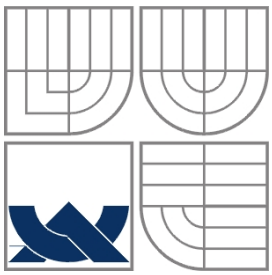
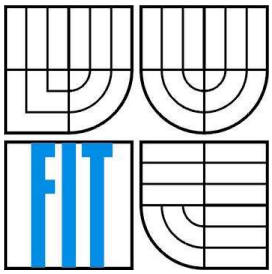


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

KONFIGURACE A ANALÝZA RŮZNÝCH TYPŮ ZAPOJENÍ BEZDRÁTOVÝCH SÍTÍ 802.11

CONFIGURATION AND ANALYSIS OF DIFFERENT KINDS OF WIRELESS NETWORKS 802.11

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE
AUTHOR

LUKÁŠ HARVÁNEK

VEDOUCÍ PRÁCE
SUPERVISOR

ING. PETR MATOUŠEK, PH.D.

BRNO 2007

Zadání bakalářské práce/4988/2006/xharva00

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav informačních systémů Akademický rok 2006/2007

Zadání bakalářské práce

Řešitel: **Harvánek Lukáš**
Obor: Informační technologie
Téma: **Konfigurace a analýza různých typů zapojení bezdrátových sítí 802.11**
Kategorie: Počítačové sítě

Pokyny:

1. Prostudujte různé typy zapojení WiFi sítí - ad-hoc, AP mode, bridge mode.
2. Vytvořte testová zapojení těchto sítí.
3. Pomocí analyzátoru Airmagnet Analyser proveďte analýzu nastavení těchto sítí, určete parametry sítí (kanály, rychlost, propustnost, zabezpečení)
4. Pro jednotlivé typy sítí vyzkoušejte vytváření mapy WiFi sítí pomocí Airmagnet Surveyor.

Literatura:

- Jim Geier: Wireless Networks, first-step, Cisco 2005
- Alexander Bruce: 802.11 Wireless Network Site Surveying and Installation

Při obhajobě semestrální části projektu je požadováno:

- body 1-3

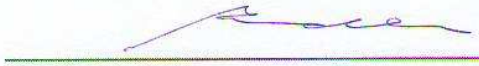
Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním paměťovém médiu (disketa, CD-ROM), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Matoušek Petr, Ing., Ph.D.**, UIFS FIT VUT
Datum zadání: 1. listopadu 2006
Datum odevzdání: 15. května 2007

L.S.



doc. Ing. Jaroslav Zendulka, CSc.
vedoucí ústavu

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami

1. Pan

Jméno a příjmení: **Lukáš Harvánek**
Id studenta: 88498
Bytem: Bobrůvka 17, 592 55 Bobrová
Narozen: 05. 07. 1984, Nové Město na Moravě
(dále jen "autor")

a

2. Vysoké učení technické v Brně

Fakulta informačních technologií
se sídlem Božetěchova 2/1, 612 66 Brno, IČO 00216305
jejímž jménem jedná na základě písemného pověření děkanem fakulty:

.....
(dále jen "nabyvatel")

Článek 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
bakalářská práce

Název VŠKP: Konfigurace a analýza různých typů zapojení bezdrátových sítí 802.11
Vedoucí/školitel VŠKP: Matoušek Petr, Ing., Ph.D.
Ústav: Ústav informačních systémů
Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v:

tištěné formě počet exemplářů: 1
elektronické formě počet exemplářů: 2 (1 ve skladu dokumentů, 1 na CD)

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizování výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti:
   - ☐ ihned po uzavření této smlouvy
   - ☐ 1 rok po uzavření této smlouvy
   - ☐ 3 roky po uzavření této smlouvy
   - ☐ 5 let po uzavření této smlouvy
   - ☒ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: .....

....

Nabyvatel Autor

Abstrakt

Tato bakalářská práce se zabývá různými typy zapojení bezdrátových sítí. Popisuje jejich možnosti využití v praxi a jejich analýzu pomocí monitorovacího zařízení Airmagnet Laptop Analyser. Dále je zde zkoumána fakultní Wi-Fi síť a vytvořena mapa pokrytí. Práce obsahuje také problematiku rozsáhlých Wi-Fi sítí – Mesh sítě, roaming a hodnotu Quality of Service (Qos).

Klíčová slova

802.11, Bezdrátové sítě, WiFi, Konfigurace, Analýza, Mesh sítě, Kvalita služby.

Abstract

This Bachelor's thesis discusses parametres of wireless networks and concentrates on questions of their security, monitoring and analysis. It describes how to configure and analyse them with monitoring device Airmagnet Laptop Analyser. As the case study we analyze the wirelless network at FIT. We create a map of wifi covering of the buildings. This work also include problems of large Wi-Fi nets – mesh networks, roaming and quality of service (QoS).

Keywords

802.11, Wireless networks, WiFi, Configuration, Analyse, Mesh networks, Quality of Servise.

Citace

Lukáš Harvánek: Konfigurace a analýza různých typů zapojení bezdrátových sítí 802.11, bakalářská práce, Brno, FIT VUT v Brně, 2007

Konfigurace a analýza různých typů zapojení bezdrátových sítí 802.11

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Ing. Petra Matouška, Ph.D.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

……
Lukáš Harvánek
14.5. 2007

Poděkování

Tímto bych chtěl poděkovat Ing. Petru Matouškovi, Ph.D. za odborné vedení, užitečné rady a konzultace.

Obsah

1 Úvod

Bezdrátová technologie dle normy 802.11, která je často označovaná zkratkou Wi-Fi (Wireless Fidelity) je dalším stupněm ve vývoji telekomunikací. Fixní spoje dostávají stále méně prostoru a důraz je kladen především na jednoduchost zapojení a mobilitu, proto jsem se rozhodl vypracovat tuto práci. V dnešní době se pro fyzickou přenosovou vrstvu Wi-Fi sítí nejčastěji používá elektromagnetické rádiové vlnění o frekvencích 2,4 GHz a 5 - 6 GHz. Uvedené frekvence pracují v tzv. bezlicenčním pásmu, z čehož vyplývá, že svou bezdrátovou síť si může postavit prakticky každý, aniž by musel žádat o povolení. Při stavbě bezdrátové sítě je nutné dodržet určité stanovy vydané telekomunikačním úřadem.

Výhody bezdrátové technologie jsou jednoznačné – mobilita, jednoduchá a levná realizace a možnost všesměrově vysílat data. Vzniká zde i několik problémů při realizaci sítě. Při frekvenci 2,4 GHz je délka vlny asi 12,5 centimetrů, což znamená, že vlnění se odrazí od jakékoliv překážky větší než 12,5 cm (délka vlny). Vlnění při této frekvenci je pohlcováno vodou a dalšími organickými látkami, jako například dřevo, listnaté stromy. Vyšší frekvence (5 – 6 GHz) mají délku vlny cca 6 cm. Tento rozdíl přinesl určité zlepšení. Není pohlcováno vodou v takové míře jako 2,4 GHz a dovoluje větší přenosové rychlosti. Šíří se přímočařeji oproti vlnám s nižší frekvencí. Při návrhu bezdrátové sítě je nutné mít na paměti klady a zápory daného zapojení. V neposlední řadě je velkým problémem bezdrátových sítí bezpečnost. V oblasti bezpečnosti se neustále vyvíjí nové možnosti zabezpečení, jak už samotného datového provozu, tak asociace s přístupovým bodem, nebo znemožnění odposlouchávání.

V této práci navazuji na bakalářskou práci Michala Weissgärbera z roku 2006 na téma Monitorování a analýza bezdrátových sítí 802.x, kde byla popsána řada základních principů bezdrátových sítí.

Cílem práce je popsat možnosti zapojení bezdrátových sítí a prozkoumat jejich vlastnosti. Na základě získaných informací sestavit doporučení pro nejlepší možné využití v praxi. Dalším cílem je zkoumat fakultní bezdrátovou síť, popsat její propustnost, dosah a další parametry. Prozkoumat vlastnosti pokročilých wifi sítí, popsat možnosti zabezpečení a kvality služeb.

V první kapitole se budeme zabývat jednotlivými typy zapojení Ad-hoc, AP mode, bridge mode. Zapojení budou představena na modelovém zapojení a po té analyzována. Na základě naměřených hodnot bude vytvořeno doporučení pro nejlepší využití. Další kapitola se bude věnovat fakultní síti na FIT. Síť bude analyzována, bude zkoumán její dosah, propustnost a také přesahy jiných sítí s možnými kolizemi. V poslední kapitole se budeme věnovat pokročilým Wi-Fi sítím. Bude zde popsáno zapojení mesh sítí, možnosti zabezpečení a kvalita služby.

2 Typy zapojení

V této kapitole si představíme ukázkové zapojení bezdrátových sítí. Postupně projdeme zapojení Ad-hoc, AP mode a bridge mode a budeme zjišťovat jejich vlastnosti a parametry.

Každá bezdrátová síť zapojená podle normy 802.11 používá stejné principy architektury. Jednoduše je lze rozdělit na dva typy sítí. Sítě s infrastrukturou a sítě bez infrastruktury. Mezi sítě bez infrastruktury patří zapojení Ad-Hoc. Toto zapojení bude popsáno v kapitole 2.1. Infrastrukturní sítě lze dále dělit na několik částí, které budou popsány níže.

Jednoduchým vodítkem, jak správně zařadit síť, je přístupový bod (Access point). Pokud je v síti obsažen přístupový bod, pak se jedná o síť s infrastrukturou.

2.1 Ad-Hoc sítě

Zapojení Ad-Hoc patří mezi sítě bez infrastruktury. Lze je označit za sítě peer-to-peer, tedy všichni jsou si rovni. Využívá se pro rychlé spojení bez použití kabelu. Jeho hlavní výhodou je snadná konfigurace a již zmíněná absence drátového spoje. Režim Ad-hoc slouží k propojení více klientských zařízení bez nutnosti přístupového bodu. V principu pak celá síť pracuje tak, že první spuštěný klient vytvoří jakýsi imaginární Access point, který pak řídí další komunikaci všech ostatních klientů, kteří však komunikují navzájem přímo, tj. bez toho jednoho "hlavního" klienta. Nevýhody jsou zjevné - při vypnutí "hlavního" počítače se na malý okamžik síť rozpadne, a to až do doby, než se funkce "hlavního" PC ujme další klient (většinou zcela náhodně).

Ad-hoc lze využít především uvnitř budov. Síť Ad-Hoc se nejlépe hodí pro domácnosti nebo kanceláře menších rozměrů, kde potřebujeme spojit menší počet počítačů. Dále můžeme bezdrátově sdílet soubory, internetovou přípojku a tisknout. Nevýhodou je, že všechny Wi-Fi zařízení musí být v rádiovém dosahu jeden druhého. Sítě Ad-hoc se tedy považují za opravdu sítě sestavené jednoduše a rychle v případě potřeby, když například potřebujete data přenést z jednoho notebooku na druhý, pro praktické a trvalé síťování se téměř nepoužívají.

Schopnost práce v Ad-hoc sítích musí být na většině zařízení aktivována v menu a protože se zařízení většinou připojují do sítí infrastrukturních a karta musí být zapnuta jen v jednom režimu, výrobci většinou nastavují infrastrukturní mód. Pokud je bezdrátová karta přepnuta do režimu Ad-hoc (novější karty se automaticky přepínají podle režimu, jakým disponuje protistrana), je třeba správně nastavit síť. V nastavení TCP/IP nastavit IP adresy lišící se až v D segmentu, tedy tak, aby první tři čísla byla stejná, například 192.168.1.1 pro první kartu a 192.168.1.2 pro kartu druhou. Stejně tak je nutno správně nastavit síťovou masku - například na 255.255.255.0. IP adresy nesmějí být shodné. Po tomto nastavení, pokud jsou oba počítače v „radiové dohledové vzdálenosti“, měly by schopny spolu komunikovat. Pro ověření komunikace lze použít např. příkaz ping a jako parametr cílovou IP adresu.

2.1.1 Modelové zapojení Ad-hoc

Pro modelové zapojení si představíme síť dvou notebooků. Tato síť je zapojena a nakonfigurována dle obrázku 2.1.1. Pro toto zapojení jsou nutné bezdrátové karty, které podporují Ad-hoc mód – klientské adaptéry. Pro běžné spojení uvnitř jedné místnosti postačuje anténa dodávaná s adaptérem.

Notebook 1:
IP Adresa: 192.168.1.1
Maska: 255.255.255.0
MAC: 00-E0-98-B7-B2-AB

Notebook 2:
IP Adresa: 192.168.1.2
Maska: 255.255.255.0
MAC: 00-90-96-29-FF-58

Obrázek 2.1.1. Modelové zapojení Ad-hoc

2.1.2 Analýza zapojení Ad-hoc

Analýza byla provedena pomocí karty Airmagnet Analyser. Počítače byly spojeny do lokální sítě a pro testování na nich byl spuštěn přenos souborů z jednoho na druhý a po té bylo vyzkoušeno hraní her po síti. Měření jsem prováděl několikrát pro odstranění náhodných chyb. Získaná data se pohybovala s drobnými odchylkami na stejných hodnotách.

Získané hodnoty:

SSID	adhoc
Kanál	6
Unicast rámců	99%
Broadcast rámců	1%
Datových rámců	56%
Kontrolních rámců	37%
CRC	7%
Typ rámce	dlouhý
Zabezpečení	WEP
Nedoručených rámců	23%
Protokol 802.11	b
Síla signálu	-49dB
Rámců 11Mbit	72%
Rámců 5,5Mbit	18%
Rámců 2Mbit	7%
Rámců 1 Mbit	3%
Průměr Ping	8ms

Z předcházející tabulky lze vyčíst, že přenosová režie (kontrolní a CRC rámce) zabírá velkou šířku pásma – celkem 44%. Úroveň signálu se pohybovala okolo -50 dB, což postačuje pro bezproblémové spojení. Velké procento nedoručených rámců (23%) poukazuje na nestabilitu spojení. Rozložení přenášených rámců na 11, 5.5, 2 a 1 Mbit ukazuje na výkyvy dosahovaných rychlostí. Průměrný ping 8ms značí latenci některých paketů, protože většina paketů měla čas 1ms.

2.1.3 Praktické možnosti využití

Sítě Ad-hoc se tedy považují za sítě sestavené jednoduše a rychle v případě potřeby, když například potřebujete data přenést z jednoho notebooku na druhý, pro praktické a trvalé síťování se téměř nepoužívají. Praktické zkoumání mě přivedlo k názoru, že Ad-hoc sítě jsou poměrně nestabilní. Objevují se zde velké latence paketů a velké výkyvy dosahovaných rychlostí. Proto bych toto zapojení doporučil pouze pro krátké a nutné spojení.

2.2 AP mode

AP mode patří mezi takzvané sítě s infrastrukturou. Součástí této sítě jsou přístupové body a klienti. Přístupové body jsou většinou samostatné jednotky s vlastním napájením, které v bezdrátové síti zastávají funkci ethernetového switche či HUBu. Často mají výstup na externí anténu a v naprosté většině případů jsou vybaveny konektorem RJ45 pro propojení se stávající 100/10 Mbps ethernetovou sítí. Kromě konektoru RJ45 se občas setkáme i s konektory USB či RS232, které však slouží pouze pro správu a konfiguraci přístupového bodu. U moderních přístupových bodů pak často najdeme i paralelní porty LPT či USB porty pro připojení a sdílení tiskáren, externích disků a webových kamer. Klientské adaptéry se nejčastěji vyrábějí v provedení PCMCIA, PCI nebo USB. Slouží pro připojení klientských stanic k přístupovému bodu, ale lze je propojit i navzájem.

Důležitý rozdíl mezi Ad-Hoc a infrastrukturní sítí je v dosahu. Jednotlivá koncová zařízení nemusí být v dosahu jeden druhého, ale stačí být v dosahu alespoň jednoho přístupového bodu a ten již komunikaci předá dále. Další nemalou výhodou je, že přístupový bod může sloužit i jako brána mezi kabelovou sítí LAN. Některé typy mají dokonce i zabudovaný router, či firewall. Pomocí roamingu se můžeme v sítích s více přístupovými body volně pohybovat a automaticky budeme připojeni k nejbližšímu bodu bez ztráty připojení.

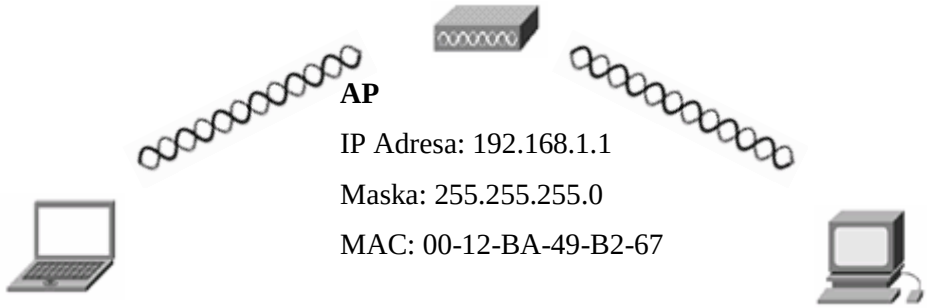
Komunikace probíhá vždy mezi klientem a přístupovým bodem, který směruje data k cíli. Každé stanici stačí, aby měla ve svém dosahu alespoň jeden přístupový bod. Pokud je k přístupovému

bodu připojeno více klientů, tak se všichni dělí o jednu šířku pásma. Například pokud bude Access-point pracovat dle standardu 802.11 b – tj. 11Mbps a bude k němu připojeno 5 klientů, tak se o rychlost 11Mbps budou dělit všichni (rychlost připojení každého klienta při plném vytížení bude okolo 2,2Mbps). I proto je maximální počet připojených klientů k jednomu přístupovému bodu omezen na 254 (některé starší modely pouze 30).

Nejčastější využití tohoto typu sítě je v domácnostech nebo v kancelářích, kde přístupový bod pokrývá místnost a klienti jsou k němu bezdrátově asociováni.

2.2.1 Modelové zapojení AP mode

Pro modelové zapojení si ukážeme síť jednoho přístupového bodu připojeného k internetu a dále dvou klientů – jednoho notebooku a jednoho počítače. Síť je sestavena a nakonfigurována dle obrázku 2.2.1. U přístupového bodu byla využita všesměrová anténa standardně dodávaná výrobcem.



AP
IP Adresa: 192.168.1.1
Maska: 255.255.255.0
MAC: 00-12-BA-49-B2-67

Notebook:
IP Adresa: 192.168.1.10
Maska: 255.255.255.0
MAC: 00-E0-98-B7-B2-AB

PC:
IP Adresa: 192.168.1.11
Maska: 255.255.255.0
MAC: 00-90-96-29-FF-58

Obrázek 2.2.1 Modelové zapojení AP mode

2.2.2 Analýza zapojení AP mode

Modelové zapojení bylo realizováno podle obrázku 2.2.1. Počítače byly spojeny do lokální sítě a pro testování na nich byl spuštěn přenos souborů z jednoho na druhý a po té bylo vyzkoušeno hraní her po síti a standardní „brouzdání“ po internetu. Měření jsem prováděl opět několikrát pro odstranění náhodných chyb. Získaná data se pohybovala s drobnými odchylkami na stejných hodnotách.

Získané hodnoty:

SSID	apmode
Kanál	6
Počet klientů	2
Unicast rámců	91%
Broadcast rámců	9%
Datových rámců	53%
Kontrolních rámců	31%
CRC	8%
Typ rámce	dlouhý
Zabezpečení	WEP
Nedoručených rámců	3%
Protokol 802.11	b
Síla signálu	-44dB
Rámců 11Mbit	85%
Rámců 5,5Mbit	9%
Rámců 2Mbit	5%
Rámců 1 Mbit	1%
Průměr Ping	2ms

Z tabulky lze vyčíst, že přenosová režie (kontrolní a CRC rámce) zabírá opět velkou šířku pásma – celkem 39%. Oproti Ad-hoc se zde zvýšil počet broadcast rámců. Úroveň signálu se pohybovala okolo -45 dB, což postačuje pro bezproblémové spojení. Nedoručených rámců (3%) už značí stabilní spojení. Rozložení přenášených rámců na 11, 5.5, 2 a 1 Mbit ukazuje na malé výkyvy dosahovaných rychlostí. Průměrný ping 2ms značí stabilní rychlost, bez výkyvů.

2.2.3 Praktické možnosti využití

Zapojení AP mode je nejčastější použití bezdrátových sítí. Obvykle se využívá pro interní potřeby – pro pokrytí domácností, kanceláří, škol, knihoven a jiných veřejných budov. Pro toto nejlépe slouží všesměrové antény.

AP mode je relativně stabilní. Pokud se nepřekrývají signály jednotlivých kanálů, sítí a přístupových bodů, pak je i velmi rychlý a spolehlivý. Před vlastní instalací je dobré tedy zjistit, zda se v oblasti nacházejí jiné bezdrátové sítě a na jakých kanálech pracují.

2.3 Bridge mode

Obecný pojem most označuje zařízení propojující dvě sítě LAN. Přístupový bod z definice zvládá pouze připojení bezdrátových klientů, nemůže připojovat jiný přístupový bod. Výrobci ale chtějí uživatelům usnadnit práci, proto vyrábějí i další samostatná zařízení a nebo jejich funkcionalitu zabudovávají do přístupových bodů. Přístupové body lze tedy nakonfigurovat tak, aby pracovaly v takzvaném bridge módu. Pokud je správně nastaven, tak je schopen spojit se s dalšími přístupovými body pomocí bezdrátové sítě. Jednoznačnou výhodou je, že pokud je klient v dosahu jednoho přístupového bodu a komunikuje s klientem připojeným k jinému přístupovému bodu, tak tyto dva přístupové body nemusejí být spojeny drátovým LAN vedením. První přístupový bod tedy funguje jako bridge.

2.3.1 Přístupový bod jako bridge

Bezdrátový bridge (most) je zařízení umožňující propojení bezdrátové sítě s běžnou LAN sítí. Touto vlastností zpravidla disponují pouze přístupové body. Navenek jí velmi lehce poznáme podle běžného síťového konektoru (RJ-45). Vzhledem k tomu, že nám v některých případech může délka anténního svodu způsobit větší problémy, nabízí se následující řešení: AP s vestavěnou funkcí bridge umístit co nejblíže k anténě (klidně i na stožár, např. do vodotěsné krabice), délka kabelu (útlum) se tak minimalizuje na zanedbatelnou hodnotu a k PC přivedeme přímo UTP, který zapojíme do síťové karty. Zde již nejsme v podstatě ničím limitováni (nezapomeňme na vlastní napájení AP), možná délka UTP kabelu je zhruba 100 metrů bez použití aktivního prvku.

2.3.2 Point to Point

Propojení dvou bodů (dvou sítí LAN) je nejjednodušší použití bezdrátového mostu. Dvě zařízení spolu komunikují skrze WiFi. Tento model se používá všude tam, kde jsou dvě oddělené LAN sítě, například ve dvou budovách a pouze do jedné budovy je kabelová přípojka internetu. Aby obě sítě LAN mohly používat internet a být propojené, propojí se právě na bázi point-to-point (PTP).

Bezdrátové připojení PTP je propojení dvou sítí za pomocí WiFi. Pokud bychom chtěli, aby obě sítě LAN fungovaly bezdrátově, musíme do návrhu začlenit vyhrazené přístupové body sloužící pro připojování klientů. Nesmíme zapomenout na správnou komunikaci klientů, aby nerušily PTP spojení.

Běžné je, že při konfiguraci mostu zadáváme MAC adresu zařízení, která se propojují. To proto, aby nedošlo k připojení jiné neautorizované stanice. Při nákupu bezdrátového mostu se můžeme setkat s označením Point to Point, LANtoLAN, interbuilding, PTP a podobně. Všechny tyto názvy označují stejný princip fungování.

2.3.3 Point to Multipoint

Díky této funkci lze k jedné síti připojit více dalších LAN sítí. Je to tedy rozšířená obdoba funkce Point to Point. Oproti módu PTP je zde více možností v konfiguraci jednotlivých zařízení různých výrobců, proto je lepší při návrhu používat zařízení od jednoho výrobce.

I u funkce Point to Multipoint platí, že slouží k propojení dvou sítí a nikoliv k připojování klientů skrze WiFi. Pokud chceme jednotlivé počítače připojit pomocí WiFi, musíme se pomoci přístupovým bodem dedikovaným pro tuto činnost.

2.3.4 Bezdrátový opakovač

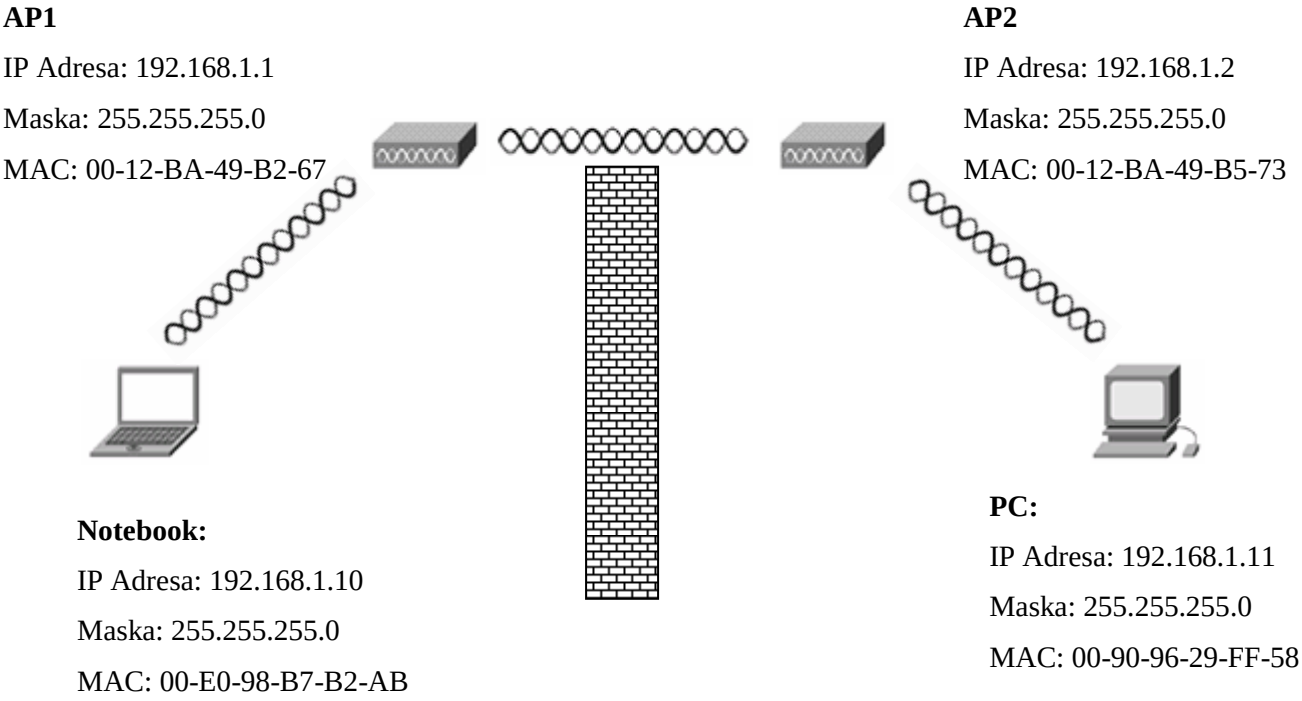
Přístupové body obyčejně potřebují ethernetový kabel, kterým se připojují k LAN síti. Pokud chceme provozovat více přístupových bodů a rozšířit tak oblast pokrytí signálem bezdrátové sítě využijeme opakovač. S funkcí opakovače je možné jednotlivé přístupové body mezi sebou propojit bezdrátově a ethernetovou přípojku použít pouze pro jeden z nich. Přístupové body s touto funkcí jsou ovšem poněkud drahé. Pokud tuto funkci opravdu potřebujeme, je výhodnější použít kombinaci přístupového bodu a mostu k zvětšení dosahu WiFi sítě bez nutnosti pokládat ethernetový kabel.

Tuto technologii objevíme u výrobců pod označením WLAP – Wireless LAN Access Point nebo WDS – Wireless Distribution Systém.

2.3.5 Modelové zapojení bridge mode

Problematika bridge mode je složitější. Pro příklad si ukážeme síť dvou přístupových bodů a dvou počítačů. Počítače nejsou spojeny přímo, ale přes dva přístupové body. Body jsou nastaveny na provoz bridge mode, aby přeposílaly pakety k cíli.

Síť byla nakonfigurována dle následujícího obrázku.



Obrázek 2.3.5.1 : Modelové zapojení bridge mode

2.3.6 Analýza zapojení bridge mode

Modelové zapojení bylo realizováno podle obrázku 2.3.5.1. Počítače byly spojeny do lokální sítě a pro testování na nich byl spuštěn přenos souborů z jednoho na druhý a po té bylo vyzkoušeno hraní her po síti. Měření jsem opět prováděl několikrát pro odstranění náhodných chyb. Získaná data se pohybovala s drobnými odchylkami na stejných hodnotách.

Získané hodnoty:

SSID	bridge
Kanál	6
Počet klientů	2
Unicast rámců	86%
Broadcast rámců	14%
Datových rámců	63%
Kontrolních rámců	32%
CRC	5%
Typ rámce	dlouhý
Zabezpečení	WEP
Nedoručených rámců	4%
Protokol 802.11	b
Síla signálu	-51dB
Rámců 11Mbit	88%
Rámců 5,5Mbit	9%
Rámců 2Mbit	3%
Rámců 1 Mbit	0%
Průměr Ping	4ms

Z tabulky lze vyčíst, že přenosová režie (kontrolní a CRC rámce) zabírá opět velkou šířku pásma – celkem 37%. Oproti Ad-hoc a AP mode se zde zvýšil počet broadcast rámců. Úroveň signálu se pohybovala okolo -50 dB, což postačuje pro bezproblémové spojení. Nedoručených rámců (4%) značí stabilní spojení. Rozložení přenášených rámců na 11, 5.5, 2 a 1 Mbit ukazuje na malé výkyvy dosahovaných rychlostí. Průměrný ping 4ms značí stabilní rychlost, bez výkyvů.

2.3.7 Praktické možnosti využití

Bezdrátový most obecně zjednodušuje návrh větší sítě postavené na WiFi. Je důležité mít na paměti, že čím více těchto prvků použijeme, tím více provozu a tedy i rušení ve WiFi pásmu vygenerujeme. Navíc dnešní rychlosti 11 Mb/s nebo 54 Mb/s nejsou vždy dostatečné. Proto je vhodné při návrhu popřemýšlet o nahrazení mostu klasickým drátovým vedením. I za cenu složitější realizace při pokládání kabelů. Dosáhneme tak vyšší rychlosti i spolehlivosti.

Také je třeba mít na paměti, že funkci point to point a někdy i point to multipoint nabízejí mnohé lepší přístupové body nebo bezdrátové směšovače. I nákupem takového zařízení můžeme oproti nákupu specializovaného zařízení hodně ušetřit.

2.4 Shrnutí naměřených hodnot

Pro každé zapojení jsem provedl 3 měření aby se minimalizovaly náhodné chyby. Naměřené hodnoty se pohybovaly až na drobné odchylky na stejných hodnotách. Ze získaných hodnot je patrné, že při přenosu dat bezdrátovým signálem je v poměrně velké míře zastoupena režie přenosu. Nejvyšších hodnot dosáhlo zapojení Ad-hoc. Počet nedoručených rámců byl také nejvyšší v zapojení Ad-hoc. V zapojeních AP mode a bridge mode byl počet nedoručených rámců podobný. Kolísání rychlosti bylo nejvíce patrné v zapojení Ad-hoc, kde byly 3% rámců přenášeny nejnižší možnou rychlostí. Zapojení Ad-hoc bylo oproti AP mode i bridge mode nejméně stabilní.

3 Analýza fakultní bezdrátové sítě

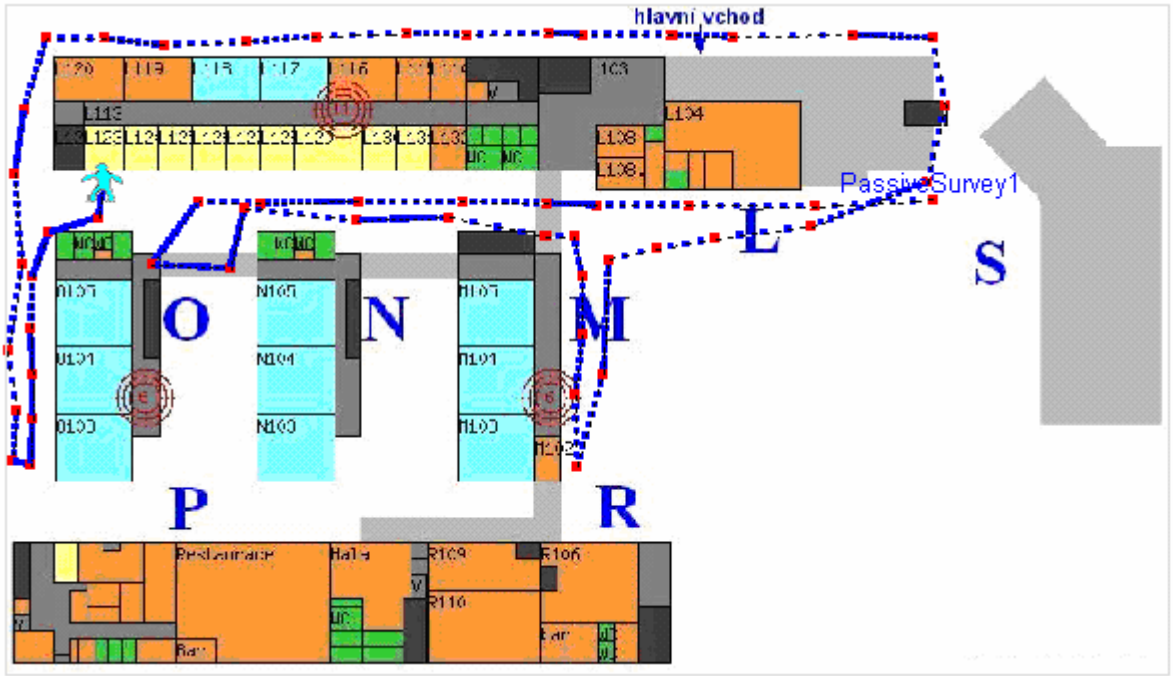
V této kapitole budeme sledovat bezdrátovou síť FIT. Provedeme pasivní a aktivní mapování sítě a pozdější analýzu naměřených hodnot.

Bezdrátovou síť na Fakultě Informačních Technologií jsem monitoroval v prostorách nové budovy Božetěchova 1. Pro monitorování jsem využil PCMCIA kartu Airmagnet Laptop Analyser a aplikaci Airmagnet Surveyor. Aplikace nabízí sadu nástrojů pro detailní analýzu sítě, které jsem využil pro získání dat.

3.1 Pasivní mapování sítě

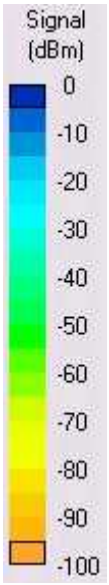
Při pasivním mapování se zaznamenávají všechna data ze všech přístupových bodů dostupných v oblasti. Díky tomu získáme přehled o sítích, které pokrývají oblast a mohou se i navzájem rušit. Z pasivního mapování vyčteme také zdroje šumu a dalších signálů, které by mohly způsobit problémy při provozu naší sítě.

Na následujícím obrázku je zobrazena trasa mého měření. Měření jsem prováděl v přízemí fakulty.



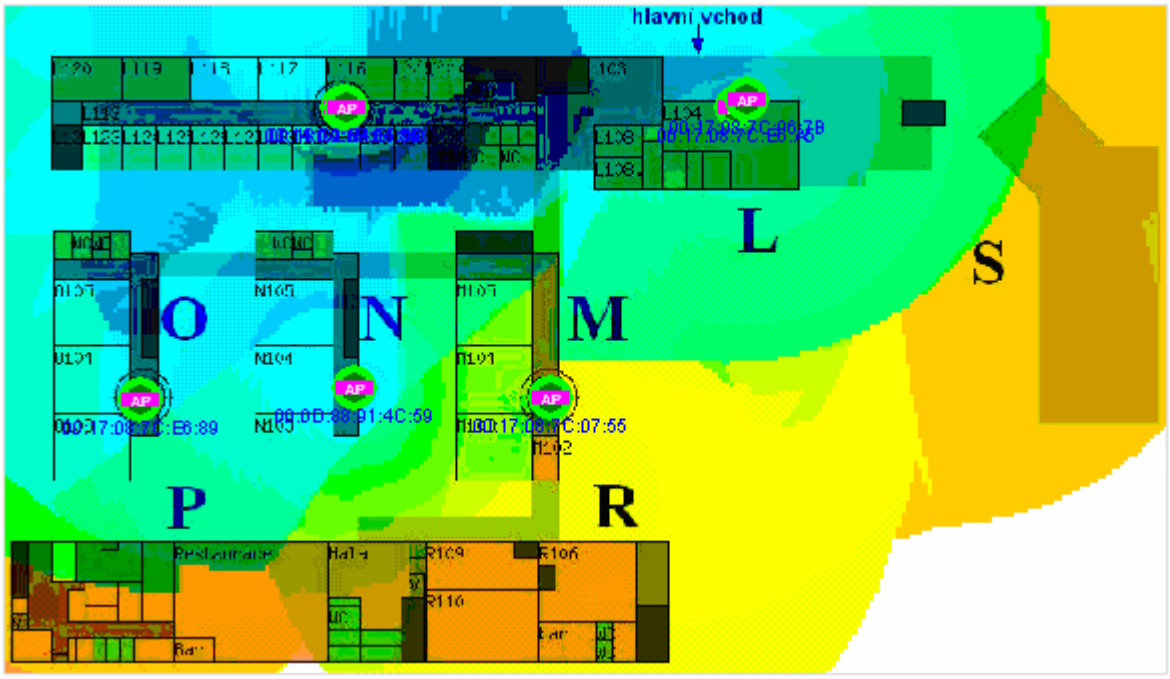
Obrázek 3.1.1 : Trasa pasivního mapování

Pro další obrázky bude důležité znát barevnou symboliku pokrytí signálem. Jednotlivé úrovně signálu zobrazuje obrázek 3.1.2.



Obrázek 3.1.2 : Barevné úrovně signálu

Následující obrázek ukazuje pokrytí fakulty bezdrátovým signálem sítě VUTBRNO.

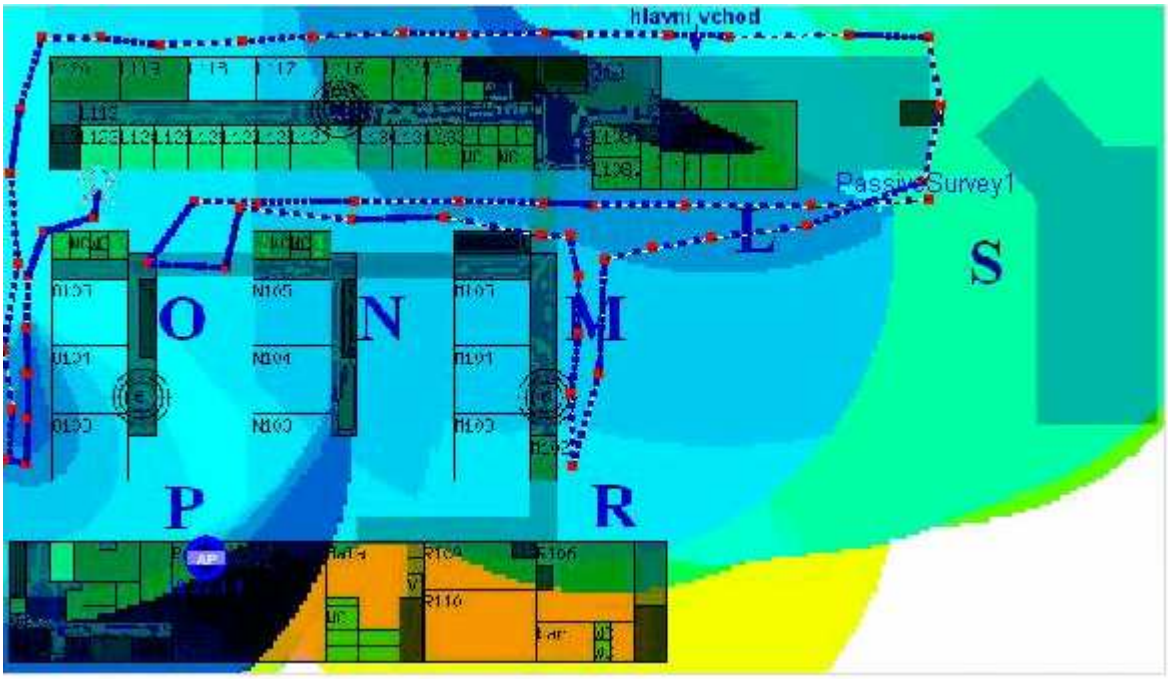


Obrázek 3.1.3 : Pokrytí fakulty bezdrátovým signálem

V místě fakulty je možné zachytit i signály jiných bezdrátových sítí. Některé tyto signály jsou poměrně silné a mohou kolidovat se signálem VUTBRNO.

Ostatní sítě zjištěné při analýze:

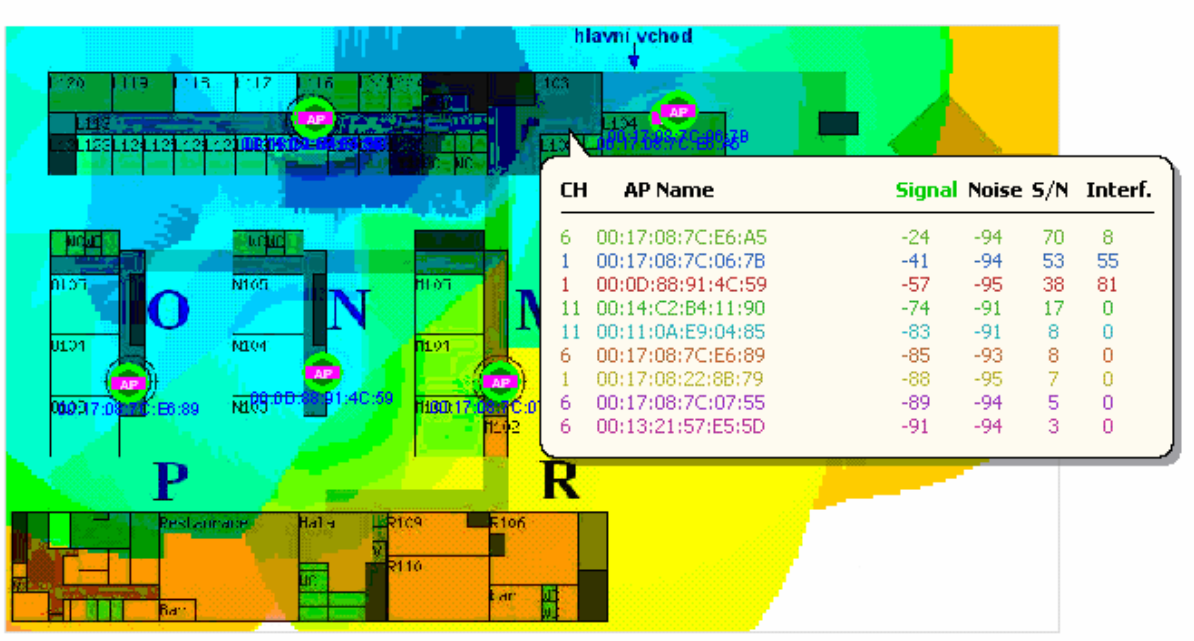
Síť SSID	Protokol 802.11	Kanál	Síla signálu (dB)
APKinA	a	40	-87
BF360	b	13	-85
Cz-Freee-Bieblova	b	5	-87
default	g	11	-38
Epsilon105	b	12	-33
internet: info.i-brno.cz	b	4	-65
KoVDusek	a	52	-50
lachema.fastnet.cz-1	b	2	-81
N24KC1	b	6	-4
netdatacomm_mojm1	b	11	-83
steinex	g	3	-78
Unknown	b	2	-16
Unknown	b	3	-56



Obrázek 3.1.4 : Přesahy jiných signálů

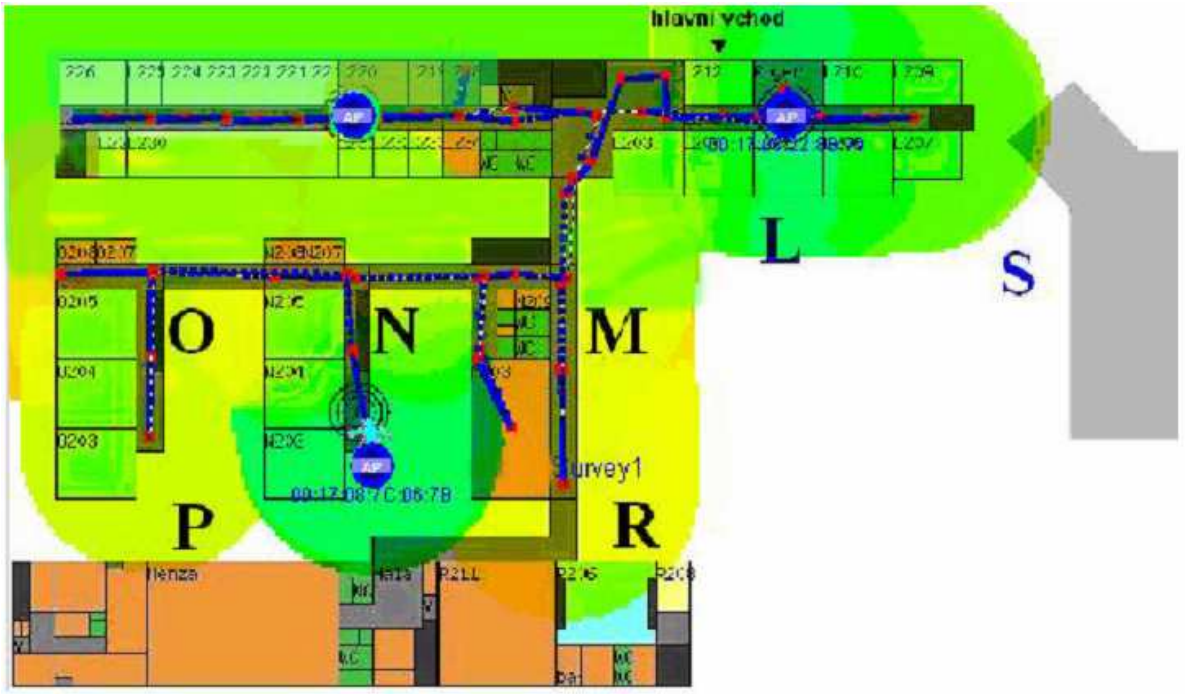
Jak je vidět na obrázku 3.1.4, signály jiných sítí jsou poměrně silné. Naštěstí však většina ze signálů pracuje na jiných kanálech, proto nenastává příliš velká interference mezi cizími sítěmi a VUTBRNO. Největší problémy by mohla způsobovat síť N24KC1, která pracuje na kanálu 6 a síla signálu je -4dB.

V přízemí lze zachytit i signály z přístupových bodů umístěných ve vyšších patrech budovy. Na obrázku 3.1.5 je zobrazena síla signálu VUTBRNO s kanály a přístupovými body ve vstupním foyeru.



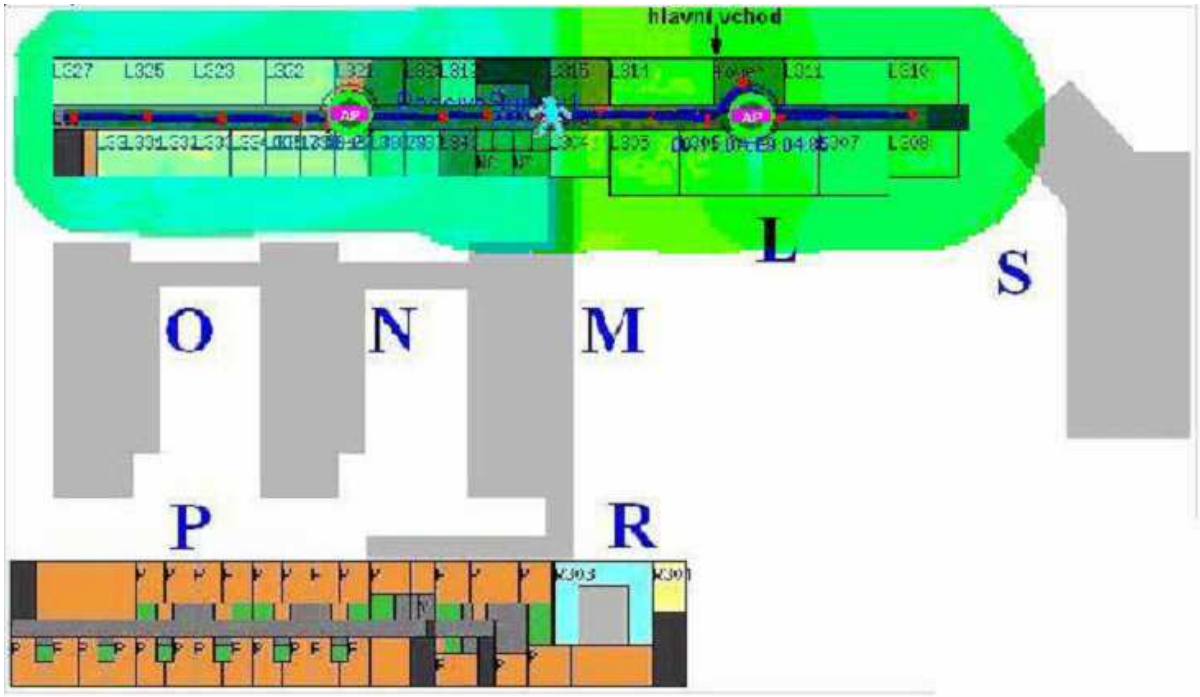
Obrázek 3.1.5 : Pokrytí signálem VUTBRNO a síla signálu

Pro úplnost monitorování jsem provedl scan sítě i v 2.NP budovy. Výsledky signálu jsou zobrazeny na následujícím obrázku.



Obrázek 3.1.6 : Pokrytí signálem VUTBRNO 2.NP fakulty

Scan signálu ve 3.NP je na obrázku 3.1.7.

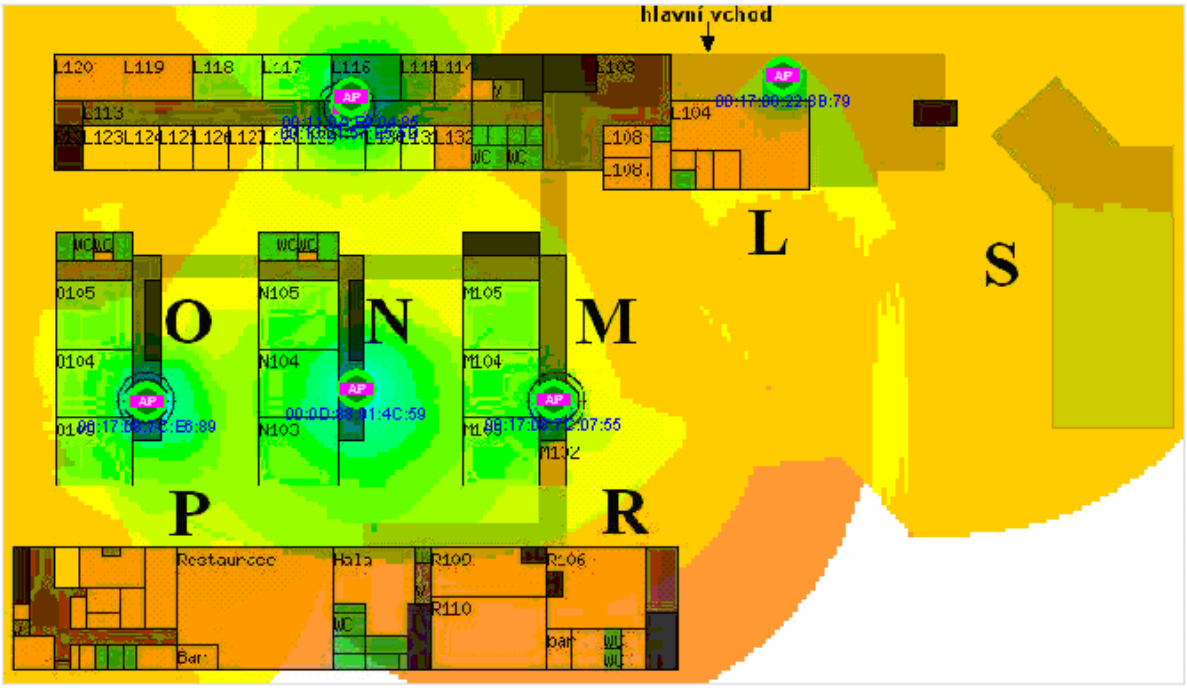


Obrázek 3.1.7 : Pokrytí signálem VUTBRNO 3.NP fakulty

3.2 Aktivní mapování sítě

Aktivní mapování sítě spočívá v asociaci s přístupovým bodem. Po asociaci se emuluje skutečný uživatel a tím získáme přesnější data pro daný přístupový bod. Můžeme tak zjistit rychlost připojení, dobu odezvy a poměr ztráty paketů.

Na obrázku 3.2.1 je zobrazeno aktivní mapování fakultní sítě s asociací k přístupovému bodu v pavilonu N. Trasa mapování je takřka shodná s trasou v pasivním mapování.



Obrázek 3.2.1 : Aktivní mapování

Získané hodnoty:

Kanál	1
Síla signálu (dB)	-47
Šum (dB)	-97
Poměr síla signálu / šum	50
Interference	0
Protokol 802.11	b
Průměr Ping	23ms

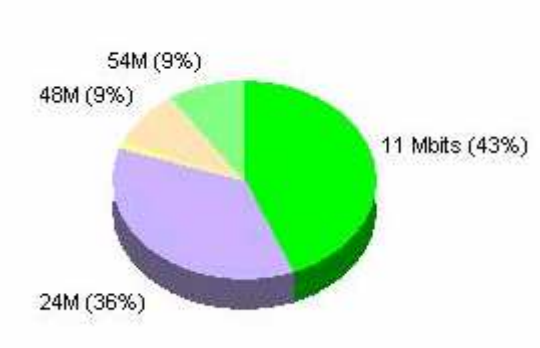
Síla signálu se pohybovala okolo -50dB. Takováto síla postačuje pro kvalitní připojení a přenášení dat. Úroveň šumu dosahovala okolo -97dB. Tato hodnota není nijak kritická a nebrání spolehlivému přenosu.

3.3 Propustnost

Testování propustnosti bezdrátové sítě jsem prováděl v budově L ve 3. patře. Měření jsem prováděl v různých hodinách, aby se projevila vytíženost v závislosti na počtu připojených klientů. Pro ukázku je zde uvedena tabulka naměřených hodnot.

Kanál	6
Počet připojených klientů	5
Unicast rámců	94%
Broadcast rámců	6%
Kontrolních rámců	65%
Datových rámců	31%
CRC	4%
Typ rámce	krátký
Zabezpečení	WEP vypnuto
Průměrné vytížení	38%
Nedoručených rámců	1%

Z tabulky lze vyčíst, že přenosová režie (kontrolní a CRC rámce) zabírá velkou šířku pásma – celkem 69%. Nedoručených rámců (1%) značí stabilní spojení. Pět připojených klientů vytěžovalo síť na 38%. Na obrázku 3.3.1 je zobrazeno procentuelní rozložení datových rámců v závislosti na rychlosti přenosu. Je zde vidět využití vysokých přenosových rychlostí (54 a 48 Mbit).



Obrázek 3.3.1 : Procentuelní zastoupení rámců

3.4 Zabezpečení

Zabezpečení fakultní bezdrátové sítě je realizováno pomocí autentizace uživatele. Po připojení k síti VUTBRNO a otevření jakékoliv webové stránky je klientovi nabídnuta stránka pro přihlášení s VUT loginem a heslem. Po přihlášení je klient autentizován a připojen do sítě. Nijak se neřeší šifrování paketů, proto se doporučuje používat VPN nebo IPSec tunelování do sítě VUT.

4 Pokročilé WiFi sítě

V této kapitole si objasníme problematiku pokročilých bezdrátových sítí. Prostudujeme mesh sítě, různé možnosti zabezpečení bezdrátových sítí a kvalitu služby.

Bezdrátové sítě se ujaly tak obdivuhodně, že další podpůrné, doplňující a rozšiřující standardy a aktivity na sebe nedaly dlouho čekat. Ke standardu 802.11 byly vytvořeny revize 802.11a a 802.11b, později i 802.11g. Maximální teoretická rychlost bezdrátové sítě se dnes uvádí 54 Mb/s. Jenže další rychlostní posun není příliš daleko. Při některých mutacích výrobců lze dosahovat rychlosti až 108 Mbit/s.

Nejnovější postupy naznačují, že lze dosáhnout přenosových rychlostí až 500 Mb/s. Tuto rychlost by měla garantovat norma IEEE 802.11n, samozřejmě při zachování zpětné kompatibility. Vysoké rychlosti lze dosáhnout několika způsoby. Jednak přechodem na frekvenční spektrum 5 GHz a použitím šířky kanálu 40 MHz, kterých je v tomto pásmu 11 (na stávající frekvenci 2,4 GHz jsou pouze dva 20 MHz) a potom sdružením více antén technikou MIMO (multiple-input, multiple-output). Rychlosti 500 Mb/s by se dalo dosáhnout vytvořením 4 „bezdrátových linek" (MIMO 4×4).

Lze tedy obecně říct, že bezdrátové sítě nenabízí jen zvyšování rychlostí, ale i nové možnosti použití a nová technologická řešení.

4.1 Mesh sítě

Mesh sítě jsou prozatím málo známý pojem. Přitom jde o velmi zajímavou technologii. Mesh sítě jsou aplikací sítí peer-to-peer do bezdrátového světa, tedy aplikace myšlenky rovnosti a nezávislosti jednotlivých síťových prvků. Zatímco klasická síť je vystavená tak, že k přístupovému bodu se uživatelé připojují klientským adaptérem, mesh síť tento rozdíl stírá. V mesh síti nejsou přístupové body ani klienti, všechna zařízení jsou si rovna. Libovolné mesh síťové zařízení je schopno poskytnout stejnou sadu služeb jako jakékoliv jiné zařízení.

Prakticky lze mesh síť přirovnat ke stávající GSM mobilní síti. V mobilní síti je zapojena základová stanice BTS (Base Transceiver Station) a k ní je připojený mobilní terminál. Každý mobil, který chce volat, musí být v dosahu BTS. V mesh síti si signál mezi sebou předávají jednotlivé mesh adaptéry, takže k tomu, abychom se připojili do internetu stačí připojit se k mesh adaptéru, jenž má připojení do internetu. A to i klidně přes jiné mesh adaptéry – vůbec nemusíme být v oblasti pokryté připojeným adaptérem. Stačí mít možnost se připojit přes ostatní adaptéry k tomu cílovému adaptéru. Mesh sítě jsou založeny na takzvaném ad-hoc peer to peer routingu – na směrování provozu mezi rovnocennými adaptéry dle potřeby.

Mezi hlavní výhody mesh sítí patří:

- Úspora pásma – na první pohled to vypadá nepravděpodobně, opak je však pravdou. Spojení v mesh síti se sestaví jen tehdy, když je potřeba a na dobu, po kterou je potřeba. V jiných sítích bývá sestavení po celou dobu, co jsou zařízení zapojena, protože připojování a odpojování se řídí ručně.
- Zastupitelnost – při výpadku jednoho prvku mesh sítě ho může jakýkoliv jiný prvek nahradit.
- Zvýšení dosahu sítě díky většímu počtu adaptérů, které mohou předávat signál.
- Nízké náklady na výstavbu a údržbu – taková síť se jednoduše staví a jednoduše udržuje, protože o všechno základní nastavení se stará roubovací protokol.

Hlavní nevýhodou mesh sítí je komplikovanost směrování. Další nevýhodou je vyšší odběr energie, což může být u mobilních zařízení problém. Novější návrhy umožňují v economy módu vypnout předávání signálu a tak spořit energii. Posledním velkým problémem je zabezpečení. Již zmíněná technologie ad-hoc prakticky nabízí všem v síti připojení k našemu počítači. V takovém případě je nutné patřičně nastavit zabezpečení počítače, případně musí obstarávat zabezpečení software mesh sítě.

Myšlenka mesh sítí je zajímavá. Namísto složité instalace nejrůznějších směrovacích protokolů stačí zakoupit WiFi kartu a připojit se do velké sítě a tím ji ještě zvětšit. Proto se vývojem těchto sítí zabývá většina velkých firem produkujících síťové a operační technologie. Prozatím lze zakoupit WiFi kartu, která podporuje mesh síťování, za cenu okolo 10 tisíc korun. Do budoucna lze odhadovat, že mesh technologie se stane běžnou součástí bezdrátových sítí.

4.2 Zabezpečení

Bezdrátová síť má proti kabelové síti nevýhodu vycházející z jejího principu – nelze dostatečně přesně omezit prostor, kde je její signál k zachycení. Pokud chceme odposlouchávat provoz v kabelové síti, je potřeba se fyzicky dostat ke kabelům. Pokud chceme odposlouchávat bezdrátovou síť, stačí se dostat pouze do prostoru, kde lze signál zachytit.

Mohlo by se zdát, že zabezpečení bezdrátové sítě není důležité v případě, že v ní nepřenášíme citlivá data a že například pro stavbu komunitní sítě, v níž se dělíme se sousedy o připojení k internetu, není potřeba zabezpečení. Není to tak docela pravda, protože k zabezpečení sítě patří i řízení přístupu do ní, tak i to, aby připojení k internetu mohli používat jen lidé, kterým to chce umožnit provozovatel sítě.

Bezpečnost bezdrátových sítí lze rozdělit do dvou hlavních skupin:

1.) autentizace a autorizace – řízení přístupu oprávněných uživatelů
2.) šifrování – zabezpečení přenášených dat před odposlechem

Obě skupiny vycházejí z již zmíněného problému radiových sítí, tedy z faktu, že jejich pokrytí lze problematicky teritoriálně vymezit, a tedy spoléhat na zabezpečení přístupu do zasíťovaného teritoria, jako je tomu u sítí kabelových (např. Ethernetu).

4.2.1 Autentizace

Řízení přístupu do sítě je důležitou součástí bezpečnostní strategie. Řízení přístupu v kabelových sítích je většinou realizováno tak, že nepovolaným osobám nejsou přístupné prostory, kde se lze do sítě připojit. V bezdrátových sítích toto realizovat nelze, protože dosah signálu nelze přesně omezit. Navíc je přístup do oblasti pokryté WiFi žádoucí – z tohoto důvodu jsou sítě zřizovány. Rozhodnout o tom, která z osob smí WiFi využívat, může pouze provozovatel.

Autentizace v 802.11 je jednosměrný proces. Stanice si musí o autentizace do sítě žádat, zatímco síť se vůči stanicím autentizovat nemusí. Tento systém bohužel umožňuje útoky main-in-the-middle, tedy možnost podvržení falešného přístupového bodu mezi klientská zařízení a skutečný síťový bod.

Standart 802.11 specifikuje dvě metody pro autentizace:

- Open–system
- Shared-key

4.2.1.1 Open-system

Autentizace open-system je jediná metoda vyžadovaná 802.11. Tato metoda spočívá v tom, že přístupový bod přijme klientské zařízení na základě údajů, které mu toto poskytne, aniž by je ověřoval. Klient pošle svoji identifikaci v podobě SSID. Pokud přístupový bod své SSID vysílá, může každá stanice, která není nakonfigurována na svoje SSID, toto SSID přijmout a použít jej pro autentizace.

Tento systém je prakticky velmi jednoduše prolomitelný. Obecně se doporučuje vypnout vysílání SSID přístupovým bodem, ovšem nové systémy i utility volně dostupné na internetu dokáží velmi rychle odhalit SSID z provozu v síti, aniž by bylo útočníkovo zařízeno autentizováno. Proto lze tuto autentizaci doporučit pouze tam, kde chceme zpřístupnit bezdrátovou síť opravdu každému, nebo použít ještě další možnosti autentizace a zabezpečení.

4.2.1.2 Shared-key

Při autentizace sdíleným klíčem je nutno v síti použít šifrovací metodu WEP. Standard 802.11 vyžaduje, aby každé zařízení s implementovaným WEP zabezpečením bylo také schopné používat autentizace sdíleným klíčem.

Pokud se chce zařízení autentizovat, pak se musí prokázat sdíleným klíčem. V případě, že je přístupový bod ověří, je zařízení autentizováno. Ověřování probíhá tak, že přístupový bod odešle náhodné číslo, to je zakódováno algoritmem RC4 podle sdíleného klíče a přístupový bod jej dekóduje. Pokud se dekódované číslo rovná číslu odeslanému, autentizace proběhla úspěšně.

Tato autentizace stojí na síle zabezpečení WEP a algoritmu RC4. Při použití této metody je nutné často obměňovat klíče, což je velmi nepraktické obzvlášť ve větších sítích. Na internetu se objevila informace, že zabezpečení WEP bylo již prolomeno. A dokonce i některé volně dostupné programy pro prolomení tohoto šifrování. Proto nelze tento postup považovat za bezpečný.

4.2.2 Filtrování MAC adres

Filtrování MAC adres bylo implementováno výrobci jako další stupeň zabezpečení. V každém přístupovém bodu je uveden seznam MAC adres, podle kterého se povolí nebo zakáže přístup klienta do sítě. Pokud klient žádá o autentizaci, je ověřena jeho MAC adresa a podle seznamu se rozhodne, zda bude nebo nebude asociován.

Existují různé varianty seznamů MAC adres. Lze vytvořit seznam zakázaných adres, nebo seznam povolených adres. Některé přístupové body umožňují i další funkce, jako například určitým MAC adresám přidělit šířku pásma, nebo asociovat zařízení na určitou dobu.

I když tento postup vypadá na první pohled přívětivě, problémů při filtrování MAC adres je hned několik. Nová klientská zařízení umožňují naprogramovat MAC adresu, kterou si útočník může měnit, jak je libo. Tím obejde zabezpečení.

Dalším úskalím je administrace většího celku. Pokud máme síť s více přístupovými body a mnoha klienty, je složité udržovat databázi MAC adres a distribuovat je k přístupovým bodům.

Kvůli těmto problémům lze filtrování MAC adres doporučit pouze pro malé bezdrátové sítě. Například pro domácí použití jako jeden z prvků ochrany před nežádoucím přístupem.

4.2.3 EAP – autentizace pomocí 802.1X

Zkratka EAP znamená Extensible Authentication Protocol (rozšířitelný autentizační protokol). IEEE 802.1x je obecný bezpečnostní rámec pro všechny typy sítí, zahrnující autentizace uživatelů, integritu zpráv (šifrováním) a distribuci klíčů. Ověřování bezdrátové sítě se realizuje na úrovni portů přístupového bodu WLAN. 802.1x blokuje přístup k segmentu lokální sítě pro uživatel bez patřičného oprávnění.

Ověřování v bezdrátové síti provádí přístupový bod pro klienty na základě jejich výzvy, pomocí seznamu nebo externího autentizačního systému založeného na serveru Kerberos nebo RADIUS (Remote Authentication Dial In User Service). Pouze ověřený uživatel má možnost přístupu k bezdrátové síti.

Ověřování probíhá dle následujícího algoritmu. Klient odešle počáteční zprávu na přístupový bod, který odpoví dotazem na totožnost klienta. Klient odpoví zprávou, která obsahuje identifikační údaje uživatele. Přístupový bod zapouzdří celou zprávu do paketu a vyšle ji autentizačnímu serveru. Server odpoví zprávou obsahující povolení/zákaz přístupu pro daného klienta do sítě. V případě povolení je příslušný port přístupu do sítě otevřen pro data daného uživatele, který je na základě výše popsaného postupu považován za autentizovaného.

802.1x používá k šifrování datové komunikace pro každé autentizované zařízení dynamické klíče. Tyto klíče jsou známy pouze danému zařízení, mají omezenou životnost a využívají se k šifrování rámců na daném portu, dokud se zařízení neodhlásí nebo neodpojí.

Dynamické klíče zajišťují značnou míru bezpečí proti pokusům o průnik do sítě. Ani 802.1x není zcela bezpečný a je zranitelný vůči útokům session hijacking a man-in-the-middle. Díky jednostranné autentizaci umožní tyto útoky útočníkovi vystupovat jako oprávněný uživatel. Ani 802.1x nelze považovat za stoprocentní řešení bezpečnosti bezdrátových sítí.

4.2.4 AAA protokoly

AAA znamená Autentizace, Autorizace, Účtování (authentication, authorization and accounting). Využívá se pro přístup k síti nebo pro IP mobilitu.

Autentizace znamená ověření, že uživatel požadující služby je platným uživatelem poskytovaných síťových služeb. Autentizace je dosažena pomocí představení identity a jistého pověření nebo tajemství. Mezi různé typy tajemství patří například hesla, pověření na jedno použití nebo digitální certifikáty.

Autorizace znamená udělení specifického typu služby (včetně „žádné služby“) uživateli, na základě jeho autentizace a služeb, které požaduje a aktuálního stavu systému. Autorizace může být založena na omezeních, například omezení na určité hodiny v rámci dne, nebo omezení na fyzickou

polohu, nebo omezení vícenásobného přihlášení jednoho uživatele. Autorizace určuje povahu služby, která je poskytnuta uživateli. Typy služeb jsou například: filtrování IP adres, přidělení adresy, přidělení cesty, QoS, řízení šířky pásma/řízení toku, tunelování do konkrétního koncového bodu, nebo šifrování.

Účtování znamená sledování využívání síťových služeb uživateli. Tyto informace mohou být použity pro správu, plánování, účtování, nebo další účely. Účtování v reálném čase je doručeno současně s využíváním zdrojů. Běžně se sbírají informace o identitě uživatele, povaze dodaných služeb a časy počátků a konců dodaných služeb.

Typickými zástupci AAA protokolů jsou RADIUS, DIAMETER, TACACS a TACACS+. Pro příklad si popíšeme princip na protokolu TACACS.

TACACS (Terminal Access Controller Access-Control Systém) je vzdálený autentizační protokol používaný ke komunikaci s autentizačním serverem, často používaný v sítích UNIX. TACACS umožňuje vzdálenému přístupovému serveru komunikovat s autentizačním serverem, aby se rozhodlo, zda má uživatel přístup k síti.

TACACS klient přijme uživatelské jméno a heslo a pošle požadavek na TACACS autentizační server (TACACS démon, TACACSD). Tento server rozhodne, zda přijmout nebo zamítnout požadavek a pošle zpět odpověď. Takto je rozhodovací proces otevřený a algoritmy a informace k němu použité jsou zcela na tom, kdo provozuje TACACS démona.

4.2.5 Zabezpečení šifrováním WEP

WEP (Wired Equivalent Privacy) je standard pro zabezpečení radiové části sítě. WEP zabezpečuje komunikaci mezi WiFi zařízeními až na úroveň přístupového bodu. Za ním již bezpečnost nezajistí, protože z WiFi zařízení již vystupuje provoz takový, jaký jej vyžadují připojení těchto zařízení. Pokud je tedy přístupový bod připojen do internetové sítě, odcházejí z něj data do internetu ve formě, v jaké vznikají na počítači, jenž je odeslal.

WEP používá symetrickou streamovou šifru RC4, tedy šifru s tajným klíčem. Odesílaná zpráva se šifruje podle nějakého klíče, obvykle slova nebo sekvence znaků. Na cílovém bodě se zase podle stejného klíče zpráva dešifruje. Tento klíč musí znát jak vysílací, tak přijímací strana. Standardní délka klíče je 40 bitů, tento klíč je rozšířen o 24 bitů, tzv. inicializační vektor. Prakticky to je 24 bitový pseudonáhodný sled znaků, který se přidá k 40 bitům klíče zadaného. Výsledkem je 64 bitový klíč.

Novější verze umožňují využívat 128 bitové klíče. Tyto klíče mají standardní délku 104 bitů a je k nim opět přidán 24 bitový inicializační vektor. Někteří výrobci nabízejí i 152 a 256 bitové šifrování. Princip je vždy stejný. Je vytvořen klíč a k němu připojeno 24 bitů pseudonáhodného čísla o stejné délce jako má šifrovaná zpráva. Tím pak dostaneme výslednou velikost šifry.

Hlavní nevýhodou je, že se inicializační vektory posílají nezašifrované. Útočník tedy může velmi snadno odposlechnout provoz a pak i určit náš klíč. Tímto lze WEP velmi snadno prolomit. Dalším problémem je změna klíče. Při změně klíče je nucen uživatel nastavit nový klíč. Vývoj WEP se prakticky zastavil. Výrobci soustřeďují svoji pozornost na WPA a 802.11i.

4.2.6 WPA

WPA je zabezpečení, které pro šifrování používá protokol TKIP (Temporal Key Integrity Protocol). TKIP využívá stejný šifrovací algoritmus jako WEP, standardně klíč o délce 128 bitů. Od WEP se liší tím, že používá dynamické dočasné klíče, které se periodicky mění každých 10 000 paketů.

Další velkou výhodou je kontrola integrity zpráv (Message Integrity Check – MIC), což je podstatně lepší zabezpečení integrity zpráv než standardní kontrolní součet CRC. MIC prakticky znemožňuje změnu zprávy po přenosu.

V současné době je WPA podporován většinou dostupných zařízení. Proto lze doporučit jeho použití.

4.2.7 802.11i

Tento standard by měl poskytnout dostatečné zabezpečení bezdrátových sítí. Je založen na odolném šifrování AES (Advanced Encryption Standard) v rámci autentizačního rámce EAP.

Velikost šifrovacího klíče AES může být zvolena jako 128, 192 nebo 256 bitů. Platí zde, že čím delší klíč, tím větší bezpečnost a také vyšší potřebný výpočetní výkon zařízení kódujících a dekódujících přenášená data.

Přepokládanou součástí je TKIP, který obsahuje dynamické klíče a zahrnuje kontrolu integrity zpráv. Zdokonalení ve standardu 802.11i jsou lepší metoda šifrování, úprava způsobu jakým sítě vytvářejí a používají inicializační vektor a klíč, ochrana proti opakovaným útokům, zapomenutým paketům a útokům kolizí inicializačního vektoru, zlepšené řízení přístupu a autentizace. Někdy lze tento standard objevit pod názvem WPA2.

4.2.8 Praktické doporučení pro zabezpečení

Z popisu možností zabezpečení uvedeného v předcházejících kapitolách lze pro zabezpečení například firemní bezdrátové sítě doporučit následujících deset bodů.

1. V Access Pointu zaveďte tabulku povolených MAC adres
2. Je-li to možné, použijte WPA, popř. zapněte WEP na 128bitový klíč
3. Pravidelně měňte klíče WEP
4. Nepovolujte DHCP a adresy přidělujte ručně
5. Pokud je to možné, nastavte také tabulku povolených IP adres
6. Zakažte SSID Broadcast
7. Znemožněte fyzický přístup uživatelů k AP
8. Pravidelně kontroluje síť i logy z AP
9. Omezte výkon tak, aby síť zbytečně nepřesahovala půdu vaší firmy
10. Používejte VPN, IPSec

4.3 Kvalita služby – QoS

Kvalita služby (Quality of service) bezdrátových sítí je definována standardem 802.11e. QoS uděluje některým datovým paketům prioritu před jinými pakety. QoS se považuje za kritický faktor pro vytvoření robustní normy z 802.11, která by byla vhodná pro hlasovou a datovou komunikaci, jakož i pro multimediální aplikace. Standard je důležitý pro aplikace citlivé na zpoždění jako jsou Voice over Wireless IP a streamy.

Pro přenos dat citlivých na zpoždění, kolísání zpoždění či ztrátu paketů je potřeba jednotlivým typům paketů zaručit správné zacházení v síti při přenosu od zdroje k cíli, tedy určitou kvalitu služby. Stávající normy řady 802.11 nečiní žádné rozdíly mezi typy provozu. Neexistuje žádný rozlišující prvek mezi daty. Řešení pro přenos hlasu po WLAN sice již nějakou dobu existují, ale nejsou zatím vzájemně příliš slučitelná, změnu by měla přinést právě specifikace 802.11e.

Mezi metriky QoS patří:

- **koncové zpoždění -** doba mezi vysláním paketu od zdroje a jeho doručením zamýšlenému příjemci
- **kolísání zpoždění** - **jitter** - rozdíl v intervalech mezi přijímanými pakety
- **ztráta paketů** - podíl přijatých paketů a vyslaných paketů za jednotku času
- **šířka pásma** - přenosová kapacita
- **propustnost** - objem dat úspěšně přenesený za jednotku času

Hlasový, respektive proudový provoz se od datového provozu značně liší svým charakterem i požadavky. Na rozdíl od dat, která jsou shluková, potřebuje hlas menší, ale zato konstantní šířku pásma (v závislosti na rychlosti vzorkování, kodeku a režii). Citlivost na zpoždění je u hlasu výrazně vyšší než u dat. Maximální jednosměrné zpoždění by se mělo pohybovat pod 200 ms a maximální kolísání zpoždění pod 30 ms. Citlivost na ztráty paketů je u hlasu menší než u dat, maximální doporučená hodnota se pohybuje kolem jednoho procenta.

Původní specifikace 802.11 protokolu pro přístup k rádiovému kanálu umožňuje dva režimy komunikace: DCF a PCF. Ani jeden nerozlišuje mezi typy provozu, takže nemohou bez rozšíření podporovat QoS.

4.3.1 Rozšíření WLAN pro QoS

Norma IEEE 802.11e na podporu QoS rozšiřuje oba stávající režimy přístupu k rádiovému kanálu. Navíc zajišťuje zpětnou slučitelnost se zařízeními nevybavenými podporou pro QoS (podle původních norem 802.11a/b/g).

Rozšíření režimu DCF představuje funkce pod označením EDCF (Enhanced Distribution Coordination Function). ECDF představuje pravděpodobnostní prioritní mechanizmus pro alokaci šířky pásma na základě kategorií provozu. Každá stanice může mít až čtyři kategorie provozu na podporu osmi úrovních priority. Každá stanice může vysílat, jakmile je médium volné, ovšem po intervalu čekání, který odpovídá dané kategorii provozu. Interval se prodlužuje se snižující se prioritou provozu, takže stanice s vysokou prioritou provozu bude čekat kratší dobu než stanice s daty o nižší prioritě. Přístup k médiu se tak stává řízeně prioritní, kdy provoz s vyšší prioritou je upřednostněn na úkor provozu s prioritou nižší.

Aby nedocházelo ke kolizím mezi provozem o stejné úrovni priority, stanice musí navíc počkat ještě určitou dobu (náhodný počet časových úseků) odpovídající oknu soupeření (contention window), než může odeslat připravená data.

Režim PCF se v 802.11e rozšiřuje o hybridní funkci HCF (Hybrid Coordination Function). Přístupový bod vyzve stanici v době bez boje o médium, a pokud stanice chce vysílat, udělí jí specifickou dobu zahájení vysílání a dobu trvání vysílání. HCF se věnuje podstatně menší pozornost než EDCF, protože i PCF se implementovalo jen zřídka.

Zastaralejší řešení pro podporu QoS existuje pod označením WME (Wireless Multimedia Extensions), které podporuje pouze některé prvky pro QoS z normy 802.11e, jako označování rámců podle priorit a odpovídající řazení do front. WME podporuje čtyři místo osmi úrovní priorit, které jsou v 802.11e.

5 Závěr

Díky této práci jsem si prohloubil znalosti v oblasti bezdrátových sítí. Vyzkoušel jsem praktické zapojení Ad-hoc, AP mode, bridge mode. Provedl jsem monitorování těchto zapojení a následně analýzu dosažených výsledků. Na základě analýzy jsem vytvořil doporučení pro ideální praktické využití jednotlivých typů zapojení.

Dále jsem prováděl monitorování fakultní bezdrátové sítě VUTBRNO v budově Božetěchova1. Dosažené výsledky jsem prozkoumal a dospěl k názoru, že fakultní síť je relativně stabilní, dobře propustná a síla signálu neklesá pod únosnou mez (-60dB). Pokrytí budovy signálem je ve všech vnitřních částech budovy. Vně budovy je postačující přesah signálu pro možné připojení. Vytížení jednotlivých přístupových bodů je závislé na počtu připojených klientů. Po dobu mého měření se vytížení pohybovalo maximálně okolo 50%. Maximální vytížení se většinou objevilo v odpoledních hodinách. Komplikace však může působit přesah signálu jiných sítí. Pokud je signál dostatečně silný a pracuje na stejném kanálu jako fakultní síť, pak je velmi pravděpodobné, že může docházet k interferenci. Z naměřených hodnot nevyplývají žádné kritické hodnoty, ovšem pro zabezpečení funkčnosti by bylo vhodné provádět pravidelné monitorování okolí budovy.

V další části jsem studoval možnosti pokročilých bezdrátových sítí. Při plánování výstavby rozsáhlé bezdrátové sítě je třeba mít na paměti všechny aspekty tohoto provedení. Je důležité si uvědomit, že přenos bezdrátovým signálem je vlastně přenos po sdíleném médiu. Tento fakt má za následek spoustu problémů, které zde byly popsány, a se kterými je nutné počítat. V dnešní době se využívají rozsáhlé WiFi sítě zejména k překonání tzv. poslední míle. To znamená, že jím jsou připojeni uživatelé a domácnosti k internetu. Poskytovatel využívá ke spojení své brány a klienta právě bezdrátový signál.

Další vývoj bezdrátových sítí lze jen těžce odhadovat, avšak dnešní trendy naznačují, že se nadále bude využívat zapojení AP mode pro kanceláře, knihovny, školy a domácnosti. Další vylepšení patrně dosáhne zabezpečení. A rozsáhlé sítě budou využívány alternativními poskytovateli internetu pro připojení klientů k internetu.

Seznam zkratek a jejich vysvětlení

WiFi (Wireless Fidelity) – komerční označení bezdrátové technologie. Zařízení s tímto logem budou mezi sebou bez problémů komunikovat.

LAN (Local Area Network) – lokální počítačová síť. Síť typu LAN se rozkládá na malém území a vyznačuje se jednotnou architekturou a schopností komunikace jednotlivých počítačů mezi sebou bez využití dalších speciálních zařízení.

MAC (Media Access Control) – MAC adresa. Jedinečný identifikátor síťového zařízení. Je přiřazena síťové kartě. U některých karet lze měnit. Přiklad: 00-E0-98-B7-B2-AB nebo 00:E0:98:B7:B2:AB nebo : 00E0.98B7.B2AB.

SSID (Service Set Identifier) – Identifikátor (název) bezdrátové sítě.

Ping (Packet Internet Groper) – jednoduchý síťový program pro testování dosažitelnosti cílového zařízení. Spouští se s parametrem a jako parametr se zadává IP adresa cíle.

Mbps (Mega bits per second) – jednotka rychlosti přenosu dat. První písmeno udává násobek, druhé jednotku (bity/Bajty).

dB (deciBel) – logaritmická jednotka používaná k vyjádření intenzity signálu. Rozdíl 20 dB znamená rozdíl 10krát větší amplitudy signálu a 100krát většího výkonu. Obvykle se používá pro vyjádření relativního poměru signálů. Udává se v záporných hodnotách.

CRC (Cyclic Redundancy Check) – kontrolní součet. Používá se pro kontrolu přenášených paketů.

RJ45 – konektor pro síťové kabely.

UTP – typ síťového kabelu. Příklad: UTP Cat 5e je 8 žilový kabel. Žíly jsou zkrouceny ve 4 párech. Přes tento kabel lze dosáhnout rychlosti až 1Gbit.

WDS (Wireless Distribution System) – bezdrátový distribuční systém. Může přeposílat pakety k cíli jako most.

WLAP (Wireless LAN Access Point) – bezdrátový přístupový bod pro LAN sítě. Má podobnou funkci jako WDS.
VPN (Virtual Private Network) – virtuální privátní síť. Prostředek pro připojení počítačů, které jsou každý v jiné síti, do jedné virtuální sítě. Po připojení mohou mezi sebou komunikovat jako by byly v jedné síti. Používá se i jako zabezpečení, protože nabízí velmi silné šifrování přenosu.

IPSec – prostředek obdobný VPN

IEEE – organizace pro standardizaci.

AP (Access Point) – přístupový bod

DHCP (Dynamic Host Configuration Protocol) – systém automatického přidělování IP adres. Když se připojí nový počítač do sítě, tak mu DHCP server přidělí IP adresu a další potřebné nastavení, aby mohl pracovat v síti.

WLAN (Wireless Local Area Network) – bezdrátová lokální počítačová síť. Obdobná LAN, ale pracuje bezdrátově.

Literatura

[1] Geier, J. : *Wireless Networks, first-step*, 2004, Cisco Press.

[2] Bruce, A. : 802.11 Wireless Network Site Surveying and Installation, 2004, Cisco Press.

[3] kolektiv autorů : Wireless Networking in the Developing World, 2006, Limehouse Book Sprint Team

[4] Gast, M. : 802.11 Wireless Networks The Definitive Guide, 2004, O'Reilly

[5] Zandl, P. : WiFi Praktický průvodce, 2003, Computer Press

[6] Dokumentace a standardy IEEE. URL http://www.ieee.org

[7] Weissgärber, M. : Monitorování a analýza bezdrátových sítí 802.x

Seznam příloh

Příloha 1. CD s naměřenými hodnotami a zdrojovými texty.