Analýza pokrytí a zabezpečení bezdrátové sítě v areálu U5

Analysis of coverage and security of wireless campus network in U5 area

Jiří Konečný

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **HAROLD, Davis. Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě. 1. vyd. Praha : Grada, 2006. 334 s. ISBN 8024714213.**
2. **ZANDL, Patrik. Bezdrátové sítě WiFi Praktický průvodce. 1. vyd. Brno : Computer Press, 2003. 189 s. ISBN 80-7226-632-2.**
3. **THOMAS, Thomas M. Zabezpečení počítačových sítí. 1. vyd. Brno : Computer Press, 2005. 344 s. ISBN 80-251-0417-6.**
4. **PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace. 1. vyd. Brno : CP Books, 2005. 179 s. ISBN 80-251-0791-4.**
5. **KÖHRE, Thomas. Stavíme si bezdrátovou síť Wi-fi. 1. vyd. Brno : Computer Press, 2004. 295 s. ISBN 8025103919.**
6. **PECHAČ , Pavel. Šíření vln v zástavbě. 1. vyd. : BEN-Technická literatura, 2006. 108 s. ISBN 80-7300-186-1.**

Vedoucí bakalářské práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato práce se zabývá problematikou přenosu dat pomocí bezdrátových sítí. Vysvětluje základní principy fungování bezdrátových sítí, jejich možné napadení, a také popisuje jejich správné a efektivní zabezpečení. Práce se zaměřuje na analýzu pokrytí budovy Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně bezdrátovými sítěmi, vytvoření mapy pokrytí a proměření datových propustností jednotlivých přístupových bodů. Je zpracován i návrh na rozšíření pokrytí bezdrátovou sítí a její zabezpečení.

Klíčová slova: Bezdrátová síť, eduroam, podlaží, přístupový bod, sektor, útočník, Wi-Fi, zabezpečení.

ABSTRACT

The bachelor thesis deals with the transfer of data by wireless network. It explains the basics principles, how the wireless networks work, possibilities of the attack on it and also it describes how to secure the net effectively. The bachelor theses focuses on the analysis of wireless network’s cover in Faculty of applied informatics in Tomas Bata University, on creation of covering map and to measure data transmission of access points. In the thesis is suggested possible extension of wireless network cover and its security.

Keywords: Wireless network, eduroam, storey, access point, sector, attacker, Wi-Fi, security.

Děkuji vedoucímu bakalářské práce Ing. Miroslavu Matýskovi, Ph.D. Za metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….……

podpis diplomanta

OBSAH

ÚVOD

Tato bakalářská práce se zabývá problematikou bezdrátových sítí. V oboru bezdrátového přenosu dat dochází k širokému rozvoji a tato tématika je stále více aktuální. Bezdrátové sítě hrají významnou roli nejen v oblasti informačních technologií, ale setkáváme se s nimi i v ostatních oborech, v neposlední řadě i v průmyslu komerční bezpečnosti. S masivním rozšířením bezdrátových sítí, také přibývá počet útočníků, kteří se snaží získat citlivé data od uživatelů. Proto je zapotřebí věnovat zvýšenou pozornost jejich zabezpečení, aby nedocházelo k zneužití těchto údajů. Uživatelé nepožadují pouze dokonalé zabezpečení, ale také rychlý přenos dat a bezproblémový chod.

Práce je zaměřena na budovu Fakulty aplikované informatiky U5, ve které využívají možnosti připojení k bezdrátové síti převážná část studentů. Univerzita Tomáše Bati je v rámci české sítě národního výzkumu a vzdělávání zapojena do projektu eduroam. Díky tomuto roamingovému systému se mohou studenti připojit nejen na fakultách univerzity, ale i kdekoli, kde je tento systém podporován.

Cílem práce je provést analýzu pokrytí bezdrátovou sítí areálu U5, vytvořit mapu pokrytí, proměřit datovou propustnost a na základě získaných výsledků navrhnout případné změny vedoucí k rozšíření pokrytí bezdrátovou sítí.

I. TEORETICKÁ ČÁST

1 BEZDRÁTOVÉ SÍTĚ

Tento druh počítačových sítí, jak název napovídá, nevyužívá k propojení mezi jednotlivými komponenty k přenosu dat klasické metalické kabely. K šíření signálů je zde využito rádiových vln a přenosovým médiem mezi přístupovým bodem a uživatelem je vzduch. Proto se tyto sítě stávají tak oblíbenými. Při absenci propojovacích kabelů vniká tzv. volnost, kdy není uživatel vázán na pevné místo, ale může se svým přenosným počítačem, nebo jinou stanicí volně pohybovat a být stále připojen v síti. V dnešní době se setkáváme s obrovskou expanzí bezdrátových sítí, jak v sektoru firemním, tak i domácím, a proto vznikají na provozovatele i uživatelé patřičné nároky ohledně zabezpečení, které je potřeba akceptovat. Lze se setkat s nepsaným pravidlem, že náklady na zabezpečení patřičné sítě by měly být přímo úměrné hodnotě přenášených dat vně sítě. Například nepřichází v úvahu, aby síť pro klasické uživatelé v rodinném domě byla zabezpečená na stejné úrovni jako síť v bankách nebo různých movitých firmách a naopak. Použití bezdrátové sítě nese další plus, a to pokud chce uživatel instalovat síť už do kompletně zařízené místnosti, kde odpadá pokládání strukturované kabeláže a stojí před námi poměrně jednoduchá montáž. Je nutné zmínit, že jejich využívání sebou nese i některé nevýhody. Jsou to zejména nižší přenosová rychlost, omezený dosah signálu, větší riziko odposlechu a napadení.

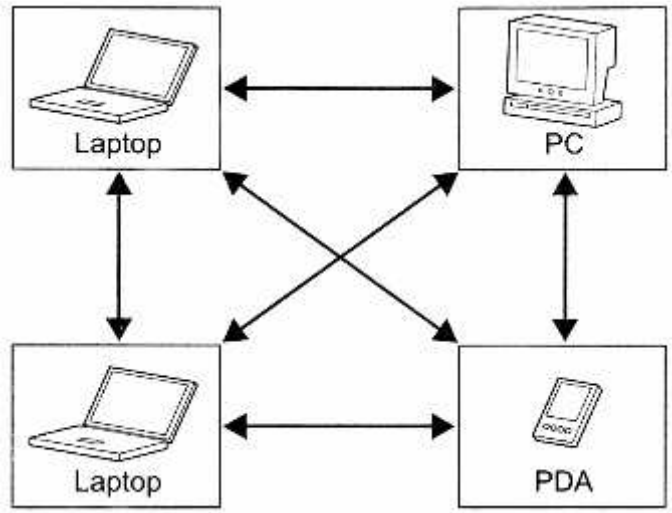
1.1 Topologie bezdrátových sítí

Bezdrátové sítě je možné rozdělit dle topologie na dva základní druhy. Jedním případem je způsob IBSS, kdy se klienti propojují přímo mezi sebou. Druhou možností je připojení klienta k centrálnímu přístupovému bodu, tento druh je nazýván (BSS/ESS).

1.1.1 Ad-hoc sítě (IBSS)

Sítě typu (IBSS) Independent Basic Service Set jsou často označovány jako též sítě Ad-hoc. Tento typ sítí nepotřebuje ke své činnosti přístupový bod a pracují v režimu peer-to-peer. Sítě tohoto typu jsou především vhodné pro krátkodobé propojení menšího počtu přenosných počítačů.

Režim Ad-hoc byl určen pro rozsáhlé sítě s neúplnou viditelností „každého s každým“, kde každý uzel funguje zároveň jako směrovač. Pro připojení do sítě Ad-hoc stačí znát použitý kanál a SSID. [1]

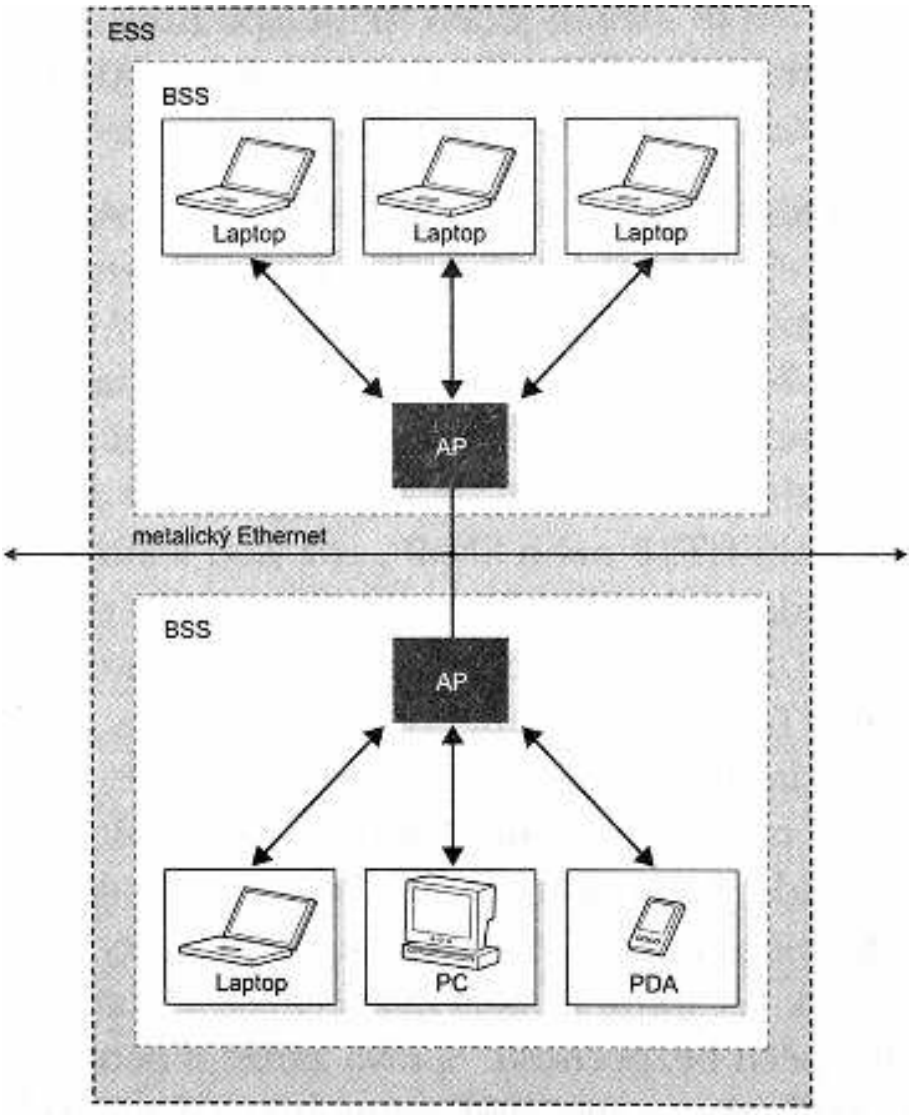


Obr. 1: Síť typu IBSS [1]

1.1.2 Režim infrastruktury sítě (BSS/ESS)

Tento typ sítí je realizován na principu připojení jednotlivých uživatelských stanic k centrálnímu přístupovému bodu a všechen provoz je prováděn přes přístupový bod. BSS (Basic Sevice Set) je přístupový bod, který je připojen k metalické síti, např. Ethernetu. Dále ESS (Extended Service Set) je více BSS vzájemně propojených distribučním systémem. Tohoto způsobu, kdy přístupový bod plní funkčnost mezi metalickou a bezdrátovou sítí, je využíváno v drtivé většině případů.

V závislosti na typu a nastavení se může chovat skutečně jako „hloupý“ most na druhé síťové vrstvě, anebo může fungovat mnohem chytřeji jako směrovač, zajišťovat překlad adres (NAT), přidělování adres (DHCP) a další. Některé přístupové body dokonce obsahují i koncentrátor VPN. Volba AP tedy v každém případě závisí na tom, jaká bude infrastruktura sítě. [1]



Obr. 2: Síť typu BSS/ESS [1]

2 WI - FI

Nejprve je důležité vymezit, co Wi–Fi zkratka znamená, protože mnoho lidí má tuto problematiku spojenou s úplně jinou skutečností. Jak již anglický název (wireless fidelity) napovídá, jde o bezdrátovou spolehlivost. Tato zkratka je vlastně název organizace Wi-Fi Aliance, která zodpovídá za standardy a protokoly využívané k bezdrátové komunikaci a vydává patřičné certifikáty k ověření kompatibility různých bezdrátových zařízení. Příčinou zavedení této organizace byl fakt, že mnoho zákazníků se začalo potýkat s problémem nekompatibility bezdrátových zařízení od různých výrobců, které mnohdy odmítaly spolu komunikovat. Cílem Wi–Fi Aliance se stala kompatibilita ve vztahu spolupráce všech bezdrátových zařízení od různých výrobků. A tu může zákazník dosáhnout zakoupením výrobku obsahující certifikát Wi–Fi Aliance. Poté si může být jist, že výrobek prošel certifikací a bude plně kompatibilní ve vztahu s ostatními prvky v bezdrátové síti. V dnešní době jsou na světě stovky výrobců a milióny výrobků, odpovídající tomuto standardu. Pro zajímavost na stránce http://www.wi-fi.org/our_members.php lze všechny výrobce najít.

Termín Wi-Fi tak v technické praxi dostal dva významy. Je to název pro výrobek splňující certifikační podmínky Wi-Fi Aliance. Dále se tohoto výrazu také používá obecně pro technologii bezdrátových sítí spadající pod standardy IEEE 802.11, o kterých bude více vysvětleno dále. [12]

Obr. 3: Wi-Fi Aliance certifikační značka [12]

Obr. 4: Logo Wi-Fi Aliance [12]

2.1 Rizika útoků na bezdrátové sítě

Jak již bylo výše zmíněno, bezdrátové sítě využívají přenosového vzduch jako přenosové médium a s touto skutečností vzniká fakt, že oblast pokrytí budovy nebo přilehlého okolí signálem nejsme často schopni zabezpečit fyzickou ochranou, a zamezit tak pohybu nežádoucích osob v dosahu signálu. A proto je mnohem jednodušší odposlouchávat konverzaci v bezdrátové síti, než v síti se strukturovanou kabeláží. K takovému napadení stačí útočníkovi pouze směrová anténa, patřičný software a odborné znalosti. Poté je schopen zachytit komunikaci v síti a tato data zneužít, nebo se do dané sítě přihlásit. Nejrozšířenější typy útoků jsou následující.

2.1.1 Rozluštění klíče WEP

Tato metoda napadení WLAN sítě je velice oblíbenou a častou. K rozluštění klíče dostačuje útočníkovi zachycení 5 až 10 miliónů paketů uživatele a to za předpokladu, že po celou dobu odposlechu nedojde k záměně WEP klíče. Útočníci tento útok realizují pomocí patřičného software jako AirSnort, WEPCrack, AirCrack.

2.1.2 Zjištění MAC adresy

Realizace tohoto útoku je velmi podobná výše zmíněné podobě rozluštění klíče WEP, při absenci WEP šifrování. Vše, co útočník potřebuje, je zachytávat komunikaci vedenou mezi přístupovým bodem a uživatelem. Poté stačí jen vyhledat a přečíst hlavičku MAC adresy. Po zjištění této adresy má možnost útočník naklonovat ukořistěnou MAC adresu své síťové kartě a poté vystupovat v síti jako oprávněný uživatel.

2.1.3 Útok typu muž uprostřed

Útoky tohoto typu se zakládají na principu vstoupení útočníka mezi přístupový bod a klienta, mezi kterými přeruší veškerý provoz. Poté zachytává data přenášená mezi nimi, z těch je schopen útočník vytvořit nepravý přístupový bod a přepojit uživatele na něj. Data přijatá na podvržený přístupový bod útočník ukládá a přeposílá na skutečný přístupový bod, a uživatel tak má pocit, že komunikuje s přístupovým bodem přímo, což není pravda. Útočník se tímto způsobem dostane ke všem důležitým datům.

2.1.4 Slovníkový útok

Útočník při realizaci tohoto útoku vychází s využíváním tzv. slovníku, který obsahuje databázi nejčastějších uživatelských jmen a hesel. Pomocí této databáze posílá výzvu a odezvu heslovaného protokolu a snaží se jej prolomit, pokud je úspěšný, získává plný přístup do WLAN sítě.

2.1.5 Session hijacking

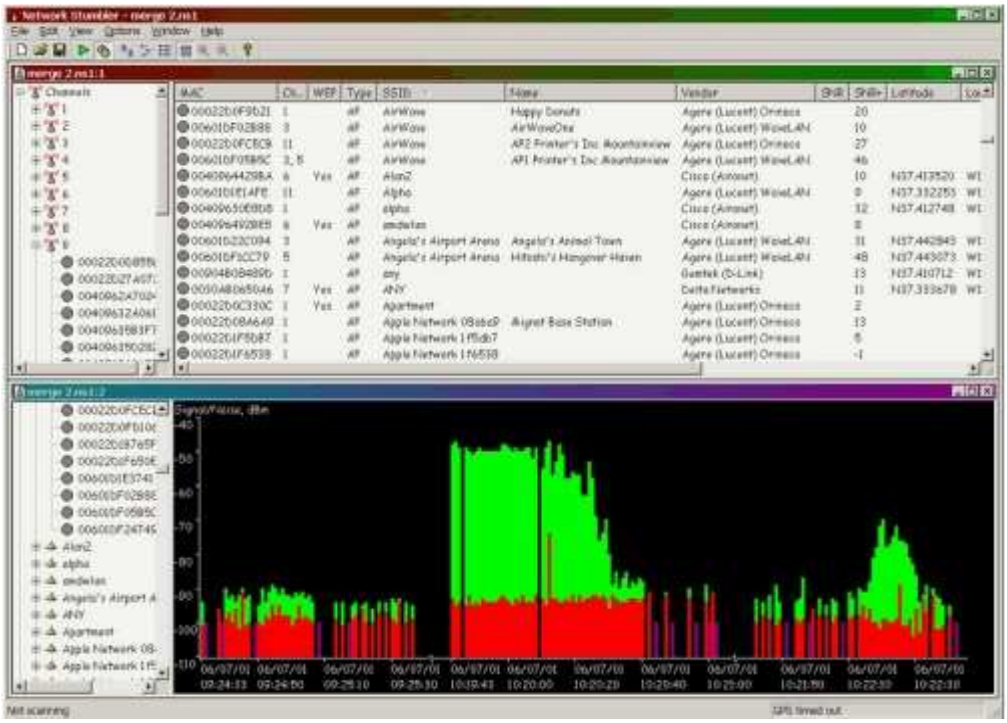
Kromě odposlechu dat jsou také útočníci schopni do přenášených dat vkládat vlastní informace. Ty se jeví jako původní data od klienta nebo přístupového bodu. A to má za následek, že je útočník schopen provoz přesměrovat z původního zařízení na sebe.

2.1.6 Denial of Service

Útoky tohoto typu se přímo neřadí mezi průniky do sítě, ale spíše jde o to, jak vyřadit síť z provozu. Útočník zahltí obrovským množstvím nesmyslných dat přístupový bod, který se jej snaží zpracovat, a tak dojde k jeho zahlcení nebo zahlcení přenosového pásma. To má posléze za následek zpomalení, nebo v horším případě úplné znemožnění připojení ostatních uživatelů.

2.1.7 War driving

Zakladatelem této techniky je jistý bezpečnostní konzultant Peter Shipley, který v roce 2000 začal realizovat projekt, kterým chtěl poukázat na možná rizika nezabezpečených bezdrátových sítí. Ten spočíval v tom, že projížděl městem a shromažďoval data o přístupových bodech, které byly v jeho dosahu signálu. Z toho vyšlo najevo, že téměř všechny sítě, na které narazil, nepoužívaly ani základní bezpečnostní opatření. Tímto pojmem War driving se označuje vyhledávání bezdrátových sítí a popřípadě následné ukořistění dat v této síti. Útočník provádějící War driving potřebuje nezbytně patřičný hardware, jako například bezdrátovou kartu, anténu a GPS pro zjištění přesného místa zjištěných přístupových bodů. Dále patřičný software, například NetStumber, Kismet, AirMagnet.



Obr. 5: Program NetStumbler [1]

2.2 Zabezpečení sítí WI-FI

2.2.1 SSID

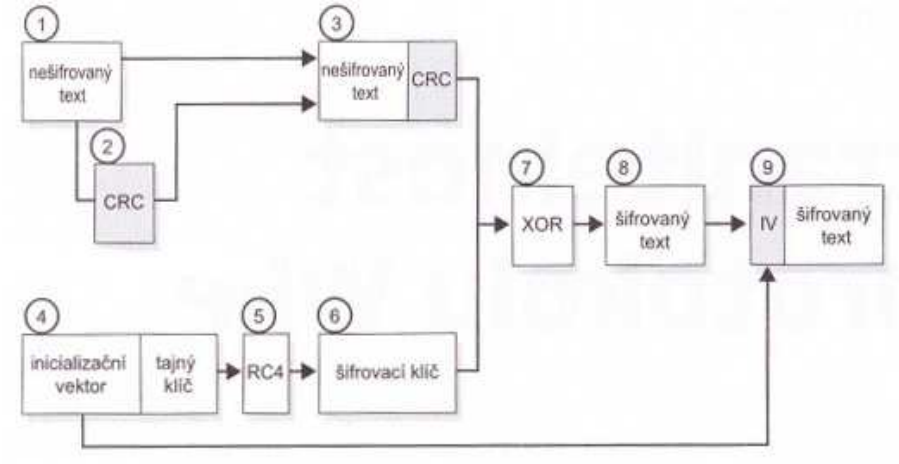
SSID (Service Set IDentifier) je pro každý přístupový bod bezdrátové sítě unikátním identifikátorem, který je vysílán jako administrativní signalizace a tím ohlašuje svou přítomnost. Jedná se o řetězec složený z 32 ASCII znaků. Pokud se chce uživatel připojit k některé z bezdrátových sítí, obdrží všesměrovým vysíláním od všech přístupových bodů v dosahu signálu své SSID, poté si může vybrat, ke které ze sítí se připojí. Spárování stanice a přístupového bodu vznikne nastavením klientova adaptéru na stejnou hodnotu SSID sítě, ke které se chce připojit. Uživatelé se mohou připojovat pouze k těm sítím, jejíž SSID znají. Tímto je zamezeno, aby se stanice omylem připojila k jinému přístupovému bodu, než chce. Zpravidla u všech přístupových bodů je možné nastavit znemožnění vysílání SSID, tím je možné síť skrýt, ale i přesto ji má možnost útočník pomocí falešného požadavku na připojení odhalit.

2.2.2 Filtrace MAC adres

Tato možnost zabezpečení přístupu do bezdrátové sítě je založena na principu udělení výrobcem jedinečné adresy MAC (Media Access Control) již při samostatné výrobě. A možnosti nastavení přístupového bodu, kteří uživatelé se mohou a naopak nemohou připojit do bezdrátové sítě, to je udržováno seznamem těchto adres. S absencí dalšího druhu zabezpečení je tato varianta nevhodná, protože útočník pomocí odposlechu provozu na síti může získat patřičnou MAC adresu a poté už jen naklonovat se svou a je mu přístup do takto chráněné sítě povolen. Proto je tento druh zabezpečení realizován spíše jako doplňková služba zabezpečení.

2.2.3 WEP

Úkolem WEP (Wired Equivalent Privacy), jak již vyplývá z názvu tohoto protokolu, je zprostředkovat uživatelům stejné zabezpečení jako u sítí metalických. Proces šifrování vždy začíná původním textem, který chceme chránit. Nejprve je z tohoto textu vypočten 32bitový cyklický redundantní součet (CRC), tedy kontrolní součet pro ověření integrity dat, tento součet je poté připojen za přenášenou zprávu. Dále se vezme tajný klíč, který je připojen k inicializačnímu vektoru (IV). Kombinaci IV a tajného klíče předáme do generátoru pseudonáhodných čísel RC4 a výstupem bude šifrovací klíč. Ten je sekvence nul a jedniček dlouhý jako původní text plus kontrolní součet. Následně mezi textem spojeným s kontrolním součtem a šifrovacím klíčem provedeme logickou operaci XOR. Výsledkem je šifrovaný text, před který připojíme hodnotu inicializačního vektoru, a pak posíláme. [2]



Obr. 6: Blokové schéma šifrování WEP [2]

2.2.4 WPA

Neboli (Wi-Fi Protected Access) je jedním ze zabezpečovacích protokolů, které mají za úkol zabránit vstup neoprávněným uživatelům do bezdrátové sítě. Tento protokol byl vyvinut v roce 2003 jako náhrada za již prolomený protokol WEP. Jeho hlavní úlohou je využití protokolu dynamicky se měnícího klíče TKIP a přijetí standardu 802.11i pro šifrování přenášených dat i přístupu bezdrátové sítě.

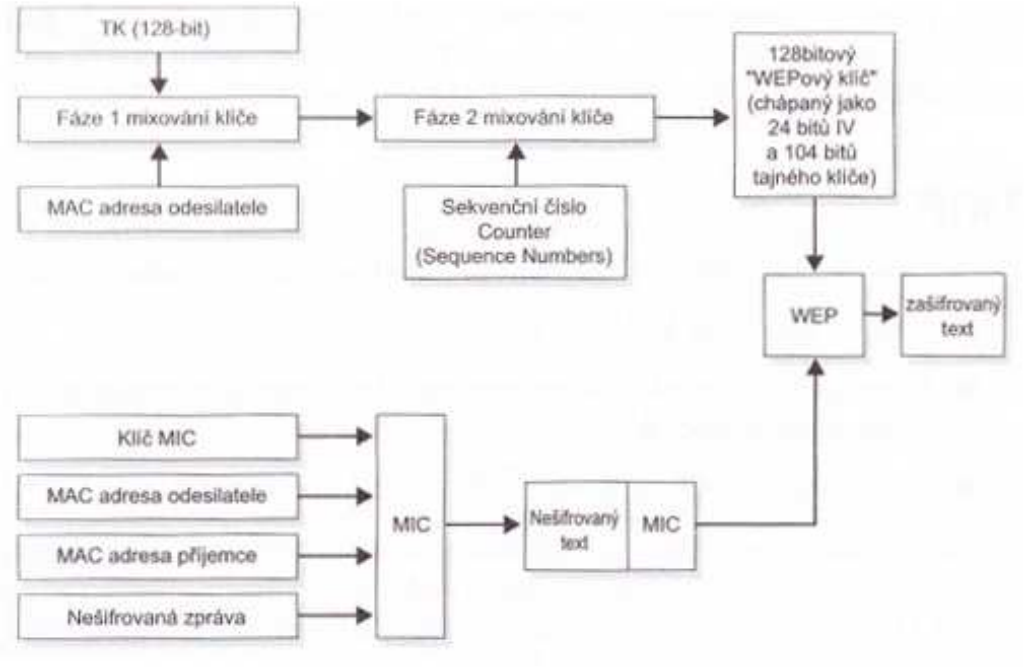
2.2.4.1 TKIP

Jedná se o protokol vyvinut za účelem bezpečnosti Wi-Fi sítí, jeho strůjcem je společnost IEEE ve spolupráci s Wi-Fi aliancí. Při jeho vytváření museli autoři počítat s faktem, že vytvářejí protokol na již zhotovený hardware, nikoliv opačně, jak tomu často bývá. I přesto v roce 2002 Wi-Fi aliance přistoupila na zahrnutí TKIP do WPA.

Mechanismus TKIP zlepšuje šifrování prostřednictvím tří hlavních prvků:

- Funkce mixování klíče pro každý paket
- Vylepšená funkce kontroly integrity (MIC, Message Integrity Code)
- Vylepšená pravidla generování IV včetně sekvenčních pravidel. [1]

Uživatel obdrží dva klíče, jeden 128bitový a druhý 64bitový pro zajištění integrity, které jsou vytvořeny protokolem 802.1x během iniciální komunikace. Šifrovací klíč nese označení TM (Temporal Key), klíč pro zajištění integrity pak MIC (Message Integrity Code). Zpočátku se provede logická operace XOR mezi MAC adresou uživatele a hodnotou TK, z těchto klíčů poté vznikne klíč označován jako Fáze1.Ten se později mixuje se sekvenčním číslem a z něj vzniká klíč nesoucí název Fáze 2, sloužící pro přenos jednoho paketu. Výstup Fáze 2 je předáván mechanismu WEP jako standardní 128bitový klíč. Zbytek procesu je prováděn jako transakce protokolem WEP s tím rozdílem, že všichni uživatelé nepoužívají stejný WEP klíč a že už není možná korekce mezi sekvenčním číslem a samotnou klíčovou sekvencí.



Obr. 7: Blokové schéma šifrování TKIP [1]

2.2.5 WPA2

WPA2 je ekvivalent pro plné znění standardu IEEE 802.11i, vydaný v květnu roku 2004, který slouží k vylepšení předchozích zabezpečovacích a autentizačních algoritmů pro bezdrátové sítě Wi-Fi. WPA2 přinesl některé změny jako oddělení autentizace uživatele od kontroly integrity a soukromí zprávy. WPA2 zároveň zneplatňuje předchozí zabezpečovací algoritmus WEP. 802.11i na rozdíl od svých předchůdců využívá symetrického blokového šifrování AES (Advanced Encryption Standard. WPA2 využívá tzv. architekturu RSN (Robust Security Network), která se skládá z Autentizace PSK nebo autentizačního systému 802.1X a šifrovacího systému CCMP k zajištěni věrnosti, integrity a oprávněné autentizace. Pokud procedura autentizace mezi stanicemi využívá čtyřcestný handshake, asociace se označuje jako RSNA (Robust Security Network Association). Takovéto sestavení bezpečné komunikace se skládá ze 4 základních prvků: [4]

- Odsouhlaseni bezpečnostních zásad
- Autentizace PSK / IEEE 802.1X
- Odvozování a distribuce klíče
- Utajení a Integrita dat RSNA [4]

3 STANDARD 802.11 A JEHO VARIANTY

Tento standard byl vytvořen společností IEEE (The Institute of Electrical and Electronics Engineers) za přispění společnosti WECA (Wireless Ethernet Compatibility Alliance) a měl za úkol specifikovat způsob, jakým budou využívat zařízení frekvenční pásma 2,4 GHz a 5 GHz. Byl určen pro bezdrátové sítě WLAN a poté k němu byly přidány dodatky, které měly za úkol vylepšovat tento standard. Tyto standardy mají však i svou stinnou stránku, a to že pracují v pásmu ISM (Industrial, Scientific and Medical), pracující na 2,4GHz, které je využíváno průmyslovými, lékařskými a vědeckými potřebami. To způsobuje poměrně velké zahlcení tohoto pásma, což může mít za následek vzájemné rušení, výpadky, snížení přenosových rychlostí.

Přehled standardů IEEE 802.11:

- **IEEE 802.11** – Jedná se o první vytvořený standard typu 802.11 společností IEEE roku 1997, který byl vyvinut a určen pro bezdrátové sítě pracující v přístupném pásmu ISM na frekvenci 2,4GHz s přenosovou rychlostí 2Mb/s a podporou až 13 kanálů. Nicméně standardy těchto kanálů se mohou různě v jiných zemích světa lišit. Tento celosvětově uznávaná standard se ukázal plně vyhovující a díky tomu se stal vzorem dalších doplňků, na kterých bezdrátové sítě fungují i v dnešní době.
- **IEEE 802.11a** – Jde o nástavbu výše zmíněného standardu 802.11, který byl vytvořen roku 1999. Tento doplněk pracuje na frekvenci 5GHz a využívá zabezpečení WEP, dále definuje podporované datové přenosy, a to 6, 12, a 24Mb/s. Také používá ortogonální multiplex s kmitočtovým dělením, což umožňuje lepší využití přenosových subkanálů. To je docíleno rozdělením 20 MHz širokého kanálu do 52 odlišných subkanálů a použití více stavových modulací a paralelního přenosu.
- **IEEE 802.11b –** Jedná se o doplněk standardu 802.11, vytvořený roku 1999, pracující ve frekvenčním pásmu 2,4GHz na 13 kanálech v rozmezí 2,412GHz až 2,472GHz. Mezi jeho vylepšení oproti původnímu standardu patří zvýšení přenosové rychlosti na 11Mb/s a používání DSSS modulace. To je technika přímo rozkládajícího spektra, která funguje na principu přenosu bitu, který je před přenosem nahrazen skupinou bitů vzniklých různými druhy kódování.

- **IEEE 802.11g –** Roku 2003 vstupuje tento dodatek v platnost a přináší zvýšení datové propustnosti až na 54Mbit/s. Dodatek pracuje ve frekvenčním pásmu 2,4GHz a využívá taktéž modulace DSSS a tím pádem je zpětně kompatibilní se zařízeními dle 802.11b a umožňuje spolupráci klientů využívajících obou standardů v jedné síti.
- **IEEE 802.11n** – Doplněk standardu, který byl uveden na trh roku 2009. Má za úkol výrazné zvýšení datové propustnosti bezdrátových sítí oproti předchozím verzím standardům až na 600Mb/s a zvýšený dosah, který sahá až k 70 metrům. Dále byla zavedena funkce MIMO (Multiple Input Multiple-Output), což znamená vícenásobný vstup a výstup. To v reálu znamená rozdělení vysílaných dat na menší toky, které jsou posléze vysílány přes více antén, což vede k zvýšení datové propustnosti za předpokladu stejné vyzářené energie.

Doplněk	Popis
802.11a	Zajišťuje rychlost až 54 Mb/s v pásmu na frekvenci 5 GHz.
802.11b	Zajišťuje rychlost až 11 Mb/s v pásmu na frekvenci 2,4 GHz.
802.11c	Určen k přemosťování v bezdrátových zařízeních.
802.11d	Úprava 802.11b na jiné kmitočty v zemích kde je pásmo 2,4 GHz nedostupné.
802.11e	Zajišťuje kvalitu služeb QoS.
802.11F	Zajištění spolupráce přístupových bodů různých výrobců.
802.11g	Zajišťuje rychlost až 54 Mb/s v pásmu na frekvenci 2,4 GHz.
802.11h	Dynamický výběr kanálu a řízení vysílacího výkonu.
802.11i	Zavádí nové metody šifrování a vede k WPA resp. WPA2.
802.11j	Umožňuje WLAN pracovat v kmitočtovém pásmu 4,9÷5 GHz v Japonsku.
802.11k	Měření a správa radiových zdrojů a optimalizace šumu.
802.11m	Revize standardů rodiny 802.11.
802.11n	Zvýšení propustnosti.
802.11p	Bezdrátový přístup pro pohybující se objekty.
802.11r	Zajištění mobility účastníka WLAN
802.11s	Technologie multi-hopping zavádějící mesh sítě.
802.11u	Vylepšení spolupráce s externími sítěmi
802.11v	Umožňuje management klientských zařízení při připojování do WLAN
802.11w	Zvýšení integrity, autencity utajení a ochrany dat.
802.11y	Umožňuje WLAN pracovat v kmitočtovém pásmu 3,65÷3,7 GHz v USA.

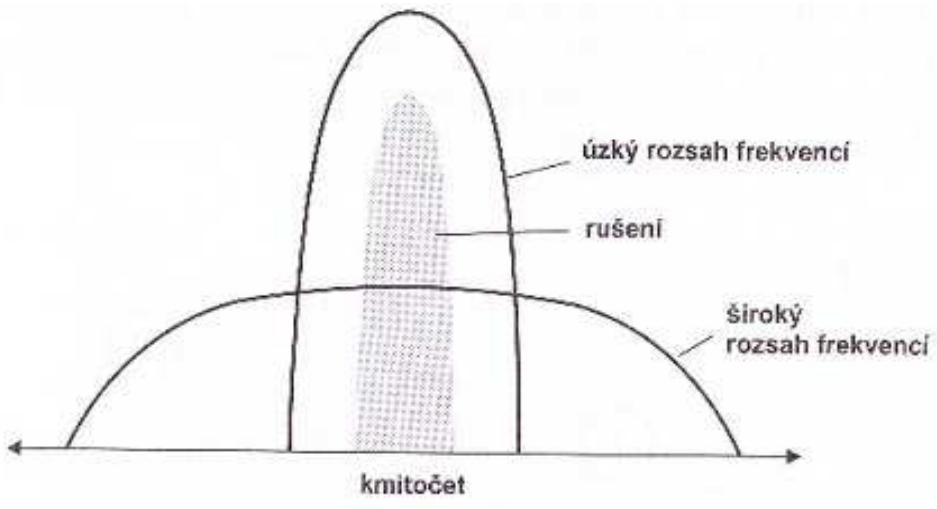
Obr. 8: Přehled všech doplňků standardu 802.11 [4]

Standard	Datum Vytvoření	Pracovní frekvence [GHz]	Bitová rychlost maximální [Mb/s]	Bitová rychlost typická [Mb/s]	Fyzická vrstva	Odhadovaný vnitřní dosah [m]
původní 802.11	1997	2,4	2	~1	OFDM	~35
802.11a	1999	5	54	~20	OFDM	~35
802.11b	1999	2,4	11	~5	DSSS	~38
802.11g	2003	2,4	54	~19	OFDM/DSSS	~38
802.11n	~2009~	2,4 nebo 5	~600	~300 (2 proudy)	MIMO	~70

Obr. 9: Přehled vybraných doplňků standardu 802.11 [4]

3.1 Rozprostřené spektrum

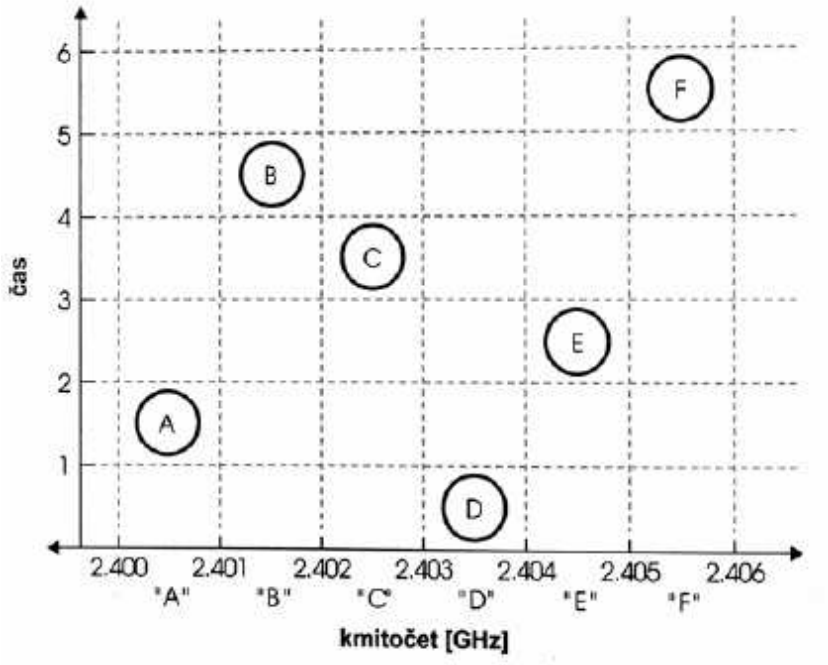
Výše uváděné metody FHSS a DSSS jsou dvěma metodami využívající technologii rozprostřeného spektra. Základní princip tohoto spektra spočívá v rozprostření signálu po širokém rozsahu frekvencí. To má za následek horší detekci datových přenosů, často je lze zaměnit za pouhý šum. Dále se snižuje náchylnost k interferencím a rušení přenášeného signálu.



Obr. 10: Rozprostřené spektrum [1]

3.1.1 FHSS

Tato metoda se v praxi využívá jen minimálně, je to dáno velikým úspěchem a masovým rozšířením metody DSS. K vynálezu této metody přispěli Hedy Lamarr a George Antheil patentem z roku 1942 s názvem Bezpečný komunikační systém. Hlavní myšlenkou byl velmi rychlý skok z jednoho kmitočtu na druhý, to mělo za příčinu vznik technologie FHSS, kde jsou přeskoky mezi kmitočty řízeny předem stanoveným obrazcem. Jedná se o minimálně 15 kanálů s maximálním setrvávajícím časem 400ms.

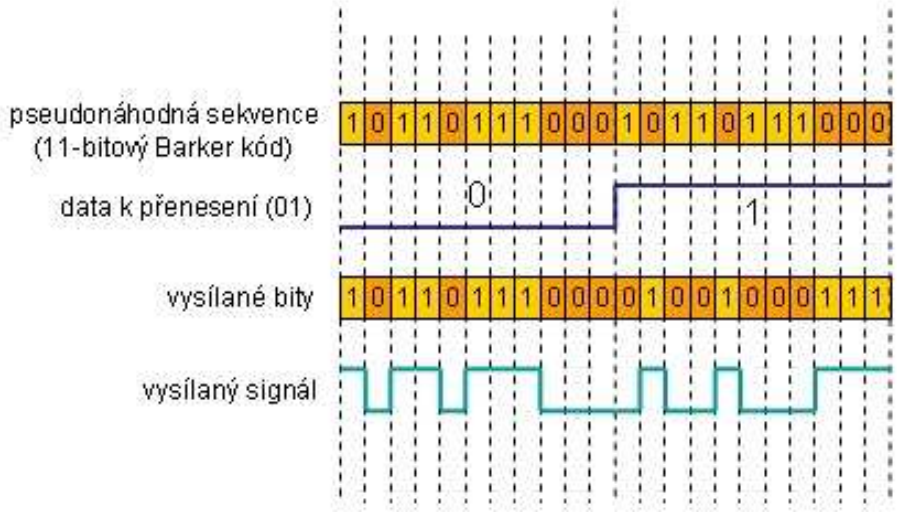


Obr. 11: Technologie FHSS [1]

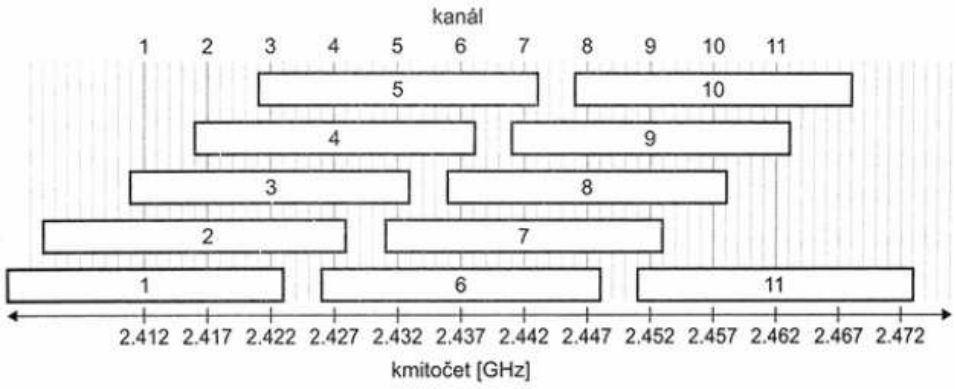
3.1.2 DSSS

Metoda DSSS má oproti již zmíněné FHSS metodě výhodu ve výrazně vyšších přenosových rychlostech. Princip této metody funguje na expandování přenášeného datového bitu do přenosového kódu, to znamená, že každý bit zastoupen obrazcem 11tibitů. Následkem toho je zpráva přenášena v širším frekvenčním spektru a použití různých sekvenčních kódů nám umožňuje výskyt více DSSS systémů v jednom místě. Metoda DSSS využívá ke své činnosti 11 kanálů o šířce 22MHz, pásmo na frekvenci 2,4GHz má šířku jen 83,5MHz, proto jsou střední kmitočty kanálů posunuty o 5 MHz.

Díky všem skutečnostem má metoda DSSS velmi dobrou odolnost vůči rušení, dojde-li k poškození části zprávy, opravné techniky budou schopny poškozenou zprávu rekonstruovat do původního znění.



Obr. 12: Technologie DSSS [11]



Kanál	Spodní kmitočet	Střední kmitočet	Horní kmitočet
1	2.401	2.412	2.423
2	2.404	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473

Obr. 13: Rozložení kanálů DSSS [1]

3.2 Komponenty sítě

Každá bezdrátová síť typu 802.11 se skládá ze čtyř základních částí, kterými jsou:

- Distribuční systém
- Přístupový bod
- Bezdrátové médium
- Stanice [8]

3.2.1 Distribuční systém

V okamžiku, kdy má více přístupových bodů tvořit rozsáhlejší síť, musí spolu komunikovat a předávat si spolu informace o pohybu mobilních stanic. Distribuční systém je logická komponenta standardu 802.11 používána k přesměrování datového toku na stanici skutečného určení podle její aktuální polohy. [8]

3.2.2 Přístupový bod

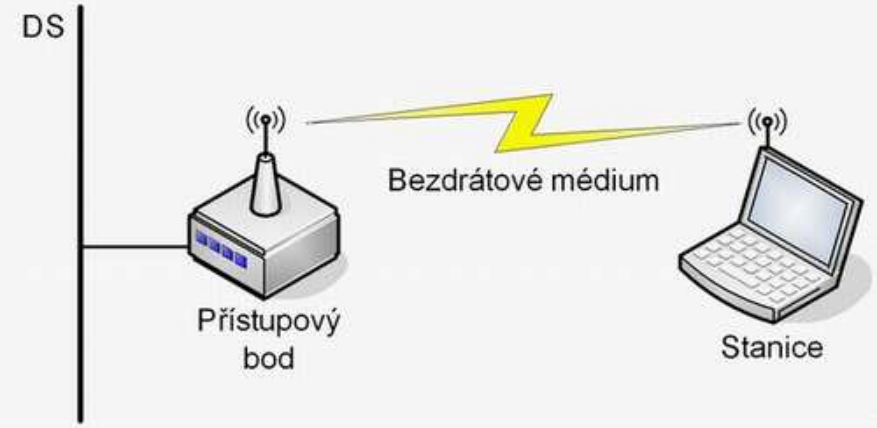
Jedná se o elektronické zařízení, které zprostředkovává přemostění mezi kabelovou a bezdrátovou sítí. Uživatelé nekomunikují spolu přímo, ale prostřednictvím přístupového bodu po připojení k němu.

3.2.3 Bezdrátové médium

Tuto komponentu u sítí WLAN lze chápat stejně jako u sítí drátových strukturovanou kabeláž, jedná se o médium, které je nosičem dat mezi přístupovým bodem a stanicí uživatele.

3.2.4 Stanice

Stanicí lze obvykle nazvat každé zařízení, které je schopno se připojit do bezdrátové sítě a nadále v ní komunikovat. Nejčastěji to jsou: počítač, notebook, PDA, herní konzole, atd.



Obr. 14: Komponenty sítě [2]

4 KOLIZNÍ MECHANISMY

4.1 CSMA/CA

Tato metoda CSMA/CA v sobě ukrývá název (Carrier Sense Multiple Access / Collision Avoidance) a je velmi podobná koliznímu mechanismu, se kterým jsme se setkali u metalických sítí CSMA/CD. Ale při rozdílu, že bezdrátová zařízení jsou polo-duplexní, tudíž postrádají možnost číst a zapisovat současně. Proto je v protokolu 802.11 zavedena kolizní metoda vyžadující, aby vysílací zařízení před zahájením přenosu chvíli naslouchalo, a navíc příjemce při obdržení paketu odpoví odesílateli potvrzovacím rámcem ACK. Při absenci potvrzovacího rámce ACK je předpokládán ztráta paketu, a proto je odeslán znovu.

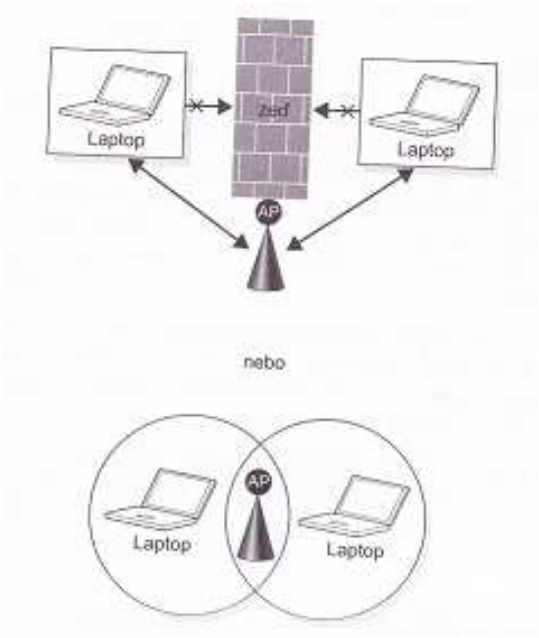
4.2 RTS/CTS

Metoda RTS/CTS (Request to Send / Clear to Send) přináší řízení provozu s cílem co nejnižšího překrytí přenosů v rušeném prostředí.

Proces je podobný tomu, jako když se hlásíte ve vyučování. Klient pošle rámec RTS a žádá o povolení promluvit. Následně AP odešle rámec CTS a povoluje klientovi mluvit. Pak teprve klient posílá data. Ostatní žáci ve třídě tuto komunikaci vidí a chápou, že nemohou mluvit, pokud byl vyvolán někdo jiný. [1]

Tímto lze v prostředí s velikým výskytem rušení výrazně zvýšit datovou propustnost, protože dojde k snížení počtu opakovaných přenosů. Mechanismus RTS/CTS lze velice dobře využít pro takzvaný případ skrytých uzlů. Ten nastává v případě, vidí-li dva klienti

přístupový bod, ale sebe navzájem ne. Metodou RTS/CTS je zajištěno současné vysílání obou klientů.



Obr. 15: RTS/CTS [1]

4.3 Fragmentace

Proces fragmentace funguje na způsobu rozdělení delší přenášené zprávy na menší části, které se posléze na straně příjemce znovu složí do jednoho celku. Tato metoda byla již i dříve využitá u Ethernetu a pracuje na stejném principu. Jedná se o velice užitečnou metodu zejména v prostředí s vyšším provozem, kdy ve finále může vést ke zvýšení propustnosti. RTS/CTS a Fragmentace jsou neopomenutelné aspekty při návrhu infrastruktury a správy bezdrátové sítě.

5 ŠÍŘENÍ RÁDIOVÉHO SIGNÁLU

Šíření rádiového signálu v pásmu nad 2GHz, kde spadá i WiFi, ovlivňuje značnou mírou hned několik neblahých faktorů, které mají za následek toto šíření komplikovat. Obecně je známo, že mezi přístupovým bodem a uživatelskou stanicí by měla být přímá viditelnost, což je mnohdy takřka nemožné. Pro bezproblémový chod bezdrátové sítě by se měli projektanti vypořádat s těmito základními potížemi:

- rušení jinými systémy ve stejném pásmu,
- přímá viditelnost,
- vícecestné šíření signálu,
- vlivy počasí. [8]

5.1 Rušení jinými systémy ve stejném pásmu

Rušení jinými systémy ve stejném frekvenčním pásmu je jedním z nejkritičtějších problémů pro správný přenos signálu z jednoho místa na druhé. Největší hrozbou jsou pak zařízení pracující na FHSS modulaci, které vysílají signál do celého pásma ISM, což může zapříčinit výpadky WiFi spojení. Možné problémy mohou také vzniknout ze strany bluetooth zařízení a bezdrátovými telefony.

Jelikož je pásmo 2,4GHz bezlicenční, může každý uživatel za dodržení regulí ČTÚ vysílat bez omezení. Dojde-li ke střetu dvou provozovatelů na stejné frekvenci, platí pravidlo “kdo dřív přijde, ten dřív mele“.

5.2 Přímá viditelnost

Dojde-li k absenci přímé viditelnosti mezi AP a uživatelem, lze očekávat jistý druh potíží ve spojení. Ty jsou závislé na druhu materiálů a počtu překážek na přenášené trase. Přenos signálů bezdrátové sítě skrz klasický železobeton je jednou z nejhorších možností pro přenášený signál. O něco lépe je to pak s cihlovým zdivem, dřevem a sádrokartonem.

5.3 Ostatní vlivy

Jak již bylo zmíněno, na přenos rádiového signálu mají neblahý vliv i stromy, počasí a další vlivy. Ty však není nutné detailněji rozebírat, jelikož se nebudou vyskytovat v prostředí, pro které bude prováděna praktická část. Dále při vysokém výskytu

pohybujících se osob může nastat problém s častým přihlašováním a odhlašováním stanice do bezdrátové sítě. To je dáno neprůchodností signálu vodou, z níž je lidské tělo z velké části tvořeno. Procházející osoba může výrazně snížit signál a při špatném vyhodnocení notebook přeroamuje na další AP, který je od uživatele dále a má slabší signál.

5.4 Výkon rádiového systému

Je zřejmé, že s vyšším vyzařovacím výkonem bezdrátové sítě dosahuje signál vyšší možné přenosové vzdálenosti. To však s sebou nese i neblahé účinky, a to větší možnost napadení dané sítě. Výstupní jednotka vysílače a vstupní jednotka přijímače je vyjádřena jednotkou Watt (W) nebo jednotkou dBm.

Vzorec pro výpočet mezi dvěma výkony P1 a P2:

$$dB = \frac{10 \times \log P1}{P2}$$

Vzorec k převodu výkonu z mW na dBm:

$$dBm = 10 \times \log_{10} \frac{P}{0{,}001}$$

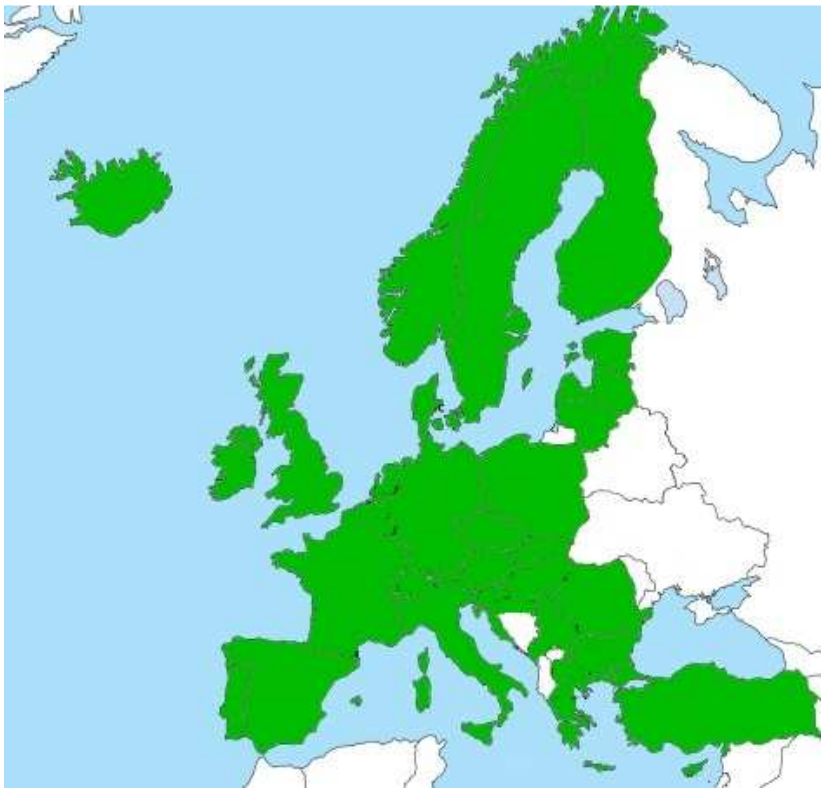
6 EDUROAM

Eduroam je akademický roamingový systém zahrnutý v rámci české sítě národního výzkumu a vzdělávání poskytující síťovou konektivitu pro své uživatele v připojených organizacích. Přístup je založen na zabezpečené autentizaci v domácí instituci. [9]

Tento projekt běží pod sdružením CESNET a klade si za cíl transparentní využívání propojených sítí, tato myšlenka vznikla na podnět pracovní skupiny TERENA mobility TF. Cílem provozovatelů je snadné používání služeb sítě jako používání roamingu mobilních operátorů. Uživatel zaregistrovaný v této síti vlastní jeden účet ve své domovské síti a ten mu dovoluje připojit se ke kterékoliv bezdrátové síti, která je členem tohoto projektu. Mapu pokrytí sítí eduroam v ČR lze vidět na Obr. 16: Pokrytí sítě eduroam v ČR [9]

Obr. 16: Pokrytí sítě eduroam v ČR [9]

Sdružení CESNET bylo založeno vysokými školami a Akademií věd ČR, má za úlohu koordinaci a propagaci aktivit ve vztahu s roamingem v počítačových sítích a provoz infrastruktury RADIUS serverů nutných pro propojení s Evropskou roamingovou strukturou. Systém eduroam nemá zastoupení jen v České republice, ale i po celé Evropě, jako Evropská eduroam konfederace, což je propojení jednotlivých eduroam federací daných zemí v rámci Evropy, zastoupených zpravidla organizací NREN.



Obr. 17: Pokrytí sítě eduroam v EU [9]

6.1 Fungování roamingu a mobility pro uživatele

Hlavní příčinou zavedení roamingu v českých organizacích v rámci NREN byla myšlenka umožnění přístupu uživatelům v co nejvíce lokalitách. Cílem mobility roamingu je bezesporu dostupnost Internetu nejen pro studenty a zaměstnance své univerzity, ale i kdekoliv jinde, kde je dostupná síť eduroam. Tato mobilita však není omezena jen na Českou republiku, ale je plně funkční i v spolupracujících zemích EU. Zaregistrovaný uživatel disponuje jedním uživatelským účtem, který je veden v jeho domácí instituci, a na ten je schopen se přihlásit do kterékoli eduroam sítě. Funkčnost systému je založena na posílání autentizacích dotazů vzniklých na základě uživatelského jména do uživatelovy domovské sítě. Zde dochází k rozhodování, zda má uživatel právo k přístupu, či ne. Pro správnou funkčnost tohoto systému je zapotřebí dvou věcí. První je uživatelské jméno, které je nositelem informací o původu uživatele, a druhé je autentizační infrastruktura, která přenáší autentizační data. Tvar uživatelského jména je striktně dán syntaxí: “jmeno@realm”, kde jméno je běžné jméno v jednotlivé instituci a realm určuje, o jakou organizaci jde. Organizace vyskytující se v České republice končí koncovkou “.cz”. Úkolem autentizační infrastruktury (AAI - autentication and authorization infrastructure) je

směrovat ověřovací údaje o uživateli do domácí sítě a přenést odpověď zpět do systému, který se dotazoval. AAI je tvořena hierarchií RADIUS serverů. Pro ověření uživatele je využíváno tří hlavních mechanizmů.

6.2 Autentizace na bázi protokolu 802.1x

Princip tohoto ověřování je založen na schopnosti přístupového bodu řídit provoz na jednotlivých portech. Uživatel se sice připojí k síti, ale všechna data jsou blokována s výjimkou autentizačního protokolu. Počítač uživatele pošle síťovému prvku uživatelské údaje a čeká, zda je vpuštěn do sítě, nebo ne.

6.3 Autentizace na bázi webového formuláře

V tomto případě je uživatel připojený do sítě vpuštěn pouze na WWW stránku, kde musí zadat uživatelské jméno a heslo. Vstup do sítě je chráněn firewallem, který povoluje další provoz, ovšem až dojde k úspěšnému ověření. Toto ověření je realizováno AAI a výsledek je směrován do domácí sítě uživatele.

6.4 Autentizace na bázi VPN spojení

Tato metoda je od výše zmíněných odlišná v tom směru, že pro ověřování identity uživatele není využito AAI. A její hlavní myšlenkou je, dojde-li k připojení uživatele na VPN (Virtual Private Network) koncentrátor, je předpokládáno, že má oprávněný přístup do této sítě. Tato ověřovací metoda dovolí uživateli připojit se k síti, ale firewall umožňuje spojení pouze na úzký počet VPN koncentrátorů v spolupracujících institucích. Připojení je omezeno pouze na VPN brány.

II. PRAKTICKÁ ČÁST

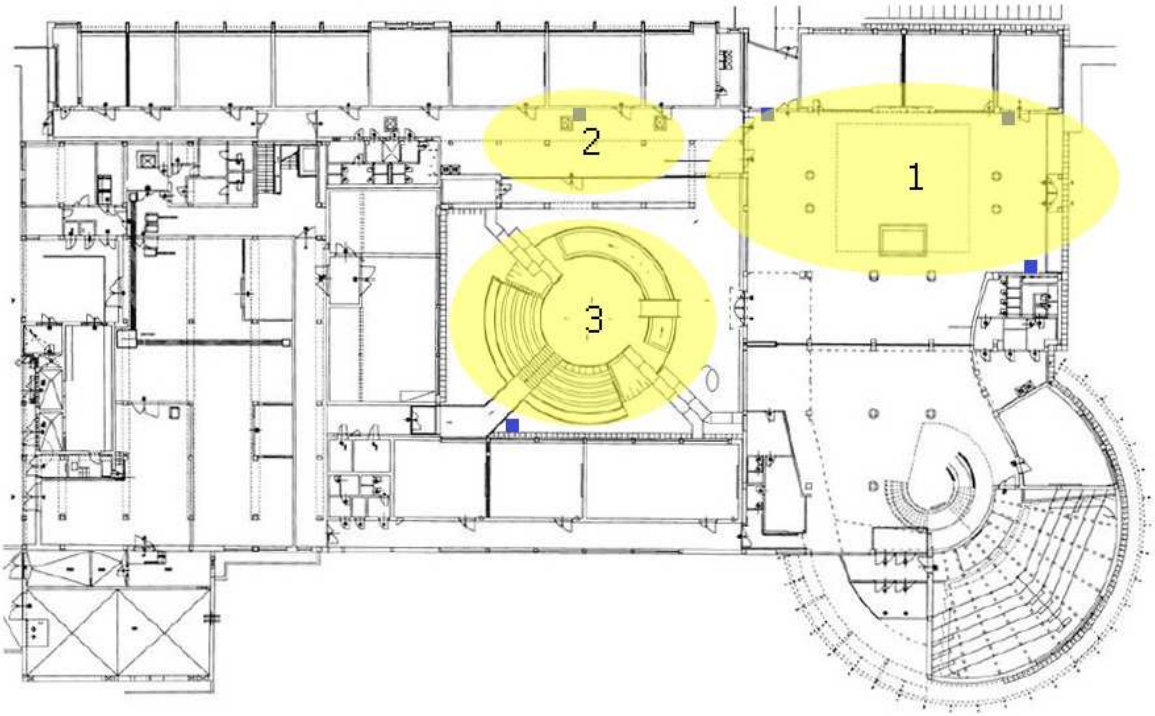
7 ANALÝZA POKRYTÍ BUDOVY U5 BEZDRÁTOVÝMI SÍTĚMI

Pro přehlednost tohoto úkolu v praktické části jsem rozdělil budovu U5 Fakultu aplikované informatiky do následujících tří podlaží a každé podlaží dále do více sektorů. Každé z těchto tří podlaží bylo zmapováno a do plánu byly vyznačeny všechny AP. Dále jsem v každém podlaží a sektoru zvlášť provedl pomocí programu CommView for WiFi a notebooku kompletní analýzu výskytu bezdrátových sítí v dosahu. Místa pro připojení studentů k síti eduroam, a tudíž k internetu, jsou vyznačena na tomu určených místech touto značkou.

Obr. 18: Značka pro připojení k Wi-Fi [18]

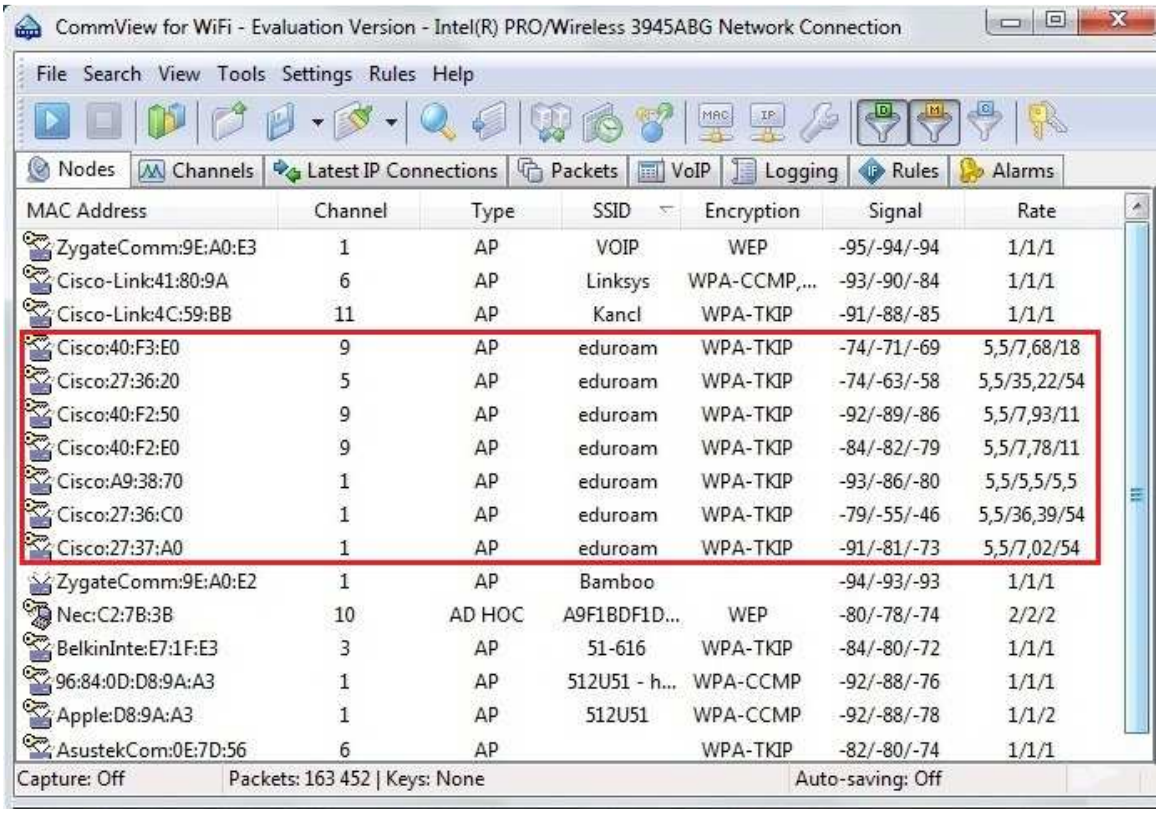
7.1 První podlaží budovy U5

Toto podlaží je nejvíce frekventované studenty, proto je zde kladen největší důraz na rychlost internetového připojení. Na tomto podlaží se nalézají prostory jako: vstupní foyer, chodba, venkovní atrium, popřípadě přilehlé třídy. Na obr. 19 jsou vyznačeny všechny AP, které jsou určeny k provozu sítě eduroam.



Obr. 19: První podlaží budovy U5

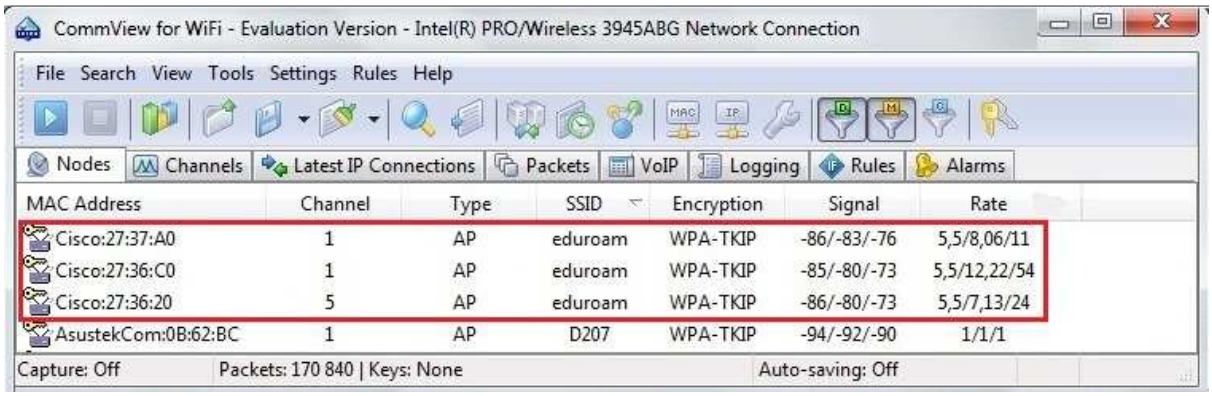
7.1.1 Výčet všech zachycených bezdrátových sítí v sektoru 1



Obr. 20: Sítě na podlaží 1v sektoru 1

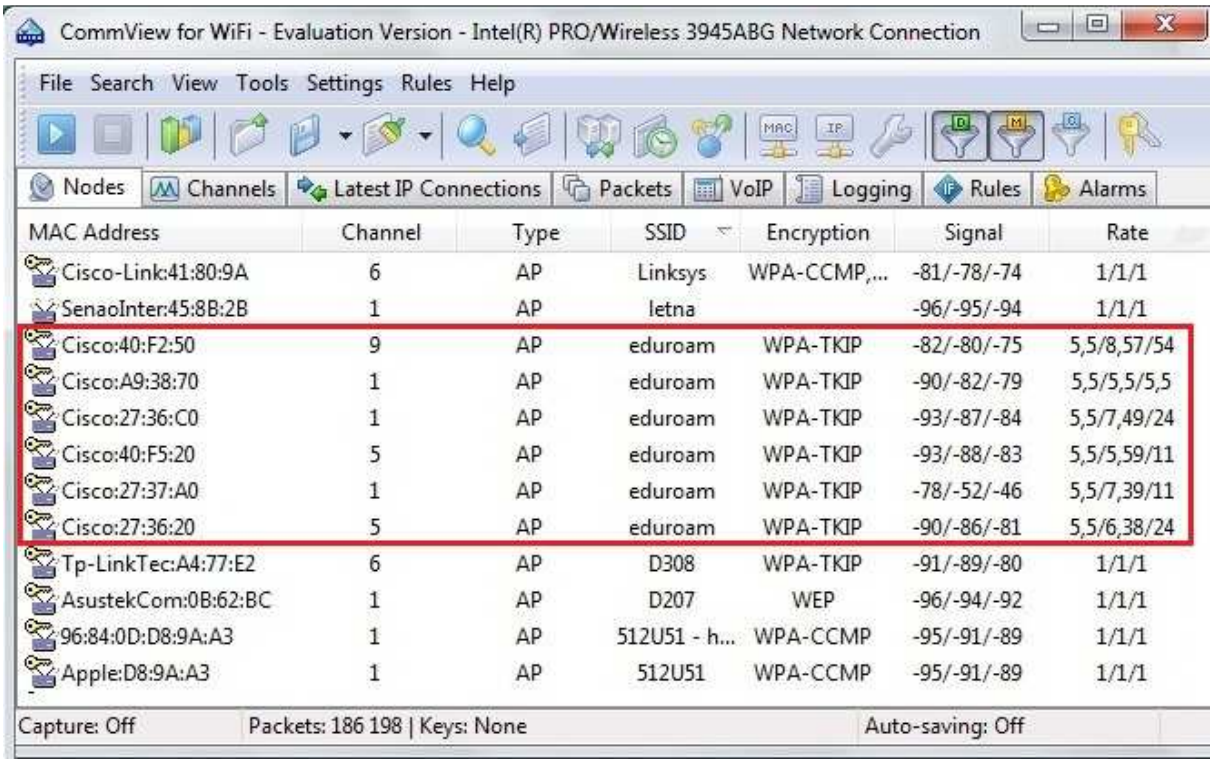
Pomocí programu CommView for WiFi jsem byl schopen zobrazit veškeré AP, které byly v dosahu mého signálu a v danou dobu vysílaly. Dále také získat o každém AP důležité informace, jako výrobce AP, MAC adresu AP, SSID, signál, způsob šifrování a kanál, na kterém vysílá. Program CommView for WiFi je také schopen zobrazit veškeré uživatele, kteří se v okruhu signálu vyskytují, ale to jsem zde nezahrnul.

7.1.2 Výčet všech zachycených bezdrátových sítí v sektoru 2



Obr. 21: Sítě na podlaží 1v sektoru 2

7.1.3 Výčet všech zachycených bezdrátových sítí v sektoru 3

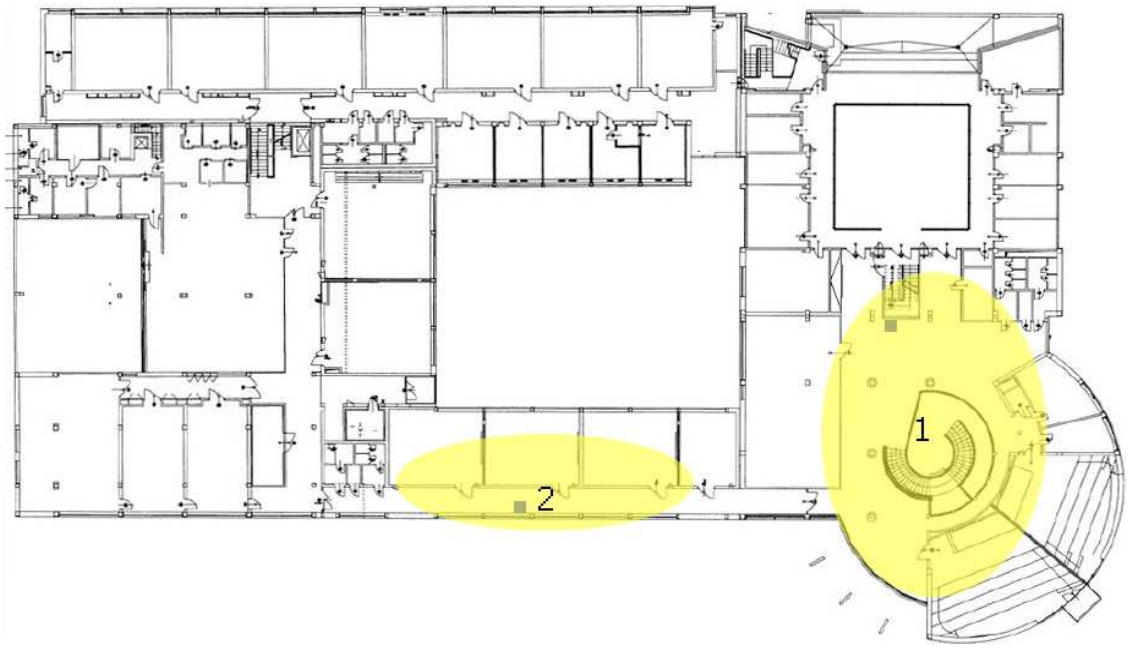


Obr. 22: Sítě na podlaží 1v sektoru 3

Již při prvním pohledu je zřejmé, že v okolí prvního podlaží se kromě sítě eduroam nachází také mnoho jiných bezdrátových sítí, které také mohou svou činností mít neblahý dopad na provoz sítě eduroam. A to z hlediska rušení v pásmu 2,4 Ghz.

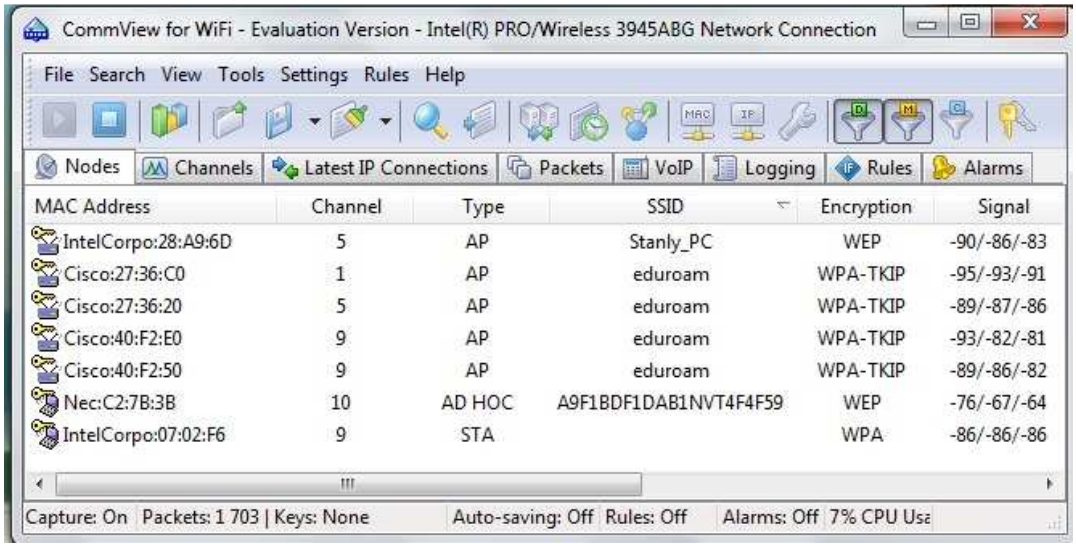
7.2 Druhé podlaží budovy U5

Toto podlaží je studenty využívající bezdrátové připojení používáno o poznání méně, než tomu bylo v předchozím případě na podlaží prvním. Avšak je zde zapotřebí zabezpečit bezdrátové připojení pro studenty, kteří nevyužívají služeb studovny, nebo studenty vyskytující se v přednáškové místnosti. Dále také studenty vyskytující se před učebnami s počítači i vně, viz Obr. 23.



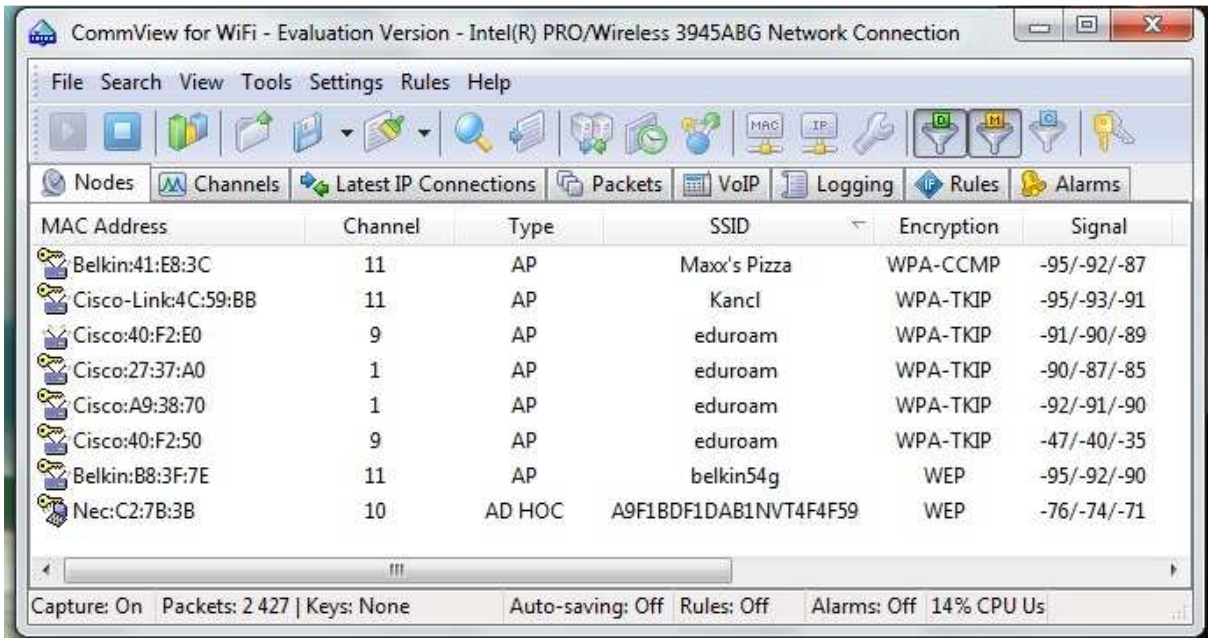
Obr. 23: Druhé podlaží budovy U5

7.2.1 Výčet všech zachycených bezdrátových sítí v sektoru 1



Obr. 24: Sítě na podlaží 2 v sektoru 1

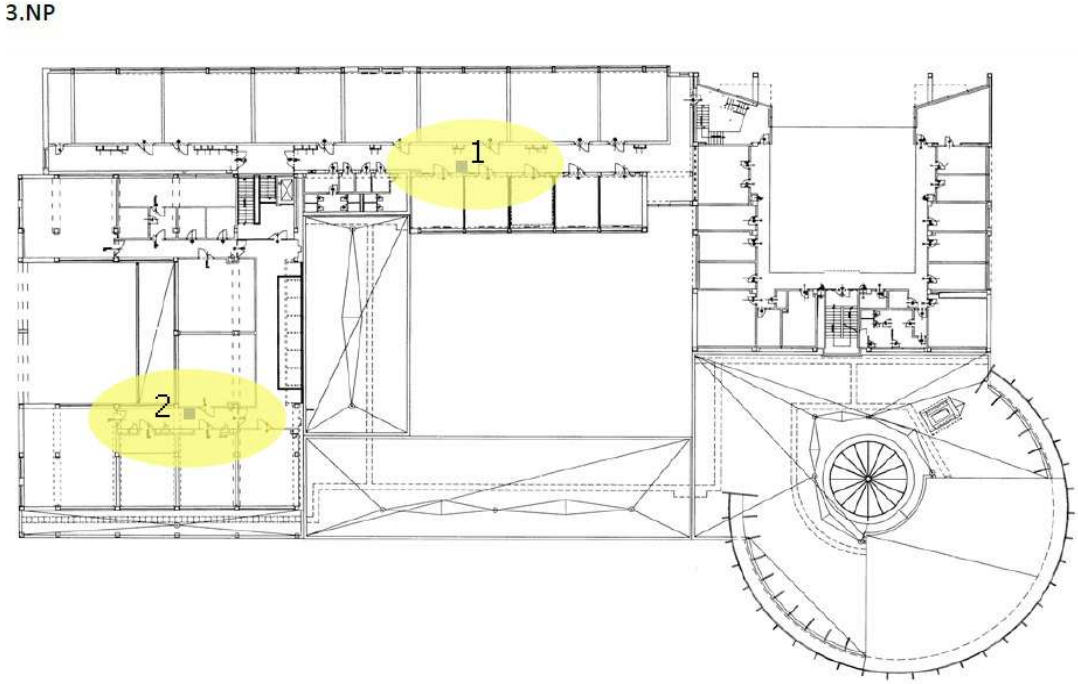
7.2.2 Výčet všech zachycených bezdrátových sítí v sektoru 2



Obr. 25: Sítě na podlaží 2 v sektoru 2

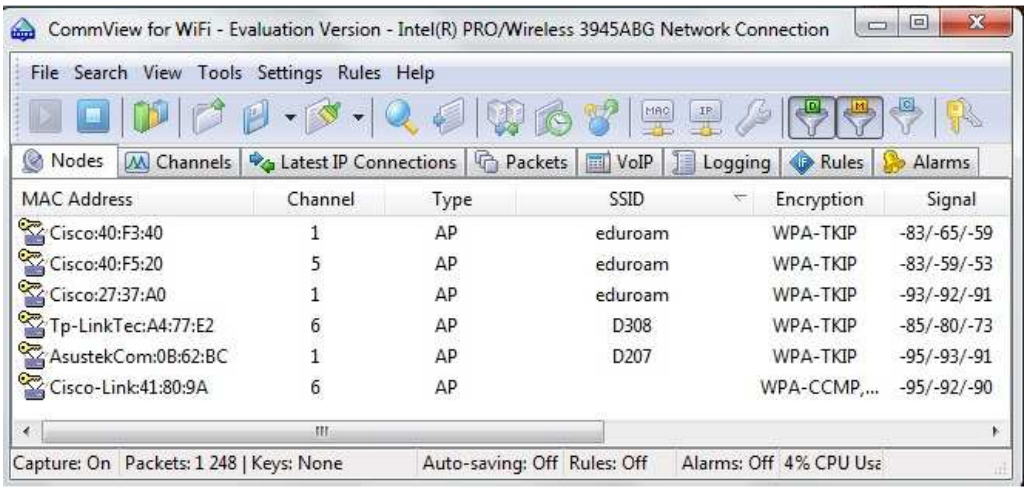
7.3 Třetí podlaží budovy U5

Na tomto podlaží se sice viditelně nalézají dva určené AP pro připojení do sítě eduroam, nicméně studenty jsou využívány jen minimálně. Jen v případě výskytu v laboratořích nebo na chodbě před nimi, vyznačených na Obr. 26.



Obr. 26: Třetí podlaží budovy U5

7.3.1 Výčet všech zachycených bezdrátových sítí v sektoru 1



Obr. 27: Sítě na podlaží 3 v sektoru 1

7.3.2 Výčet všech zachycených bezdrátových sítí v sektoru 2

Obr. 28: Sítě na podlaží 3 v sektoru 2

Jak lze vidět, toto podlaží je pokryto nejmenším počtem bezdrátových sítí a je zde i nižší počet AP k síti eduroam. Dá se to očekávat i z důvodu z důvodu prakticky nulového výskytu studentů, kromě návštěv laboratoří.

8 MAXIMÁLNÍ DATOVÉ PROPUSTNOSTI

Tato kapitola se zabývá proměřením datové propustnosti v jednotlivých podlažích a místech určených pro studenty k připojení k internetu. Měření probíhalo ve dvou časových obdobích, první série večer, když ve škole nebyli prakticky žádní studenti připojení k bezdrátové síti, a druhé během všedního dne za plného provozu, pouze ale v těch sektorech, kde se obvykle nacházejí studenti využívající bezdrátovou síť. Proměření datových propustností jsem realizoval pomocí stránky http://www.speedtest.net/, díky které jsem byl schopen změřit rychlosti stahování dat, odesílání dat a odezvy. Pro eliminaci chyb bylo každé měření prováděno pětkrát. Naměřené hodnoty byly zprůměrovány a ty poté sloužily jako podklad pro vytvoření srovnávajících grafů.

8.1 Datové propustnosti změřené na prvním podlaží bez zátěže

Tab. 1: Sektor 1

Download [Mb/s]	Upload [Mb/s]	Ping [ms]
18,81	18,79	5
17,12	18,59	5
16,62	18,45	5
16,29	18,94	5
16,36	18,91	5
17,04	18,736	5

Tab. 2: Sektor 2

Download [Mb/s]	Upload [Mb/s]	Ping [ms]
20,22	19,21	5
18,38	19,35	5
18,71	18,28	5
18,92	19,39	5
17,36	19,46	5
18,718	19,138	5

Tab. 3: Sektor 3

Download [Mb/s]	Upload [Mb/s]	Ping [ms]
17,66	18,69	5
16,86	18,93	5
16,77	19,84	5
18,9	19,79	5
19,16	19,75	5
17,87	19,4	5

8.2 Datové propustnosti změřené na prvním podlaží při zátěži

Tab. 4: Sektor 1

Download [Mb/s]	Upload [Mb/s]	Ping [ms]
17,63	18,63	5
17,22	18,45	5
17,12	17,2	5
16,12	17,31	5
16,01	16,78	5
16,82	17,674	5

Tab. 5: Sektor 2

Download [Mb/s]	Upload [Mb/s]	Ping [ms]
12,89	12,73	5
12,93	12,95	5
12,31	12,11	5
11,86	11,32	5
12,02	11,92	5
12,402	12,206	5

8.3 Datové propustnosti změřené na druhém podlaží bez zátěže

Tab. 6: Sektor 1

Download [Mb/s]	Upload [Mb/s]	Ping [ms]
15,75	15,25	5
16,45	15,27	5
16,47	15,3	5
16,17	15,18	5
16,71	15,16	5
16,31	15,232	5

Tab. 7: Sektor 2

Download [Mb/s]	Upload [Mb/s]	Ping [ms]
12,58	12,05	5
13,61	12,8	5
13,58	12,39	5
13,5	12,09	5
13,71	12,27	5
13,396	12,32	5

8.4 Datové propustnosti změřené na druhém podlaží při zátěži

Tab. 8: Sektor 1

Download [Mb/s]	Upload [Mb/s]	Ping [ms]
15,93	15,21	5
15,21	15,29	5
16,2	15,67	5
16,01	14,32	5
15,89	14,98	5
15,848	15,094	5

8.5 Datové propustnosti změřené na třetím podlaží

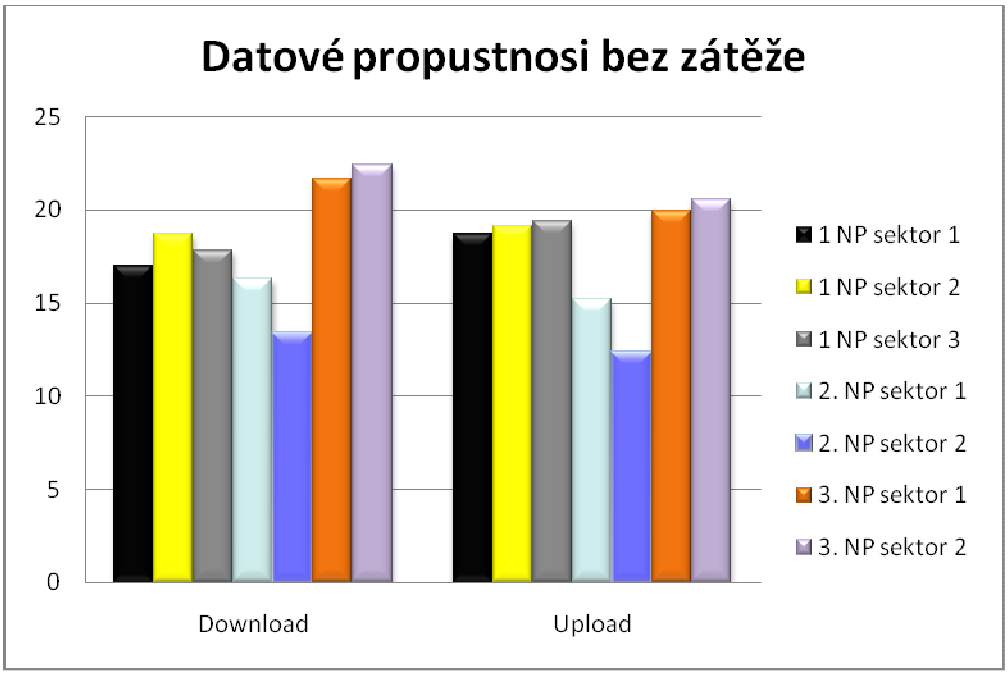
Tab. 9: Sektor 1

Download [Mb/s]	Upload [Mb/s]	Ping [ms]
21,85	19,98	5
21,67	19,89	5
21,83	19,9	5
21,81	19,94	5
21,46	20,01	5
21,724	19,944	5

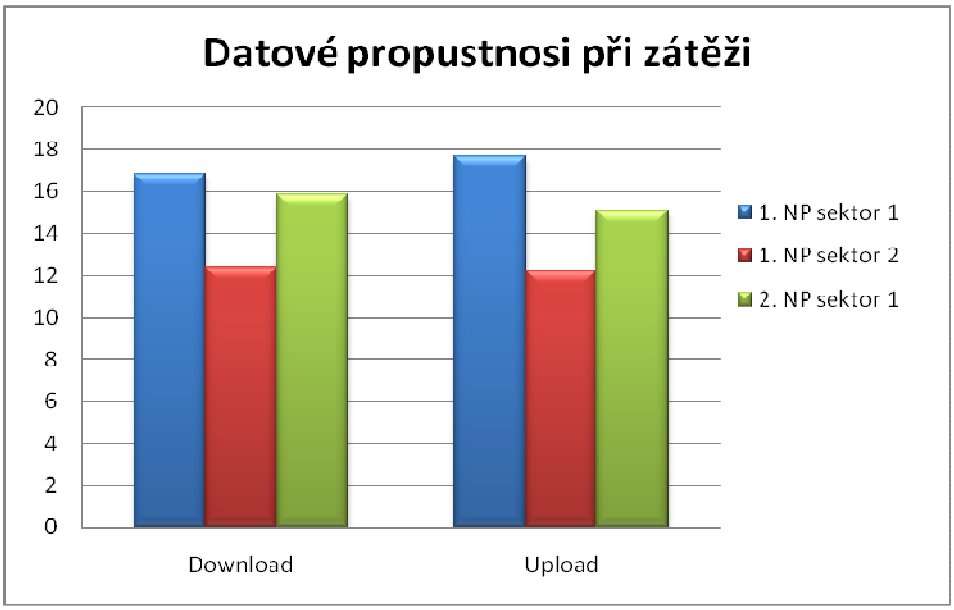
Tab. 10: Sektor 2

Download [Mb/s]	Upload [Mb/s]	Ping [ms]
22,59	20,89	5
22,41	20,52	5
22,47	20,58	5
22,42	20,39	5
22,53	20,59	5
22,484	20,594	5

8.6 Srovnání datových propustností v daných částech budovy U5



Obr. 29: Graf datové propustnosti bez zátěže



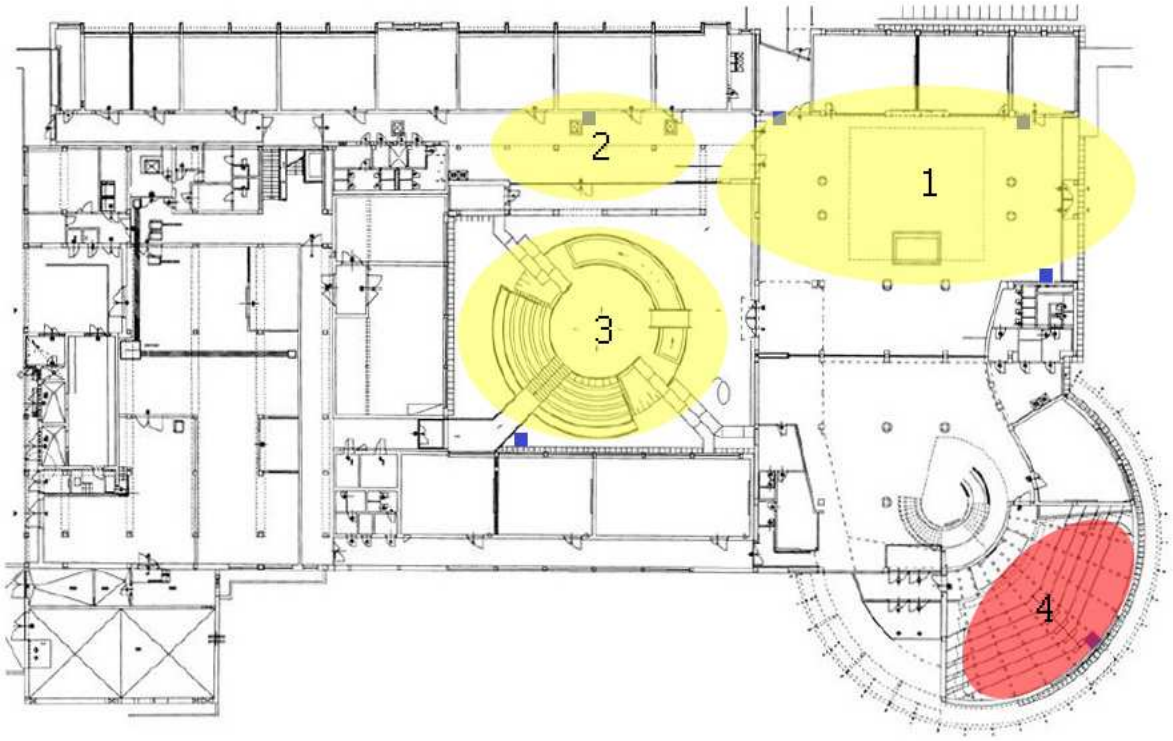
Obr. 30: Graf datové propustnosti při zátěži

Ve výše uvedených grafech lze vidět rozdílnost naměřených maximálních datových propustností v různých částech budovy U5. Obr. 29 zobrazuje datové propustnosti naměřené v místech určené pro přístup do sítě eduroam při připojení minimálního počtu uživatelů. Z grafu je zřejmé, že maximální datová propustnost byla naměřena v třetím podlaží sektoru dvě, viz Obr. 26. Naopak minimální datová propustnost byla naměřena

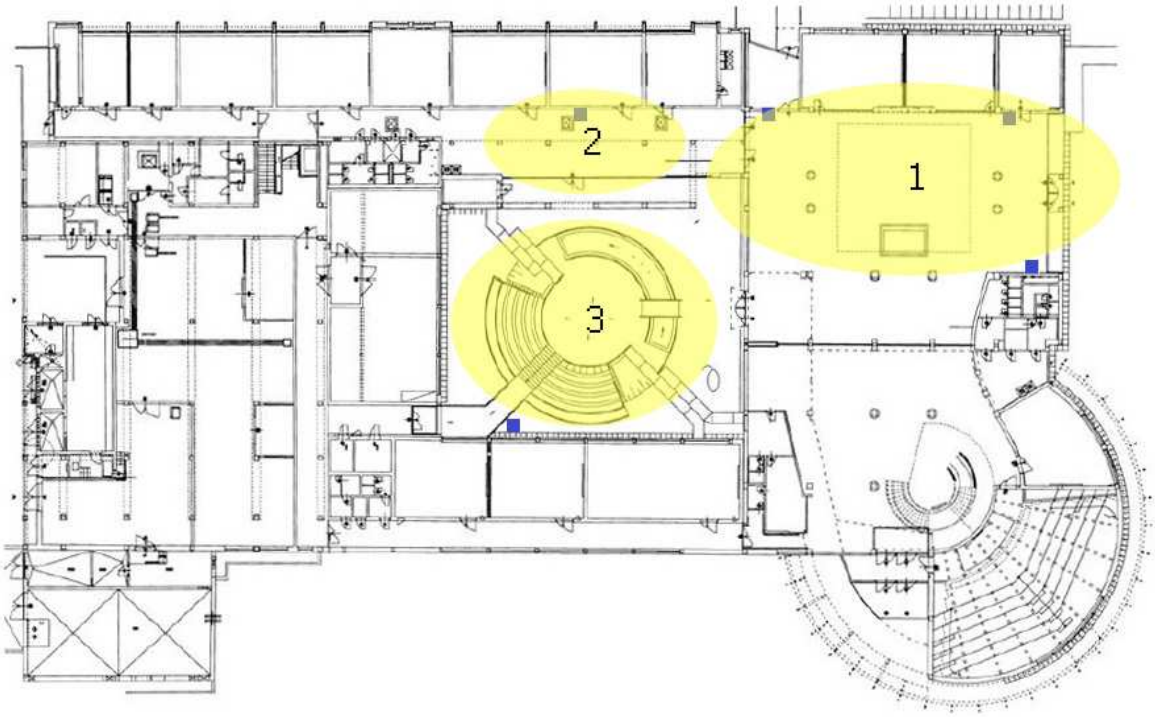
v druhém podlaží sektoru dvě, viz Obr. 23. Další graf, Obr. 30, zobrazuje naměřené datové propustnosti propustností, které jsem získal v místech určených pro přístup do sítě eduroam při plném počtu uživatelů. Zahrnuta jsou zde jen ta místa, kde je častý výskyt uživatelů, což jsou sektory jedna a dva v prvním podlaží a sektor jedna v podlaží druhém. Z grafu je patrné, že maximální datová propustnost byla naměřena v prvním podlaží sektoru jedna a minimální v sektoru dva podlaží prvního.

9 NÁVRH ZMĚN V UMÍSTĚNÍ AP V BUDOVĚ U5

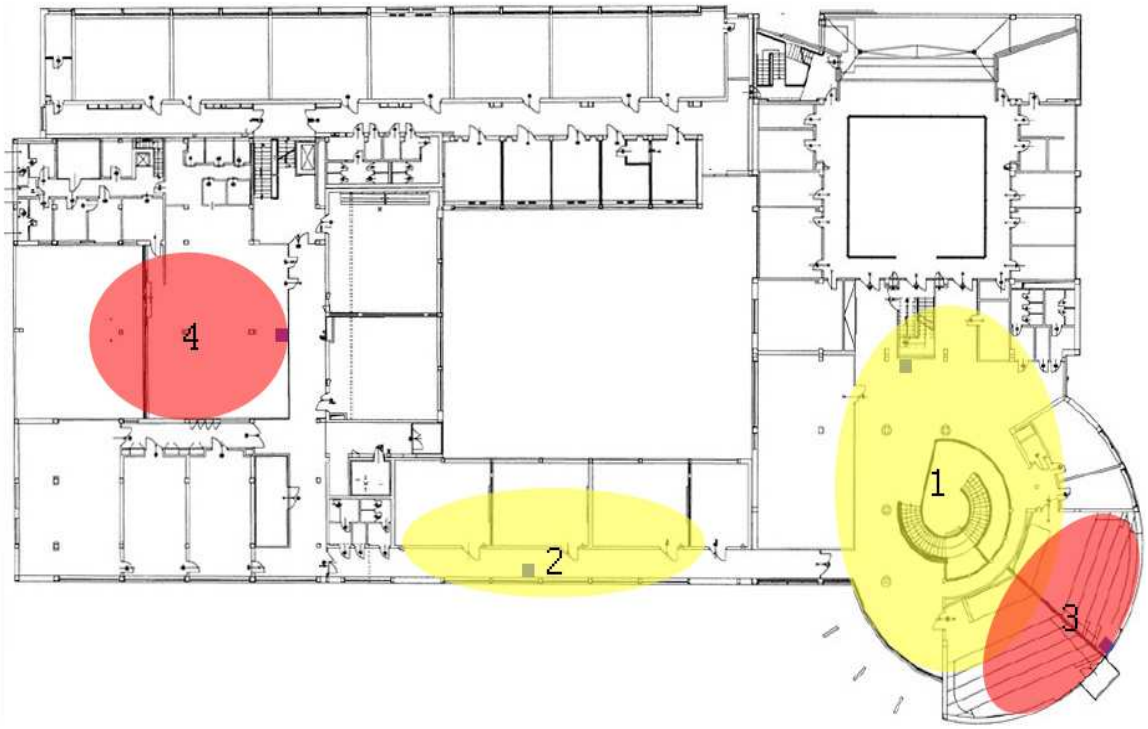
V kapitole číslo 7 nazvané Analýza pokrytí budovy U5 bezdrátovými sítěmi bylo provedeno zmapování rozmístění jednotlivých AP sloužící k připojení do sítě eduroam. Dále také i míra pokrytí signálem jednotlivých sektorů, které lze vidět na



Obr. 31: Návrh rozšíření bezdrátové sítě v prvním podlaží



Obr. 19, Obr. 23, Obr. 26. Musím konstatovat, že na prvním podlaží sektory 1 a 2 a na druhém podlaží sektor 1 jsou prakticky denně v značné míře vytíženy studenty, zatímco ostatní sektory jsou využívány opravdu minimálně, hlavně na třetím podlaží je využití skoro nulové. Co se týče návrhu na změny v umístění AP, došel jsem k závěru, že by bylo vhodné rozšířit pokrytí signálem na obě auly, kde je velikost signálu minimální a připojení je velice nestabilní, nebo se úplně nejde připojit. V úvahu by připadala také oblast menzy. Jedná se sice o místo určené ke stravování, ale domnívám se, že zde mnoho studentů tráví dost času před obědem i během něj a postrádají možnost připojení k bezdrátové síti. Následující rozšiřující návrh rozmístění AP je vyobrazen na obrázcích Obr. 31, Obr. 32 červenou barvou.



Obr. 32: Návrh rozšíření bezdrátové sítě v druhém podlaží

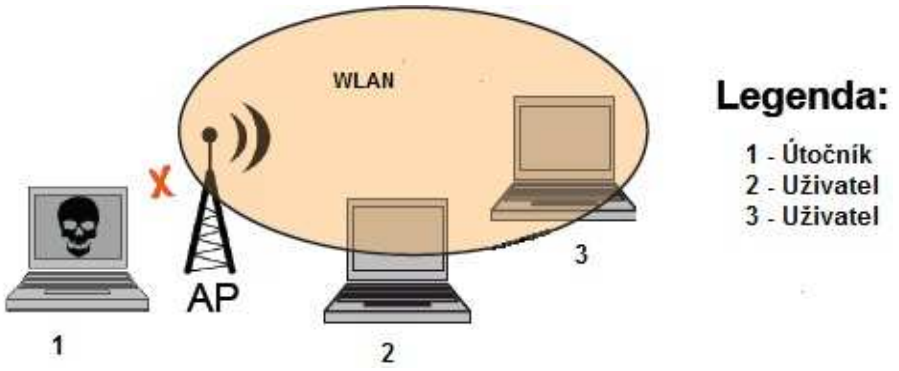
Je to však pouze návrh pro rozšíření pokrytí bezdrátové sítě eduroam na třech místech fakulty díky kterému by byli schopni studenti využívat bezdrátové připojení na více místech. Je jen na posouzení, zda by to mělo určitý přínos.

10 NÁVRH ALTERNATIVNÍHO ZABEZPEČENÍ BEZDRÁTOVÉ SÍTĚ V AREÁLU U5

Jak již víme, sítě standardu 802.11, patří do skupiny, ve kterých je přístup k informacím z pohledu nepovolené osoby velmi jednoduchý. Nejčastějším terčem útoků je pro svou dostupnost, může se jednat o útoky ze strany zaměstnanců, nebo i cizí osoby, která má za cíl získat citlivé informace. Mnohdy je tato snaha o průnik do bezdrátové sítě nedetekovatelná. Dále následuje několik bezpečnostních opatření, která by přispěla k zvýšení bezpečnosti bezdrátové sítě v budově U5, při absenci dosavadního zabezpečení roamingovým systémem eduroam, jež byl popsán v teoretické části.

10.1 Omezení dosahu sítě

To lze realizovat dvěma prvky, prvním je použití směrových antén, které jsou schopny určit tvar vyzařovaného diagramu. Vhodnou volbou této antény jsme schopni omezit pokrytí bezdrátové sítě na požadovanou oblast. Druhým prvkem je korekce vyzařovaného výkonu P_{max}, který je stanoven ČTÚ v pásmu ISM na 100mW. Proto lze tento výkon regulovat v intervalu <0,100> mW.



Obr. 33: Omezení dosahu WLAN

Útočník však může být vybaven citlivou směrovou anténou a i přes toto opatření je schopen odposlouchávat provoz na síti. Proto je potřeba rozšířit zabezpečení sítě o další prvky.

10.2 Využití zabezpečovacího protokolu

Síť 802.11 leze zabezpečit třemi různými šifrovacími protokoly, jejichž podstata byla rozebrána v teoretické části, zde je uvedeno porovnání bezpečnosti jednotlivých protokolů.

Metoda	Autentizace	Síla šifry	Použitelnost pro menší sítě	Použitelnost pro větší sítě
WEP	Žádná	Slabá (RC4)	Nevhodná	Nevhodná
WPA s PSK	Slabá (PSK)	Dobrá (TKIP)	Dobrá	Nevhodná
WPA2 s PSK	Slabá (PSK)	Výborná (CCMP)	Velmi dobrá	Nevhodná
WPA	Dobrá (IEEE 802.1x)	Dobrá (TKIP)	Dobrá	Velmi dobrá
WPA2	Dobrá (IEEE 802.1x)	Výborná (CCMP)	Výborná	Výborná

Obr. 34: Srovnání bezpečnostních protokolů [4]

Z výše uvedeného Obr. 34: Srovnání bezpečnostních protokolů [4] je patrné, že nejvhodnějším typem bezpečnostního protokolu je využití WPA2, který poskytuje nejvyšší míru zabezpečení ze všech zmíněných a také se je vhodný pro použití pro rozsáhlejší sítě.

10.3 Volba silného hesla

Tento prvek tvoří nejzákladnější část a závisí na něm míra zabezpečení celé sítě. Je nutné, uchovávat heslo sloužící k přístupu do bezdrátové sítě utajené a vyvarovat se jeho umístění na lehko dostupných místech. Zapotřebí je, aby nebylo možné jej rozluštit slovníkovým útokem více teoretická část. Doporučuje se využívat velké a malé písmena, číslice a speciální znaky za účelem větší odolnosti vůči rozluštění. Důležité je heslo v pravidelných intervalech měnit, např. pro náš případ by bylo vhodné jej zasílat studentům v intervalu jednoho měsíce na ověřený studentský email v šifrované podobě.

10.4 Volba autentizace

Typ autentizace v sítích 802.11 závisí na druhu použitého zabezpečovacího protokolu. Mnou zvolený protokol WPA2 poskytuje autentizaci uživatele dvojím způsobem. Prvním je autentizace PSK, která je v dnešní době nejvíce využívána a závisí na síle používaného hesla. Druhý způsob autentizace je 802.11x, který je vhodný pro rozsáhlé sítě s výskytem mnoha uživatelů. Informace potřebné ke vstupu do sítě jsou uložená na autentizačním serveru a ne v AP. Zabezpečení je poté dáno více parametry uživatele.

11 TIPY K NASTAVENI PŘIPOJENÍ BEZDRÁTOVÉ SÍTĚ

Místy mohou nastat různé problémy při užívání sítě eduroam, jejíž příčiny byly popsány v teoretické části. Nejčastěji to jsou však problémy spjaté s častým odpojováním a připojováním. Proto je v této kapitole uvedeno pár tipů k vyvarování se těmto potížím.

11.1 Řešení problému

- Aktualizace ovladače bezdrátového adaptéru,
- nastavení úsporného režimu bezdrátového adaptéru,
- nastavení agresivity roamingu (pouze pro Wi-Fi adaptéry Intel). [10]

11.1.1 Aktualizace ovladače bezdrátového adaptéru

K bezproblémovému provozu Wi-Fi je doporučováno mít nainstalováno nejnovější verzi ovladače bezdrátového adaptéru, které postupem času opravují nedostatky u těchto adaptérů. Je tedy doporučeno ovladače několik let aktualizovat na novější verzi, stávající verze lze zjistit v nabídce síťové adaptéry v záložce driver. Ve většině notebooků jsou ovladače od firmy Intel nebo Atheros.

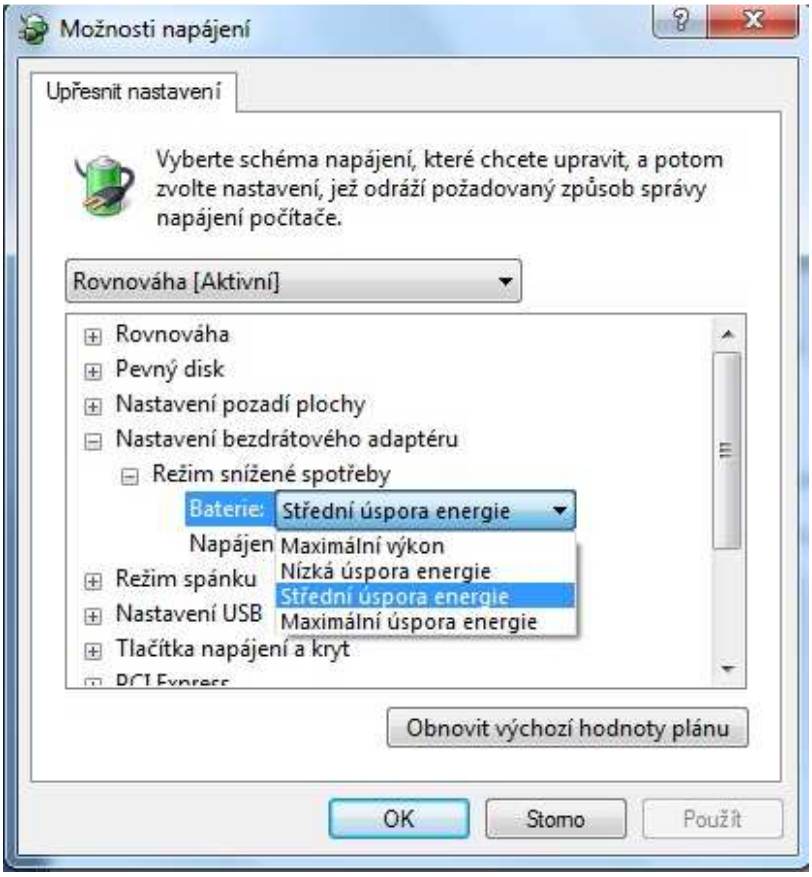
Adresa pro aktualizaci ovladačů:

- Intel – http://downloadcenter.intel.com/
- Atheros - http://www.atheros.cz/

11.1.2 Nastavení úsporného režimu bezdrátového adaptéru

Mnohým uživatelům ve škole běží notebook na baterii, který v rámci úspory energie snižuje frekvenci procesoru, sníží jas displeje, omezuje výkon bezdrátového adaptéru. Má-li uživatel nastaven úsporný režim provozu, může dojít k situaci, kdy dojde k snížení vysílacího výkonu adaptéru, nebo při delší neaktivitě dokonce k odpojení adaptéru od sítě. To vše lze konfigurovat pomocí nastavení úsporných režimů.

Návod: Při kliknutí na ikonu baterie v dolní liště -> Možnosti napájení -> Změnit nastavení schématu -> Změnit pokročilé nastavení napájení -> Nastavení bezdrátového adaptéru.



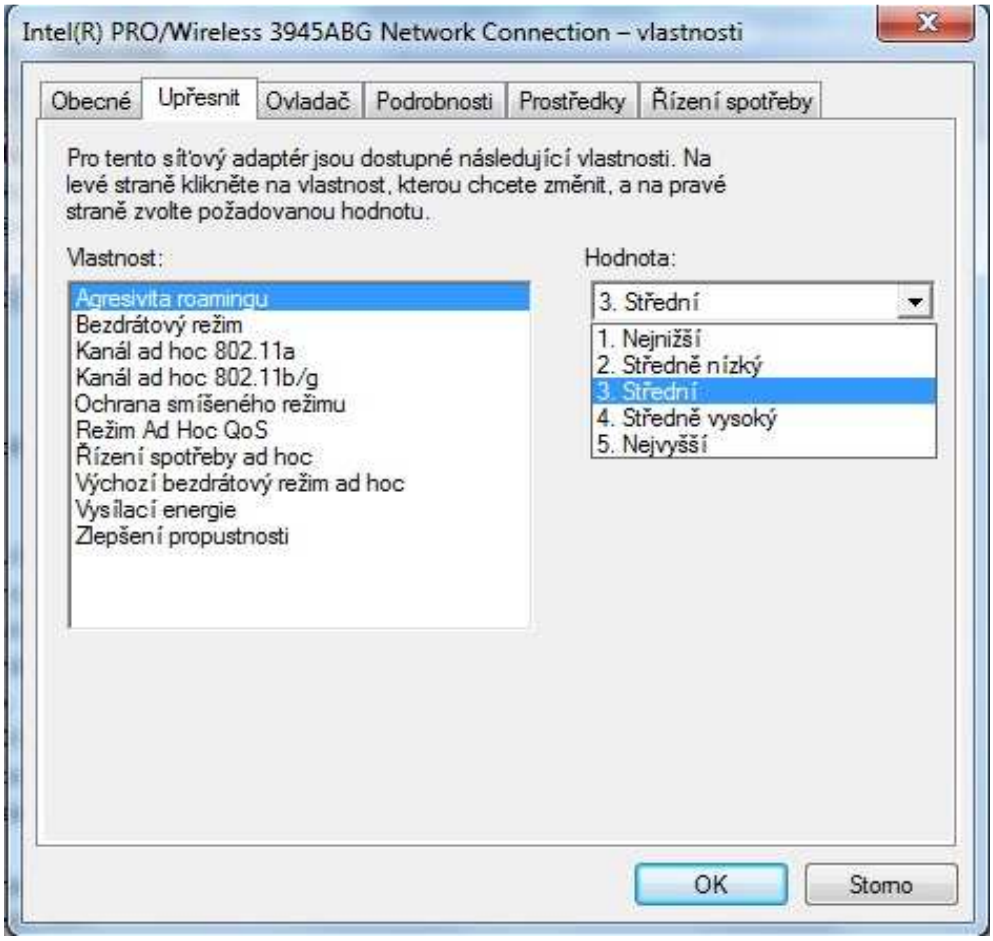
Obr. 35: Změna nastavení napájení bezdrátového adaptéru

11.1.3 Nastavení agresivity roamingu (pouze pro wi-fi adaptéry Intel)

V některých případech lze samovolnému odpojování a připojování zabránit nastavením snížení agresivity roamingu. Toto nastavení dává pokyn bezdrátovému adaptéru, aby bezdrátový adaptér chvíli setrval připojen AP i s menším signálem. Pokud ale uživatel často využívá připojení v pohybu, například za chůze, je doporučeno tento parametr nechat na původní hodnotě.

Návod: Správce zařízení -> Síťové adaptéry -> Vlastnosti -> Upřesnit -> Agresivita roamingu

Zde lze zvolit požadovanou míru agresivity roamingu dle potřeby uživatele. Avšak při nejnižší hodnotě může nastat problém, že adaptér nepřeroamuje na jiný AP, i když by už dávno měl. Poté jen zbývá vypnout a zapnout bezdrátový adaptér.



Obr. 36: Změna nastavení agresivity roamingu

ZÁVĚR

Tato bakalářská práce byla zaměřena na celkovou analýzu bezdrátové sítě nacházející se v areálu U5 Univerzity Tomáše Bati Fakulty aplikované informatiky.

V teoretické části byly podrobně přiblíženy základní principy fungování bezdrátových sítí, co se týče jejich provozu, způsoby zabezpečení a možné druhy útoku na tyto sítě. Dále byla představena činnost Wi-Fi aliance, která se zaměřuje na certifikaci zařízení, sloužící pro realizaci bezdrátové sítě. Také bylo provedeno detailní vysvětlení problematiky celosvětového roamingového systému eduroam, který Fakulta aplikované informatiky využívá pro účely připojení studentů k síti Internet.

Praktická část byla nejvíce zaměřena na zmapování výskytu AP, které jsou v budově U5 instalovány za účelem pokrytí bezdrátovou sítí. Ze získaných poznatků byla vytvořena mapa pokrytí, kde se lze k bezdrátové síti připojit v jednotlivých částech budovy. Následně bylo provedeno proměření maximálních datových propustností v jednotlivých sektorech areálu za běžného provozu i v době bez připojených uživatelů, tato naměřená data sloužila k porovnání rychlosti stahování a odesílání dat v jednotlivých sektorech. V další kapitole byl vypracován návrh na změny, v podobě rozšíření pokrytí sítě v dalších třech sektorech. Poslední kapitola praktické části se zabývala alternativním návrhem zabezpečení bezdrátové sítě, za předpokladu, že by zde nebyl instalován roamingový systém eduroam, který úlohu zabezpečení plní dobře. Tento návrh by byl dle mého názoru pro účely zabezpečení budovy U5 plně dostačující.

V závěru bylo uvedeno pár rad pro uživatele, které mají za úkol zlepšit plynulý chod sítě eduroam a vyvarovat se případným nedostatkům v podobě občasných výpadků.

CONCLUSION

This bachelor thesis has been focused on analysis of wireless network in areal of U5 at Tomas Bata University at Faculty of applied informatics.

In theoretical part I described basic principles of working of wireless networks, their operating, security and possible attacks on these networks. I also described function of Wi-Fi alliance, which is focused on certification of devices that are used for establishing of wireless network. I also explained function of worldwide roaming system eduoram, which Faculty of applied informatics uses for the connection of students on the internet.

In practical part I focused on mapping of AP, which are, in building U5, installed for covering of wireless network. From the gained information I created a map of cover, where is possibility to have access on the internet from different parts of building. I measured maximal data transmission in various parts of areal during working day and also in the time, when nobody was connected on the network. The data that I gained were used for comparism of download speed and upload speed in different parts of areal. In the next chapter I made a suggestion of new wireless cover in the next three sectors of building. The last chapter of practical part is focused on alternative suggestion of wireless network security, in case that roaming system Eduoram, which provides the security, would not be installed. In my opinion, my suggestion would be effective and the network would be secured. In the conclusion, I mentioned some advices, for users, which should improve the function of Eduoram network and make the wireless network more stable.

SEZNAM POUŽITÉ LITERATURY

Monografické publikace:

[1] BARKEN, Lee. *Wi-Fi : Jak zabezpečit bezdrátovou síť*. Vyd. 1. Brno : Computer Press, 2004. 174 s. ISBN 8025103463.

[2] HAROLD, Davis. *Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě.* 1. vyd. Praha : Grada, 2006. 334 s. ISBN 8024714213.

[3] KÖHRE, Thomas. *Stavíme si bezdrátovou síť Wi-fi.* 1. vyd. Brno : Computer Press, 2004. 295 s. ISBN 8025103919.

[4] NEČAS, Ondřej. *Možnosti zabezpečení bezdrátové sítě*. Brno, 2009. 72 s. Bakalářská práce. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ Fakulta elektrotechniky a komunikačních technologií.

[5] PECHAČ , Pavel. *Šíření vln v zástavbě.* 1. vyd. : BEN-Technická literatura, 2006. 108 s. ISBN 80-7300-186-1.

[6] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace*. 1. vyd. Brno : CP Books, 2005. 179 s. ISBN 80-251-0791-4.

[7] THOMAS, Thomas M. *Zabezpečení počítačových sítí*. 1. vyd. Brno : Computer Press, 2005. 344 s. ISBN 80-251-0417-6.

[8] ZANDL, Patrik. *Bezdrátové sítě WiFi Praktický průvodce*. 1. vyd. Brno : Computer Press, 2003. 189 s. ISBN 80-7226-632-2.

WWW stránka – elektronická monografie:

[9] *Eduroam.cz* [online]. 2009, 2009-12-02 [cit. 2011-04-18]. Dostupné z WWW: <http://eduroam.cz/doku.php?id=>.

[10] PAVLÍČEK, Luboš. *Eduroam Oddělení síťové infrastruktury Vysoké školy ekonomické v Praze* [online]. 2010, 2010-12-10 [cit. 2011-05-06]. Časté odpojování a připojování do sítě. Dostupné z WWW: <http://osi.vse.cz/eduroam/tipy-k-nastaveni-wifi/caste-odpojovani-a-pripojovani-do-site/>.

[11] STEJSKAL, Petr. *Bezdrátové sítě - Wi-Fi* [online]. 2003 [cit. 2011-04-18]. Bezdrátové sítě-Wi-Fi-DSSS. Dostupné z WWW: <http://www.kiv.zcu.cz/~simekm/vyuka/pd/zapocty-2003/wi-fi/index.php?id=6>.

[12] *Wi-Fi Alliance* [online]. 2011 [cit. 2011-04-18]. Wi-Fi Alliance: Wi-Fi CERTIFIED™ Products. Dostupné z WWW: <http://www.wi-fi.org/certified_products.php>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAI	Autentication and authorization infrastructure.
AP	Access point.
BSS	Basic Sevice Set.
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance.
ČTÚ	Český telekomunikační úřad
ESS	Extended Service Set.
IBSS	Independent Basic Service Set.
IEEE	The Institute of Electrical and Electronics Engineers.
ISM	Industrial, Scientific and Medical.
MAC	Media Access Control.
MIC	Message Integrity Code.
NREN	National research and education network
RADIUS	Remote Autentication Dial In User ServiceRSN
RSN	Robust Security Network.
RSNA	Robust Security Network Association.
RTS/CTS	Request to Send / Clear to Send.
SSID	Service Set IDentifier.
VPN	Virtual Private Network.
WEP	Wired Equivalent Privacy.
Wi–Fi	Wireless fidelity.
WLAN	Wireless local area network.
WPA	Wi-Fi Protected Access.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK