionály vybraných oblastí, usnadňovat vzájemnou komunikaci, pořádat konference, vydávat výzkumné články a podílet se na definici průmyslových standardů.[4] Zde se opět dostáváme ke skupině standardů 802, která se věnuje místním (případně městským) sítím s proměnnou velikostí přenášených datových jednotek – paketů a zaměřuje se přitom na spodní 2 vrstvy 7vrstvého ISO/OSI síťového modelu – fyzickou a linkovou. Druhou zmíněnou vrstvu – linkovou pak rozděluje na 2 dílčí podvrstvy – MAC a LLC.

Podskupinou skupiny 802 je mimo jiné skupina s číslem 11, která bude pro následující text nejpodstatnější a jenž se věnuje právě lokálním bezdrátovým sítím - odtud tedy výše uvedený celý název standardu IEEE 802.11. Zaměříme–li se pouze na skupinu standardů 802.11, pak zjistíme, že existuje další členění utvořené přidáním písmene (případně i více písmen) za číslo 11.

Tabulka 1.1: Srovnání standardů skupiny 802.11

	802.11a	802.11b	802.11g	802.11n
Datum schválení	1997/07	1997/07	2003/06	2009/10
Max. př. rychlost	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Modulace	OFDM	CCK DSSS	CCK DSSS OFDM	CCK DSSS OFDM
Frekvenční pásmo	5 GHz	2,4 GHz	2,4 GHz	2,4 nebo 5 GHz
Šířka kanálu	20 MHz	20 MHz	20 MHz	20 nebo 40 MHz

Počínaje tak abecedně standardem 802.11a se konečně dostáváme ke srovnání komunikačních standardů, jež lze použít pro komunikaci v lokálních sítí.

Tabulka 1.1[5] obsahuje základní charakteristiky jednotlivých standardů pro srovnání. Uvedenou hodnotou 20MHz v tabulce u šířky přenosového kanálu se ještě budu v práci dále zabývat.

Jak lze pozorovat z dat v tabulce 1.1, původními standardy byly 802.11a a 802.11b. Ty se lišily nejen použitým rozsahem frekvencí ale i modulací a maximální přenosovou rychlostí. I přes lepší parametry standardu 802.11a došlo z počátku k rychlejšímu rozšíření a výrobě zařízení s podporou standardu 802.11b. Na tento standard později (v roce 2003) bylo navázáno standardem 802.11g. Ten zachovával zpětnou kompatibilitu zařízení s 802.11b a zároveň rozšiřoval o použití modulace OFDM na stejných vysílacích frekvencích/kanálech.

Standard 802.11n pak rozšiřuje obě základní větve (a, b/g) o možnost použití více anténních vstupů a výstupů na straně přijímače a vysílače, rozšíření používaného frekvenčního pásma a možnost zvětšení šířky kanálu. Ve výsledku tak lze dosáhnout navýšení maximální teoretické přenosové rychlosti na teoretickou hodnotu 600 Mbps.

Komunikace v bezdrátových sítích
Základní členění bezdrátových sítí rozdělujeme podle typu infrastruktury zúčastněných komunikujících zařízení. V případě tzv. „ad-hoc“ sítí komunikují každá 2 zařízení spolu napřímo, zatímco u sítí typu „infrastructure“ je v síti kromě počítačů (obecně jakékoliv uživatelské zařízení) přítomný další prvek pojmenovaný jako AP – „přístupový bod“. Tento prvek je důležitým komunikačním uzlem, neboť zprostředkovává veškerou komunikaci mezi jednotlivými síťovými zařízeními. V případě, že je AP připojen pomocí dalšího rozhraní

(např. ethernet) s další síťovou infrastrukturou, může zprostředkovávat bezdrátovým zařízením, s nimiž komunikuje, komunikaci i s touto infrastrukturou. Přístupové body zpravidla (pokud není vypnuto) periodicky v nastaveném intervalu vysílají specifické rámce – tzv. „beacon frames“ pomocí nichž informují uživatelská zařízení v okolí o své přítomnosti a základních síťových parametrech a především názvu sítě – SSID.[6]

Před zahájením samotné komunikace mezi síťovým zařízením a přístupovým bodem musí úspěšně proběhnout připojovací proces. Ten se sestává z autentizace a asociace[7]. Nejprve je zařízení, jenž se chce připojit k bezdrátové sítí pomocí konkrétního přístupového bodu ve stavu, kdy je neautentizované a neasociované.

1. V prvním kroku vyšle zařízení tzv. „probe request“ buď se zadanou cílovou adresou na 2.vrstvě nebo na broadcastovou adresu (tj. rámec bude zpracován všemi AP, jež rámec zachytí) a se svojí nastavenou zdrojovou adresou. V tomto rámci zařízení deklaruje podporované a konfigurované komunikační rychlosti.

2. Přístupový bod příp. body, jež obdržely rámec vyslaný v předchozím kroku zkontrolují, zda má konfigurovanou kompatibilní sadu přenosových rychlostí a odešle původnímu odesílateli odpověď označovanou jako „probe response“.

3. Síťové zařízení, které se chce připojit k bezdrátové síti, po přijetí “probe response” zkontroluje kompatibilitu parametrů a odešle přístupovému bodu rámec s příznakem žádosti o autentizaci. Konkrétně se do pole autentizační sekvence nastaví hodnota 0x0001.

4. Přístupový bod po obdržení rámce nesoucího žádost o autentizaci odesílající stanice buď odpoví s autentizační sekvencí = 0x0002 v případě, kdy je zabezpečení nastavení do tzv. „Open“ režimu nebo pakliže je přístupový bod konfigurován pro autentizaci typu „Shared“, následuje odeslání „challenge“ výzvy stanici, která pokud vlastní správný klíč, odešle přístupovému bodu zpět správně zakódovaný řetězec. Na tomto popsaném mechanismu s odesláním výzvy pracuje princip „zabezpečení“ WEP.

5. Stanice žádající o připojení po obdržení potvrzovacího autentizačního rámce odešle rámec s žádostí o asociaci. Tento asociační rámec obsahuje mimo vybraný typ šifrování (pokud je toto možné) také informace, jež se liší v závislosti na typu použitého standardu 802.11.

6. V posledním kroku tohoto procesu odpovídá vysílač na přijatou žádost o asociaci. Spojení mezi AP a zařízením je sestaveno a obě strany mohou zahájit přenos dat.

Po úspěšné autentizaci a asociaci může být zahájena obousměrná komunikace mezi uživatelským zařízením a přístupovým bodem. Bezdrátová zařízení standardů 802.11 implementují verzi přístupové metody CSMA ke sdílenému médiu s názvem CSMA/CA - Carrier Sense Multiple Access / Collision Avoidance. Tento mechanismus (protokol) operuje na 2.vrstvě ISO/OSI modelu.[8] Jedná se o mechanismus řízení přístupu ke komunikačnímu médiu se snahou o vyhnutí se kolizím narozdíl od metody CSMA/CD (používané např. u IEEE 802.3), kdy se síťová zařízení nesnaží proaktivně kolizím zabránit. Namísto toho kolize na médiu pouze detekují a až následně reagují. Kolize na médiu způsobují defekt přenášených informací a nemožnosti jejich příjmu nebo příjmu v poškozené podobě na straně příjemce. Během přenosu musejí být poškozené rámce následně znovu přeneseny, což zvyšuje latenci komunikace a snižuje datovou propustnost spoje.

Síťová zařízení standardu IEEE 802.11 nejsou schopna současného přenosu dat a detekce provozu na daném frekvenčním rozsahu, proto musí před zahájením přenosu na vybraném komunikačním kanálu naslouchat, zda v okolí neprobíhá přenos někoho jiného, s nímž by mohl odesílatelovy datové rámce po spuštění přenosu kolidovat. V případě úspěšného doručení rámce je příjemcem emitován malý potvrzovací ACK rámec pro odesílatele. V případě, že odesílatel neobdrží potvrzovací rámec během definovaného časového intervalu, je původní nepotvrzený datový rámec odesílatelem znovu odeslán.

Metoda naslouchání a přístupu k médiu v rámci protokolu CSMA/CA se označuje zkratkou DCF (Distributed Coordination Function) a skládá ze několika částí.[8] Základní část definuje naslouchání na médiu za účelem detekce cizího přenosu a specifikuje např. časový interval, po jehož trvání zařízení odloží připravené rámce k odeslání před opětovným pokusem. Rozšíření pak obsahuje přístupovou metodu RTS/CTS, jejíž popisu se věnuji dále v práci v souvislosti s vlivem kolizí na kvalitu bezdrátové sítě.

1.1.2 Faktory ovlivňující výkon a kvalitu bezdrátové sítě

Antény
Anténa je upravený vodič, sestrojený za účelem přenosu rádiového signálu. K tomu dochází za přeměny elektrické energie na elektromagnetické vlny a naopak. Každá anténa může už z principu fungovat jako vysílač i jako přijímač.

Antény dělíme na základě mnoha parametrů do různých kategorií. Pro účely této práce se budu zabývat pouze anténami určenými pro přenos WiFi signálu a pouze základními parametry, mezi něž patří:

- zisk

- směrová charakteristika
- polarizace

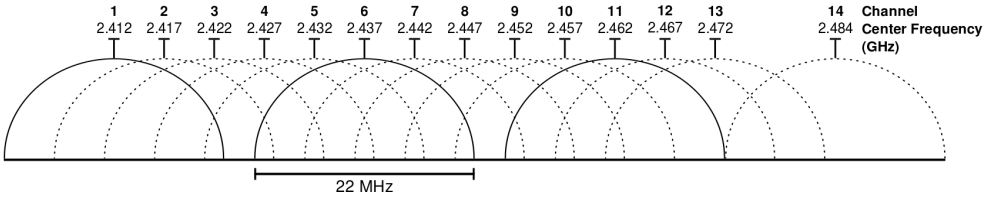
Volba antény se velkou měrou promítá do výsledného pokrytí bezdrátovým signálem. Záleží přitom zejména na jejím tvaru a velikosti. V různých situacích a podmínkách proto volíme rozdílné typy antén. Základní rozdělení antén tvoří 2 kategorie - směrové a všesměrové. U všesměrových antén je signál šířen rovnoměrně všemi směry v horizontální rovině a jen v omezeném úhlu ve vertikální rovině - typicky cca 30°až 40°. Hodnota tohoto úhlu u konkrétní antény se definuje tak, že v tomto úhlu naměříme poloviční vyzářený výkon oproti úhlu 0°tzn. rozdíl **3dB**. Naopak směrové antény mají (v závislosti na konstrukčním provedení) vyzařovací úhel zpravidla velmi omezený v obou zmíněných rovinách. Směrové antény mají praktické využití při budování spojů Point-To-Point, naopak všesměrové antény se používají takřka výhradně u Point-To-Multipoint síťových architektur. Typicky nalezneme všesměrové antény u bezdrátových přístupových bodů a směrové antény pak na straně klientů, kteří se do sítě připojují.

Z výše uvedeného vyplývá, že je při plánování pokrytí prostoru rádiovým signálem volba antény velmi důležitá a stejně tak tomu je i při použití více kusů antén a jejich rozmístění v prostoru. Typicky u všesměrových antén je třeba brát v potaz směrovou charakteristiku jejich vysílání. V patrových budových se antény umisťují zpravidla tak, aby se signál šířil po patře a nikoliv budovou svisle. Je to tak efektivnější z hlediska šíření a ztrát (za předpokladu, že zdi jsou tenčí a z lépe prostupného materiálu než stropní konstrukce). Důležité je počítat s jevem, kdy se tvoří hluchá místa nad (a pod) anténou vlivem jejího konstrukčního řešení a vyzařovací charakteristiky. Pokud se s touto vlastností nepočítá, mohou vzniknout problémy s nedostatečným pokrytím. Složitost úkolu plánování rozmístění vysílacích jednotek narůstá s členitostí terénu nebo budov a v nich použitých stavebních materiálech a konstrukcí.

Jako záludná se jeví i problematika používaných antén v dnešních mobilních telefonech - smartphonech. Výrobci jsou nuceni s ohledem na design a rozměry finálního výrobku vymýšlet sofistikované konstrukce pro anténní systémy. Při nedostatečném otestování výsledného řešení pak může docházet ke kuriózním problémům jako např. u výrobce Apple a konkrétně produktu iPhone 4, kdy uživatelé ztráceli mobilní signál při sevření telefonu dlaní tak nešikovně, že došlo k propojení dvou částí antény.[9] V tomto případě byla ovlivněna anténa pro příjem mobilního signálu, ale totéž může platit i pro bezdrátové přenosy ve wifi sítích. Svou roli při komunikaci ve wifi sítích prostřednictvím mobilního telefonu pak určitě má i způsob a poloha, v jaké jej při používání držíme. A tak by měli například návrháři bezdrátových VOIP zařízení počítat s horším příjmem signálu resp. vyšším útlumem při přiložení zařízení k hlavě.

Volba vysílacích kanálů
Mezi základní úkony při tvorbě a konfiguraci nově budované sítě by mělo určitě patřit správné rozmístění vysílacích kanálů mezi spravované přístupové body takovým způsobem, aby se žádné dva vysílače v prostoru nepřekrývaly použitým rozsahem vysílacích frekvencí.

V České republice je podle aktuální platné legislativy možné vysílat podle specifikovaných podmínek na frekvencích od **2400** MHz do **2483,5** MHz[10]. Tento interval odpovídá frekvenčnímu rozsahu pro kanály 1 až 13.



Obrázek 1.1: Grafické znázornění přesahů kanálů v pásmu 2,4GHz

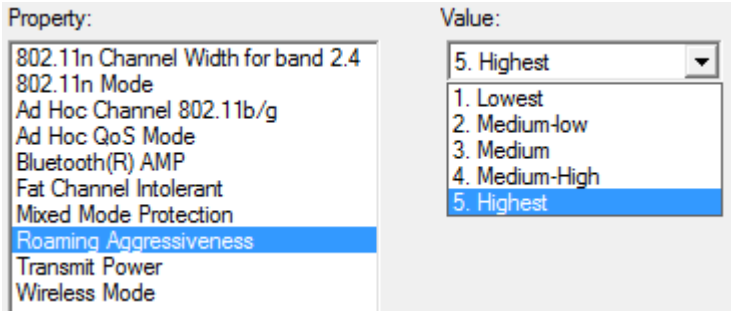
Modulační schéma standardu 802.11g je, jak už jsem se v práci výše zmínil, OFDM a při rádiové komunikaci se využívá podstatně větší interval, než je vzdálenost mezi jednotlivými kanály - obrázek 1.1. V případě uvedeného standardu 802.11g je přenosu vyhrazeno pásmo široké 22MHz. Z tohoto rozsahu je 20MHz efektivně využité pásmo a zbývající 2MHz pak tvoří takzvané ochranné pásmo (resp. po jednom MHz na každém konci intervalu), které v praxi není využito a slouží k oddělení 2 širších sousedních frekvenčních pásem za účelem zabránění možného vzájemného rušení.[11]

Abychom zajistili, že se nebude v pokrývaném prostoru rádiovým signálem vyskytovat rušení vzniklé používáním překrývajících se frekvenčních pásem, musíme na těch vysílačích, u kterých se rádiusy jejich dosahu překrývají (sousední vysílače), nastavit používání takových kanálů, aby se skutečně používané frekvenční rozsahy vůbec nepřekrývaly. Takovou vlastnost u 802.11b/g poskytuje kombinace kanálů 1,6 a 11, jak lze pozorovat na obrázku1.1 [12].

Možnosti roamingu
Velmi významným faktorem u rozsáhlejších sítí, který ovlivňuje zejména uživatelské pohodlí z používání bezdrátového připojení, je mechanismus nazývaný jako „roaming“. Podstata tohoto mechanismu spočívá v tom, že připojení klienti se automaticky přepínají mezi jednotlivými přístupovými body bez nutnosti jakéhokoliv uživatelského zásahu spolu s tím, jak se klientské bezdrátové zařízení pohybuje po pokrytém prostředí.

Druhy roamingu bychom mohli ještě rozdělit na ty případy resp. konfigurace, kdy je přepojení klienta z jednoho na druhý přístupový bod řízeno „sítí“ a klienta si přístupové body defacto předají a na případy, kdy je přepojení na jiný přístupový bod inicializováno na straně klienta. Ve druhém případě o sobě dva dotyčné přístupové body dokonce ani nemusejí „vědět“, ale naopak v prvním případě je třeba spolupráci zajistit pomocí tzv. controllerů. To jsou síťové prvky, které jak již plyne z jejich názvu mají na starost on–line optimalizaci vysílacích parametrů na přístupových bodech, správu a roaming bezdrátových uživatelů a případně se zapojují i do autentizačního procesu.

Nejhorší variantou (pokud nejde o záměr) je situace, kdy uživateli s přenosným síťovým zařízením po přemístění v rámci nějakého pokrytého areálu dramaticky poklesne úroveň signálu, ale nedojde k automatickému přepojení na mnohem bližší a z hlediska kvality spojení výhodnější přístupový bod. Tyto situace zhoršují v očích uživatelů dojem z kvality bezdrátové sítě a jejich důvodem může být, že klientské zařízení neví, že bližší přístupový bod patří do stejné sítě například protože má nakonfigurováno vysílání jiného SSID. Ani sjednocený název sítí ale nemusí zaručit, že k výše popsané situaci nedojde, protože v sítích, kde není použit protokol pro přepojení, je roaming (do doby než klientské zařízení „ztratí“ signál úplně nebo je v důsledku nízké kvality toto spojení přístupovým bodem ukončeno) řízen z klientského zařízení. Uživatel má alespoň zpravidla možnost prostřednictvím konfiguračního rozhraní OS upravit v ovladačích míru agresivity s jakou se bude jeho síťová karta přepojovat z jedné sítě na druhou. Možná ukázka, jak taková konfigurace vypadá, se nachází na obrázku 1.2.



Obrázek 1.2: Konfigurace agresivity roamingu na klientském zařízení

Využití vysílacího času

V bezdrátových sítí jsou data zapouzdřena do rámců, jež jsou pak mezi jednotlivými bezdrátovými prvky přenášeny. Mimo přenosu rámců s užitečnými daty vyšších protokolů je ale potřeba přenášet i rámce s kontrolními a řídícími zprávami. Kontrolní zprávy nenesou žádný tzv. payload a protože musí

být zachytitelné všemi stanicemi, jsou vysílány na tzv. „basic rates“ neboli základních přenosových rychlostech. Vysílání těchto zpráv zaměstnává vysílač na úkor vysílání rámců s daty a snižuje se tak maximální možné využití bezdrátové sítě k přenosu užitečných dat a tím klesá i její kvalita. Do další skupiny tzv. řídících zpráv patří mimo jiné autentizační, asociační zprávy a jejich analogické protiklady. Dále pak beacon a probe rámce, jejichž význam jsem již rozebral výše v práci.

Z výše uvedeného vyplývá, že by mělo být snahou každého správce bezdrátové sítě její nastavení tak, aby nedocházelo ke zbytečně častým přenosům rámců s „neuživatelskými“ daty. Příkladem je použití více SSID na jednom fyzickém rozhraní bez prodloužení časového intervalu vysílání beacon rámců, což může mít za následek značné snížení užitečně využitelného vysílacího času.

Použité komunikační rychlosti
Kvalita přenosových parametrů mezi klientským zařízením a přístupovým bodem se odvíjí mimo jiné i od aktuálně používané komunikační rychlosti neboli tzv. „data rates“, rozlišujeme přitom rychlosti ve směru příchozím - **Rx** a odchozím - **Tx**. Každý ze standardů 802.11a/b/g/n obsahuje sadu předdefinovaných komunikačních rychlostí, jejichž podpora a použití je také předmětem vyjednávání během procesu připojování klientského zařízení k přístupovému bodu.

V praxi se určuje aktuální komunikační rychlost na základě výpočtů vycházejících minimálně z těchto faktorů:

- vzdálenost mezi síťovými zařízeními
- míra ztrátovosti a kolizí při přenosu dat
- úroveň kvality přijímaného signálu a rušení

Komunikační rychlosti se v čase mohou měnit. Jejich hodnota přitom představuje pro daný směr komunikace v danou chvíli teoretickou maximální rychlost. Změnou komunikační ryhlosti tak dochází k přímému ovlivnění kvality sítě z pohledu připojených uživatelů a maximální teoretické rychlosti datového přenosu.

Podpora zastaralých zařízení
Zachování podpory klientských síťových zařízení staršího data výroby s sebou může v praxi nést úskalí, v podobě nejen nemožnosti použití modernějších a tím pádem zpravidla výkonnějších protokolů a standardů, ale i zhoršení výkonu.

Například zařízení podporující pouze standard 802.11b používají k přenosu modulaci DSSS spolu s kompresním mechanismem CCK. Standard 802.11g přináší v rámci modulace OFDM výhodu v možnostech částečné adaptace na rušení pomocí dynamického vyřazení zarušených přenosových frekvencí z používání, dynamické alokace kanálů pro využití k odesílání a příjmu a pomáhá minimalizovat efekt odrazu rádiového signálu na příjmu. [13]

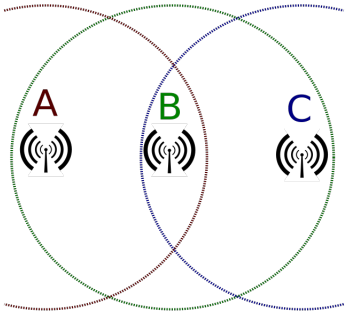
Povolíme-li na rozhraní přístupového bodu použití standardu 802.11b, dojde po připojení prvního 802.11b zařízení k plošnému poklesu výkonnosti v důsledku toho, že všechny přenosy resp. jejich hlavičky musejí být přenášeny za pomoci CCK. Děje se tak z důvodu zachování funkce CSMA/CA. V každém případě má podpora tzv. „legacy“ zařízení za efekt snížení kvality sítě.[13]

Kolize na médiu
Kolize je efekt, kdy dojde při přenosu k poruše rámce a příjemce tak neodešle odesílateli ACK potvrzení, který má naopak signalizovat jeho úspěšné přijetí. Fragmentací rámců rozumíme jejich dělení na menší části, které jsou následně přeneseny k příjemci a zde znovu poskládány do původní podoby. V případě komunikace v zarušeném prostředí dosahují takto upravené (menší) rámce větší pravděpodobnosti úspěšného přenosu, poněvadž čas potřebný na jejich přenos je kratší. Nevýhodou tohoto procesu může být vyšší výpočetní náročnost než při přenosu stejného datového objemu bez využití fragmentace a zvýšená latence komunikace v důsledku nutnosti odeslání více rámců s potřebnou režií.

Nastavení optimální velikosti fragmentace se u bezdrátových sítí může lišit. Při určování velikosti fragmentů bychom měli brát v úvahu zejména (relativní) množství kolizí, ke kterým přirozeně dochází. Zmenšováním fragmentů bychom měli pozorovat zmenšující se počet kolizí a tedy vyšší úspěšnost přenosu.

Fragmentace rámců nemůže úplně zbavit bezdrátově sítě kolizí a zvláště ne v případě tzv. „hidden node“ problému - problému skrytého vysílače. Schéma tohoto problému je znázorněno na obrázku 1.3. Přístupový bod B komunikuje s klientskými zařízeními A,C. Tato zařízení sice mohou komunikovat s přístupovým bodem, ale k problému dochází tehdy, když chtějí tato zařízení komunikovat s přístupovým bodem současně. K tomu může snadno dojít, protože tato zařízení nejsou schopna (vlivem např. veliké vzdálenosti nebo útlumu signálu) zachytit vysílaný provoz vysílaný zařízením na, z jejich pohledu, opačné straně.

Tyto případy lze částečně řešit rozšířením standardu 802.11 - protokolem RTS/CTS. Protokol RTS/CTS pomáhá snižovat počet kolizí rámců na sdíleném médiu tím, že implementuje do komunikace 2 bezdrátových stanic



Obrázek 1.3: Ilustrační obrázek demonstrující problém skrytého uzlu[14]

RTS/CTS handshake. Tento handshake se navazuje před odesláním rámce (typicky většího, než zadaná nakonfigurovaná hodnota) a až teprve po jeho úspěšném dokončení odesílatel začne s vysíláním připravených dat. Princip tohoto mechanismu tak spočívá jednak v potvrzení odesílateli, že může zahájit přenos dat. Ale protože je komunikační médium sdílené, je handshake, jenž se sestává z malých rámců, zachycen i dalšími stanicemi, než jenom původním adresátem. Odesílatel tak nejenom přijetím rámce CTS (Clear To Send) dostává od protistrany informaci, že jsou jeho data u příjemce očekávána ke zpracování, ale zároveň je to i informace pro další stanice v okolí, že mají ještě pozdržet svá data k odeslání (pokud nějaké měly), protože je velká pravděpodobnost, že bude příjemce v danou chvíli zaneprázdněn přijímáním dat od strany, se kterou provedl handshake.

Vzhledem k režii RTS/CTS protokolu se zpravidla neprovádí handshake automaticky u všech přenášených rámců, ale až od určité nastavené velikosti rámce. Ideální nastavení pro danou bezdrátovou síť tak vychází z kompromisu, kdy je výhodnější rychleji odeslat menší rámce s tím rizikem, že protistrana nebo využívané médium může být plně zarušené jinými komunikacemi a na druhé straně solidní jistotou doručení. Tu se vyplatí mít například u větších rámců, kdy by opakovaný přenos zabral časový interval delší, než by bylo provedení RTS/CTS handshake.

Fragmentace u standardu 802.11 se vztahuje pouze na rámce s unicastovou adresou příjemce. Nefragmentují se tak rámce adresované na všechny stanice v okolí (např. beacon rámce). [15]

Agregace je naopak proces, kdy se více rámců před odesláním složí do jednoho. Na tomto principu pracuje tzv. *block acknowledgement* (BA) mechanismus, kdy není odesíláno potvrzení pro každý přijatý rámec zvlášť. Místo toho je odeslán jeden BA rámec s bitmapou, ve které je vždy uvedeno poře-

dové číslo potvrzovaného rámce (a případně i jeho segmentu) v bitové formě a informace o úspěchu/neúspěchu doručení dříve odeslaného rámce.[16]

QoS mechanismus
Mechanismus QoS slouží k prioritizaci kritického síťového provozu za účelem zachování určité úrovně kvality vybraných (síťových) služeb. Síťový provoz je při zpracování na vstupu do hraničního síťového prvku zařazen do kategorie (fronty) dle přednastavených pravidel a následně označkován. Značkou se v tomto případě rozumí nastavení číselné hodnoty ve vyhrazeném a definovaném poli hlavičky pro tyto účely. Průchod resp. prioritu zpracování síťovou infrastrukturou takto „označkovaného“ síťového provozu lze následně řídit na jednotlivých směrovačích. Základní princip přitom spočívá v upřednostňování provozu z prioritnějších skupin na úkor ostatního (méně prioritního) provozu na základě klasifikace provozu.

Síťoví administrátoři mají možnost definovat vyhrazené šířky pásma pro konkrétní vybrané typy služeb a nastavovat algoritmy pro práci směrovače nad jednolivými frontami datových jednotek, jež čekají na zpracování směrovačem.

Mezi základní QoS algoritmy[17] patří:

- FIFO
- PQ
- CQ
- WFQ
- CBWFG
- LLQ

Jednotlivé přístupy se vyznačují různými charakteristikami - některé zaručují maximální dobu zpoždění dat při jejich průchodu - např.: LLQ, u dalších pak naopak hrozí situace, kdy méně prioritní provoz utrpí při průchodu síťovým zařízením velké zpoždění v důsledku neustálého upřednostňování příchozího prioritnějšího provozu - např.: PQ.

Popsaný mechanismus QoS pomáhá v řízení datových toků v místech, kde se v síti vyskytují úzká hrdla. To jsou místa (spojení) v páteřní síti, kde jsme v danou chvíli nějakým způsobem nejvíce limitováni - např. množstvím dostupné konektivity. V ideálním případě máme možnost konfigurovat QoS fronty na obou koncích spoje - obou směrovačích. Tehdy máme nejlepší předpoklady k tomu, abychom dosáhli nejlepších výsledků. Tak tomu nemusí být vždy - např. u přípojky k ISP, kdy dochází ke značkování přenášených dat až po

přijetí hraničním směrovačem a tedy může dojít k saturaci přípojky méně prioritním provozem, neboť síťové zařízení na straně ISP nebude rozlišovat prioritu jednotlivých datových toků.

Rušení
Další příčinou nestabilní bezdrátové sítě a velmi důležitým faktorem pro posouzení kvality sítě bývá rušení. K tomu dochází tehdy, když komunikace mezi stanicemi na fyzické úrovni při průchodu médiem koliduje s jiným rádiovým přenosem na stejném nebo částečně shodném frekvenčním rozsahu.

Wifi zařízení operují dle standardu 802.11b/g v pásmu 2,4 GHz na frekvencích, jejichž účel použití má vícero podob. S komunikací resp. vysíláním vln těchto frekvencí se setkáme u technologie BlueTooth, bezdrátových myší, klávesnic, náhlavních souprav ale například i u mikrovlnných trub. Přítomnost uvedených zařízení a jejich výskyt v okolí může mít negativní vliv na provozovanou bezdrátovou síť v lokalitě.

Známým nástrojem k průzkumu bezdrátového prostředí je např. program InSSIDer z dílny MetaGeek. Jedná se o program s přehledným grafickým rozhraním, jenž má primárně uživateli poskytnout přehled o bezdrátových sítích v okolí a jejich základních vlastnostech – typ použitého zabezpečení, použitý frekvenční kanál, 802.11 standard a další. Pomocí tohoto a podobných programů jsme schopni si vytvořit relativně rychle základní přehled o „bezdrátovém okolí“ – výskytu přístupových bodů a případně alespoň přibližně jejich umístění či vzdálenosti.

Důmyslnější je při analýze bezdrátového prostředí využít spektrálního analyzátoru, jenž umožňuje analýzu signálu v určitě definované frekvenční oblasti. S jeho pomocí tak jsme schopni v reálném čase sledovat nejen přenášená data v rámci bezdrátové sítě ale i kompletní rádiový provoz generovaný výše uvedenenými typy zařízení.

Použité protokoly na vyšších vrstvách ISO/OSI modelu
Výslednou kvalitu připojení přes bezdrátovou síť ovlivňuje v neposlední řadě i chování použitých protokolů vyšších vrstev nad linkovou vrstvou 802.11. Vhodným příkladem je uvedení velmi používaného transportního protokolu TCP v počáteční fázi přenosu.

Jedním z mechanismů, jež TCP protokol využívá je tzv. „TCP slow start“. Tento mechanismus slouží protokolu k šetrnému otestování kvality přenosové linky následujícím způsobem: vysílací strana odešle paket a čeká na potvrzení od zařízení na druhém konci TCP spojení. Pokud obdrží odesílatel potvrzení o přijetí ve stanoveném čase, odešle dvojnásobek paketů (a adekvátně zvětší

okno). Takto odesílatel postupuje do okamžiku, kdy se některý z paketů nebo potvrzení ztratí či opozdí. V takovém případě odesílatel zareaguje zmenšením okna a pokračuje v jeho zvětšování do další chyby přenosu. Výsledkem tak je zpomalení datového toku od odesílatele vlivem ztrátovosti linky a/nebo její vysoké latenci[18].

Zabezpečení
Velmi důležitou metrikou při posuzování kvality bezdrátové sítě je úroveň jejího zabezpečení. V současnosti je známa řada útoků na bezdrátové sítě a desítky volně dostupných nástrojů pro jejich provedení.

Základní kategorie útoků rozdělujeme podle jejich zaměření na:

- útok na integritu přenášených dat
- útok na autentizační proces
- útok na dostupnost služby

V dnešní době je otázka bezpečnosti přenášených dat i díky medializovaným kauzám velmi sledována. Objevují se léta staré chyby v obecně velmi používaných protokolech (SSLv3 - BEAST, POODLE, HeartBleed, FREAK[19]) určených k šifrovaní přenosů a zajištění důvěrnosti komunikace mezi uživatelem a serverem. Používání moderních, spolehlivých a ověřených protokolů je esenciální záležitostí při snaze o zabezpečení bezdrátové sítě a snížení rizika a dopadu případných útoků.

Autentizační proces
Na přítomnost a implementaci autentizačního procesu pro přístup k bezdrátové síti lze také nahlížet jako na kvalitativní kritérium sítě. U bezdrátových sítí se lze setkat s různými metodami autentizace, např. to jsou: zadání přihlašovacích údajů pomocí webového formuláře, sdílené heslo - tzv. PSK zadávané při připojování k zabezpečené WPA síti nebo autentizační protokol standardu 802.1x „EAPOL“.

Metody autentizace se liší zejména uživatelskou příjemností a administrační složitostí a mnohdy se může autentizační proces na zařízeních různých výrobců mírně lišit v závislosti na konkrétní implementaci (např. různé implicitní kořenové certifikáty certifikačních autorit ve vnitřním úložišti).

Granularita autentizačních údajů může mít rozpětí od sdílení jednoho hesla mezi uživateli až po unikátní uživatelské účty s případnou integrací s dalšími systémy. V prostředí, kde se každý uživatel autentizuje se svými přihlašovacími údaji lze implementovat logovací systém, který lze využít jak pro vyšetřování a reakce na bezpečnostní incidenty (zablokování přístupu konkrétnímu účtu k síti) tak např. ke statistickým či dalším monitorovacím účelům. Správci sítě

se tak snáze dostanou k informacím o síti, kterou spravují a mohou na vzniklé situace reagovat.

Autentizační proces je tématem, jímž se v poslední době věnují i tvůrci operačních systémů do nejrozšířenějších mobilních platforem. Mám na mysli automatickou funkci, která na mobilním zařízení ihned po připojení k bezdrátové wifi síti testuje, zda je funkční připojení k vybraným serverům v internetové síti. Jako příklad uvádím odkaz na zdrojové kódy OS android verze 4.0. Testovací URL je přímo v kódu definovaná proměnnou *DEFAULT_WALLED_GARDEN_URL* s poznámkou, že má klient očekávat návratový kód 204 oproti klasické hodnotě 200. I změna v hodnotě návratového kódu totiž může znamenat, že připojení k danému není dostupné a požadavek zařízení mohl být přesměrován např. na jiný server v síti.

Na proces autentizace pak musí navázat autorizace, v rámci které dochází v kontextu bezdrátových sítí k přidělení oprávnění přístupu ke konkrétní skupině síťových zdrojů na základě ověřené identity.

Síťová omezení
Kvalita sítě je dána i možnostmi jejího využití a úrovní ochrany jejích uživatelů. Možnosti využití udává zejména latence (zpoždění) sítě a konektivita dostupná koncovému uživateli.

Každý uživatel má typické jiné potřeby a tedy i jiné nároky na síť resp. internetovou konektivitu. Účelem síťových omezení je vytvořit takové prostředí, které bude poskytovat uspokojivé podmínky pro většinu uživatelů, kteří by bez potřebných omezení byli možná i podstatně více omezováni menšinou uživatelů s podstatně vyššími nároky. Vyššími nároky rozumím kontinuální stahování/nahrávání velkých objemů dat, používání velmi náročných síťových protokolů zejména ze skupiny P2P jako např. BitTorrent a provozování dalších potenciálních aktivit na síti, jež mají za následek výrazné zhoršení okolní uživatelské zkušenosti s konkrétní síťovou infrastrukturou.

Efektivita administrace sítě
Z pohledu správce sítě lze o kvalitě bezdrátové sítě hovořit i ve smyslu možnosti a jednoduchosti její administrace a údržby. Posuzovat lze přitom náročnost přidání/ubírání jednotlivých přístupových bodů do/ze síťové infrastruktury, možnosti konfigurace specifických přenosových parametrů, náročnost a počet kroků vedoucích k vykonání určitého administrátorského zásahu a tak dále.

Za účelem zefektivnění a zjednodušení správy bezdrátových sítí o desítkách či stovkách AP byly vyvinuty síťové prvky označované obecně jako "Controller" nebo konkrétněji "Wireless LAN Controller". Tyto kontrolery vytvářejí

hlavní uživatelské rozhraní pro správu vysílacích rozhraní AP, poskytují dohledové funkce, centrální logování událostí a usnadňují hledání a odstraňování možných poruch v síti. V neposlední řadě kontrolery přebírají od AP roli autentizační jednotky - například RADIUS klienta v případě použití 802.1x protokolu. Přenesení funkcí a konfigurace na centrální prvek umožňuje výrobcům síťových technologií vyrábět AP méně náročná na výpočetní prostředky, protože jedinou funkcí těchto AP (označovaných jako LWAP - LightWeight AP) je navázání a udržení (šifrovaného) spojení s klientskými zařízeními.

Kontrolery komunikují s vysílači po řídících spojeních. Tato spojení mohou být v závislosti na výrobci a jeho technologii sestavena již na základě funkční linkové vrstvy mezi kontrolerem a přístupovými body (např. LWAPP L2). Další řídící protokoly pak umožňují i tunelování či průchod skrz Firewall a NAT. Tato funkce nalezne využití zejména v případě, že organizace potřebuje vytvořit a spravovat bezdrátovou síť v detašových pracovištích, přičemž správa, autentizace a konfigurace síťových politik jsou aplikovány z jednoho centrálního místa.

Monitoring sítě
Správa svěřených systémů obsahuje kromě vývoje a implementace nových řešení, úkonů denní údržby i řešení nestandardních situací a vzniklých problémů. Nejinak tomu je i v případě bezdrátových sítí. Významným pomocníkem při řešení událostí ze všech uvedených oblastí činnosti se pak stává monitorovací systém. S jeho pomocí jsme schopni nejenom plánovat kapacitu pořizované konektivity, generovat statistiky využití, hlídat dostupnost a funkčnost všech přístupových bodů ale i jejich zátěž a případně získávat další informace o připojených klientských zařízeních pro další zpracování. Monitorovací systém přitom vůbec nemusí být nákladnou položkou v rozpočtu organizace. V současnosti existuje mnoho spolehlivých a kvalitních opensource projektů jako např. Nagios, Icinga, Shinken dále pak Cacti, Zabbix a zástupy dalších. Ná správci je už vlastně jenom, aby se s nástrojem dostatečně seznámil a přizpůsobil jeho konfiguraci pro svěřené prostředí. S pomocí kvalitního monitoringu dokážeme rychleji a spolehlivěji určit možnou příčinu vzniknuvších problémů. Také proto se domnívám, že by přítomnost a rozsah lokálního monitorovacího systému měla být dalším kritériem kvality bezdrátové sítě.

Aktualizovaný software
Významnou součástí správy a možným dalším kritériem kvality bezdrátové sítě je kontinuální proces aktualizace systémů na všech aktivních prvcích sítě. Aktualizace obecně obsahují mimo oprav funkčních a výkonnostních chyb i opravy vztažené k zabezpečení. Proto by mělo být v zájmu nejenom každého správce bezdrátové sítě udržovat systémy na síťových prvcích aktualizované a minimalizovat tak potenciální riziko zneužití přítomné zranitelnost v neaktu-

alizovaném zařízení, jež by mohlo vést k ohrožení nejen síťové infrastruktury ale i jejích uživatelů.

1.2 Praktická část

1.2.1 Základní informace o školní síťové infrastruktuře

V prostorách školy se nacházejí 4 významné lokality z pohledu architektury počítačové sítě. Jedná se o:

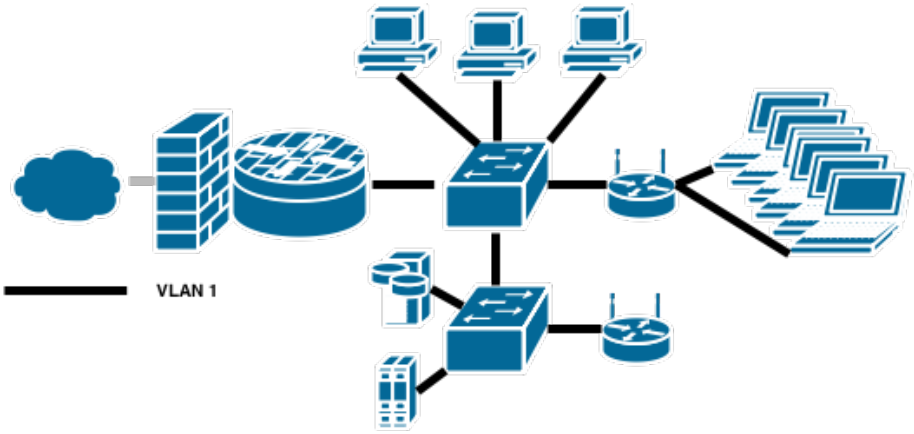
- sklad prádla v 1.patře, kde se nachází rack s aktivním přepínačem a PoE adaptéry pro 5ks bezdrátových přístupových bodů
- archiv v 1.patře. Zde je umístěn rack se serverovou infrastrukturou, síťový přepínač, síťový firewall, PoE adaptéry pro 4ks bezdrátových přístupových bodů, záložní napájení v podobě UPS
- počítačová učebna v suterénu – aktivní síťový prvek – přepínač
- počítačová učebna v 2.patře – aktivní síťový prvek – přepínač

Konektivita k internetu s objednanou kapacitou linky 10/10 Mbps je do školy přivedena průchodem z přímo sousedící obchodní akademie pomocí optického kabelu. Před vstupem do firewallu je optický kabel připojen do převodníku na ethernet a do firewallu přiveden klasicky kabelem UTP kategorie 5E (na druhém konci opt.kabelu se nachází identický převodník). Připojení zajišťuje externí dodavatel.

Páteřní síť školy tvoří 2 přepínače D-Link DES 1210-28 a D-Link DES 1210-52 a jeden síťový firewall Fortigate 50B od výrobce síťových zařízení Fortinet. Ve školní síti se ale vyskytují i přepínače bez možnosti konfigurace - tzv. unmanaged přepínače, jejichž pozice ani počty jsem ale nemapoval, protože nesousedí s bezdrátovými přístupovými body a ani netvoří jádro sítě a nejsou tak pro tuto práci podstatné.

Serverovou infrastrukturu tvoří dohromady 3 fyzické servery, z nichž jeden server je poháněn Linux distribucí Ubuntu. Ve fyzickém Ubuntu serveru, který slouží jako terminálový server pro počítače v knihovně, je virtualizován server s distribucí Debian, kde běží dohledový systém Nagios+Centreon. Ostatní 2 fyzické stroje fungují na platformě Windows 2008R2 a stejně tak i jejich virtuální servery. Každý fyzický server přitom obsahuje jeden virtuální server. Oba fyzické stroje s OS Windows mají ve školní síti roli doménových řadičů a vzájemně tak replikují obsah adresářové služby Active Directory.

Bezdrátovou infrastrukturu školy tvoří celkem 9 přístupových bodů. Všechna tato zařízení pocházejí z dílny jednoho výrobce - MikroTik. Jedná se o síťové prvky z výrobcem označené produktové řady RouterBOARD. Konkrétně se na škole nacházejí 2ks RB411AR a 7ks RB411AH. Všech 9 přístupových bodů je napájeno na dálku pomocí technologie Power Over Ethernet přes nevyužité vodiče v propojovacích síťových kabelech.



Obrázek 1.4: Architektura školní sítě

Nejedná se již o nejnovější, ale přesto jde o poměrně výkonné modely. Takt CPU je u modelu 411AH = 680MHz[20], 411AR = 300MHz[21]. Desky 411AH jsou osazeny miniPCI bezdrátovými kartami typu R52 od stejného výrobce jako základní desky. Tyto bezdrátové karty podporují nejenom standardy 802.11b/g ale i 802.11a. V případě výměny stávajících připojených antén lze vysílač přepnout z rádiového pásma 2,4GHz na 5GHz. Desky 411AR nejsou osazeny žádnou externí miniPCI kartou a anténa je pigtailem připojena přímo na integrovanou komunikační jednotku.

Na všech přístupových bodech ve škole jsou použity stejné všesměrové otočné prutové antény se ziskem 8dBi a lineární polarizací. Rozsah vysílacího laloku u této konkrétní antény činí dle výrobce horizontálně 360°a vertikálně 40°.[22]

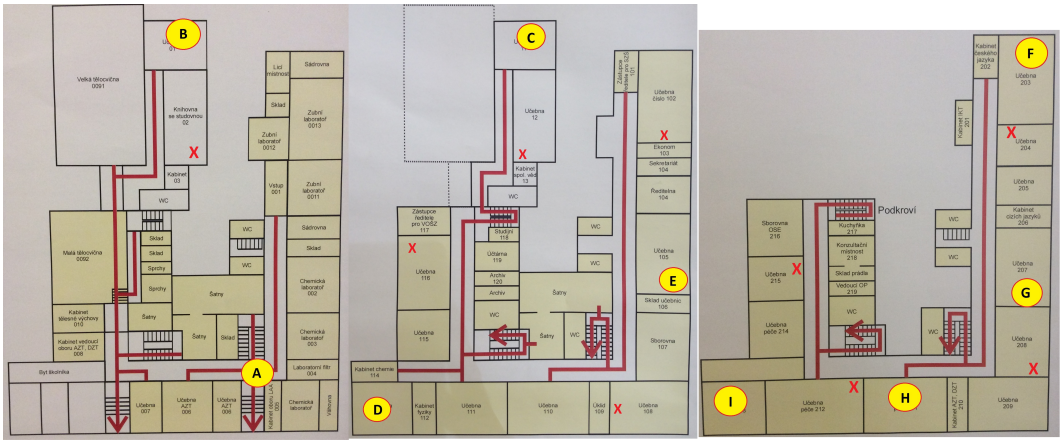
1.2.2 Analýza stávajícího řešení bezdrátové sítě

Pokrytí školního areálu a fyzické umístění přístupových bodů
Pro zjištění rozsahu pokrytí školního areálu bezdrátovou sítí jsem vytipoval 9 lokalit, v nichž jsem následně změřil úrovně síly signálu z jednotlivých přístupových bodů. Záměrně jsem vybíral místa v budově, kde jsem se vzhledem k jejich umístění a vzdálenosti od přístupových bodů domníval, že by mohla být problematická ve smyslu nedostatečného pokrytí. Měření jsem prováděl mimo

Tabulka 1.2: Měření síly přijímaného signálu ve vybraných lokalitách dle jednotlivých AP - rb0 až rb8. Údaje v tabulce jsou záporné hodnoty v jednotkách **dBm**

	A	B	C	D	E	F	G	H	I
rb0		-71	-84		-94				
rb1		-72	-50	-77	-88	-86		-90	-84
rb2	-80	-89	-89	-63	-86	-87		-82	-66
rb3	-71			-79	-75	-95	-80	-65	-92
rb4	-88	-78	-77		-95	-61	-65	-89	-89
rb5				-82					-93
rb6	-80			-63			-89	-52	-57
rb7	-73			-89	-75	-74	-63	-68	-69
rb8			-95		-71	-72	-72		

výuku v prázdné budově, přičemž v každém z vybraných bodů jsem naměřil nejméně 5 hodnot s mírně pozměněnou polohou přijímače v horizontální rovině v rozsahu +- 2metry a tyto naměřené hodnoty jsem následně zprůměroval.



Obrázek 1.5: Plánek školy s vyznačenými pozicemi přístupových bodů křížky a písmeny vybrané lokality, kde jsem prováděl kontrolu pokrytí měřením úrovní síly přijímaného signálu

Přístupové body jsou po škole rovnoměrně rozmístěny a to jak ve vertikální tak i horizontální rovině s ohledem na členitost budovy. V učebnách jsou přitom přimontovány buď na čelní stěnu nad tabuli nebo do rohu a přitom vždy přibližně 50cm pod stropem. Základní deska spolu s komunikační miniPCI jednotkou je umístěna v plastové krycí krabici s přimontovanou externí všesměrovou anténou, jenž směřuje vždy hrotem k zemi. Instalaci AP jsem pro

ukázku zachytil na fotografii, která je přiložena jako obrázek 1.6.

Obrázek 1.6: Fotografie jednoho z instalovaných přístupových bodů s odkrytým víkem.

Analýza bezdrátové sítě na fyzické a linkové vrstvě
Před provedením podrobnější analýzy bezdrátové sítě jsem musel nejprve identifikovat data, která by mi mohla být užitečná a jež by se dala pro analýzu sítě využít. Prozkoumáním dostupných výstupů z přístupových bodů a konzultováním s dokumentací výrobce se mi podařilo dohledat vybrané parametry v tabulce připojených klientských zařízení, jejichž hodnoty jsem se jal sledovat. Jednalo se především o počty odeslaných a přijatých rámců bez započtení opakování přenosu, počty skutečně přenesených rámců se započtením opakovných přenosů, ukazatel Tx-ccq a Rx-ccq, úroveň síly signálu, teoretickou propustnost bezdrátového spojení spočtenou do parametru p-throughput a aktuálně použité komunikační rychlosti „Rx rate“ a „Tx rate“.

V souvislosti s tím jsem se musel zabývat i problémem, jak lze efektivně a pokud možno co nejvíce automaticky provozní data o síti získávat a zpracovávat. Po zvážení jsem se rozhodl pro sběr dat částečně jednak využít a přitom i rozšířit stávající dohledový systém Nagios a za druhé vytvořit skript pro zaznamenávání aktuálních hodnot a nastavit jeho automatické spouštění s četností danou definovaným časovým intervalem. Jak jsem ale brzy zjistil, dohledový systém není navržen pro získávání a zpracování větších dat a navíc práce s ním při analýze hodnot byla velmi nepraktická. Uvedu příklad: pro vyčítání hodnot z přístupových bodů pomocí protokolu snmp je nejprve nutné získat unikátní identifikátor hodnoty tzv. Object Identifier neboli OID. Některé hodnoty jako například údaje o systému mají OID pevně stanovené,

dohledatelné v dokumentaci a v čase neměnné. Není tomu tak bohužel ale v případě hodnot o připojených bezdrátových zařízení. Zde se na platformě MikroTik používají vygenerované OID a je proto nutné tyto OID nejprve zjistit odesláním odpovídajícího dotazu (/interface wireless registration-table print oid), následně obdrženou odpověď rozparsovat a teprve poté odeslat dotaz na zjištění hodnoty pomocí protokolu snmp. Pokud bych se rozhodl složitě překonávat tuto překážku, tak bych následně narazil na vysokou složitost při zpracování takto získaných dat a proto jsem se raději rovnou rozhodl o automatické stahování všech dat pomocí bash skriptu spouštěném plánovačem cron přes SSH spojení. Zde bych ještě rád zmínil, že při automatickém stahování dat z vysílacích bodů jsem se zprvu potýkal s problémem, kdy přístupové body náhodně odpovídaly po zadání příkazu na výpis dat chybovou hláškou „failed to open file: No such file or directory“. Tento problém jsem naštěstí vyřešil upgradem vnitřního systému RouterOS na všech přístupových bodech na nejnovější verzi v**6.27** z původní verze **4.14** na 2 AP a verze **5.00** na zbývajících 7 AP.

Výše popsaný způsob sběru dat jsem označil jako pasivní. Pro získání podrobnějších informací o kvalitě bezdrátové sítě jsem ale potřeboval i data získaná z připojených uživatelských bezdrátových zařízení. Za tímto účelem jsem sestavil měřící sondu - NetBook Toshiba NB100 s externím bezdrátovým komunikačním modulem TP-Link TL WN722N. Vytvořil jsem sadu testů v nástroji JMeter, jehož oblast použití se nachází v provádění zátěžových testů a měření výkonnosti různých systémů a provedl jsem měření za běžného provozu školy. Měření probíhalo během pracovních dní od cca 8:00 do cca 14:00 s tím, že měřící sonda zůstala ve statické pozici po celou dobu měření na stole v kabinetě IKT. V jiné lokalitě jsem bohužel nemohl zajistit provoz sondy po takto relativně dlouhou dobu bez obav o její poškození či ztrátu.

Tento způsob měření lze rozšiřovat o počty měřících sond po areálu a tím případně zlepšovat a zkvalitňovat získané výsledky. V případě použití jedné sondy mohou být získané výsledky zkreslené a vyvozené závěry nemusejí být vztažené ke všem lokalitám v bezdrátové síti. Nicméně pro účely mého měření, kdy je cílem i otestování navrhnuté metodiky měření a relativně velmi omezeným podmínkám, co se týče vybavení a krátkému časovému horizontu měření, jsem se byl nucen spokojit pouze s jednou testovací sondou. Možným vylepšením metodiky by mohla být rotace sondy na jednotlivých určených lokalitách ve škole. Já jsem se ale rozhodl měřit pouze z jedné lokality, abych nasbíral během daného časového intervalu více hodnot a naměřená data tak byla relevantnější skutečnosti pro konkrétní pozici v budově a s menší statistickou chybou, která se s rostoucím množstvím naměřených hodnot přirozené snižuje.

Pro měření kvality jsem vybral služby postavené na protokolech HTTP a IMAP. HTTP protokol jsem použil pro načítání titulní webové stránky školního informačního systému (bakaláři) a titulní stránky školního vzdělávacího systému (moodle) a měřil jsem nástrojem JMeter čas potřebný k jejich načtení. Oba systémy jsou hostovány na školních serverech ve školní LAN síti a mají dostatečnou výkonnostní kapacitu stejně jako jejich síťová připojení. Protokol IMAP jsem použil k načítání 5 hlaviček nejnovějších emailových zpráv z příchozí schránky nepoužívaného poštovního účtu u největšího českého poskytovatele neplacených emailových schránek a měřil jsem dobu jejich načtení. Vzhledem ke kvalitnímu optickému připojení školní sítě k internetu a předpokládané vysoké kvalitě infrastruktury poskytovatele poštovních služeb jsem si dovolil případné ovlivňující vlivy na trase od přístupového bodu k poštovnímu serveru pro účely tohoto měření zanedbat.

V každém cyklu měření jsem měřil čas potřebný k úplnému načtení všech prvků webové stránky v případě měření založeném na HTTP protokolu a čas potřebný k načtení záhlaví 5 nejnovějších emailových zpráv z poštovní schránky pomocí protokolu IMAP s využitím protokolů SSL/TLS pro zabezpečený přenos dat. Tento výše popsaný způsob získávání dat o kvalitě sítě jsem označil jako aktivní a konkrétní použitou testovou sadu lze nalézt v přiložené příloze v podobě template pro nástroj JMeter s příponou *.jmx.

Prezentace naměřených hodnot z obou uvedených druhů měření, vztažená diskuze a zdokumentovaná snaha o optimalizaci za účelem dosažení lepších výsledků následuje v další části práce.

Zabezpečení přenosu dat
Bezdrátové přístupové body jsou nakonfigurovány do režimu, kdy není použito žádné zabezpečení přenosu síťového provozu. To znamená, že veškerý provoz mezi přístupovými body a klientskými zařízeními může být odposlechnut, pokud nejsou přenášená data chráněna např. šifrováním na některé z vyšších vrstev ISO/OSI modelu (se zabezpečeným autentizačním mechanismem).

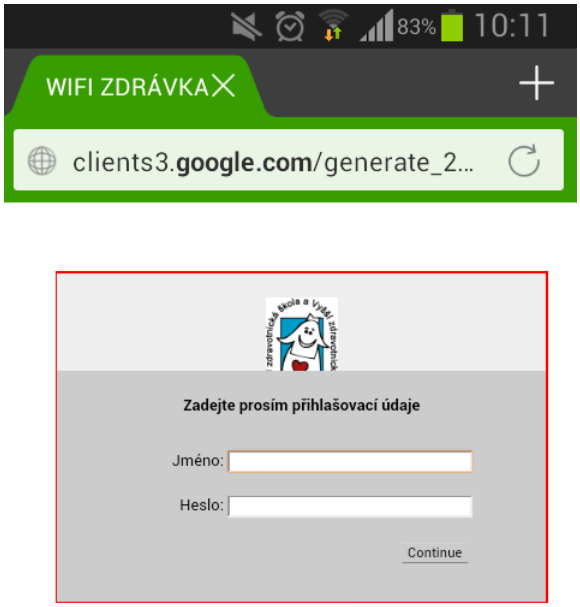
Autentizační proces
Aby mohl připojený uživatel k bezdrátové školní síti v současnosti využívat služby v internetu, je zapotřebí, aby se nejprve úspěšně autentizoval a autorizoval a měl tak na firewallu vytvořenou svou aktivní “session". Autentizační proces zajišťuje funkce firewallu „Identity Based Policy“. Tato funkce se konfiguruje na firewallu u existujícího pravidla a funguje na principu toho, že poté, co pravidlo nejprve zachytí nový uživatelův požadavek, pro který zatím neexistuje aktivní sezení a jedná se (v defaultním nastavení) o provoz na protokolu HTTP, HTTPS, FTP nebo Telnet, je takový požadavek zachycen a uživateli je místo odpovědi od serveru (tzn. původního příjemce požadavku) odeslána

a zobrazena výzva k zadání přihlašovacích údajů. Forma výzvy přitom záleží právě na použitém komunikačním protokolu, ale protože vyhrazená čísla portů pro protokoly FTP a Telnet nejsou na škole ve směru komunikace do internetu vůbec povoleny, můžu se omezit pouze na popis v případech protokolů HTTP a HTTPS. Tehdy je uživateli zobrazen firewallem vygenerovaný webový formulář, jehož podobu lze na firewallu upravovat v sekci System - Config - Replacement Message - Login Page. Prostřednictvím tohoto formuláře jsou od uživatele na firewall přeneseny přihlašovací údaje - jméno a heslo. Platnost přihlašovacích údajů se následně ověřuje pomocí LDAP protokolu proti konfigurovanému serveru - doménovému řadiči se zadanými domenovými přihlašovacími údaji v konfigurační sekci User - Remote - LDAP. Autentizační formulář je zachycen na obrázku 1.7.

Při kontrole platnosti kombinace přihlašovacích údajů dochází i k procesu autorizace, kdy firewall rovněž pomocí protokolu LDAP kontroluje členství přihlašovaného uživatele v doméně v globální skupině „Wifi Users“ - nastavení ověření členství ve skupině v doméně se konfiguruje v sekci User - User Group - User Group. Standartně jsou členy skupiny „Wifi Users“ všechny zaměstnanecké a studentské doménové účty. Pakliže je uživatel úspěšně autorizován, dojde k automatickému přesměrování na původně požadovanou webovou stránku.

Výše popsaný proces autentizace neplatí pro protokol DNS, jehož použití je na firewallu povoleno i bez autentizace a to kamkoliv do internetu. Údajně tak má být zaručena správná funkčnost autentizačního formuláře i pro uživatele, kteří si nenechají přidělit IP adresy DNS serverů protokolem DHCP z místní sítě a místo toho používají své předkonfigurované DNS servery. Tato konfigurace, leč to nemusí být na první pohled zřejmé, může být velmi nebezpečná. Jsou známy techniky a software s jejichž pomocí lze takto přihlašovací stránku obejít vytvořením virtuálního “DNS tunelu” a komunikováním uvnitř tohoto tunelu jen za pomoci odesílání DNS zpráv s požadavkem na přeložení doménového názvu na IP adresu.[23] Na místo subdomény v doménovém názvu do požadavku útočník dosadí zakódovaná data např. pomocí *base32* a tato data jsou následně řetězem DNS serverů dopravena k útočníkem upravenému autoritativnímu názvovému serveru pro danou doménu vyššího řádu použitou v odeslaném požadavku. V odpovědi jsou poté stejným nebo podobným způsobem (např. *base64*) zakódována data pro klienta, jenž požadavek odeslal. Nutnost existence pravidla povolujícího DNS provoz pro správnou funkčnost tohoto autentizačního mechanismu je zanesena i v oficiální dokumentaci.[24]

Další zranitelností stávajícího autentizačního schématu je použití nešifrovaného protokolu HTTP pro přenos přihlašovacích údajů od uživatele, jež se do sítě připojuje, přes otevřenou (nezabezpečenou) bezdrátovou síť k firewallu.



Obrázek 1.7: Autentizační formulář, který se uživateli zobrazí v případě, kdy se uživatel snaží inicializovat spojení do internetu HTTP nebo HTTPS protokolem.

Potenciální útočník by mohl tohoto stavu využít tak, že nastaví na své síťové kartě zachytávání i datových rámců, jež nenesou jeho MAC adresu v poli příjemce a ze zachycených dat přihlašovací údaje jednoduše extrahovat, neboť nejsou nijak šifrována. Zachycenou sadu přihlašovacích údajů lze následně zneužít tak, že se útočník s takovými údaji přihlásí a bude v síti vystupovat pod identitou oběti. Zde je vhodné doplnit, že útočník nemá možnost takto získané přihlašovací údaje oběti změnit a nelze tyto přihlašovací údaje použít pro přihlášení do dalších školních informačních systémů.

Velmi výraznou nevýhodou popsaného autentizačního řešení je i maximální doba vypršení neaktivního uživatelského sezení na firewallu konfigurovatelná na 480minut - tj. 8hodin od poslední uskutečněné komunikace.[25] V praxi to znamená, že se uživatelé musejí každý den při prvním připojení (resp. odeslání prvního HTTP(S) požadavku) k bezdrátové školní síti znovu přihlašovat přes webový formulář.

Další nevýhodou uvedeného řešení, kdy jsou na firewallu vytvářena aktivní sezení, je jeho náročnost na systémové prostředky síťového firewallu - konkrétně výpočetní jednotky. Při zběžném sledování zátěže pomocí protokolu SNMP se dalo pozorovat výstřely zatížení CPU i přes hranici 90%.

A nakonec úplně největší nevýhodou tohoto řešení je nutnost opakované autentizace v případě, že se zařízení přepojí na jiné AP, kde po obdržení jiné IP ještě nemá vytvořené autentizované spojení na firewall v rámci zmíněné „Identity Based Policy“.

Směrování v síti - role firewallu, služba DHCP
Po prozkoumání sítě z pohledu fyzického propojení síťových zařízení bylo potřeba zjistit, jak je školní síť členěna logicky na případné menší segmenty, jak vypadají a kde se nachází jednotlivé broadcastové domény a jaké se používají adresní rozsahy na 3.vrstvě ISO/OSI. Důležité je pro tuto analýzu nejprve identifikovat všechna síťová zařízení, jež mohou mít svou konfigurací vliv na výše uvedené vlastnosti. V případě této školy jsou zkoumané prvky: firewall FortiGate 50B a 2 “managed” D-Link přepínače a samozřejmě bezdrátové přístupové body. Slovo “managed” u přepínačů značí, že se jedná o přepínače, které mají konfigurovanou adresu na 3.ISO/OSI vrstvě, lze jejich konfiguraci měnit pomocí připojení přes telnet, ssh a webový interface.[26]

Kontrolou konfigurace uvedených síťových zařízení jsem zjistil, že škola používá pro místní LAN jednu broadcastovou doménu resp. jeden adresní rozsah a to: 192.168.1.0/24. V tomto rozsahu se nachází firewall v roli brány s adresou 192.168.1.1 a dále pak školní servery, bezdrátové vysílače RouterBOARD, počítače v učebnách a další síťové prvky.

Přístupové body mají na svých ethernetových rozhraních konfigurovány staticky přiřazené IP adresy z uvedeného adresního rozsahu 192.168.1.5x, kde x je z intervalu hodnot <0;8>. Na bezdrátovém rozhraní *wlan1* potom nalezneme u každého vysílače konfigurovanou IP adresu 10.x.0.1 s 16 bitovou velikostí síťové masky, kde x odpovídá stejné hodnotě poslení číslice jako u IP adresy z rozsahu 192.168.1.0/24. Například vysílač s konfigurovanou IP adresou 192.168.1.56 na ethernetovém rozhraní, disponuje IP adresou 10.6.0.1 na bezdrátovém rozhraní.

Směrovací tabulky uvedených síťových prvků jsou konfigurovány s následujícími záznamy: Firewall: statické záznamy pro sítě 10.[0-8].0.0/16 s bránou 192.168.1.5[0-8] Přístupové body: výchozí route 0.0.0.0/0 s bránou 192.168.1.1

Každý přístupový bod směruje provoz mezi firewallem a zařízeními z bezdrátového rozhraní a pracuje tím pádem na 3. ISO/OSI vrstvě. Na každém vysílači je spuštěn pro bezdrátové rozhraní DHCP server s rozsahem IP adres k výdeji 10.x.[1-100].[1-255], kde x je pro každý vysílač jiné - viz odstavce výše.

Pro shrnutí ještě uvádím, že firewall slouží jako defaultní výchozí brána pro komunikaci do všech teoretických okolních sítí. V tomto případě ale žádné

okolní sítě neexistují vyjma spoje k ISP do internetu. FortiGate 50B tak používá pouze 2 ze 3 dostupných fyzických ethernetových rozhraní. Firewall operuje v režimu NAT, kdy dochází při komunikaci hostů z vnitřní sítě s hosty v internetu k překladu adres z privátního rozsahu na IP adresu rozhraní.

Název sítě - SSID
Každý přístupový bod vysílá na bezdrátovém rozhraní *wlan1* stejné SSID a to "ZDRAVKA". Použitím stejného identifikátoru v rámci celé sítě lze docílit toho, že se bezdrátová klientská zařízení budou pokoušet v případě poklesu kvality přenosových parametrů resp. nekvalitního spojení o přepojení na sousední přístupový bod se stejným SSID v beacon rámci.

Správa přístupových bodů
Všechny přístupové body ve školní síti jsou postaveny na MikroTik RouterOS, což je operační systém vyvíjený společností MikroTik přímo pro síťová zařízení označovaná jako RouterBOARD. Tento použitý OS vychází z jádra Linuxu v2.6 a jeho vývojáři si kladou za cíl rychlou instalaci a jednoduchou a uživatelsky přívětivou obsluhu zařízení ze všech dostupných možností připojení. Konfigurace zařízení je tak možná buď za pomoci klávesnice a monitoru přímo připojených k základní desce, připojením přes sériovou konzoli terminálovou aplikací nebo vzdáleně s využitím protokolu Telnet, případně šifrovaného SSH spojení. K dispozici je i možnost vzdálené konfigurace pomocí tlustého klienta označovaného jako Winbox, přes klasické webové rozhraní nebo specifické API rozhraní.

Možnosti přístupu ke správě přístupových bodů, jež tvoří páteř bezdrátové školní sítě jsou velmi široké a skýtají i bohaté možnosti automatizace. V současnosti na škole není zaveden žádný systém pro správu přístupových bodů a všechny případné konfigurační zásahy tak jsou prováděny ručně (teoreticky z libovolného počítače, jenž se nachází ve školní síti) a bez použití skriptů či administrační konzole.

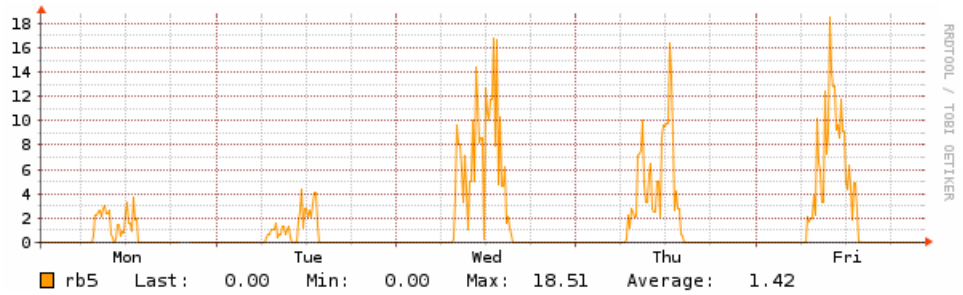
Monitoring sítě
Pro sledování a zasílání notifikací o dosažení mezních hodnot systémových prostředků Windows serverů a dostupnosti vybraných síťových zařízení se na škole používá monitorovací nástroj Nagios s grafickou nadstavbou Centreon. Jedná se o dva opensource projekty, které spolu spolupracují a tvoří jeden funkční celek s uniformním pohodlným webovým konfiguračním rozhraním. Funkcionalitu tohoto dohledového systému lze rozšiřovat pomocí takzvaných pluginů. Jako pluginy se označují skripty spouštěné jádrem (resp. plánovačem) Nagiosu a jejichž výstup je pro Nagios engine vracen zpět ve zpracovatelném formátu. Pluginy/skripty mohou být napsané v různých jazycích a jediné 2

podmínky kompatibility jsou: aby návratová hodnota skriptu nebo spustitelného souboru nabývala jedné z následujících hodnot 0;1;2;3, a aby skutečně data na výstupu z pluginu byla v takovém formátu, v jakém je Nagios standartně očekává a může je zpracovat[27]. V době analýzy a získání přístupu k tomuto dohledovému systému jsem měl možnost si prohlédnout konfiguraci monitoringu přístupových bodů, která spočívala pouze v kontrole dostupnosti síťového zařízení pluginem check_host_alive na bázi protokolu ICMP.

Počet uživatelů a využití bezdrátové sítě
Pro získání lepší představy o skutečném počtu uživatelů/zařízení školní bezdrátové sítě jsem využil tabulku s přehledem autentizovaných sezení na síťovém firewallu. Z každého zařízení, z nějž je požadován přístup do internetu, je potřeba v současnosti denně provést autentizaci pomocí již výše popsaného mechanismu. Pro každé úspěšně autentizované zařízení je na firewallu následně vytvořeno sezení s časově omezenou platností po ukončení komunikace (tzv. „timeout“), přičemž maximální konfigurovatelná hodnota je 480 minut – tedy 8 hodin. Několik dní po sobě jsem si proto vždy po skončení poslední vyučovací hodiny nechal na firewallu vypsat počet záznamů v tabulce sezení – hodnoty se pohybovaly v rozmezí 260–300 unikátních uživatelů. Zde je potřeba zdůraznit, že z tohoto údaje nelze zjistit informaci o skutečném počtu současně připojených síťových zařízení ale jenom počet unikátních připojených uživatelů v daném dni.

1.2.3 Návrh úprav k vylepšení bezdrátové sítě

Pokrytí
Analýzou naměřených hodnot síly signálů při kontrole bezdrátového pokrytí školního areálu ve vybraných lokalitách a zanesených do tabulky 1.2 jsem zjistil, že úroveň síly signálu jednoho z přístupových bodů je obecně velmi špatná. A to především v lokalitách, kde bych očekával podstatně vyšší než naměřené hodnoty (v pláncích na obrázku to jsou lokality označené písmeny D,H a I). Paralelně jsem v rámci rozšiřování funkcionalit dohledového systému implementoval i odečítání počtu připojených bezdrátových zařízení a tyto hodnoty vykresloval do grafu. Pohled na historické nízké hodnoty počtu připojených bezdrátových zařízení k tomuto AP ve mne vzbudil podezření, že je s vysílačem něco v nepořádku. Při kontrole registration-table tj. tabulky aktuálně připojených zařízení jsem pak viděl velmi nízké úrovně síly signálů u všech přípojených klientů (rozmezí -80 až -95 dBm). Rozhodl jsem se proto provést výměnu bezdrátového modulu - miniPCI kartičky. Po výměně karty, v úterý po skončení výuky, lze pozorovat na obrázku 1.8 resp. grafu počtu připojených zařízení značný nárůst počtu připojených klientů k dotyčnému AP v následujících dnech. Výměna komunikačního modulu tak byla oprávněná.



Obrázek 1.8: Na tomto grafu lze sledovat vývoj počtu připojených zařízení k AP=rb5 s podezřením na vadný komunikační modul před a po jeho výměně.

Úprava konfigurovaných vysílacích kanálů
Při provádění průzkumu bezdrátového prostředí ve škole pomocí SW nástroje *inSSIDer* a bezdrátového usb modulu jsem zjistil, že všechny přístupové body používají pro komunikaci s bezdrátovými uživatelskými zařízeními stejný frekvenční rozsah se středem na 2412MHz, což odpovídá kanálu číslo 1. S největší pravděpodobností se jedná o defaultní nastavení.

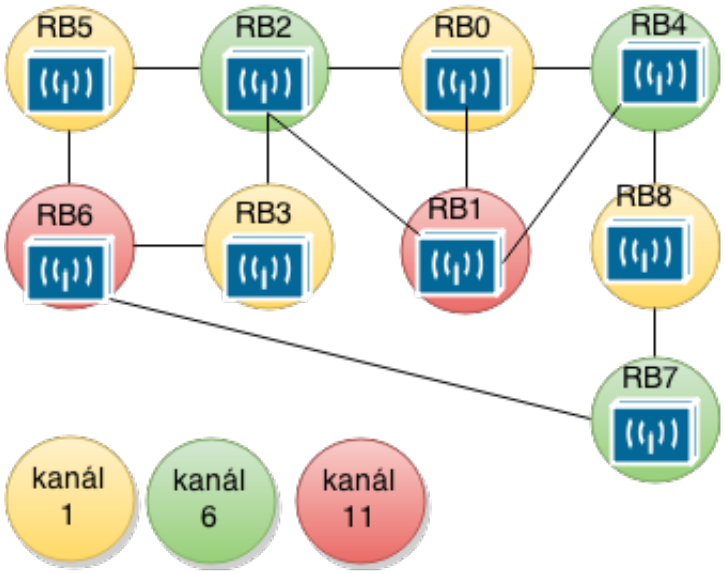
Problematice překryvu používaných vysílacích frekvencí u sousedících kanálů v pásmu 2,4GHz jsem se věnoval již v teoretické části práce a nyní je potřeba tyto znalosti aplikovat do praxe. V praxi máme v tomto frekvenčním pásmu k dispozici 3 kanály (1,6,11) a musíme je rozdělit mezi jednotlivé přístupové body tak, aby se v éteru 2 přístupové body se stejným konfigurovaným kanálem překrývaly co nejméně – v ideálním případě vůbec. Jedná se vlastně o problém barvení grafu, což je jedna z disciplín teorie grafů, jejíž podstatou je obarvení vrcholů/hran/stěn takovým způsobem, aby žádné dva sousední prvky neměly stejnou barvu.

Při řešení tohoto problému jsem postupoval tak, že jsem přístupové body zakreslil do grafu na obrázku 1.9 jako vrcholy a následně zkonstruoval hrany označující vzájemnou sousednost, přičemž vztah sousednosti jsem stanovil na základě skutečné fyzické sousednosti 2 zařízení. Vzhledem k relativně nízkému počtu vrcholu jsem následně mohl začít ručně s obarvováním vrcholů (přiřazováním čísel kanálů) a postupovat až do úplného obarvení grafu při zachování základní podmínky, aby žádné 2 sousední vrcholy neměly stejnou barvu. Jedno z možných řešení, které jsem následně aplikoval na konfiguraci kanálů přístupových bodů je uvedeno v přiložené tabulce 1.3.

Optimalizace přenosových parametrů na bezdrátovém rozhraní přístupových bodů
V této návrhové části se zabývám optimalizací přenosu na fyzické a linkové

Tabulka 1.3: Úprava vysílacích kanálů, řešení nalezené barvením grafu.

AP	Zvolený kanál
rb0	1
rb1	11
rb2	6
rb3	1
rb4	6
rb5	1
rb6	11
rb7	6
rb8	1



Obrázek 1.9: Na obrázku jsou znázorněny všechny školní přístupové body a hrany jako vztahy sousednosti mezi nimi ve skutečnosti. Každé barevné kolečko symbolizuje odpovídající vysílací kanál. I letmým pohledem lze snadno zkontrolovat, že žádné 2 sousední vrcholy grafu nejsou stejně obarvené.

vrstvě bezdrátové části sítě. Metodiku prováděných měření jsem, jak již bylo uvedeno výše v práci, rozdělil na pasivní a aktivní. Jako pasivní jsem označil vyčítání hodnot z čítačů na přístupových bodech. Naopak při aktivním měření je měřící zařízení připojeno k bezdrátové síti při běžném provozu a podle mnou navrhnutého scénáře provádí předkonfigurované síťové testy, jejichž výsledky zaznamenává.

Vzhledem k relativně rozsáhlé složitosti této problematiky jsem potřeboval oproti ostatním implementačním úsekům této práce podstatně více času pro nastudování materiálů, návrhu testovacích scénářů a celkové metodiky měření. S tím jak jsem se v průběhu provádění dílčích menších testů a měření kontinuálně vzdělával a doplňoval znalosti o fungování bezdrátových technologií, vyvíjela se i metodika navrhovaného měření. Výsledkem je možnost aplikování vyvinuté měřící metodiky pro porovnání 2 stavů resp. konfigurací bezdrátové části přístupových bodů před začátkem úprav (defaultní konfigurace) a po implementaci navrhovaných úprav.

U tzv. pasivního měření (detailní vysvětlení tohoto pojmu se nachází výše v úvodu analytické části) jsem sbíral bash skriptem přes ssh automaticky se zadanou frekvencí data z tabulky „registration-table“. Tato tabulka obsahuje jak aktuální a proměnlivé hodnoty jako sílu signálu, aktuální data-rate, ccq a p-throughput tak i počítadla s počtem rámců k přenesení a skutečně přenesených a to o každém aktuálně připojeném klientském zařízení od okamžiku jeho asociace s rozhraním přístupového bodu. Při odpojení jsou data z tabulky resp. z paměti přístupového bodu ihned odstraněna a při případném opětovném připojení klientského zařízení jsou všechna počítadla inicializovány na nulové hodnoty.

Zde uvádím názvy a popis sledovaných parametrů, jak je lze najít u každého klientského zařízení v tzv. registration-table což je tabulka s evidencí připojených zařízení v AP. Následující zaznamenávané hodnoty jsou unikátní pro každé připojené klientské zařízení:

- **hw-frames-Rx/Tx** - počet skutečně přenesených rámců na rozhraní v obou směrech
- **frames Rx/Tx** - celkový počet rámců k odeslání resp. počet potvrzovaných přijatých rámců
- **Rx/Tx-rate** - aktuálně používané komunikační rychlosti ve směrech z pohledu AP
- **signal-strength** - průměrná síla klientského signálu přijímaná přístupovým bodem v jednotkách dBm

- **signal-to-noise** - odstup síly signálu od šumu, vyjádřeno v decibelech
- **hw-frame-bytes Rx/Tx** - souhrnná velikost přenesených dat v obou směrech včetně dat v hlavičkách
- **tx-ccq** - proměnná vyjádřená v procentech, která má vyjadřovat, jak efektivně je využito v danou chvíli dostupné rychlostní pásmo (bandwidth) ve vztahu k teoretické maximální hodnotě vypočtené šířky pásma. Hodnota se vypočte jako poměr Tmin/Treal přičemž tento poměr se počítá pro každý odeslaný rámec (z pohledu přístupového bodu) a tento mezivýsledek se aplikací váženého průměru promítá do finální hodnoty. Tmin je přitom teoretická hodnota, která vyjadřuje dobu přenosu rámce na nejvyšší možné komunikační rychlosti bez opakování přenosu. Treal je skutečný, naměřený čas doby přenosu včetně případných opakovaných přenosů. Proměnná se v GUI rozhraní - WinBox aktualizuje každou vteřinu a údajně se dle popisu v oficiální dokumentaci počítá jako vážený průměr několika hodnot, ale bohužel se mi nepodařilo dopátrat se bližších podrobností k výpočtu.
- **p-throughput** - vysílačem vypočtená přibližná hodnota teoreticky maximální dostupné šířky pásma v kbps ve směru od AP ke klientskému zařízení. Údajně je do výpočtu zahrnuta i aktuální používaná komunikační rychlost a opakované přenosy. Hodnota se aktualizuje každých 5 sekund. Přesný vzorec výpočtu této proměnné bohužel není veřejně k dispozici.
- **mac-address** - MAC adresa připojeného klientského zařízení

V části práce věnované analýze současného stavu sítě, jsem již nastínil metody a způsob získávání dat pro účely změření a budoucího porovnání kvality bezdrátové sítě, přičemž jsem rozdělil měření na 2 oddělené části - **aktivní** a **pasivní**. Při aktivním měření jsem přenášel data pomocí vybraných základních síťových protokolů přes bezdrátovou infrastrukturu školy a zaznamenával jsem naměřené hodnoty. Pasivní měření pak spočívalo v návrhu a sestavení mechanismu pro automatický sběr dat o navázaných spojeních bezdrátových zařízení přímo z přístupových bodů v definovaném časovém intervalu 2minut. Na následujících řádcích se chci věnovat navrhnutým metrikám a způsobu vyhodnocování naměřených dat.

Metriky pasivního měření

Ze sledovaných hodnot pasivním měřením lze jednoduchými úpravami získat zajímavé údaje. Prvním z jmenovaných je počet opakovaných pokusů o přenesení rámce. Jedná se o poměr hodnoty hw-frames (Rx/Tx) ku odpovídající hodnotě frames (Rx/Tx). Čím menší je tento poměr, tím je spojení mezi přístupovým bodem a klientským zařízením kvalitnější ve smyslu toho,

že při opakovaných přenosech rámců tato hodnota roste a dochází ke snížení propustnosti a navýšení latence komunikace. Vypočtený poměr 1,5 například vyjadřuje, že na úspěšný přenos 100 rámců bylo zapotřebí přenést rozhraním 150 rámců. K opakovaným přenosům dochází v důsledku chyby přenosu, při kolizích při přenosu rámců nebo jejich potvrzení, v zarušeném prostředí nebo nekvalitním bezdrátovém spoji(hardware závada). Agregací hodnoty tohoto ukazatele podle MAC adres a zprůměrováním všech takto získaných hodnot za dané období lze získat bezrozměrnou číselnou hodnotu, jíž se snažím vyjádřit průměrnou kvalitu spojení pro dané zařízení ve smyslu nutnosti opakovaných přenosů (výpočty jsou příloze, vypočteno pomocí kontingenčních tabulek) resp. průměrnou hodnotu pro získání orientační informace o celé bezdrátové síti např. pro účely porovnání vlivu 2 různých konfigurací. Tuto průměrnou hodnotu označuji v přiloženém dokumentu s analýzou jako *avg grouped tx-hw-frames / tx-frames* pro odchozí směr resp. *avg grouped rx-hw-frames / rx-frames* pro příchozí směr. Hodnota v mnou definovaném ukazateli *avg tx-hw-frames / tx-frames* resp. *avg rx-hw-frames / rx-frames* potom obsahuje aritmetický průměr ze všech získaných poměrů. Každá MAC adresa tak vkládá do výpočtu namísto jedné hodnoty poměru v každém směru celou řadu hodnot v závislosti na délce trvání připojení k AP v dané periodě.

Další metriky, které jsem použil pro vyhodnocení vhodnosti konfigurace k nasazení do provozu, jsou porovnání hodnoty aritmetického průměru od všech zahrnutých připojených zařízení u parametru **p-throughput** a **tx-ccq**.

Důležitým dodatkem k pasivnímu měření resp. k vyhodnocování naměřených hodnot jsou filtry, které jsem na posbíraná data před jejich zpracováním aplikoval. Z jakéhokoliv zpracování jsem totiž vyloučil ty řádky (záznamy z výše popsané registration-table), které neměly alespoň více než 200 úspěšně přenesených rámců v každém směru. Důvodem pro toto opatření byla má obava ze zkreslování výsledků zařízeními neautentizovaných uživatelů. Škola se nachází na rušné ulici v centru města a přímo sousedí s další střední školou(bez identifikované bezdrátové sítě), dvěma restauračními zařízeními s celkovou kapacitou v řádu desítek míst a v těsné blízkosti školní budovy najdeme i dvě zastávky pro několik páteřních linek městské hromadné dopravy. Uvedené faktory mají za následek desítky vygenerovaných připojení a stovky záznamů od původem „cizích“ uživatelů ke školní síti denně. Kvalita spojení u těchto zařízení může být negativně ovlivněna tím, že se nenacházejí v dobře pokryté oblasti rádiovým signálem, na což není síť navržena. Tím dochází ke zkreslení naměřených resp. vyhodnocovaných hodnot u vybraných a definovaných metrik. Tento filtr samozřejmě odfiltruje i hodnoty těch uživatelů, jejichž zařízení se čerstvě k síti připojilo. I u těchto naměřených hodnot si ale myslím, že je žádoucí je z vyhodnocení vynechat, poněvadž jejich vypočtené poměry

opakovaných přenosů vycházejí z nízkých a tím pádem méně vypovídajících či přesných hodnot stavu spojení.

Metriky aktivního měření
Aktivní měření probíhalo za pomoci sestavené sondy z laptopu Toshiba NB100, Windows XP Home s externím USB modulem TP-Link TL-WN722N s externí 4dBi všesměrovou dipólovou anténou a open-source software JMeter.

- „Latence bakaláři“ - průměrný čas načtení všech prvků titulní webové stránky z rozhraní školního systému “bakaláři” pomocí síťového protokolu HTTP.
- „Latence moodle“ - průměrný čas načtení všech prvků titulní webové stránky z rozhraní školního systému “moodle” pomocí síťového protokolu HTTP.
- „Latence imap“ - průměrný čas načtení hlaviček 5 nejnovějších zpráv v inboxu pomocí protokolu IMAP.

Po stanovení metrik pasivních a aktivních měření jsem se podrobně seznámil s konfiguračními možnostmi bezdrátového rozhraní, jež platforma MikroTik nabízí. Následně jsem navrhnul možné konfigurační úpravy, jejichž efekt jsem měřil pomocí výše definovaných metrik. Mým cílem byla přitom jednak snaha o dosažení lepších přenosových parametrů v síti a druhak i otestování reálného využití navržených metrik.

Popis všech parametrů, jež lze konfigurovat na bezdrátovém rozhraní, lze nalézt v příslušné sekci v oficiální dokumentaci[28]. Zde uvádím ty nejzásadnější parametry, jejichž efekt jsem se rozhodl v nějakém rozsahu otestovat a změřit.

- **basic–rates-a/g** – seznam komunikačních rychlostí, které budou na rozhraní AP použity. Všechny rychlosti uvedené v tomto výčtu musejí být podporovány i klientským zařízením, jinak nebude spojení navázáno.
- **supported–rates-a/g** – seznam komunikačních rychlostí, jež mohou být použity pro komunikaci AP na daném bezdrátovém rozhraní pro komunikaci s klientskými zařízeními.
- **hw–retries** – počet pokusů o odeslání rámce, které ještě přístupový bod nevyhodnotí jako chybu přenosu. 3 opakované chyby přenosu v řadě za sebou [tj. celkem 3*(hw-retries+1) chybných pokusů] na nejnižší podporované komunikační rychlosti mají za následek pozastavení přenosu na dobu stanovenou parametrem „on-fail-retry-time“. Po vypršení této lhůty se AP pokusí znovu o odeslání rámce příjemci.

- **hw–fragmentation–threshold** - hodnota v jednotkách Byte, která určuje maximální velikost odesílaného rámce. Rámce větší než konfigurovaná hodnota budou před odesláním fragmentovány.

- **hw–protection–mode** - volba přídavného mechanismu pro ochranu a zvýšení úspěšnosti doručení přenášených rámců s možnostmi *none*, *cts-to-self* a *rts-cts*. Režim ochrany *rts-cts* se skládá ze standartního RTS/CTS handshake před odesláním dat příjemci. V případě hodnoty *cts-to-self* před odesláním dat neprobíhá standartní handshake, namísto toho přístupový bod jako vysílač před odesláním rámce vyšle pouze malý rámec „sám sobě“ s příznakem CTS, na kterou všechna 802.11 kompatibilní zařízení, která tuto zprávu zachytí, reagují tak, že odloží plánované vysílání o stanovený časový interval. Tento mechanismus by tak měl zabránit situacím, kdy jeden klient začne přijímat data od vysílacího bodu ve stejný okamžik, jako sousední klient začne vysílat data pro vysílač. Vysílání dat jiného klienta tak v takových případech může způsobit kolize, nutnost opakovaného přenosu vysílačem a tím snížit užitečnou propustnost bezdrátové sítě. hw-protection-threshold - hranice v jednotkách Byte, která určuje od jaké velikosti rámců se má aplikovat typ mechanismu ochrany přenosu rámců specifikovaný v parametru *hw-protection-mode*.

- **frame–lifetime** - časové omezení pro odesílání rámce. Pokud se rámec nepodaří odeslat resp. přijmout potvrzení o přijetí od příjemce před uplynutím tohoto intervalu, rámec bude vyřazen z přenosu a zařízení bude pokračovat v přenosu dalšího rámce z fronty rámců čekajících k odeslání. Časovač je vynulován vždy před prvním pokusem o odeslání každého jednotlivého rámce. Pokud je hodnota nastavena na nulu, platnost rámce nevyprší.

- **adaptive–noise–immunity** - toto nastavení se týká zařízení s chipsetem Atheros AR5212 nebo novějších a dává správci možnost zapnout/vypnout patentovanou proprietální metodu dynamického automatického upravování parametrů na přijimací straně přístupového bodu. Volbou odpovídajícího prostředí by mělo dojít k minimalizaci rušení a vlivu šumu a ve výsledku ke zvýšení kvality přijímaného rádiového signálu.[29]

- **disconnect-timeout** - časový interval, k jehož startu odpočtu dojde při třetím opětovném selhání odeslání rámce resp. po 3 * (hw-retries + 1) chybném pokusu o odeslání na nejnižší podporované komunikační rychlosti (1Mbps). Během odpočtu dochází k opakovaným pokusům o přenos v intervalu daném hodnotou konfigurační položkou „on-fail-retry-time“. Pokud nebude během intervalu disconnect-timeout obdrženo žádné potvrzení o přijetí rámce, spojení s daným zařízením bude ukončeno a do logu se zapíše hláška „extensive data loss“.

- **on-fail-retry-time** - časový interval, jehož význam jsem již částečně popsal u specifikace parametrů *hw-retries* a *disconnect-timeout*. Jedná se o dobu, na kterou odesílající zařízení odloží odesílání rámce po třetí chybě přenosu a je to také interval s jakým se během periody disconnect-timeout zařízení pokouší o odeslání rámce.

Syntetický distribuovaný test s měřením

Na následujících odstavcích se vracím do úvodní fáze zkoumání vlivu jednotlivých konfigurovaných parametrů, kdy jsem hledal způsob, jak lze provádět měření, která by změny v konfiguraci odrážela do naměřených hodnot. Navrhnul jsem proto měření, při kterém jsem rozmístil rovnoměrně po lavicích v jedné ze školních učeben po skončení výuky 9 zapůjčených laptopů z inventáře školy, na které jsem nainstaloval prostředí pro spouštění přeložených programů v jazyce JAVA, nahrál nástroj JMeter a laptopy připojil ke školní bezdrátové síti. Všechny počítače přitom byly připojené ke stejnému přístupovému bodu, autentizované a s platnou konfigurací na síťovém rozhraní. Na obrázku 1.10 je fotografie pořízená z tohoto měření. Následně bylo potřeba na zapůjčených laptopech spustit nástroj JMeter v režimu server a zaznamenat si IP adresu. Při volbě režimu „server“ dochází k tomu, že JMeter spustí naslouchání na daném portu, kde přijímá testovací konfiguraci od tzv. prvku, který se značí jako „master“.

Prvek **master** byl v tomto případě můj laptop, jenž jsem rovněž připojil do téže sítě. Na **master** stroji jsem potřeboval upravit konfigurační soubor nástroje JMeter tak, že jsem přidal zaznamenané IP adresy připojených školních laptopů jako parametry do sekce „remote hosts“[30] a sadu testů jsem omezil pouze na testy na bázi HTTP protokolu bez použití protokolu IMAP. Činil jsem tak proto, že jsem nechtěl zatěžovat servery třetí strany bez povolení, protože se v tomto případě zcela jistě nejedná o standartní využívání poskytovaných služeb.

Při spuštění testu pak bylo třeba namísto klasické volby „Start“ spouštět test volbou „Start All“. Tím došlo k předání testovací konfigurace všem serverům uvedeným ve výčtu konfigurační položky „remote hosts“, jež začaly ihned s testováním a následně i předáváním výsledků testů prvku **master**, který se staral o jejich zpracování a uložení. Měření tak probíhalo formou distribuovaného testu s centrálním ukládáním výsledků.

Přestože byl tento popsaný distribuovaný test plně funkční tzn. **master** node úspěšně spouštěl testy a sbíral naměřené hodnoty od jednotlivých stanic,

Obrázek 1.10: Fotografie pořízená při provádění měření v rámci distribuovaného testu. Po lavicích jsou rovnoměrně rozmístěny zapůjčené školní laptopy.

tak bohužel absolutně neodpovídal realitě, což jsem si uvědomil až po jeho provedení a to na základě následujících faktů:

- V tomto případě se nacházely všechny laptopy relativně blízko u sebe a v jedné místnosti. Výrazně lépe tak zde mohl fungovat mechanismus CSMA/CA, než když jsou síťová zařízení rozprostřena po členité budově.

- Ve skutečnosti je spolu s komunikujícími síťovými zařízeními v místnosti někdy i více než 20 žáků. Přítomnost osob v prostorách pokrývaných bezdrátovým signálem by neměla být zanedbatelná informace, o čemž se přesvědčili např. i inženýři při návrhu pokrytí wifi signálem prostor v trupech letadel výrobce Boeing.[31]

- Typickým zařízením, které ve škole žáci a zaměstanci používají pro připojení k bezdrátové síti není laptop, ale mobilní telefon nebo tablet. Jak jsem se sám přesvědčil za dobu strávenou v budově, kdy jsem nezahlédl na škole jediného žáka/žákyni s laptopem.

- Dodatečně lze podpořit tezi, která vede k zavrhnutí tohoto měření i tím, že v průběhu měření se pohybovala průměrná síla přijímaného signálu na AP od klientských stanic kolem hodnoty -50dBm. Pozdějším měřením jsem zjistil, že průměrná hodnota síly signálu se ve škole pohybuje okolo -70dBm – viz. tabulka na obrázku A.1 a řádek „avg signal strength“.

Výsledky tohoto měření tak přikládám pouze na datový nosič a nikoliv do papírových příloh. I přes vynaložené úsilí a strávené odpoledne měřením ve výsledku zbytečných hodnot mi toto měření ukázalo, že musím pro měření skutečné kvality bezdrátové sítě využít jiných metod a to konkrétně již v textu zmíněné dvojice **aktivního** a **pasivního** měření.

Konfigurace access-list na AP pro podporu roamingu
V průběhu provádění analýzy pokrytí školního areálu bezdrátovou sítí jsem procházel budovou vybaven několika bezdrátovými síťovými zařízeními, připojenými k bezdrátové síti - laptop, mobilní telefon a tablet. Při přemisťování mezi lokalitami, ve kterých jsem prováděl měření, mne zaujala místy až neochota zařízení provést přepojení na mnohem bližší/výhodnější přístupový bod. Namísto toho zařízení zůstavalo připojeno k původnímu vysílači ještě po relativně dlouhou dobu než došlo k jeho přepojení. Vzhledem k změřenému relativně dobrému pokrytí jsem proto navrhnul a následně aplikoval změnu na všech (do té doby prázdných) „access list“ seznamech na přístupových bodech.

Access List slouží v RouterOS k nastavení některých parametrů (např. omezení datového toku) případně k omezení autentizace a/nebo asociace vybraných MAC adres klientských síťových zařízení[28]. Jednotlivé záznamy v tomto seznamu jsou před každým přijatým požadavkem postupně vyhodnoceny a podle pravidla first-match se v připojovacím procesu aplikuje odpovídající pravidlo. Navržená úprava spočívala v přidání sledu pravidel, jež měla vést k tomu, že autentizovaná a asociovaná zařízení s bezdrátovým rozhraním budou vynuceně odpojena, pokud klesne síla signálu pod stanovenou hranici, kterou jsem zprvu nastavil na hodnotu -90dBm. Tuto hodnotu jsem stanovil na základě zběžné analýzy hodnot v „registration table“ několika přístupových bodů.

Bohužel po aplikaci výše uvedeného mechanismu docházelo na některých uživatelských zařízení k situaci, kdy pokud bylo zařízení přístupovým bodem aktivně odmítnuto z důvodu nevyhovující kvality/síly signálu, zařízení následně rezignovalo na snahu o opakování pokusu o připojení k síti a zůstalo nepřipojené po dobu řádově jednotky až desítky sekund než se opět pokusilo navázat spojení. Toto chování jsem pozoroval jak na mobilním telefonu (Samsung GT-I8730, Android 4.1.2), tak na laptopu (HP Probook 430, OS Win7 Enterprise). Konfiguraci access list jsem proto z přístupových bodů odstranil a řešení kvality roamingu ve školní síti zůstává otázkou individuálního nastavení agresivity roamingu klientských zařízení, o kterém jsem se zmiňoval v teoretické části práce.

Vytvoření separátní VLAN pro bezdrátovou síť (sítě)
Při pohledu na stávající síťovou architekturu školy je ihned patrný tzv. „flat network“ design sítě. Ten se vyznačuje rozsáhlou (a často jedinou) broadcastovou doménou, absencí směrovačů a dalších prvků pro směrování nemluvě o nulové redundanci a v neposlední řadě i jakéhokoliv omezení na síťové vrstvě.[32]

Vzhledem k faktu, že škola disponuje firewallem, jenž je schopný směrovat provoz mezi jednotlivými subinterface mezi virtuálními i fyzickými sítěmi v režimu známém jako „router-on-the-stick“[33], volným ethernetovým portem a přepínači s podporou značkování rámců podle protokolu 802.1Q, navrhuji propojit dalším ethernetovým kabelem síťový přepínač s firewallem, zavést tagování rámců a vytvořit tak vyhrazený prostor pomocí virtuálních sítí (VLAN) na druhé vrstvě ISO/OSI modelu pro provoz přístupových bodů resp. připojených uživatelských zařízení. Veškerý provoz z bezdrátové sítě do internetu/pevné sítě tak bude procházet přes firewall a bude možné jej na jednom místě upravovat. Nahrazeny tak budou jednotlivé tabulky s pravidly na přístupových bodech, jejichž správa určitě není jednoduchá. Zakončení virutálních sítí do nevyužitého portu na firewallu není v tomto případě podmínkou, ale pokud by pro dotyčný fyzický port nebylo plánováno jiné využití, tak z kapacitních důvodů i přehlednějšího zapojení určitě doporučuji jeho využití pro implementaci virtuálních sítí.

Výhodou bude i podstatně vyšší bezpečnost a ochrana pevné sítě před případnými potenciálními útočníky z bezdrátových rozhraní vysílačů. Pravidla pro směrování provozu mezi jednotlivými (bezdrátovými) sítěmi mohou být takto spravována centrálně, přehledně a s využitím podstatně širších možností logování než v dosavadním zapojení.

V případě úspěšného zavedení značkování rámců v síti a vytvoření trunk spojů z páteřních spojení jsou další zásahy v podobě zavedení další virtuální sítě již triviální záležitostí a proto se dle mého mínění jedná o velice logický a do budoucna užitečný návrh.

Úprava IP adresního rozsahu a DHCP protokolu
V návaznosti na separaci bezdrátových přístupových bodů do vyhrazené virtuální sítě jsem se zabýval možnostmi úprav na třetí ISO/OSI vrstvě u aktivních síťových prvků. Ani při podrobnějším zkoumání jsem si nedokázal vysvětlit, proč by bylo nutné zachovat v rámci nově vytvářené VLAN směrování provozu v jiném bodě sítě, než pouze na školním firewallu.

Dospěl jsem tak k závěru, že pro správu sítě bude výhodnější, když budou bezdrátová rozhraní přístupových bodů v režimu bridge s fyzickým portem,

jenž zajišťuje spojení s firewallem. Implementací této úpravy se značně zjednoduší konfigurace na přístupových bodech a to i co se týče protokolu DHCP. Současný stav, kdy každý přístupový bod disponuje vlastní DHCP službou a poskytuje IP adresy připojeným zařízením z menších rozsahů je velmi nepřehledný, proto navrhuji provést přenesení služby buď na firewall nebo na jiné dedikované zařízení tak, aby všechna síťová zařízení připojená k bezdrátové síti čerpala z jednoho společného IP poolu adres.

Centrální autentizace po zabezpečeném kanálu
Popsaný, v současnosti používaný, autentizační mechanismus trpí již od návrhu několika bezpečnostními slabinami. Jako nejzávažnější bych označil fakt, že přístupové body nejsou pro uživatelská zařízení důvěryhodné resp. nelze v současnosti ověřit jejich pravost a uživatelé se tak mohou omylem připojit na přístupový bod, který se bude vydávat za jedno ze školních AP a uživatel o tom nemusí vůbec vědět.

Možným řešením tohoto problému je navázání zabezpečeného autentizačního kanálu s centrální autentizační jednotkou (RADIUS serverem), kdy se autentizační služba musí prokázat takovým certifikátem, který bude vydán uživatelem důvěřovanou certifikační autoritou. Tímto způsobem má uživatel možnost ověřit, že se připojuje skutečně k pravému školnímu přístupovému bodu. V implementační části popisuji realizaci tohoto navrženého řešení.

Konfigurace zabezpečení přenosu dat a centrálního autentizačního mechanismu
V předchozí kapitole jsem podrobně analyzoval stávající autentizační mechanismus. Nyní již proto nejprve jenom stručně připomenu jeho největší nevýhody:

- Uživatelé se musí každý den znovu přihlašovat i když používají stále stejné síťové zařízení.
- Pro vytvoření sezení na firewallu je zapotřebí otevřít prohlížeč a zadat své přihlašovací údaje do webového formuláře.
- Uživatel při zadávání přihlašovacích údajů nemá jistotu, že se přihlašuje k bezpečné a známé síti i když tato síť má shodný název.

Tyto uvedené problémy kladou následující požadavky:

- aby bylo možné přihlašovací údaje do síťového zařízení bezpečně uložit

- aby se přihlášení k síti provádělo automaticky na pozadí bez nutnosti lidské interakce
- aby se síť prokazovala takovým „průkazem“, který nelze nikým zfalšovat a síťové zařízení uživatele mohlo ověřit jeho platnost

Součástí řešení by mělo být i šifrování komunikace mezi přístupovými body a uživatelskými zařízeními.

Napojení na Autentizační a Autorizační Infrastrukturu sítě eduroam

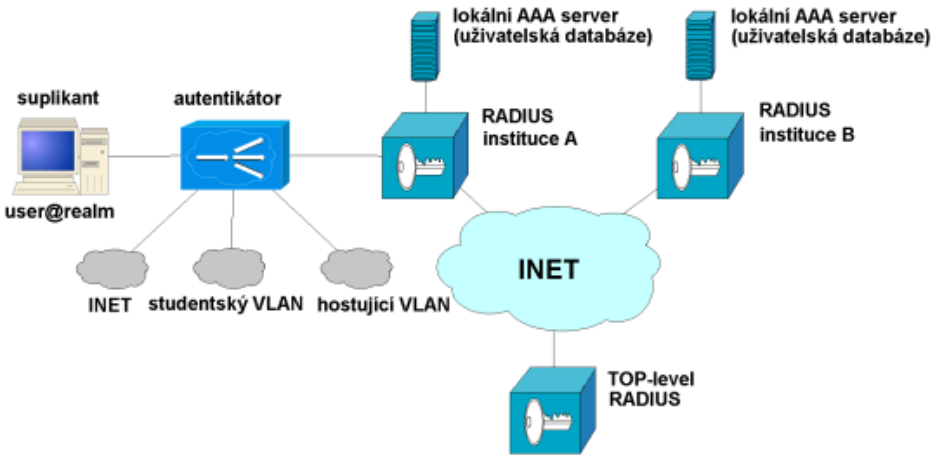
Eduroam je název infrastruktury podporující transparentní přístup k internetu a roaming uživatelů mezi organizacemi v celosvětovém měřítku. Základním principem spolupráce participujících organizací je poskytnutí wifi (případně kabelem) připojení k internetu v každé jednotlivé organizaci všem uživatelům i z ostatních partnerských sítí. V praxi to pro organizaci znamená, že její infrastruktura resp. internetová konektivita je nabízena k využití uživatelům ostatních organizací a naopak členové místní organizace mohou využívat připojení v lokalitách dalších členských organizací. [34]

Předpokladem pro fungování takového sdílení infrastruktur je nasazený a integrovaný autentizační systém v rámci každé organizace, jenž je schopný ověřit platnost identity resp. pravosti přihlašovacích údajů “svých” uživatelů. Autentizační systémy jsou hierarchicky uspořádány do stromové struktury, přičemž instituce v dané zemi spadají pod národní server. Ten zajišťuje předávání autentizačních požadavků mezi institucemi v rámci územního celku a přeposílá požadavky pro cizí státy na tzv. top–level RADIUS server, který je provozován společností SURFNet v Holandsku a ten zajistí předání požadavku mezi národními servery. Komunikace mezi RADIUS servery je přitom šifrována zpravidla protokoly RadSec nebo IPSec. V tuzemsku mluvíme v této souvislosti o projektu eduroam.cz, jehož koordinaci u nás zajišťuje společnost CESNET.

Členství organizace ve spolku je pro organizace bezplatnou záležitostí. Existuje ovšem sada podmínek, které musejí být před vstupem do eduroamu (alespoň v České republice) splněny a jejich dodržování je pravidelně kontrolováno. Jedná se o administrativní procesy, podporu, vytvoření specifických uživatelských účtů pro testování a další. [34]

Potenciální VÝHODY pro školu plynoucí z napojení AAI na síť eduroam:

- žáci a personál školy by získali možnost využívat internetové konektivity v oblastech pokrytých kooperujícími organizacemi



Obrázek 1.11: Globální pohled na fungování protokolu 802.1x[35]

Potenciální NEVÝHODY pro školu plynoucí z napojení AAI na síť eduroam:

- nutnost aktivního řešení případných incidentů souvisejících s provozem sítě eduroam
- nutnost důkladného zaškolení správce sítě do problematiky
- vytvoření procesů správy, udržování dokumentace
- potenciální nárůst využití systémových prostředků síťových prvků a vyšší využití nakupované internetové konektivity

V současnosti jsou pokryta sítí eduroam ve městě, kde se škola nachází, následující lokality[36] :

- univerzitní kampus a fakultní budovy při JČU
- 1 soukromá střední škola
- hvězdárna a planetárium

Z tohoto stručného výčtu rovněž plyne, že potenciální přínos pro žáky a zaměstnance v podobě roamingu po síti eduroam není v rámci domovského města nikterak oslnivý.

Další komplikací zjištěnou při analýze možných postupů integrace s AAI sítě eduroam byly špatné zkušenosti jiných správců s integrací RADIUS serveru v podobě NPS na Windows 2008. Ty spočívaly v nutných zásazích do atributů v AD, vytvoření speciálních skupin a komplikovanější konfiguraci IPSec spojení s národním RADIUS serverem.[37]

Vzhledem k výše uvedeným okolnostem, výhodám, nevýhodám a celkovému poměru možného získaného přínosu ku vložené práci a přidané administrační zátěži jsem se s člověkem zodpovědným za správu školních serverů dohodl na tom, že **nebudu pokračovat v integraci** školního autentizačního systému pro bezdrátovou síť s AAI sítě eduroam.

Ovládací skripty
Jak jsem rozebral již v analýze stávajícího řešení, přístupové body nejsou nikterak centrálně spravovány, přestože se naskýtá skutečně velké množství možností, jak lze toto prakticky realizovat. Domnívám se, že minimálně následující uvedené základní operace by měly být zautomatizovány, protože jejich ruční provádění je zbytečným plýtváním času a správu sítě zbytečně zesložitůje:

- provedení zálohy konfigurace do souboru
- obnovení konfigurace ze zadaného souboru
- restart (reboot) zařízení
- odeslání libovolného příkazu (např. kvůli sběru dat či úpravě konfigurace)

Uvedené funkce by mělo být možné spouštět z jednoduchého rozhraní, bez nutnosti další ruční autentizace na jednotlivých zařízeních a volitelně buď na jednom vybraném zařízení nebo dávkové na všech přístupových bodech v síti.

Kapitola 2

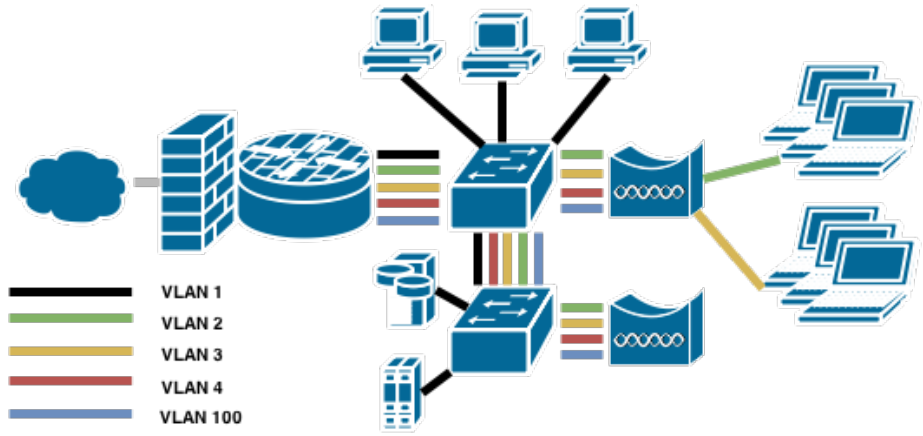
Popis řešení

Úprava logické architektury sítě
Návrh vytvoření logického členění za pomoci implementace podpory virtuálních sítí se zprvu jevil jako velmi zásadní zásah do stávající (jednoduché) školní síťové architektury. Musel jsem si proto tuto akci dobře promyslet a ujistit správu školní sítě, že neúměrně nenaroste náročnost správy sítě a že současně nebude ohrožen provoz školní sítě např. dlouhodobou ztrátou konektivity v důsledku možné miskonfigurace některého z dotčených síťových prvků.

Implementovat značkování VLAN jsem proto začal na firewallu. Zde jsem vytvořil na třetím ethernetovém rozhraní, značeném jako WAN2 a nepoužívaném, 4 subinterface, které jsem přiřadil VLAN identifikátory a pojmenoval:

- **wifi-open** - VLAN ID = 2
- **wifi-wpa2** - VLAN ID = 3
- **wifi-test** - VLAN ID = 4
- **wifi-mgmt** - VLAN ID = 100

Vytvořil jsem 4 rozhraní, protože do jednoho jsem chtěl překlopit provoz ze stávající bezdrátové sítě, další subinterface s VLAN ID=3 pak měl sloužit pro nově budovanou zabezpečenou bezdrátovou síť, třetí subinterface jsem vytvořil čistě pro testovací účely nebo do budoucna pro možnost vytvoření např. bezdrátové sítě s méně restriktivní síťovou politikou na firewallu - to ale přesahuje obsah této práce a žádná taková síť zatím nevznikla. Poslední zmíněný interface pak slouží pro komunikaci s přístupovými body protokoly SNMP, SSH, DHCP a RADIUS.



Obrázek 2.1: Architektura školní sítě po úpravách

Další na řadě po konfiguraci subinterface na firewallu byla konfigurace síťových přepínačů D-Link. Vzhledem k tomu, že jsou přístupové body a firewall fyzicky zapojeny pouze do 2 přepínačů, které jsou spojeny jedním ethernetovým kabelem, byla konfigurace relativně snadná. Spočívala ve vytvoření VLAN s ID 2,3,4,100 na přepínačích a přenastavení portu, kam byl nově připojen firewall z režimu untagged do režimu tagged pro všechna uvedená VLAN ID. Dále pak porty, kde byla připojena AP z režimu untagged do režimu tagged pro VLAN ID = 2,3,4 a naopak změna untagged z defaultní VLAN ID = 1 na VLAN ID = 100. Porty na přepínačích, které zajišťovaly jejich vzájemné propojení (tzv. trunk port) se staly také tagged pro VLAN ID = 2,3,4,100 s tím, že netagovaný provoz spadal k VLAN ID=1 tj. defaultní VLAN.

Označení portu untagged znamená, že jde o tzv. „access port“ a tedy případné hlavičky protokolu *802.1Q* jsou na příjmu u tohoto portu z rámců odstraněny a stejně tak se děje i u rámců na odchodu z tohoto portu po jejich přijetí některým z „trunk“ portů [38].

U portů označených pro konkrétní VLAN ID jako tagged se při příjmu rámce přepínač rozhoduje, zda jej přijme podle VLAN ID v hlavičce porovnáním s konfigurací na portu a přeposílá rámec na přístupové untagged porty této konkrétní VLAN ID.

Zajímavá pak pro mne byla implementace značkování VLAN na přístupových bodech, protože s tím jsem ještě neměl žádnou předchozí zkušenost. Hledal jsem proto v dokumentaci výrobce až jsem narazil na oficiální wiki MikroTik na následující článek: `http://wiki.mikrotik.com/wiki/Vlans_on_Mikrotik_environment`, podle kterého jsem si nastudoval konfigurační logiku za po-

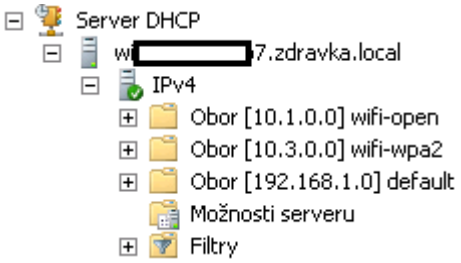
užití rozhraní v režimu bridge a následně jsem změny implementoval postupně na všechny přístupové body v síti. Konfigurace portů je k nahlédnutí na obrázku 2.2.

```
[admin@RB - ucebna10] > interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic
 #     INTERFACE                 BRIDGE
 0     vlan2                     br2
 1     vlan3                     br3
 2     vlan4                     br4
 3 I   wlan1                     br2
 4 I   wlan2                     br3
 5 I   wlan3                     br4
```

Obrázek 2.2: Konfigurace portů do jednotlivých bridge na jednom z AP

Konfigurace DHCP serveru

Navržené sloučení DHCP serverů do jednoho jsem realizoval na existujícím DHCP serveru na jednom ze školních Windows 2008R2 serverů. Na přiloženém obrázku 2.3 jsou viditelné různé obory pro distribuci IP adres v rámci protokolu IPv4. Rozsah „default“ je určený pro „pevnou“ síť školy, zatímco rozsahy s předponou „wifi-“ poskytují adresy bezdrátovým klientům. O to, aby se klienty všesměrově vysílané zprávy protokolu DHCP dostaly ke zpracování až na tento DHCP server, se stará funkce DHCP relay, kterou jsem zapnul na obou „wifi rozhraní“ síťového firewallu. Tato funkce pracuje tak, že zachytává DHCP zprávy s broadcastovou adresou příjemce a přeposílá je (spolu s informací na jakém rozhraní byla zpráva zachycena) na konfigurovanou IP adresu DHCP serveru[39] - na obrázku 2.4 ve sloupci s názvem „Options“. DHCP server tuto unicastovou zprávu přijme, v ideálním případě přidělí IP adresu z patřičného oboru a odesílá zpět zprávu bezdrátovému klientovi prostřednictvím síťového firewallu, který se postará o její doručení.



Obrázek 2.3: IP rozsahy na školním DHCP serveru

Autentizační systém

Pro nasazení centrálního autentizačního systému jsem zvolil implementaci RA-

	Interface	Mode	Type	Options	Enable
☐	wifi-open	Relay	Regular	192.168.1.14	✓
☐	wifi-wpa2	Relay	Regular	192.168.1.14	✓

Obrázek 2.4: Konfigurace DHCP relay na firewallu

DIUS protokolu od společnosti Microsoft s názvem „Network Policy Server“ – dále jako **NPS**. K nasazení tohoto řešení jsem dospěl na základě následujících zjištění:

- bude zachována relativní jednoduchost správy bezdrátové sítě (OS Windows)
- budou využity stávající serverové kapacity bez nutnosti instalace nového stroje
- relativně snadná integrace s adresářovou službou ActiveDirectory

Implementace řešení s RADIUS protokolem se tak skládalo z těchto činností:

- instalace role NPS na Windows 2008R2 server
- konfigurace síťových zásad + vytvoření certifikátu pro RADIUS server a export certifikátu CA
- konfigurace RADIUS klientů na straně serveru
- konfigurace přístupových bodů pro komunikaci
- povolení průchodu spojení RADIUS protokolu přes firewall

Přidání role „Network Policy Server“ na školní server s členstvím ve školní doméně jsem provedl za pomoci „průvodce přidáním role“ v administrační konzoli pro správu serveru.

Síťové zásady v rámci „Network Policy Server“ jsou konfigurační sady, které umožňují určit uživatele, jež mají oprávnění připojit se k dané (bezdrátové) síti a okolnosti, za kterých se lze či nelze připojit. Vytvořil jsem proto 2 zásady s příznakem povolujícím přístup - pro učitele a pro žáky. U odpovídající zásady jsem pak omezil množinu uživatelů na globální skupinu z Active Directory *ZDRAVKA\Učitelé* resp. *ZDRAVKA\Žáci*. Možnost specifikace globální skupiny z adresářové struktury pomocí vestavěného průzkumníka je velmi velké ulehčení a zjednodušení např. proti integraci některého z linuxových RADIUS serverů s doménovým kontrolerem.[40]

Jako povolenou metodu ověřování v kartě "Omezení" jsem zvolil metodu PEAP resp. EAP-MSCHAPv2. Pro vyšší bezpečnost autentizačního procesu předkládá RADIUS server v rámci použité sady protokolů pro ověřování PEAP a EAP-MSCHAPv2 klientům certifikát[41], jehož platnost si musí klient za pomoci importovaného kořenového certifikátu certifikační autority, která RADIUS serveru certifikát vystavila, ověřit.

Vzhledem k finančním důvodům a možnostem správy certfikátu jsem se rozhodl využít existující školní certifikační autoritu, s níž jsem vystavil pro RADIUS server certifkát. Tento vystavený certifikát jsem následně importoval do úložiště RADIUS serveru a nakonfiguroval síťové zásady pro použití tohoto certifikátu před zahájením autentizační výměny challenge řetězců. Pro uživatele z této konfigurace plyne, že pokud chtějí mít jistotu, že při autentizačním procesu skutečně ověřují svou identitu se školním RADIUS serverem, tak si musejí buď do svého síťového zařízení naimportovat certifikát použité školní certifikační autority mezi důvěryhodné kořenové certifikační autority do patřičného úložiště nebo při předložení certifikátu protistraně prostě důvěřovat, případně lze částečně ověřit pravost pohledem na data v otisku certifikátu.

Po konfiguraci síťových zásad a omezení povolených uživatelů na vybrané globální skupiny ze školní domény jsem musel RADIUS serveru nastavit tzv. seznam RADIUS klientů - v tomto případě přístupových bodů. Konfigurace spočívala v přidání IP adresy každého přístupového bodu na seznam v konfigurační položce NPS serveru a specifikaci tzv. sdíleného tajemství. V principu se jedná o sdílený klíč mezi serverem a klienty používaný za účelem primitivní vzájemné autentizace protistran, zajištění integrity přenášených zpráv a šifrování přenášených dat resp. přihlašovacích údajů od klientských zařízení.[42]

Konfigurace na přístupových bodech spočívala v nastavení IP adresy a portu RADIUS serveru, sdíleného tajemství a vytvoření tzv. *security profile* s nastavením autentizačního typu WPA2-EAP a volbou módu šifrování, kde jsem upřednostnil variantu AES CCM před TKIP a to zejména na základě ohlášených výskytů zranitelností v TKIP protokolu.[43] Jako zmíněný *security profile* se v prostředí RouterOS označuje kompletní konfigurační sada, která se věnuje zabezpečení. Takto předkonfigurované uživatelské sady pak lze aplikovat na bezdrátové rozhraní.

Centrální správa přístupových bodů

Výše v práci jsem se věnoval analýze stavu správy přístupových bodů, načež jsem navrhnul možná vylepšení, která by měla vést ke zkvalitnění bezdrátové sítě tím, že ulehčí administrátorům čas a práci při její správě. Vzhledem k potenciálnímu prospěšnému přínosu a snahy maximálně zkvalitnit různé aspekty

bezdrátové sítě jsem se rozhodl pro implementaci řešení pro centrální správu bezdrátových přístupových bodů.

Pro automatizaci autentizačního procesu při vstupu do konfiguračního rozhraní přístupových bodů jsem musel nejprve vybrat síťové zařízení v síti, ze kterého bude automatizovaná centrální správa vykonávána. Logicky jsem vzhledem k paralelně řešenému rozšiřování monitorovacího systému dospěl k závěru, že pro tyto účely bude nejvhodnější využít právě virtuálního stroje, z nějž je vykonáván prostřednictvím služby Nagios dohled síťových prvků školní sítě. Vygeneroval jsem proto na dohledovém stroji dvojici SSH klíčů (soukromý a veřejný) pro účet "Nagios", přičemž veřejný klíč jsem pomocí FTP protokolu a následně GUI rozhraní klienta Winbox importoval na všechny přístupové body. Autentizaci tak lze provádět automaticky bez zadávání přihlašovacích údajů jen s využitím vygenerovaného privátního klíče a veškerá přenášená data jsou po navázaném spojení šifrována s využitím protokolu SSH.

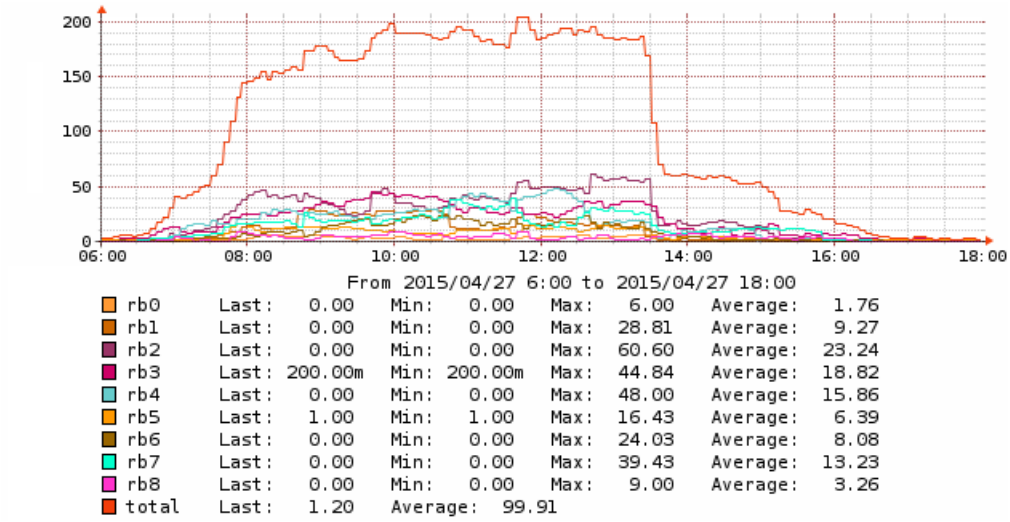
Za účelem implementace základních administrativních operací jsem se rozhodl vytvořit interaktivní bash skript controlAP.sh. Tento skript provede akci v závislosti na hodnotě parametru při svém spuštění. Podporované operace jsou přitom: save, saveAll, restore, restoreAll, command, commandAll, reboot a rebootAll. Parametry s příponou -All značí, že se akce provede na všech přístupových bodech a v takovém případě se skript na nic neptá a koná. Naopak při spuštění některé z variant parametrů bez přípony All se skript nejprve dotáže na IP adresu konkrétního přístupového bodu a až následně akci na něm vykoná.

Přínosy realizace tohoto navrženého a realizovaného řešení jsem ocenil zejména při plošných změnách konfigurace mezi jednotlivými intervaly prováděných měření kvality bezdrátové sítě.

Identifikace bezdrátové sítě
Jednotným názvem pro bezdrátovou síť resp. její SSID jsem ponechal původní název *ZDRAVKA* a později jsem přidal pro paralelně budovanou zabezpečenou(WPA2 enterprise) síť i vysílání SSID *ZDRAVKA2* na vytvořených virtuálních interface přístupových bodů v celém areálu školy.

Rozšíření monitorovacího systému
Pro monitorování přístupových bodů jsem chtěl primárně využít možností síťového protokolu SNMP. Jedním z pluginů, které obsahuje systém Centreon, je plugin check_centreon_snmp_value. Tento skript jazyka perl je nutno spustit s následujícími vstupními parametry: IP cílového zařízení, verze SNMP, OID a hodnoty threshold pro přechod do WARNING a CRITICAL stavů. Pro zjištění zátěže CPU pomocí protokolu SNMP tak bylo nejprve potřeba

zjistit identifikátor, pod kterým se u přístupových bodů nacházelo vytížení CPU. K tomu v RouterOS slouží příkaz **print** s parametrem *oid* [44].



Obrázek 2.5: Monitoring počtu připojených uživatelů ke školní bezdrátové síti

Analogicky jako u zjištění zátěže jsem si na každém AP vypsal *OID* identifikátor pro hodnotu *overall-tx-ccq*, která podle dokumentace vyjadřuje hodnotu využití dostupného pásma v rámci celého interface, jak jsem se dočetl ve starší verzi příručky [45]. Podrobnější popis bohužel není k dispozici, nicméně jsem implementoval monitorování této proměnné pro interface *wlan1* (ZDRAVKA) a *wlan2* (ZDRAVKA2). Popisu významu hodnoty CCQ se věnuji v analytické části práce u optimalizace parametrů konfigurace bezdrátové části. Od zaznamenávání této hodnoty do monitorovacího systému jsem si sliboval možnost sledování stavu sítě pro účely porovnávání efektu a vlivu různých konfigurací. Analýze naměřených hodnot se věnuji u vyhodnocení naměřených hodnot pasivním měřením v praktické části práce v sekci optimalizace přenosových parametrů.

Pro zjištění počtu připojených zařízení na bezdrátový interface a početní rozložení aktuálně používaných komunikačních rychlostí jsem se rozhodl napsat jednoduché skripty v bash. Vytvořené skripty bylo následně potřeba do systému zaevidovat přes rozhraní systému Centreon v sekci commands. S každým nově vytvořeným/nahraným pluginem do adresáře pluginů je potřeba i zadokumentovat způsob použití nového pluginu včetně nastavení a popisu spouštěcích argumentů. V systému Centreon jsou pak tyto uživatelem vložené informace uchované a samotné vytvoření služby je už jenom otázkou aplikace

vytvořené služby na konkrétní zařízení - v terminologii dohledového systému Nagios: “hosta”.

Aktualizace systému na přístupových bodech
Při snaze o provádění pasivního měření kvality bezdrátové sítě jsem se potýkal s problémy blíže popsanými v sekci, jež se zabývá analýzou sítě. V rámci řešení problému s komunikací mezi linuxovým strojem s instalovaným dohledovým systémem a přístupovými body jsem se snažil nejprve vyhledat příčinu problému v oficiální dokumentaci, avšak protože jsem nebyl úspěšný, rozhodl jsem se na základě jedné proběhnuvší diskuze na zahraničním diskuzním fóru, kde se několik uživatelů fóra vyjadřovalo k tomuto problému, provést upgrade verze systému RouterOS na všech AP. Nejprve jsem stáhnul z oficiálních webových stránek výrobce MikroTik `http://www.mikrotik.com/download` nejnovější verzi systému v rámci řady 5 a to konkrétně verzi **5.26**. Po jejím úspěšném nasazení a ověření, že nedošlo k poškození konfigurace jsem pokračoval k nasazení verze **6.27**, kdy jsem posléze opět ověřil funkčnost a správnost konfigurace. Po provedení upgrade jsem přestal mít problémy s komunikací pomocí ssh protokolu a navíc došlo k opravě řady chyb a vylepšení, jejichž konkrétní výčet je k nalezení v dokumentu “Changelog” na oficiálních stránkách výrobce[46]. Upgrade jsem prováděl pomocí nástroje WinBox v**2.2.13**.

Kapitola 3

Testování

3.1 Testování vhodnosti konfigurace pro bezdrátovou síť

V analytické části jsem se věnoval popisu metodik měření kvality bezdrátové sítě, které jsem rozdělil na **aktivní** a **pasivní**. Popsal jsem sledované parametry a jejich význam a navrhnul jsem vlastní metriky a ukazatele. V následujících odstavcích se věnuji prezentaci a analýze naměřených hodnot pro vybrané konfigurace přístupových bodů. Odkazuji se přitom na tabulku s testovanými konfiguracemi, která je přiložena v příloze a označena jako Tabulka A.1.

Prezentace sumarizovaných výsledků se nachází rovněž v příloze na obrázcích v tabulkách A.1, A.2 a A.3 a koláčových grafech. Výsledky jsou exportovány z tabulkového procesoru a pro lepší přehlednost a orientaci obarveny, proto jsou tabulky v textu označeny jako obrázek, přestože se jedná o tabulky s hodnotami. Kompletní nezpracovaná data získaná měřením jsou k nalezení na přiloženém datovém nosiči v příslušném adresáři. Pro případ zhoršené čitelnosti údajů z této tabulky se na CD v adresáři *passive* nachází soubor analyza.xlsx s elektronickou verzí.

V prvním sloupci na obrázcích A.1, A.2 a A.3 jsou hodnoty naměřené při ponechané defaultní konfiguraci. Ve sloupcích napravo se pak nacházejí hodnoty z dalších konfigurací, jež jsou označeny čísly. Konfigurace jsou popsány v tabulce A.1. Procenty je v tabulce zachycena změna od hodnoty při defaultní konfiguraci, proto jsou ve sloupci s defaultní konfigurací nuly. Barevně jsou pak odlišeny hodnoty v rámci každého řádku tak, aby bylo na první pohled rozpoznatelné, která konfigurace dosahuje nejlepších a která nejhorších výsledků.

Výsledky testování uvedených konfigurací bych mohl shrnout do následujících zjištění:

- Snížením přenosových rychlostí sice relativně výrazně klesne průměrný poměr opakovaných přenosů v síti, ale děje se tak na úkor velmi výrazného zhoršení metrik v paralelně probíhajícím aktivním měření

- Fragmentace zvyšuje úspěšnost přenosu resp. při snižování hodnoty fragmentace docházelo i ke snižování poměrů opakovaných přenosů. Mnohem výrazněji však ve směru Tx z pohledu AP, což je předpokládané, protože na směr Rx se fragmentace neaplikovala.

- Fragmentace rámců neměla negativní vliv na hodnotu ukazatele *p-throughput*. Naopak při zavedení fragmentace došlo vždy k nárůstu tohoto ukazatele, což je pozitivní.

- Po zapnutí speciální patentované funkce čipu Atheros (adaptive noise immunity) došlo ke zhoršení všech metrik sledovaných aktivním a pasivním měřením ve srovnání se stavem, kdy byla tato funkce vypnutá. Rozdíl lze sledovat na naměřených hodnotách u konfigurací 3 a 6.

- Podle očekávání neměla žádná z testovaných konfigurací výrazný vliv na hodnotu průměrné síly signálu. Odchylka jednotlivých konfigurací se od defaultní konfigurace pohybovala maximálně v řádu 2 procentních bodů.

- Důležitým ukazatelem je hodnota *avg sonda* v tabulce aktivních metrik. Tento ukazatel vyjadřuje poměr opakovaných přenosů u sondy, jež prováděla aktivní měření. Porovnáním této hodnoty s hodnotou v řádku *avg-grouped* ve stejném sloupci u pasivní metriky vidíme, že je sonda mimořádně úspěšná v doručování rámců vysílači. To si vysvětluji zejména kvalitní 4dBi externí prutovou anténkou, kterou byla sonda vybavena.

Výsledkem provedených měření je identifikace minimálně 2 konfigurací, jejichž aplikací by mělo dojít ke zlepšení kvality bezdrátové sítě. Jedná se o konfigurace 3 a 7. V případě konfigurace 3 bylo dosaženo cca 32% poklesu průměrné hodnoty poměru opakovaných přenosů na agregovaných hodnotách podle MAC adres ve směru Tx. V případě konfigurace 7 se pak jedná o cca 18% pokles.

Poměr opakovaných přenosů rámců ze všech vysílačů v síti za sledované období lze sledovat v ukazateli AVG TOTAL Tx (Rx). V případě konfigurací 3 a 7 došlo téměř shodně ke zlepšení cca o 21% proti defaultní konfiguraci v Tx směru.

Konfigurace 7 přitom dosáhla nejlepších výsledků v metrikách aktivního měření ze všech měřených konfigurací. Specifikou této konfigurace je to, že využívá částečně RTS/CTS mechanismu a to konkrétně pouze jeho CTS části. V případě, že má AP rámec k odeslání, který je větší než zadaná prahová hodnota(v tomto případě 512 Byte), vyšle před začátkem přenosu rámec CTS adresovaný samo sobě do éteru. Tento rámec je zachycen klientskými zařízeními a je to pro ně známka toho, že bude následovat přenos a zdrží se tak případného začátku vlastního přenosu. Tím se šance na úspěšný přenos rámce ke klientskému zařízení zvýší, protože poklesne pravděpodobnost vzniku kolize rámce s některým z klientských vysílání.

Pro zajímavost a srovnání jsem sebral a následně vzestupně seřadil naměřené agregované hodnoty podle MAC adres z měření konfigurací default, 3 a 7. Ze seřazené řady jsem následně určil hodnoty jednotlivých decilů. Ty jsou pak zaneseny do tabulky na obrázku A.3. Podle rozložení decilů v tabulce lze usuzovat, že se změny dané úpravou konfigurace pozitivně promítly napříč spektrem klientských zařízení a nikoliv např. pouze na zařízení s horšími či lepšími přenosovými parametry.

Zlepšení kvality bezdrátové sítě v případě konfigurací 3 a 7 jsem se snažil demonstrovat i prostřednictvím koláčových grafů na přiložených obrázcích A.4, A.5, A.6, A.7, A.8, A.9. Tyto grafy zachycují procentuální rozložení klientských stanic podle jejich poměru opakovaných přenosů za období měřené periody. Vytvořil jsem proto intervaly 1 až 1.25 , 1.25 až 1.5, 1.5 až 1.75, 1.75 až 2.0 a 2.0 a více a klientské stanice do těchto intervalů rozřadil. Porovnáním grafů defaultní konfigurace ve směru Tx z pohledu AP s konfiguracemi 3 a 7 je na první pohled vidět na posledních dvou uvedených konfigurací výrazné zlepšení reprezentované početnějším zastoupením klientů v nižších hladinách intervalů.

3.2 Kontrola prostředí spektrálním analyzátorem

V závěru realizace prací jsem po dohodě s vedoucím práce měl možnost si zapůjčit od školy profesionální spektrální analyzátor **Agilent N1996A**. Toho jsem velmi rád využil za účelem ověření správnosti a demonstrace mnou navrhnutého řešení rozdělení frekvenčního pásma mezi jednotlivé přístupové body. Bohužel nemám možnost srovnání dvou stavů bezdrátové sítě - před a po realizaci navrženého řešení, protože jsem neměl v inkriminované době před realizací spektrální analyzátor k dispozici.

Pro ověření konfigurace kanálů na přístupových bodech jsem navrhnul a realizoval měření, při kterém jsem se pohyboval s analyzérem po školním areálu

během normálního provozu a pořizoval jsem snímky spektrogramu z vybraných lokalit. Celkem jsem takto stanovil 9 míst, vždy v blízkosti některého přístupového bodu. Nejbližší přístupový bod jsem následně cca 2minuty před sejmutím snímku vždy vypnul, abych na obrazovce analyzéru neviděl provoz z daného vysílače (a asociovaných klientů) a naopak jsem mohl sledovat ostatní provoz na sdíleném médiu.

Snímky pořízené spektrálním analyzátorem se nacházejí na přiloženém datovém nosiči. Zde uvádím mé komentáře a poznatky z provedeného měření:

- **AP_10_100_0_2.png, AP = RB0, konfigurovaný kanál = 1**
  Na frekvenčním rozsahu, který odpovídá konfigurovanému kanálu 1, nebyl pozorován žádný datový přenos, který by mohl způsobovat interferenci s vysíláním vysílače umístěného ve školní knihovně - RB0.

- **AP_10_100_0_3.png, AP = RB1, konfigurovaný kanál = 11**
  Z odpovídajícího spektrogramu vychází jako nejvhodnější volba skutečně konfigurovaný kanál 11. Interferenci v odpovídajícím frekvenčním pásmu pro tento kanál může teoreticky způsobovat ze školních AP pouze datový přenos vysílače RB6. Ten je situován o poschodí výše, v hlavní budově a vzdálený přibližně 30 metrů vzdušnou čarou. Zachycené intenzivnější datové přenosy v pásmu odpovídající kanálu 11 proto budou nejspíše tvořeny některým z mobilních hotspotů resp. připojeného(připojených) zařízení, případně z AP ze sousedních budov - školy a restauračního zařízení.

- **AP_10_100_0_4.png, AP = RB2, konfigurovaný kanál = 6**
  Kanál 6 se při měření v prostoru školní budovy před účtárnou jevil jako skutečně nejvhodněji zvolený z kanálů. Na tomto kanálu byla pozorována nejmenší aktivita.

- **AP_10_100_0_5.png, AP = RB3, konfigurovaný kanál = 1**
  V prostoru vchodových dveří do školní sborovny nebyla zaznamenána žádná výraznější aktivita na kanálu č.1, která by v případě zapnutého RB3 mohla mít zásadní vliv na kvalitu rádiového signálu z tohoto AP.

- **AP_10_100_0_6.png, AP = RB4, konfigurovaný kanál = 6**
  V prostorách před ředitelnou jsem zaznamenal zvýšený provoz, na frekvencích odpovídajících kanálu 6, jenž jsem nakonfiguroval i na AP v učebně sousedící s ředitelnou - RB4. Prostor před ředitelnou je velmi odkrytý a okna na chodbě směřují na přístavbu, kde se však žádné školní AP, jež by vysílalo na identickém kanálu, nevyskytuje. I přes zvýšenou aktivitu (max. cca -75dBm) si myslím, že je konfigurace v této lokalitě v pořádku, protože měření jsem prováděl na chodbě, kde nestojí v cestě signálu z jiných AP na stejném patře tolik pevných překážek. Situace v

učebně s dotyčným RB4 a přilehlých kancelářích tak bude jenom lepší, než právě zde. Jednak budou zařízení uživatelů ještě blíže tomuto AP a v neposlední řadě přibude vstupem do místnosti další překážka v šíření signálu ze sousedních vysílačů.

- **AP_10_100_0_7.png, AP = RB5, konfigurovaný kanál = 1**
  Snímek spektrogramu pořízený na chodbě před učebnou 215, kde se nachází vysílač RB5, jenž za normálního provozu vysílá na kanálu 1, jasně ukazuje, že je konfigurovaný kanál nejvhodnější volbou s minimálním vlivem ostatních bezdrátových zařízení.

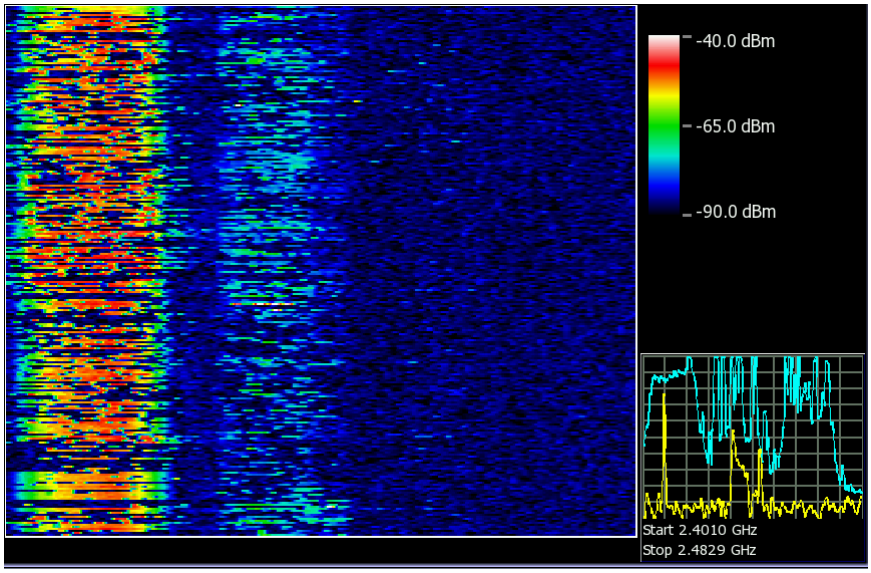
- **AP_10_100_0_8.png, AP = RB6, konfigurovaný kanál = 11**
  Zachycený spektrogram na obrázku 3.1 v prostorách specializované učebny s vysílacím bodem RB6 na stěně ukazuje velmi intenzivní aktivitu na frekvenčním pásmu, které svým rozsahem odpovídá kanálu 1. Kanál 11 je ale "volný" a tím pádem i vhodný k využití a pokrytí v této lokality vysílačem RB6.

- **AP_10_100_0_9.png, AP = RB7, konfigurovaný kanál = 6**
  Snímek z měření z rohové učebny ukazuje na intezivní aktivitu na sousedním kanálu 11. Nízké využití kanálu 6 v této lokalitě dává prostor AP RB7 k pokrytí.

- **AP_10_100_0_10.png, AP = RB8, konfigurovaný kanál = 1**
  Spektrální analyzátor v prostoru na chodbě před učebnou výpočetní techniky zaznamenal relativně vysokou zátěž na kanálu 11 - pravděpodobně se jedná o provoz vztažený k AP v protější učebně v přístavbě. Situace na kanále 1 při pohledu na spektrogram nevypadá příznivě, avšak platí zde stejné podmínky jako v lokalitě před ředitelnou. Dveře od učebny s výpočetní techniky jsou navíc potažené tenkou vrstvou plechu, která sníží propustnost wifi signálu z ostatních AP do učebny, ve které je umístěno AP RB8.

3.3 Kontrola pokrytí prostoru bezdrátovou sítí

Analýzu kvality pokrytí bezdrátovým signálem jsem provedl již v analytické části, kdy jsem ve vytipovaných a zadokumentovaných lokalitách měřil sílu přijímaného signálu z okolních přístupových bodů. Avšak i kvůli zvědavosti jsem se rozhodl pro kontrolu specializovaným nástrojem „HeatMapper" od výrobce **ekahau**. Výstupem z tohoto nástroje je barevně odstupňovaná heatmapa, která demonstruje pokrytí prostoru bezdrátovým signálem z vybraného přítupového bodu. Jedná se o volně dostupný nástroj, přičemž ke stažení je na adrese `http://www.ekahau.com/wifidesign/ekahau-heatmapper`.

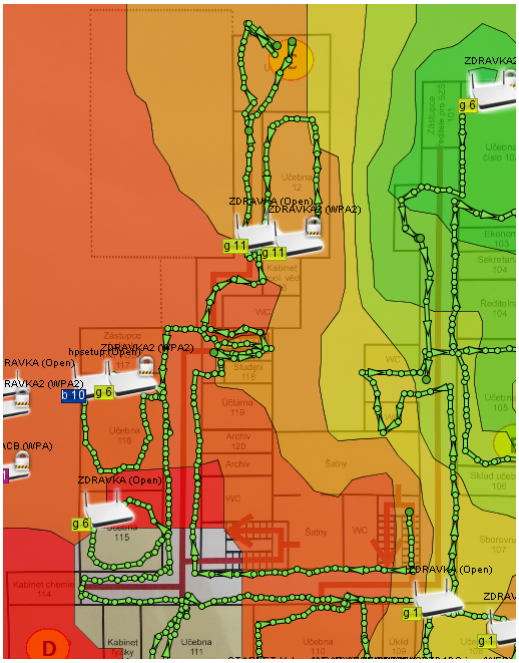


Obrázek 3.1: Jeden z pořízených snímků spektrálním analyzátorem v prostředí školy. Konkrétně se jedná o snímek AP__10__100__0__8.png. Popis snímku je k nalezení u příslušného bodu v textu.

Po krátkem seznámení se s tímto jednoduchým nástrojem jsem prošel a zaznamenal úroveň síly šířeného signálu s laptopem použitým během aktivního měření. Ve výsledku se mi přitom potvrdilo, že je škola ve všech důležitých lokalitách pokryta přítomnou bezdrátovou sítí. Ukázka jednoho z pořízených snímků je na obrázku 3.2. Další snímky se nacházejí na přiloženém datovém nosiči.

3.4 Ověření funkčnosti WPA2 sítě

Po konfiguraci WPA2 sítě, jejímuž popisu se věnuji v předchozí kapitole, bylo zapotřebí nově vzniklou síť otestovat. Přestože jsem nikde po škole nešířil informaci o vzniklé síti, rychle jsem zaznamenal pokusy o připojení k ní. Velká část z těchto pokusů byla úspěšná. Příklad úspěšného připojení z logu AP na obrázku 3.3. Během cca 2 týdnů se pak nashromáždilo v logu na DHCP serveru cca 50 unikátních MAC adres zařízení, jejichž majitelé se úspěšně autentizovali. Neúspěšné pokusy o připojení byly z velké části způsobeny chybnou kombinací přihlašovacích údajů. Vytvořená síť tak překvapivě rychle získala své uživatele ještě před jejím oficiálním představením a poměr uživatelů fungujících v nové síti se každým dnem zvětšuje na úkor původní sítě, jejíž provoz bude zachován v původní podobě předběžně do konce aktuálního školního roku.



Obrázek 3.2: Kontrola pokrytí prostoru přístupovým bodem rb4 – v pravém horním rohu. Na pozadí je půdorys školy v 1.poschodí

I přes sledovaný pozitivní trend vývoje počtu připojujících se uživatelů jsem provedl úspěšný test připojení s laptopem s OS Windows 8.1, mobilním telefonem s Android v4.2 a tabletem iPad s iOS v 8.3. Sekvence snímku z připojovacího procesu je k nalezení na přiloženém datovém nosiči.

Apr/07/2015 14:47:36	wireless info	00:08:	07:4F@wlan2: connected
Apr/07/2015 14:47:36	wireless debug	00:08:	07:4F@wlan2: got identity
Apr/07/2015 14:47:36	wireless debug	00:08:	07:4F@wlan2: EAP going to pass through
Apr/07/2015 14:47:36	wireless debug	00:08:	07:4F@wlan2: EAP success from RADIUS

Obrázek 3.3: Na obrázku je snímek části logu, který demonstruje přijetí Radius-Accept zprávy od RADIUS serveru po připojení klientského zařízení k nově zřízené zabezpečené bezdrátové síti

Závěr

Na závěr této práce bych rád nejprve shrnul přínosy, jichž bylo dosaženo realizací navržených úprav:

- Implementací VLAN do síťové infrastruktury došlo k logickému oddělení síťových segmentů. To mimo jiné přináší možnost vytvářet bezdrátové sítě s různou úrovní zabezpečení a typem autentizace. Veškeré prostupy mezi virtuálními sítěmi jsou spravovány na firewallu, což je zjednodušení proti původnímu stavu.

- Vytvořená bezdrátová síť *ZDRAVKA2* výrazně uživatelům ulehčuje a zpříjemňuje autentizační proces, protože lze po prvním „interaktivním" přihlášení uložit přihlašovací údaje do svého síťového zařízení. Další přihlášení pak probíhají automaticky a okamžitě, jakmile je síť v dosahu.

- Autentizační mechanismus u původní nezabezpečené sítě byl vylepšen tím způsobem, že není zapotřebí provádět autentizaci po přepojení z vysílače na vysílač, protože klientům v takovém případě ponovu zůstane jejich původní IP adresa a tím pádem i autentizované sezení na firewallu.

- U nově vybudované bezdrátové WPA2 sítě musím vyzvdihnout, že poskytuje šifrování pomocí AES-CCM a autentizační server se prokazuje certifikátem, jehož platnost si může uživatel ověřit. Tím odpadá hrozba odposlechu a zneužití přenášených dat v rámci školní bezdrátové sítě.

- Implementací automatického sběru dat z přístupových bodů získává správce sítě podstatně více informací o jejím stavu, než tomu bylo doposud.

- Migrací DHCP služby na jeden server došlo k velkému zjednodušení, kdy jsem sice musel přidat funkcionalitu DHCP relay na firewall, zato je veškerá správa této služby centralizovaná do jednoho místa a případné úpravy tak jsou jednodušší.

- V průběhu analýzy pokrytí školní budovy bezdrátovou sítí jsem identifikoval přístupový bod, jehož komunikační miniPCI karta byla poškozená. Její výměnou došlo ke zlepšení přenosových parametrů a nárůstu počtu připojených klientů k danému vysílači.
- Vytvořený skript pro centrální správu nabízí správě sítě možnost editovat konfiguraci na všech vysílačích najednou. Já sám jsem tohoto komfortu využil v průběhu ladění a zkoumání vlivu jednotlivých parametrů na přenosové parametry nesčetněkrát.
- Rozšíření monitorovacího systému o sledování zátěže na přístupových bodech, aktuálního počtu připojených klientů a dalších kvalitativních parametrů jako např. *overal-tx-ccq* poskytuje administrátorovi nejenom informace na bázi online, ale zároveň jsou tato data uchována a mohou být kdykoliv v budoucnu zpracována k dalším účelům např. porovnání nebo sledování vývoje trendu.
- V rámci testování možných konfigurací bezdrátového rozhraní přístupových bodů se mi podařilo sestavit takovou konfiguraci, která snižuje počet opakovaných přenosů v síti a dosahuje i lepších výsledků v navrženém aktivním měření kvality bezdrátové sítě.

Jsem rád, že se mi podařilo splnit všechny body zadání. Jedinou nerealizovanou položkou zůstalo napojení školní autentizační a autorizační infrastruktury na AAI sítě eduroam. Důvody vedoucí k rozhodnutí o nevytváření tohoto spojení jsou podrobněji uvedeny v praktické části práce, kde se věnuji možným vylepšením. Ve zkratce zde jenom připomenu, že jsem po poradě s odpovědným zástupcem za školní infrastrukturu dospěl k názoru, že by přínos z této akce nebyl takový, aby vyvážil vynaložené úsilí do implementace a zejména pak i následné údržby a nutné technické podpory.

Jak jsem již předeslal v úvodu práce, tak bych zde chtěl uvést možnosti dalších vylepšení, na které jsem narazil až v průběhu nebo v samotném závěru realizace prací v rámci této práce. Možným vylepšením by mohla být například aplikace dynamických pravidel na firewallu v závislosti na příslušnosti uživatele k určité skupině v doméně. Touto problematikou jsem se zabýval jen zběžně, nicméně mne zaujala funkcionalita dynamických profilů na firewallech FortiGate, kterou by teoreticky mělo být možné toto zrealizovat. Dále jsem v této práci neřešil možnosti vylepšení v oblasti hardware, neboť jsem pro případný nákup neměl žádný rozpočet.

Veškeré realizované úpravy a zřízené autentizační prostředky (např. sdílené tajemství mezi RADIUS serverem a klienty) byly zadokumentovány do aktualizované dokumentace školní sítě, která však z pochopitelných důvodů nemůže být přílohou této práce.

Literatura

[1] Střední zdravotnická škola a Vyšší odborná škola zdravotnická, České Budějovice, Husova 3: *WWW prezentace SZŠ ČB [online]*. [cit. 2015-03-03]. Dostupné z: http://www.szscb.wz.cz/

[2] 7Signal: *Experience WLAN Performance Management [online]*. [cit. 2015-03-20]. Dostupné z: http://7signal.com/products/sapphire-platform-overview/

[3] Česká televize: *Většina Čechů surfuje na internetu bez kvalitního připojení [online]*. [cit. 2015-03-17]. Dostupné z: http://www.ceskatelevize.cz/ct24/ekonomika/305000-vetsina-cechu-surfuje-na-internetu-bez-kvalitniho-pripojeni/

[4] IEEE: *History of IEEE [online]*. [cit. 2015-03-22]. Dostupné z: https://www.ieee.org/about/ieee_history.html?WT.mc_id=lp_ab_hoi

[5] Radio-Electronics.com: *IEEE 802.11 Wi-Fi Standards [online]*. [cit. 2015-03-22]. Dostupné z: http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php

[6] Lammle, T.: *CCNA Wireless Study Guide: IUWNE Exam 640-721*. Wiley, první vydání, 2011, ISBN 9780470901717.

[7] Cisco Systems, I.: *802.11 Association process explained [online]*. [cit. 2015-04-09]. Dostupné z: https://kb.meraki.com/knowledge_base/80211-association-process-explained

[8] Gast, M.: *802.11 Wireless Networks The Definitive Guide*. O'Reilly, 2005, ISBN 0-596-10052-3.

[9] Mafra a.s. , Adam Novák: *Apple má vážný problém. U nového iPhonu 4 vypadává signál [online]*. [cit. 2015-04-12]. Dostupné z: http://mobil.idnes.cz/apple-ma-vazny-problem-u-noveho-iphonu-4-vypadava-signal-pja-/iphone.aspx?c=A100624_150448_iphone_ada

[10] Český telekomunikační úřad: *Všeobecné oprávnění č. VO-R/10/05.2014-3 [online]*. [cit. 2015-03-25]. Dostupné z: https://www.ctu.cz/cs/download/oop/rok_2014/vo-r_10-05_2014-03.pdf

[11] Techopedia, C. J.: *Techopedia explains Guard Band [online]*. [cit. 2015-04-20]. Dostupné z: http://www.techopedia.com/definition/7494/guard-band-telecommunications

[12] *Wireless Networking in the Developing World 2nd Edition p.15*. 2007, ISBN 978-0-9778093-6-3.

[13] Tech Republic, James McPherson: *SolutionBase: 802.11g vs. 802.11b [online]*. [cit. 2015-03-18]. Dostupné z: http://www.techrepublic.com/article/solutionbase-80211g-vs-80211b/

[14] Stroe, A.: *Wifi hidden station problem [online]*. [cit. 2015-03-24]. Dostupné z: http://commons.wikimedia.org/wiki/File:Wifi_hidden_station_problem.svg

[15] Jim Geier: *Improving WLAN Performance with Fragmentation [online]*. [cit. 2015-04-07]. Dostupné z: http://www.wi-fiplanet.com/tutorials/print.php/1468331

[16] Cho, K.: Method and apparatus for transmitting block ACK frame. Březen 2 2006, uS Patent App. 11/209,697. Dostupné z: https://www.google.com/patents/US20060048034

[17] PacketLife.net: *QoS [online]*. [cit. 2015-04-07]. Dostupné z: http://packetlife.net/media/library/19/QoS.pdf

[18] Stretch, J.: *TCP Slow Start [online]*. [cit. 2015-03-29]. Dostupné z: http://packetlife.net/blog/2011/jul/5/tcp-slow-start/

[19] Spagnuolo, M.: *Disable SSLv3 [online]*. [cit. 2015-03-30]. Dostupné z: http://disablessl3.com/

[20] Routerboard.com: *RB411AH [online]*. [cit. 2015-03-20]. Dostupné z: http://routerboard.com/rb411AH

[21] Routerboard.com: *RB411AR [online]*. [cit. 2015-03-20]. Dostupné z: http://routerboard.com/rb411AR

[22] wifi.aspa.cz: *Anténa Pacific všesměr.duck anténa 8dBi, 2,4GHz, RP-SMA konektor [online]*. [cit. 2015-03-26]. Dostupné z: http://wifi.aspa.cz/antena-pacific-vsesmer-duck-antena-8dbi-2-4ghz-rp-sma-konektor-z86880

[23] InfoSec Institute: *DNS Tunnelling [online]*. [cit. 2015-03-26]. Dostupné z: http://resources.infosecinstitute.com/dns-tunnelling/

[24] Fortinet: *FortiOS Handbook v3 for FortiOS 4.0 MR3 p.50 [online]*. [cit. 2015-03-27]. Dostupné z: http://docs.fortinet.com/uploaded/files/1050/fortigate-firewall-40-mr3.pdf

[25] Fortinet: *User Authentication for FortiOS 4.0 MR3 p.28 [online]*. [cit. 2015-03-27]. Dostupné z: http://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigate-authentication-40-mr3.pdf

[26] D-Link: *DES-1210-28 [online]*. [cit. 2015-03-30]. Dostupné z: http://us.dlink.com/products/business-solutions/28-port-fast-ethernet-websmart-switch-including-2-gigabit-base-t-and-2-gigabit-combo-base-tsfp/

[27] Nagios Enterprises, L.: *Nagios Plugin Development Guidelines [online]*. [cit. 2015-03-20]. Dostupné z: https://nagios-plugins.org/doc/guidelines.html

[28] MikroTik: *MikroTik Documentation - Manual:Interface/Wireless [online]*. [cit. 2015-03-14]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:Interface/Wireless

[29] Husted, P.; Ye, H.; Singla, A.: Adaptive interference immunity control. Březen 25 2008, uS Patent 7,349,503. Dostupné z: http://www.google.com/patents/US7349503

[30] The Apache Software Foundation: *User Manual - Remote Testing [online]*. [cit. 2015-03-15]. Dostupné z: https://jmeter.apache.org/usermanual/remote-test.html

[31] Jason Keyser, A. P.: *Boeing engineers use spuds to improve in-air Wi-Fi [online]*. [cit. 2015-03-24]. Dostupné z: http://news.yahoo.com/boeing-engineers-spuds-improve-air-220847344.html

[32] eTutorials.org: *Flat Network Topology [online]*. [cit. 2015-04-01]. Dostupné z: http://etutorials.org/Networking/Lan+switching+first-step/Chapter+10.+LAN+Switched+Network+Design/Flat+Network+Topology/

[33] Cisco: *Fundamentals of VLAN's - Router on a stick [online]*. [cit. 2015-04-20]. Dostupné z: https://learningnetwork.cisco.com/docs/DOC-23481

[34] CESNET, z.s.p.o.: *Roamingová politika [online]*. [cit. 2015-04-02]. Dostupné z: https://www.eduroam.cz/_media/cs/cz_roam_policy_v2.0.pdf

[35] CESNET, z.: *Autentizace na bázi protokolu 802.1x [online].* [cit. 2015-04-25]. Dostupné z: http://eduroam.cz/cs/spravce/uvod

[36] CESNET, z.s.p.o.: *Pokrytí [online].* [cit. 2015-04-02]. Dostupné z: https://www.eduroam.cz/pokryti/pokryti_fullscreen_cs.html

[37] Microsoft: *EAP-PEAP-MSCHAPv2 Realm Stripping [online].* [cit. 2015-04-11]. Dostupné z: https://social.technet.microsoft.com/Forums/windowsserver/en-US/e73183d4-7b2f-48a7-9246-97ed711e8e8d/eappeapmschapv2-realm-stripping?forum=winserverNAP

[38] David Hucaby, S. M.: *VLANs and Trunking [online].* [cit. 2015-04-21]. Dostupné z: http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=2

[39] Microsoft: *DHCP Relay Agent [online].* [cit. 2015-04-08]. Dostupné z: https://technet.microsoft.com/en-us/library/cc783103(v=ws.10).aspx

[40] Network RADIUS: *Installation of FreeRADIUS [online].* [cit. 2015-04-13]. Dostupné z: http://wiki.freeradius.org/guide/FreeRADIUS-Active-Directory-Integration-HOWTO

[41] Protected EAP (PEAP) Application Note. [cit. 2015-03-29]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/wireless/technology/peap/technical/reference/peap4/PEAP_D.pdf

[42] Microsoft: *Shared Secrets for NPS and RADIUS Clients [online].* [cit. 2015-04-12]. Dostupné z: https://technet.microsoft.com/en-us/library/cc771660(v=ws.10).aspx

[43] Cisco: *Cisco Response to TKIP Encryption Weakness [online].* [cit. 2015-04-13]. Dostupné z: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20081121-wpa

[44] MikroTik: *Manual:SNMP - Object identifiers (OID) [online].* [cit. 2015-03-28]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:SNMP#Object_identifiers_.28OID.29

[45] MikroTik: Wireless Client and Wireless Access Point Manual. 2007, wireless Manual p. 13. Dostupné z: http://www.mikrotik.com/testdocs/ros/3.0/interface/wireless.pdf

[46] MikroTik: *Upgrading RouterOS [online].* [cit. 2015-04-02]. Dostupné z: http://www.mikrotik.com/download/share/routeros_devnote.txt

Příloha A

Data z měření

	konfigurace								
	default	1	2	3	4	5	6	7	
AVG GROUPED Tx	2,02	1,30	1,88	1,36	1,57	1,57	1,46	1,66	[poměr]
	0%	-35,75%	-6,75%	-32,74%	-22,30%	-22,23%	-27,75%	-17,64%	
AVG GROUPED RX	1,53	1,54	1,85	1,35	1,53	1,45	1,55	1,52	[poměr]
	0%	0,58%	21,28%	-11,71%	0,05%	-5,06%	1,41%	-0,49%	
AVG Tx	2,07	1,34	2,31	1,52	1,62	1,68	1,72	1,56	[poměr]
	0%	-34,99%	11,60%	-26,49%	-21,65%	-18,96%	-16,90%	-24,63%	
AVG Rx	1,78	1,63	2,04	1,54	1,68	1,72	1,66	1,75	[poměr]
	0%	-8,71%	14,83%	-13,47%	-5,38%	-3,13%	-6,65%	-1,80%	
AVG TOTAL Tx	1,56	1,19	1,44	1,23	1,26	1,25	1,23	1,23	[poměr]
	0%	-23,96%	-7,68%	-21,03%	-19,20%	-19,79%	-21,46%	-21,14%	
AVG TOTAL Rx	1,25	1,25	1,39	1,12	1,22	1,22	1,20	1,26	[poměr]
	0%	-0,45%	10,94%	-10,90%	-2,61%	-2,39%	-4,48%	0,78%	
avg signal strength	-69,33	-68,92	-69,04	-69,07	-67,58	-68,18	-69,17	-67,91	[dBm]
	0%	-0,59%	-0,42%	-0,37%	-2,52%	-1,65%	-0,22%	-2,04%	
avg SNR	31,12	31,00	31,57	31,35	32,79	32,22	30,94	32,69	[dB]
	0%	-0,37%	1,47%	0,74%	5,38%	3,56%	-0,55%	5,07%	
avg Tx Rate	28,18	9,77	8,80	31,08	31,51	31,46	30,29	30,74	[Mbps]
	0%	-65,33%	-68,75%	10,30%	11,83%	11,66%	7,51%	9,11%	
avg Rx Rate	28,56	8,92	9,04	28,76	30,33	29,41	29,48	29,83	[Mbps]
	0%	-68,78%	-68,35%	0,68%	6,20%	2,98%	3,22%	4,43%	
avg tx-ccq	62,59	77,52	66,97	67,90	68,12	67,57	66,56	67,05	[%]
	0%	23,86%	7,00%	8,50%	8,84%	7,96%	6,35%	7,14%	
avg p-throughput	14264	7105	5721	15724	15978	15907	15469	15766	[kbps]
	0%	-50,19%	-59,89%	10,24%	12,02%	11,52%	8,45%	10,53%	

Obrázek A.1: Měření vlivu konfigurace na přenosové parametry a charakteristiky - pasivní. Procentuální hodnoty vyjadřují změnu proti defaultní konfiguraci.

	konfigurace								
	default	1	2	3	4	5	6	7	
IMAP latency	1193	6067	2981	1227	1247	1013	1284	1016	[ms]
	0%	408,68%	149,93%	2,90%	4,58%	-15,09%	7,67%	-14,82%	
Moodle latency	5940	12641	6228	6180	6347	6317	6889	5917	[ms]
	0%	112,82%	4,85%	4,05%	6,86%	6,35%	15,99%	-0,38%	
Bakalari	9228	20938	10121	10041	10091	10457	10957	9492	[ms]
latency	0%	126,90%	9,68%	8,82%	9,35%	13,32%	18,74%	2,86%	
Sonda AVG	1,33	1,58	1,91	1,26	1,34	1,45	1,42	1,33	[poměr]
GROUPED Tx	0%	18,81%	44,04%	-4,91%	0,91%	9,57%	6,59%	0,00%	
Sonda AVG	1,00	1,02	1,00	1,01	1,00	1,00	1,00	1,00	[poměr]
GROUPED Rx	0%	1,37%	0,17%	0,43%	-0,03%	0,11%	0,08%	0,00%	

Obrázek A.2: Měření vlivu konfigurace na přenosové parametry a charakteristiky - aktivní. Procentuální hodnoty vyjadřují změnu proti defaultní konfiguraci.

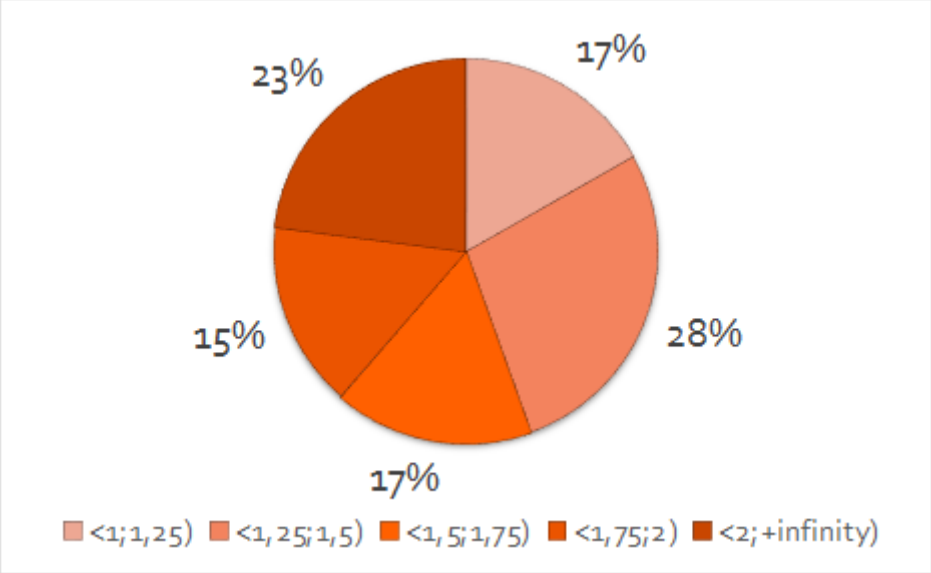
	konfigurace					
	default		3		7	
	Tx	Rx	Tx	Rx	Tx	Rx
1.decil	1,19	1,05	1,09	1,05	1,10	1,04
2.decil	1,27	1,08	1,12	1,07	1,14	1,09
3.decil	1,35	1,13	1,15	1,10	1,18	1,13
4.decil	1,44	1,18	1,17	1,14	1,20	1,16
5.decil	1,55	1,26	1,21	1,18	1,26	1,22
6.decil	1,71	1,34	1,27	1,23	1,35	1,30
7.decil	1,85	1,45	1,33	1,32	1,44	1,40
8.decil	2,10	1,63	1,46	1,45	1,64	1,53
9.decil	2,96	2,22	1,72	1,72	2,11	2,07

Obrázek A.3: V tabulce jsou hodnoty jednotlivých decilů klientských zařízení pro Tx a Rx směr a 3 vybraných porovnávaných konfigurací - default, 3 a 7. Decily byly určeny z hodnot průměrného poměru opakovaných přenosů agregovaných dle MAC adres klientských zařízení.

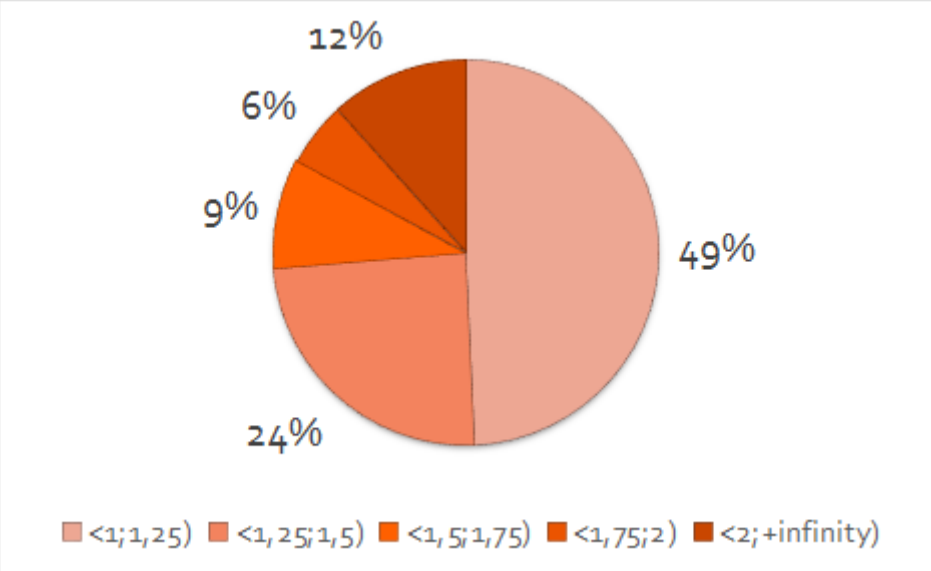
Tabulka A.1: Testované konfigurace

konfigurace	default	1	2	3
sup.rates	all	1,2,5.5 6,9,12	1,2,5.5 6,9,12	all
distance	dynamic	dynamic	indoors	dynamic
hw-retries	7	4	11	4
hw-fragmentation-threshold	disabled	256	1480	512
hw-protection-mode	none	none	none	none
hw-protection-threshold	n/a	n/a	n/a	n/a
frame-lifetime	0	0	0	0
adaptive-noise-immunity	none	ap-and-client-mode	none	none
disconnect-timeout	3	2	3	2
on-fail-retry-time	100	250	250	100

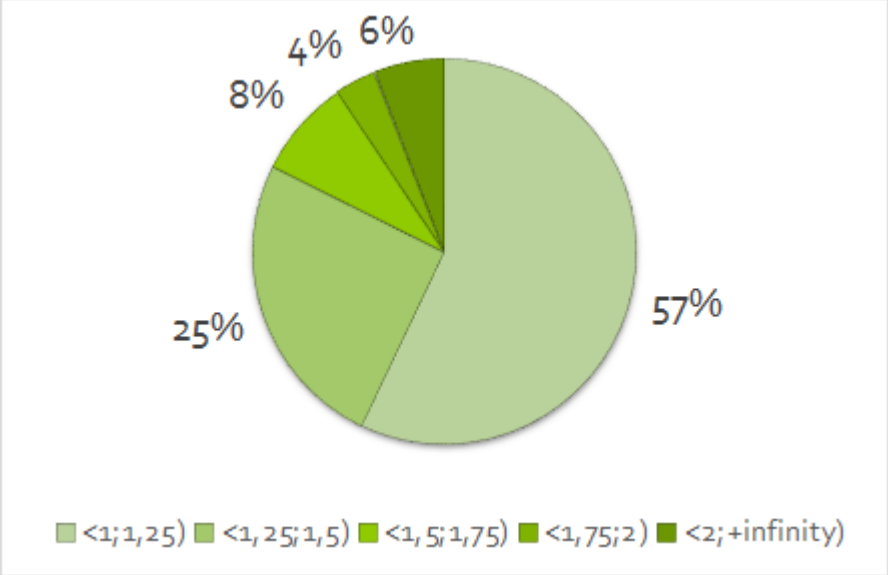
konfigurace	4	5	6	7
sup.rates	all	all	all	all
distance	dynamic	indoors	dynamic	dynamic
hw-retries	4	4	4	4
hw-fragmentation-threshold	1024	512	512	1024
hw-protection-mode	none	none	none	cts-to-self
hw-protection-threshold	n/a	n/a	n/a	512
frame-lifetime	0	0	0	0
adaptive-noise-immunity	none	none	ap-and-client-mode	none
disconnect-timeout	2	2	2	2
on-fail-retry-time	100	100	100	100



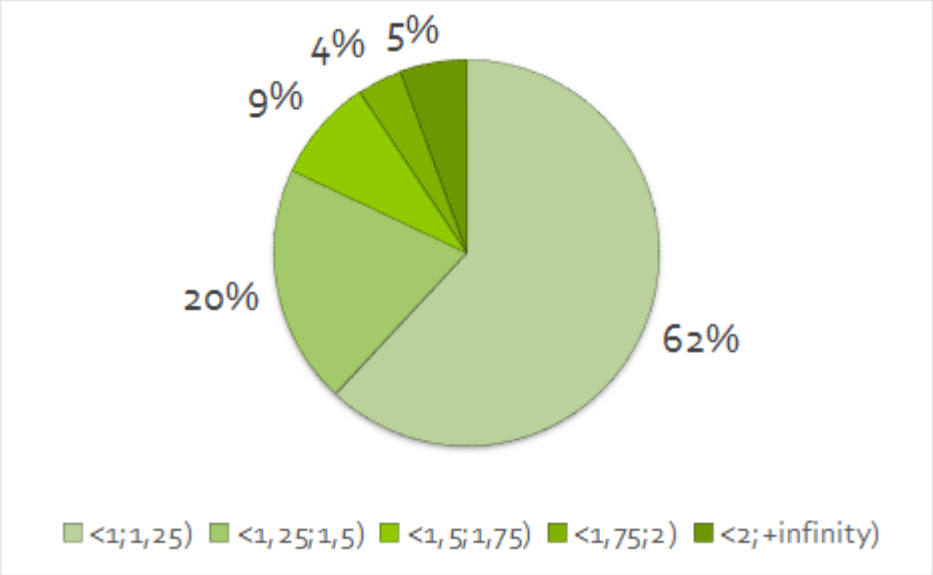
Obrázek A.4: Graf procentuálního rozložení klientů v intervalech podle naměřené hodnoty průměrného poměru opakovaných přenosů, defaultní konfigurace, směr Tx



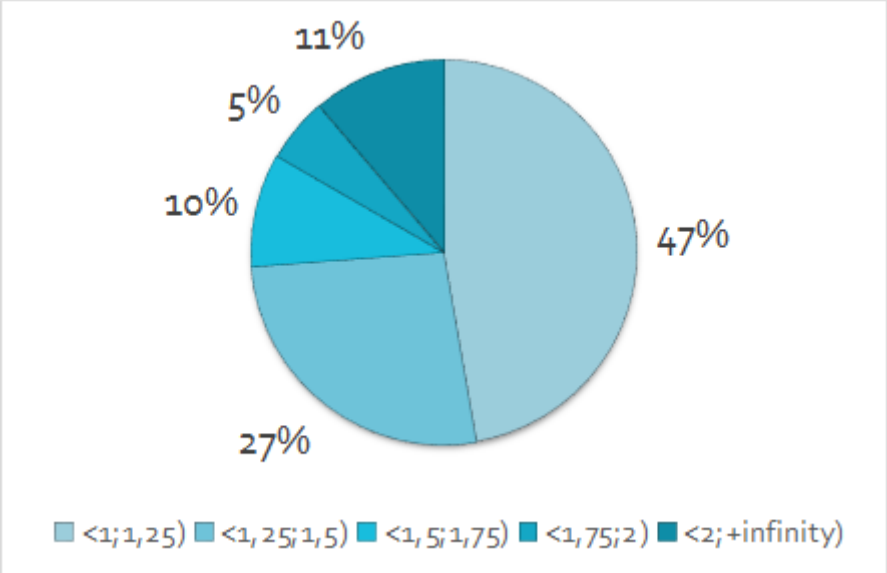
Obrázek A.5: Graf procentuálního rozložení klientů v intervalech podle naměřené hodnoty průměrného poměru opakovaných přenosů, defaultní konfigurace, směr Tx



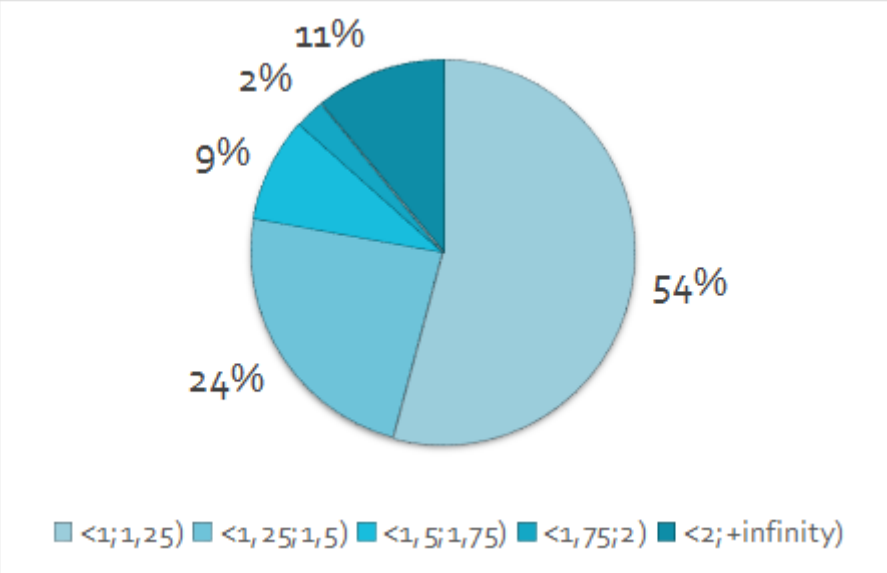
Obrázek A.6: Graf procentuálního rozložení klientů v intervalech podle naměřené hodnoty průměrného poměru opakovaných přenosů, konfigurace 3, směr Tx



Obrázek A.7: Graf procentuálního rozložení klientů v intervalech podle naměřené hodnoty průměrného poměru opakovaných přenosů, konfigurace 3, směr Rx



Obrázek A.8: Graf procentuálního rozložení klientů v intervalech podle naměřené hodnoty průměrného poměru opakovaných přenosů, konfigurace 7, směr Tx



Obrázek A.9: Graf procentuálního rozložení klientů v intervalech podle naměřené hodnoty průměrného poměru opakovaných přenosů, konfigurace 7, směr Rx

Příloha B

Seznam použitých zkratek

AAI Autentizační a Autorizační Infrastruktura

AES Advanced Encryption Standard

AP Access Point

BEAST Browser Exploit Against SSL/TLS

CA Certifikační Autorita

CBWFQ Class-Based Weighted Fair Queuing

CCM Cipher Block Chaining Message Authentication Code

CCQ Client Connection Quality

CPU Central Processing Unit

CQ Custom Queuing

CSMA/CA [CD] Carrier Sense Multiple Access/Collision Avoidance [Collision Detection]

ČSÚ Český statistický úřad

DCF Distributed Coordination Function

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

FIFO First In First Out

FREAK Factoring Attack on RSA-EXPORT Keys

FTP File Transfer Protocol

GUI Graphic User Interface

HTTP Hypertext Transfer Protocol

IEEE Institute of Electrical and Electronics Engineers

IP Internet Protocol

ISP Internet Service Provider

JČU Jihočeská univerzita v Českých Budějovicích

L2,3,4 ISO/OSI Layer 2,3,4

LLC Logical Link Control

LLQ Low Latency Queuing

LWAPP Lightweight Access Point Protocol

MAC Media Access Control

MPDU MAC Protocol Data Unit

MS Microsoft

NAT Network Address Translation

OFDM Orthogonal Frequency Division Multiplexing

OID Object Identifier

OS Operační Systém

POE Power Over Ethernet

POODLE Padding Oracle On Downgraded Legacy Encryption

PQ Priority Queuing

PSK Pre Shared Key

QoS Quality of Service

RADIUS Remote Authentication Dial In User Service

RB RouterBOARD

RTS/CTS Request To Send / Clear To Send

Rx/Tx Receive/Transmit

SNMP Simple Network Management Protocol

SSH Secure Shell

SSL Secure Sockets Layer

TCP Transport Control Protocol

TKIP Temporal Key Integrity Protocol

TLS Transport Layer Security

UPS Uninterruptible Power Supply

UTP Unshielded Twisted Pair

(V)LAN (Virtual) Local Area Network

VOIP Voice Over IP

WFQ Weighted Fair Queuing

WPA Wi-Fi Protected Access

Příloha C

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
  - `impl`
    - `measuring` .... adresář s výstupy a dokumenty provedených měření
      - `active` ..... adresář s výstupy z aktivního měření
      - `coverage` ..... adresář s výstupy z měření pokrytí
      - `distribtest` ..... adresář s výstupy z distribuovaného testu
      - `heatmaps` .... adresář se snímky heatmapy bezdrátového pokrytí
      - `jmeter` ..... adresář s konfigurací nástroje JMeter
      - `passive` ..... adresář s výstupy z pasivního měření
      - `maps` ..... adresář s plánky školní budovy
      - `spectograms` ..... adresář se zachycenými snímky spektrálním analyzátorem
    - `pictures` ..... adresář s pořízenými fotografiemi
    - `screencaptures` ..... adresář se snímky obrazovek
    - `scripts` ..... adresář s vytvořenými skripty
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF