UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Podpora laboratorní výuky bezdrátových sítí LAN

Marcel Pašta

Bakalářská práce
2012

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2011/2012**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Marcel Pašta**
Osobní číslo:	**I08133**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Podpora laboratorní výuky bezdrátových sítí LAN**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem bakalářské práce je připravit laboratorní úlohy zaměřené na procvičení problematiky bezdrátových sítí LAN. Součástí práce bude podrobná dokumentace a přesné návody jak postupovat při plnění laboratorních cvičení.
V teoretické části budou popsány principy bezdrátových sítí LAN, používané standardy a faktory ovlivňující bezdrátové přenosy. Praktická část bude obsahovat podrobné a přesné zadání laboratorních úloh, zaměřených na procvičení principů bezdrátových sítí LAN. Dále bude obsahovat přesný popis řešení dané úlohy a použitého softwaru a hardwaru. Součástí úloh bude popis způsobu odchytávání provozu na bezdrátových sítích. Zakreslení schématu zapojení bude vytvořeno pomocí Microsoft Office Visio s doplňky od Cisco Icons (http://resources.cisco.com/app/tree.taf?asset_id=64914&public_view=true).

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

J. CARROLL, Brandon. Bezdrátové sítě Cisco. Brno : Computer Press, 2009. 478 s. ISBN 978-80-251-2884-8.
SOSINSKY, Barrie. Mistrovství ? počítačové sítě. Brno : Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.
PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace. Brno : Computer Press, 2005. 200 s. ISBN 80-251-0791-4.

Vedoucí bakalářské práce: **Ing. Soňa Neradová**
Katedra softwarových technologií

Datum zadání bakalářské práce: **16. prosince 2011**
Termín odevzdání bakalářské práce: **11. května 2012**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Cegan, Ph.D.
vedoucí katedry

V Pardubicích dne 30. března 2012

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 16. 8. 2012 Marcel Pašta

Poděkování

Na tomto místě bych chtěl vyjádřit poděkování Ing. Soně Neradové za poskytnutí studijních materiálů a připomínek vedoucí k vypracování této práce. Stejně tak bych chtěl poděkovat své rodině jak za finanční, tak i psychickou podporu.

Anotace

V teoretické části se tato bakalářská práce věnuje vysvětlení základních principů bezdrátových sítí LAN. Popisuje, jakým způsobem se bezdrátové sítě rozdělují, jaké standardy se používají a jakým způsobem se sítě zabezpečují proti útočníkům. Navíc jedna z kapitol popisuje faktory, které ovlivňují funkčnost bezdrátových sítí.

Praktická část je věnována laboratorním úlohám. Celkem je sepsáno sedm různých cvičení, které procvičují znalosti nabyté z teoretické části. Ve většině případů na sebe jednotlivé úlohy navazují a každá další úloha obohacuje předcházející o další nový úkol. U každého cvičení je napsáno, jaké hardwarové a softwarové vybavení je ke zdárnému splnění potřeba. Pro kontrolu, zda se úkony podařilo správně vykonat, je v přílohách této práce obsažen jak postup instalace, tak i odpovědi na všechny zadané otázky.

Klíčová slova

bezdrátová síť, Wi-Fi, WLAN, IEEE 802.11, WEP, WPA, WPA2, laboratorní úloha

Title

Support of laboratory education of wireless LAN.

Annotation

The theoretical part of this bachelor thesis is devoted to the explanation of basic principles of wireless LANs. It describes how the typical WLAN networks are divided, which standards are commonly used and which ways are used to secure the network against intruders. In addition, one of the chapters describes factors that affect performance of wireless networks.

The practical part is devoted to laboratory tasks. In total there are seven different exercises that practice newly acquired knowledge gained from theoretical part of this thesis. In most cases, the individual tasks follow each other and enhance previous ones with another new challenge. The summary of all needed hardware and software equipment that are needed to successful completion are also written in each exercise. The complete installation procedure and answers for all given questions are included in some appendixes of this thesis to check whether the tasks are properly done.

Keywords

wireless network, Wi-Fi, WLAN, IEEE 802.11, WEP, WPA, WPA2, laboratory task

Obsah

Seznam zkratek

AAA	Authentication, Authorization, and Accounting
ACS	Cisco Secure Access Control Server
AES	Advanced Encryption Standard
AP	Access Point
ASCII	American Standard Code for Information Interchange
BSA	Basic Service Area
BSSID	Basic Service Set Identification
CA	Certificate Authority
CCK	Comlementary Code Keying
CCMP	Cipher Block Chaining Message Authentication Code
CDMA	Code Division Multiple Access
DBPSK	Differential Binary Phase-Shift Keying
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DQPSK	Differentially-Encoded Quadrature Phase-Shift Keying
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESA	Extended Service Area
ESS	Extended Service Set
FHSS	Frequency-Hopping Spread Spectrum
GSM	Global Systém for Mobile Communication
GTK	Group Transient Key
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industry, Scientific, and Medical
IV	Inicializační vektor
MAC	Media Access Control
MIMO	Multiple-Input, Multiple-Output
OFDM	Orthogonal Frequency Division Multiplexing
PDA	Personal Digital Assistant
PEAP	Protected Extensible Authentication Protocol
PMK	Pairwise Master Key
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
RADIUS	Remote Authentication Dial In User Service
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol
WEP	Wireless Equivalent Privacy

WI-FI	Wireless Fidelity
WPAN	Wireless Personal Area Network
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WMAN	Wireless Metropolitan Area Network
WWAN	Wireless Wide Area Network

Seznam obrázků

Seznam tabulek

Seznam příloh

Úvod

Studium oboru počítačových sítí se na většině vysokých škol zaměřuje zejména na výuku klasických pevných sítí. Důvodem, proč je právě toto téma tak častou náplní předmětu bývá možnost souběžného studia e-learningových kurzů CCNA I-IV od firmy Cisco. Cisco akademie se však v základních kurzech Wi-Fi sítím věnuje pouze v jedné kapitole, a to jen velice okrajově. Ovšem v případě většího zájmu o tuto problematiku nabízí firma Cisco poměrně pokročilý kurz výuky bezdrátových sítí CCNA Wireless.

Cílem této práce je pojednání o základních principech bezdrátových sítí a jejich aplikace na konkrétních vybraných laboratorních úlohách.

Teoretická část práce by měla čtenářům osvětlit, jakými prvky jsou vlastně sítě tvořeny a podle jakých pravidel spolu daná zařízení mají komunikovat. Krom toho by v úvodní části také měla popsat, jaké druhy bezdrátových sítí existují a podle jakých kritérií jsou rozdělovány.

U všech oborů informatiky platí, že zařízení musí být naprogramovány tak, aby při zachování stejných podmínek vykonávaly vždy stejný úkon. Proto i oblast bezdrátových sítí má svá určitá pravidla a normy, které udávají, jakým způsobem má být vedena vzájemná komunikace koncových uzlů. Tyto normy jsou vydávány a aktualizovány jedenáctou pracovní skupinou organizace IEEE. Mezi nejznámější patří verze IEEE 802.11 a, b, g, n. V dnešní době organizace pracuje na novém režimu 802.11ac, který je zatím ve formě konceptu.

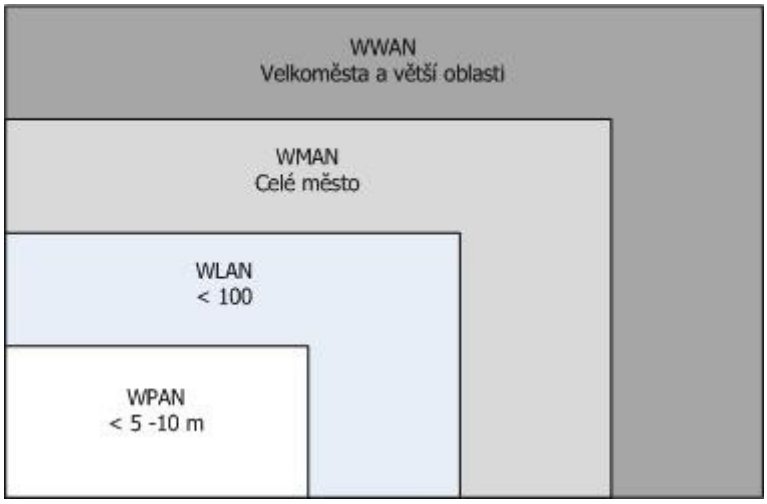
Obdobně jako přenos televizního signálu, pro přenos signálu využívají Wi-Fi sítě elektromagnetického vlnění, které je však v obou případech značně ovlivňováno okolními podmínkami. Většina z nás již určitě zažila, jak bouřka, či silný déšť, dokážou znehodnotit televizní signál. Kvalita spojení bezdrátových zařízení podléhá stejným přírodním podmínkám také. Jakým způsobem a jakými vnějšími faktory se signál dokáže zkreslit, o tom pojednává třetí kapitola této práce.

Kromě přírodních podmínek jsou sítě vystaveny i jiným druhům ohrožení. Jedním z nich jsou hackeři, počítačoví experti, kteří se snaží sítě nabourat a odcizit z nich důvěrná data. Tomuto nešvaru informatiky je potřeba se intenzivně věnovat a sítě zabezpečovat tak kvalitně, jak to je jen možné. Poslední, za to nejrozsáhlejší teoretická kapitola, se nejen věnuje různým druhům útoků, ale také rozlišným způsobům, jak se jim úspěšně ubránit.

Praktická část je tvořena především laboratorními úlohami. Celkem je uvedeno sedm různých úloh, které mají za úkol propojit znalosti nabyté v předcházejících kapitolách s aplikací do praxe. Na každou teoretickou kapitolu se tak odkazuje jedna až dvě úlohy. Vzhledem k tomu, jakou rychlostí se obor informatiky vyvíjí, tak jsou úlohy psány v co možná nejobecnějším ražení. Každá úloha obsahuje zadání, soupis potřebného hardware i software, nástin správného postupu a také správné řešení.

1 Rozdělení bezdrátových sítí

Bezdrátová síť se používá k propojení a následnému přenosu dat mezi různými zařízeními, a to bez pomoci metalické kabeláže. K přenosu signálu se na rozdíl od klasické kroucené dvojlinky využívá elektromagnetických vln. Komunikujícími uzly na této síti nemusí být jen počítače, ale mohou jimi být například i mobilní telefony, PDA nebo bezdrátové tiskárny. Bezdrátové sítě se obdobně jako pevné standardně rozdělují do čtyř skupin, podle jejich rozsáhlosti. Nejmenší z nich je přitom tzv. osobní síť, která má za úkol hlavně připojení různých druhů periférií k počítačům. Naopak největší je takzvaná rozsáhlá bezdrátová síť, která je používána zejména k propojování větších měst. Každá z těchto čtyř skupin využívá ke svému provozu jiných technologií a pomocných zařízení, lišících se například používanou frekvencí, šířkou pásma a řadou dalších charakteristik. Ty se týkají zejména dosahu, síly signálu, používaného spektra a přenosové rychlosti. Na obrázku 1 je znázorněn rozsah všech čtyřech typů bezdrátových sítí. [17]



Obrázek 1 - Přehled rozlehlosti bezdrátových sítí

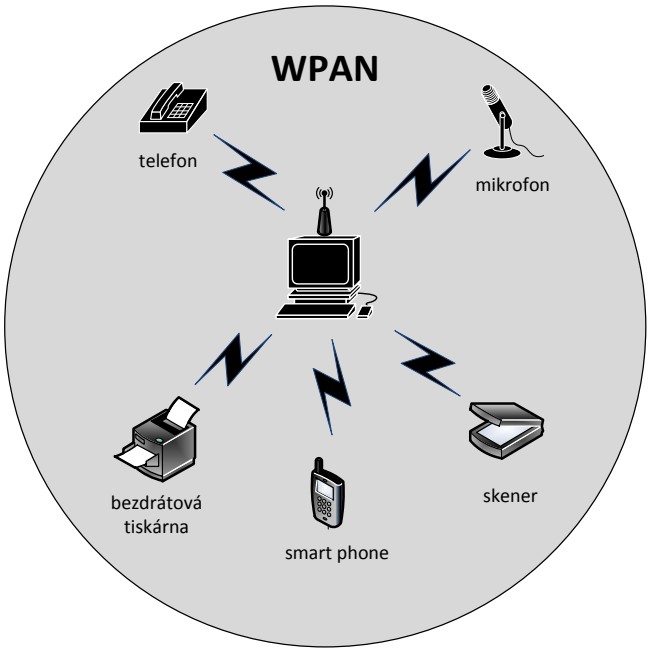
1.1 Bezdrátová osobní síť (WPAN)

Tato síť se anglicky nazývá Wireless Personal Area Network (WPAN). Jejím hlavním účelem je propojování menších zařízení, zejména periférií. Nejznámějším typem této malé sítě je Bluetooth. Ta je známa jako jeden ze způsobů, jak propojit dva mobilní telefony navzájem, ale také jako možnost připojení bezdrátových sluchátek, tiskáren, či jiných periférií k počítači. Na jedné takovéto síti může existovat větší množství zařízení, ačkoliv aktivních může být jen 8 z nich ve stejnou dobu. Jejich vzájemná komunikace probíhá v nelicencovaném 2,4 GHz pásmu přenosovou rychlostí až 3 Mbit/s. Bluetooth je detailně popsán pracovní skupinou IEEE 802.15.1. Některá zařízení, která mohou na síti typu WPAN pracovat, jsou vyobrazena na obrázku 2. [17]

Další známou osobní sítí je ZigBee, která našla uplatnění především v průmyslové automatizaci. Ta je popsána normou IEEE 802.15.4.

Charakteristika osobních sítí WPAN: (převzato z [2], str. 70)

- Krátký dosah – jen asi do 6 metrů.
- Osm aktivních zařízení.
- Nelicencované pásmo 2,4 GHz.
- Nazývá se také piconet.



Obrázek 2 - Charakteristické znázornění sítě WPAN (Bluetooth)

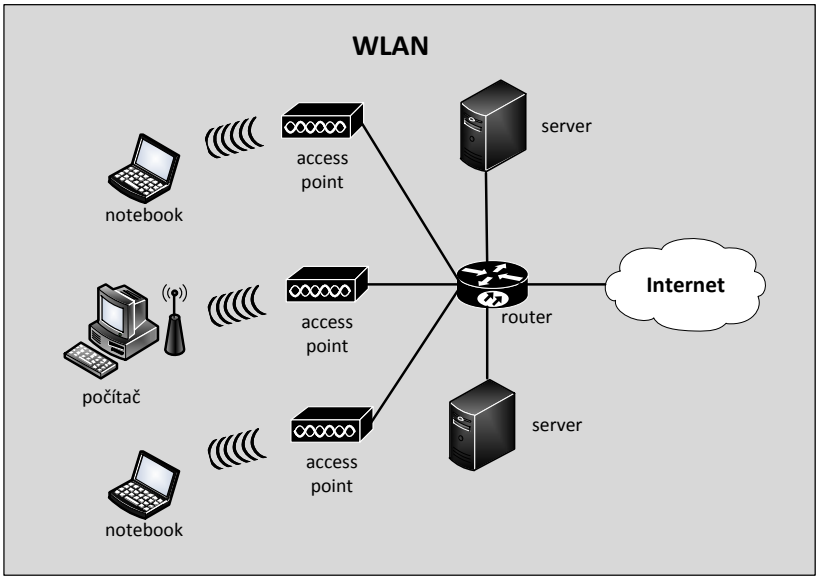
1.2 Bezdrátová místní síť (WLAN)

Obdobu klasické kabelami propojené LAN najdeme v bezdrátových sítích také, a to pod anglickým názvem Wireless Local Area Network (WLAN). Bývá vytvářena jak v domácnosti, tak v kanceláři, či kterémkoliv větším podniku. Slouží jak k přímému propojení jednotlivých počítačů mezi sebou anebo i přes routery, či přístupové body, tzv. access pointy. Na rozdíl od předcházejícího typu, WLAN sítě dokážou pracovat v několika různých režimech. Prvním, který na trh výrazněji prorazil, byl 802.11b, pracující v pásmu 2.4 GHz. Jako další následoval standard 802.11a, využívající druhé pásmo, 5 GHz. Kromě těchto dvou zmíněných se dnes používají i jiné verze, zejména pak 802.11g a 802.11n. Všechny zmíněné sítě používají obdobně jako WPAN nelicencované frekvenční pásmo.

Dosah sítě se zvýšil z délky pokoje na hodnoty blízké i 100 metrů. Tohoto čísla lze však dosáhnout pouze na otevřeném prostranství. S vyšším dosahem se však také častěji stává, že se na větším prostoru potkává více sítí zároveň. Jelikož se dvě vlnění vysílané na stejné frekvenci ovlivňují, častěji pak dochází ke kolizím signálu a k nefunkčnosti sítí. Dalším věcí, na kterou je potřeba myslet, je vyzařovací výkon antény, který je limitován státem. Příklad sítě WLAN, kde se propojuje několik počítačů pomocí access pointů přes router k servrům, je zobrazen na obrázku 3. [17]

Charakteristika místních sítí WLAN: (převzato z [2], str. 71)

- Frekvenční pásmo 2,4 GHz (IEEE 802.11b, g) nebo 5 GHz (IEEE 802.11a).
- Větší dosah než síť WPAN – od přístupového bodu ke klientovi až 100 metrů.
- Pro dosažení větší vzdálenosti je potřeba vyšší vysílací výkon.
- Nejedná se o osobní síť; zpravidla bývá zapojeno více klientů.
- Sítě WLAN jsou velmi flexibilní, protože na rozdíl od sítě WPAN mohou obsahovat více než osm aktivních zařízení (klientů).



Obrázek 3 - Příklad sítě WLAN

1.3 Bezdrátová metropolitní síť (WMAN)

Bezdrátové místní sítě, jak bylo řečeno výše, dokážou pokrýt i 100 metrovou vzdálenost, což ovšem není vždy úplně dostačující. Představme si firmu, která se z původního malého sídla rozrostla a začala si vytvářet další pobočky v různých částech větších měst. V tomto případě pak podnik musí implementovat metropolitní síť, anglicky známou jako Wireless Metropolitan Area Network (WMAN). WMAN se zejména využívá jako páteřní síť, která buď propojuje dvě místa pomocí dvoubodového spojení (point-to-point), nebo několik míst pomocí vícebodového připojení (point-to-multipoint). [17]

Bohužel hlavním záporem větší WMAN sítě je, že s rostoucí vzdáleností propojovaných uzlů také roste počet zařízení, které signál po své cestě ovlivňuje. Právě z tohoto důvodu se tento druh sítě obvykle nesestrojuje v nelicencované podobě. Proto je v mnoha případech nezbytné zaplatit nemalý licenční poplatek, ale mít za to určité frekvenční pásmo pouze pro sebe. [17]

S rostoucí vzdáleností koncových uzlů sítě se také snižuje přenosová rychlost, které lze dosáhnout. Nejznámějším realizováním velké rozlehlé sítě je WiMax (802.16b). Jelikož náklady na provozování jsou bohužel obrovské, a tak je často výhodnější využít již některé stávající sítě a platit pak poskytovali služeb za poskytnutou šířku pásma. [17]

Charakteristika metropolitních sítí WMAN: (převzato z [2], str. 72)

- S rostoucí vzdáleností klesá přenosová rychlost.
- Její rychlost je blízká spíše širokopásmovému připojení než ethernetu.
- Používá se jako páteřní síť, dvoubodové spojení nebo vícebodové připojení.
- Nejznámější je pod zkratkou WiMax.

Příklady používaných norem:

- IEEE 802.16 (WiMax)

1.4 Bezdrátová rozlehlá síť (WWAN)

Poslední a také největší sítí je takzvaná bezdrátová rozlehlá síť (Wireless Wide Area Network – WWAN). Na rozdíl od jejich menších předchůdců ji již zpravidla nelze vytvořit a provozovat bezplatně, ba naopak, veškeré náklady s ní spojené se šplhají do poměrně vysokých částek. Její rychlost je v porovnání s ostatními o dost menší, pohybuje se většinou okolo 115 Kb/s. Nejrozšířenějšími typy WWANu jsou mobilní sítě GSM (Global Systém for Mobile Communication) a CDMA (Code Division Multiple Access). [2], [17]

Charakteristika rozlehlých sítí WWAN: (převzato z [2], str. 72)

- Nízká přenosová rychlost.
- Platba za používání
- Vysoké náklady na provozování

1.5 Rozdělení sítí podle IEEE 802.11

Na předchozích řádcích byly bezdrátové sítě rozděleny z hlediska jejich rozlehlosti. Následující kapitoly se budou věnovat již přímo nejběžnějšímu druhu sítě, a to konkrétně místní, WLAN. Jak však taková WLAN síť vypadá a jaké zařízení na ní fungují a hlavně, jakým způsobem spolu komunikují, tomu se bude tato práce věnovat v dalších kapitolách, věnovaných topologii 802.11.

Původní návrh pracovní skupiny 802.11 neobsahoval pouze jednotlivé typy sítí, ale také topologie, jak kterou danou síť postavit. Základními typy jsou ad-hoc a síť v režimu infrastruktury.

1.5.1 Ad-hoc

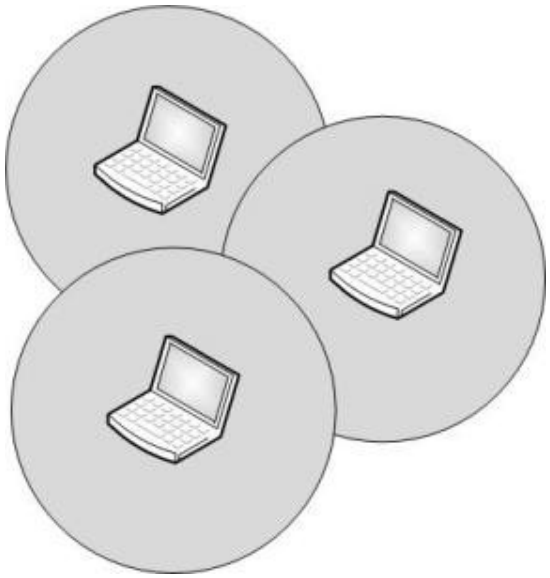
Ad-hoc síť vznikne v případě, že se spolu chtějí dvě zařízení propojit napřímo. Obvykle se tak činí v případech, kdy není nutné síť budovat natrvalo. Klasickým případem může být situace, kdy se dva kamarádi dohodnou na společné návštěvě, kde chce jeden druhému nakopírovat některé svá data. Ad-hoc síť je tak velmi podobná metalické síti zvané peer-to-peer, jen k propojení účastníků nepotřebuje síťový kabel. Výhodou těchto sítí je, že její koncové uzly nepotřebují žádné další fyzické zařízení, které by datový tok mezi nimi usměrňovalo. Nevýhodou pro změnu je, že tuto roli musí jeden z účastníků převzít. Představte si místnost, ve které by stálo 5 lidí, a všichni by najednou začali hovořit a navíc ještě ke všemu každý jiný jazykem. Proto v každé síti musí být jakýsi rozhodčí, který bude udávat, podle jakých pravidel bude komunikace probíhat. Po technické stránce je v to modelu ad-hoc ten, který danou síť vytváří. Na tento rozhodující počítač se pak ostatní napojí. Při vytváření sítě musí uživatel ještě nastavit některé základní parametry, aby pak komunikace stanic bezproblémově fungovala. Na rozdíl od přístupového bodu má však u toho jen velmi omezené možnosti. Například nemůže použít žádné pokročilé mechanismy, jako je třeba autentizace. Za zmínku také stojí, že bez jakékoliv centrální správy musí také rozhodující stanice určovat pořadí vysílání všech ostatních tak, aby nedocházelo ke zbytečným kolizím signálu. [21]

Když vezmeme všechna zařízení, která se takto navzájem propojí, tak nám vytvoří množinu zvanou Basic Service Set (BSS). Pro pořádek nutno dodat, že jelikož tato síť neobsahuje žádný přístupový bod, ani router, lze název ještě poupravit na Independent [1]Basic Service Set (IBSS). Síť totiž není na žádném centrálním zařízení závislá. [20]

Při tvorbě ad-hoc sítě může na rozdíl od pevné nastat ještě jeden zajímavý problém. Vzhledem k tomu, že každé zařízení může využívat jinak silnou anténu, tak jedno zařízení může o svém protějšku vědět, zatímco druhé o prvním ne. Tato situace se může přihodit zejména při tzv. roamingu, čili činnosti, kdy jedno zařízení někdo přenese například do vedlejší místnosti. Proto je důležité vědět, že síť bude fungovat pouze tehdy, když se obě zařízení navzájem „uvidí“. [21]

[1] Slovo independent znamená v překladu do češtiny nezávislý.

Na obrázku 4 je znázorněn příklad sítě, kde spolu komunikují tři zařízení v režimu ad-hoc. Okolo každého je také zobrazena oblast dosahu jejich vysílání. Pokud „hlavní“ stanice vypadne, ať už z jakéhokoliv důvodu, síť se na chvilku rozpadne a dojde tak ke ztrátě komunikace. Naštěstí však roli suplujícího hlavního zařízení po malé chvíli převezme jiný počítač, a síť funkčnost sítě se tím navrátí do původního stavu.



Obrázek 4 - Ad-hoc síť

Značným nedostatkem ad-hoc sítě je, že každý její účastník je vlastně přijímačem a vysílačem zároveň. Jelikož pracovní stanice mají obvykle jen jednu anténu, musí spolu komunikovat v polovičním duplexu (half duplex). To znamená, že nemohou přijímat a odesílat data současně. Právě proto spolu jednotlivé strany nemohou komunikovat plnou rychlostí.

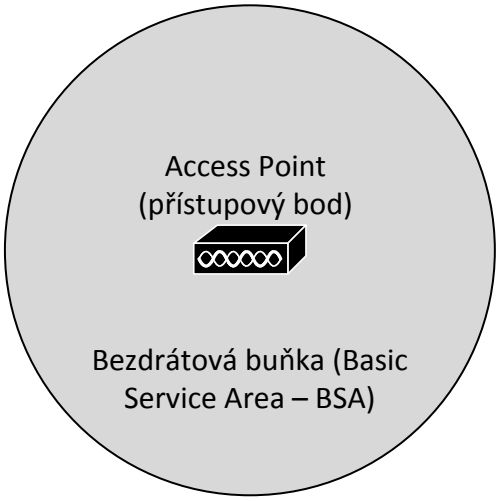
1.5.2 Infrastrukturní síť

Druhou a častěji používanou topologií je takzvaná síť v režimu infrastruktury. Oproti předcházející modelu již obsahuje alespoň jeden centrální prvek, ke kterému se pracovní stanice připojují. Toto centrální zařízení nazýváme přístupovým bodem (access pointem, AP). Na rozdíl od ad-hoc sítí, není v dnešní době neobvyklé, že nová, ale také dražší zařízení disponují více anténami, některými určenými k vysílání a některými k příjímání. Bohužel pro každou anténu stále platí, že může v jednu chvíli buď vysílat anebo přijímat. A pokud navíc má přístupový bod anténu pouze jednu, je na tom s vysíláním obdobně, jako na tom byl klasický počítač v ad-hoc síti. Celá síť pak musí pracovat v tzv. polovičním duplexu (half-duplexu).

Z těchto vět se na první pohled může zdát, že přístupový bod je vlastně pouhým rozbočovačem. Rozdílem mezi těmito dvěma zařízeními je, že access point má již jistou inteligenci a data jen dál surově nepřeposílá. Dokáže totiž z hlaviček příchozích rámců vyčíst MAC adresy a pomocí nich rozhodnout o tom, kam vlastně má rámec putovat dál. O této problematice dále pojednává kapitola 2.6 Hlavičky rámců v bezdrátové síti. [21]

Centrálním prvkem WLAN sítě v režimu infrastruktury je tedy již zmíněný access point, na kterého se klienti napojují. Oblast, kterou dokáže jeden bod pokrýt, se nazývá Basic Service Area (BSA), česky znám jako bezdrátová buňka. Krom BSA je často používaným pojmem ještě celková oblast pokrytí dané sítě. Tato oblast je rovna součtu všech BSA od všech vysílačů, které v síti působí. V případě, že má síť pouze jeden vysílací bod, tak se oblast BSA a oblast pokrytí celé sítě rovnají. Názorný příklad jednoho přístupového bodu a tudíž i jedné bezdrátové buňky je zobrazen na obrázku 5.

V podnikových sítích je ale samozřejmé, že jeden přístupový bod pro pokrytí celého sídla stačit nebude. Proto se vícero přístupových bodů zpravidla napojuje na společnou síť pomocí metalické kabeláže. Poskytují pak svým klientům přístup do sítě na mnohem větším prostoru. V tomto případě access point je zároveň přemostěním mezi sítí pevnou (definovanou v IEEE 802.3) a bezdrátovou (definovanou v IEEE 802.11).



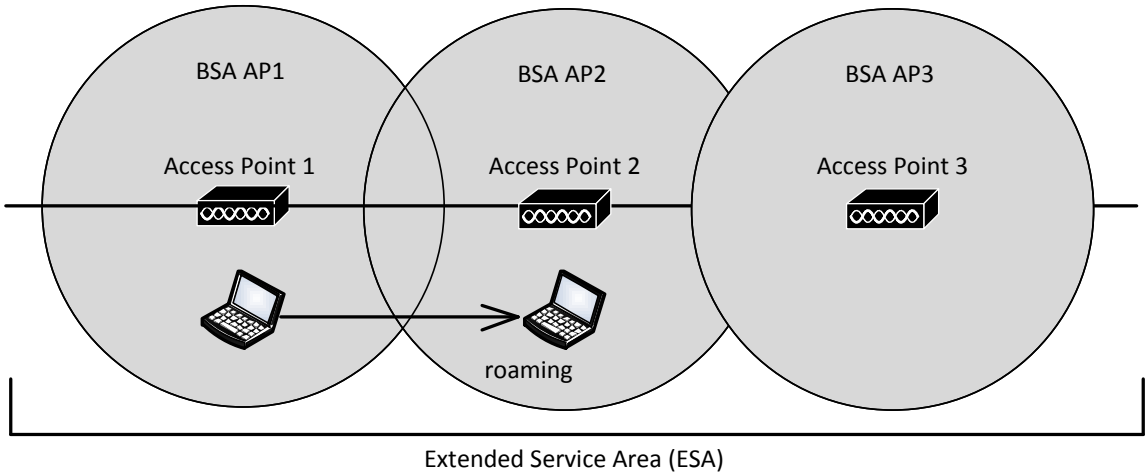
Obrázek 5 - Basic Service Area (BSA)

Větší podnikové sítě obsahují více jak jeden přístupový bod, což klientským zařízením na síti poskytuje značné výhody. Prvním a hlavním důvodem nasazení dalších přístupových bodů do sítě je, že se oblast celkového pokrytí signálem značně zvyšuje. Oblast, ve které působí více než jedno vysílací zařízení, nazýváme rozšířenou, Extended Service Area (ESA). Pro klienty to nese tu výhodu, že se na území celé ESA mohou pohybovat dle libosti a jejich bezdrátová zařízení přitom zůstávají nadále připojena ke stále stejné síti LAN. Tato činnost, kdy díky pohybu jedno zařízení mění přístupový bod, ke kterému je napojen, je označována slovem roaming. Na obrázku 6 jsou zobrazeny 3 přístupové body, které jsou zároveň propojeny a zvětšují tak dosah jedné sítě. Zároveň na stejném obrázku lze spatřit příklad roamingu, kdy se laptop přesunul natolik, že ho již první přístupový bod nemohl obsluhovat a přístup k síti mu tak musí poskynout bod druhý. [21]

Po technické stránce funguje roaming tak, že jakmile kterékoliv zařízení zjistí pokles signálu pod určitou hranici, začne v okolí vyhledávat jiné přístupové body. Vybere si pak takový, který mu dokáže momentálně poskytnout nejvyšší signál. Pro správnou

činnost roamingu je důležité síť postavit tak, aby se oblasti pokrytí signálem jednotlivých přístupových bodů částečně překrývaly. Kdyby tomu tak nebylo a signál by v určitých místech klesl na hodně nízkou hodnotu, zařízení by začalo ztrácet přístup k síti. Pro jednoduchou představu, jak roaming pracuje, nemusíme od bezdrátových sítí chodit daleko. Stačí si vybavit, na jakém principu pracují mobilní GSM sítě. Operátoři jednotlivých společností rozmístili po celé republice vysílače tak, aby jejich signál pokryl pokud možno co nejvíce míst v celé republice. Mobilní telefon si pak vysílač vybírá podle toho, který mu poskytne lepší signál. Uživatel je navíc o kvalitně připojení informován přímo na displeji telefonu. [19]

Výše zmíněný případ, kdy je nutné do sítě přidat další přístupový bod však samozřejmě není jediným. Dalším může být, když v jedné BSA je napojeno mnoho klientů a access point pak lidově řečeno nestíhá. Tento případ uživatelé obvykle poznají velmi rychle, protože se rychlost přenosu dat pro ně rapidně snížila. Proto je pak administrátor nucen umístit další přístupový bod poblíž existujícího a tím zajistit, že se ne všechny stanice napojí jen na jeden bod, ale rozprostřou se na oba.



Obrázek 6 - Extendead Service Area (ESA)

1.5.3 Pojmenování sítí (Service Set Identifier - SSID)

Na předcházejících řádcích byly popsány různé druhy sítí. Nebylo však popsáno, jak se na jednotlivé sítě napojit. Jako každý člověk má své jméno a příjmení, tak i síť má své pojmenování. Tomuto názvu se říká identifikátor množiny služeb (Service Set Identifier – SSID). A jak takový název zjistit? Možnosti jsou dvě, buďto administrátor síť nastavil tak, že přístupový bod o své přítomnosti své okolí sám informuje anebo se uživatel musí jméno sítě dozvědět od administrátora osobně.

V prvně zmíněném případě přístupový bod vysílá každých pár vteřin tzv. majákový rámec obsahující SSID sítě spolu se svoji MAC adresou. Z hlediska bezpečnosti je však toto tovární nastavení jistou slabinou, ačkoliv pro uživatele mnohem snadnější volbou, než možnost druhá. Je pochopitelné, že pokud útočník síť a její SSID neuvidí, nemusí si ji ani všimnout a nebude se tak do ní snažit nabourat. V praxi však zakázat vysílání SSID

do okolí bohužel nestačí, jelikož útočník může zachytit komunikaci jakéhokoliv klienta s přístupovým bodem a tak se dozvědět, že síť v okolí existuje.[5]

Údaje, které poskytují majákové rámce, jsou poměrně důležité při již několikrát zmiňovaném roamingu. Pokud klientovi klesne signál od jednoho přístupového bodu, začne číst všechny majákové rámce, které uslyší a vybere si z nich všechny takové, které obsahují shodné SSID se sítí, ke které je momentálně napojen. Z nich pak vybere ten s co možná nejvyšším signálem.[5]

Praktickým příkladem roamingu může být uživatel, který vlastní bezdrátového klienta (např. laptop) a připojuje se k jedné síti s určitým SSID (např. Linksys) a určitou MAC adresou (00:00:00:00:00:AA). Pokud pak přenese svůj laptop na druhou stranu budovy, pravděpodobně mu síla signálu od původního přístupového bodu klesne natolik, že se jeho zařízení pokusí vyhledat nějaký jiný vysílací bod, který mu poskytne silnější signál. Přičemž platí, že oba vysílací body budou mít stejné SSID (v tomto případě Linksys), ale jinou MAC adresu (druhý bod např. 00:00:00:00:00:BB).[5]

2 Standard 802.11

Na bezdrátových sítích typu LAN existuje několik protokolů, standardů, které popisují, jak se má daná síť chovat, a podle jakých pravidel se mají řídit. Na standardizaci těchto protokolů se podílí organizace IEEE, konkrétně její 11. pracovní skupina. Nejznámějšími protokoly, které se na místních sítích využívají, jsou 802.11 a, b, g, n. Kromě těchto čtyř však existují i další dodatky (c-f, h, j), ale ty jen upřesňují výše zmíněné varianty. Protokoly a, b, g, n se liší od sebe navzájem především v použitém frekvenčním pásmu. Mimo to však také ještě v typu modulace signálu, či kódování dat. Díky těmto dvěma parametrům se výrazně liší teoretické i maximální přenosové rychlosti, které s daným protokolem lze na síti dosáhnout a to i za použití jedné a té samé antény. [22]

2.1 Původní návrh 802.11

První návrh, od kterého se datuje vznik bezdrátových sítí, byl vydán v roce 1997. Dnes se však již sítě využívající tento původní návrh téměř nevyskytují. Jeho zánik byl zapříčiněn především jeho maximální přenosovou rychlostí, která činila na dnešní dobu pouhých 1-2 Mb/s. Standard 802.11 uměl využívat dvou modulačních technik signálu, a to FHSS (Frequency-Hopping Spread Spectrum) a DSSS (Direct Sequence Spread Spectrum).[2]

Byl navržen pro komunikaci v bezlicenčním pásmu ISM (Industry, Scientific, and Medical) a operoval pouze v rozsahu 2,4 GHz. Toto pásmo zahrnuje celkem 14 různých kanálů pro komunikaci, ovšem uvolněných k volnému použití bývá zpravidla buď prvních 11 (USA) nebo 13 (Evropa). Počet těchto uvolněných kanálů není na celém světě jednotný, každý stát ho definuje dle svých úvah. Jelikož je 2,4 GHz pásmo poměrně náchylné k rušení, a to jednak ostatními spotřebiči v dosahu, tak ale i ostatními sítěmi, tak se jako prevence proti vzájemnému rušení sítí obvykle používají kanály 1, 6 a 11.

Základní charakteristiky původního návrhu 802.11 jsou napsány v následující tabulce č. 1.

Tabulka 1 - Charakteristika původního návrhu 802.11 (převzato z [2], str. 112)

Schválen	1997
Radiofrekvenční technologie	FHSS a DSSS
Frekvenční spektrum	2,4 GHz

[2] Vzhledem k rozsáhlosti tématu modulačních technik se jim tato studie dále věnovat nebude. Pokud by však někdo chtěl tuto tématiku pochopit, dobré vysvětlení lze nalézt například v anglicky psaném článku na http://sorin-schwartz.com/white_papers/fhvsds.pdf. Alternativou může být kapitola Jak fungují modulační techniky z knihy Bezdrátové sítě Cisco (viz použitá literatura).

2.2 Protokol 802.11a

O dva roky později, roku 1999, ratifikovala 11tá pracovní skupina nový standard pro bezdrátové místní sítě, a tím byl 802.11a. Ten na rozdíl od původního návrhu pracuje v pásmu 5 GHz. Tato změna poskytuje sítím několik výhod a nevýhod zároveň. Kvůli jinému frekvenčnímu pásmu není kompatibilní s protokoly 802.11, 802.11b a 802.11g. Na druhou stranu však sítě využívající tyto protokoly síť na protokolu 802.11a nikterak neruší a proto je možné je provozovat vedle sebe navzájem. [22]

Velký problém 2.4 GHz pásma je jeho velké přeplnění. Z toho důvodu pak často dochází k výpadkům sítí. V jednom místě se daly bez vzájemného rušení nasadit pouze 3 sítě, využívající kanály 1, 6 a 11. Oproti tomu 802.11a začal původně nabízet 12 kanálů, které se navíc díky modulaci OFDM mohou i částečně překrývat. Nedávno však větší množství států uvolnilo frekvenční pásmo v rozsahu 5,47 až 5,725 GHz také k nelicencovanému použití. Počet nepřekrývajících se kanálů se tak zdvojnásobil. Poslední velkou a velmi příjemnou změnou, kterou tento standard přinesl, je maximální přenosová rychlost. Tento protokol je postaven tak, aby umožňoval přenášet data rychlostmi 6, 12, 24 a 54 Mb/s, což je oproti původnímu návrhu velké plus. [22]

Protokol 802.11a se do praxe začal zavádět právě z důvodu vyšší přenosové rychlosti. Bylo však nutné vyměnit většinu zařízení na síti, jelikož staré přístupové body nebyly na 5 GHz pásmo konstruovány. Díky této skutečnosti byl jeho rozkvět mírně zpomalen. Navíc, s příchodem variant 802.11g a n, se jeho nasazování ještě více zmenšilo.

Charakteristické vlastnosti protokolu 802.11a jsou napsány v následující tabulce č. 2.

Tabulka 2 - Charakteristika protokolu 802.11a (převzato z [2], str. 118)

Schválen	1999
Radiofrekvenční technologie	OFDM
Frekvenční spektrum	5 GHz
Kódování	Točivé kódování
Modulace	BPSK, QPSK, 16-QAM, 64-QAM podle dílčího přenašeče
Přenosové rychlosti	6, 9, 12, 18, 24, 36, 48, 54 Mb/s s modulací OFDM
Nepřekrývající se kanály	Každé pásmo má 4; prostředních 8 se používá s 52 dílčími přenašeči na každém kanálu

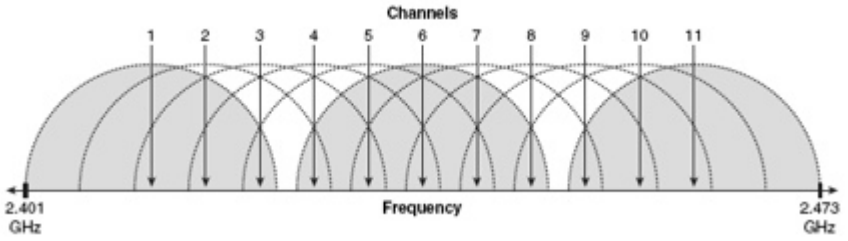
2.3 Protokol 802.11b

S příchodem kabelových sítí, které nabízely rychlosti 10 Mb/s, začal původní protokol 802.11 rychle zastarávat. Jeho rychlost, a to 1-2 Mb/s, přestala uspokojovat potřeby zákazníků, kteří požadovali rychlosti značně vyšší. Proto dodavatelé začali vyvíjet vlastní metody, jak vyšších rychlostí dosáhnout. Díky tomu začal hrozit problém

nekompatibility zařízení od různých firem. Úlohou organizace IIEE tak bylo navrhnutí standardu, který by měli dodavatelé dodržovat, aby spolu dvě zařízení od jiných firem mohly bez problémů pracovat. A aby role pracovní skupiny IEEE nebyla tak snadná, musela navíc řešit problém zpětné kompatibility se staršími zařízeními, jelikož po celém světě existovalo mnoho sítí pracujících dle původního návrhu 802.11. Jinak by totiž kvůli zavedení nových zařízení, které budou nový protokol podporovat, bylo nutné vyměnit všechny prvky v celé síti, což je záležitost značně finančně nákladná. Pracovní skupině IEEE se i přes toto všechno podařilo v září roku 1999 vydat doplněk 802.11b, který rozšiřuje a obohacuje původní návrh 802.11. Tento protokol se stal rychle velmi oblíbeným a dodnes (rok 2012) je ještě často používán. [22]

Přenosová rychlost nového protokolu 802.11b je až 5x vyšší než ta, kterou poskytoval původní návrh. Technika přenosu signálu na původních rychlostech (1-2 Mb/s) zůstala beze změny, právě z důvodu zachování kompatibility s původním návrhem. Za to nový režim pracující rychlostí 5,5 Mb/s a 11 Mb/s využívá odlišné kódování i jiný druh modulace. Kódování se změnilo z Barker 11 na CCK (Comlementary Code Keying) a modulace z DBPSK (Differential Binary Phase-Shift Keying) na metodu DQPSK (Differential Quadrature Phase-Shift Keying). Popis a vysvětlení těchto technik je značně obsáhlý a pro níže uvedené úlohy není důležitý, proto se mu tato práce věnovat podrobně nebude. [22]

Rozdělení 2.4 GHz pásma v protokolu 802.11b zůstává stejné jak v původní variantě, tedy je k dispozici 11 kanálů v USA a 13 v Evropě. Na obrázku 7 je znázorněno těchto 13 použitelných kanálů, každý o šířce 22 MHz. Novinkou však je, že varianta 802.11b obsahuje metodu DRS (Dynamic Rate Shifting). Tato metoda umožňuje dynamicky měnit rychlost připojení zařízení podle změny okolních podmínek, kterými může být šum anebo také změna vzdálenosti komunikujících zařízení.



Obrázek 7 - Kanály pracující na frekvenci 2,4 GHz[3]

[3] Obrázek z http://farm4.static.flickr.com/3511/3896175717_1c00ccd917.jpg

Charakteristika protokolu 802.11b jsou napsány v následující tabulce č. 3.

Tabulka 3 - Charakteristika protokolu 802.11b (převzato z [2], str. 113)

Schválen	1999
Radiofrekvenční technologie	DSSS
Frekvenční spektrum	2,4 GHz
Kódování	Barker 11 a CCK
Modulace	DBPSK a DQPSK
Přenosové rychlosti	1, 2, 5,5 a 11 Mb/s
Nepřekrývající se kanály	1, 6, 11

2.4 Protokol 802.11g

Protokol 802.11g byl zveřejněn organizací IEEE v roce 2003 jako rozšíření standardu 802.11b. Hlavním podnětem, proč nový protokol vytvořit, byl opět požadavek klientů na zavedení vyšší přenosové rychlosti. Nový standard jim tedy vyhověl a zvýšil maximální přenosovou rychlost na 54 MB/s. Právě tímto krokem se vyrovnala maximální přenosová rychlost, kterou jsme schopni dosáhnout na obou nelicencovaných pásmech, jak na 2,4 GH, tak na 5GHz. Standard 802.11g je dalším, který operuje v pásmu 2.4 GHz a je navíc kompatibilní s předchozími variantami 802.11 a 802.11b. Díky těmto dvěma novinkám začal protokol 802.11a pomalu ztrácet na oblibě ve prospěchu variant b/g. [22]

Kvůli kompatibilitě se staršími protokoly je ve verzi g pro rychlosti 1, 2, 5,5 a 11 Mb/s využita stejná modulace i kódování signálu stejně jako v protokolu 802.11b. Pro vyšší rychlosti přenosu dat je použita modulace metodou OFDM (Orthogonal Frequency Division Multiplexing), kterou už několik let využíval protokol 802.11a. [22]

Bohužel na rozdíl od varianty 802.11a v době zavedení tohoto standardu bylo již frekvenční pásmo 2.4 GHz často přeplněné a docházelo na něm k rušení a následným výpadkům signálu. Z důvodu zpětné kompatibility však varianta 802.11b využívá stále stejné kanály jako předcházející varianty a tak tento problém neřeší.

Poslední poznámkou je, že u vyšších rychlostí poskytovaných variantou g je kvůli modulaci metodou OFDM nutné kontrolovat nastavení výstupního výkonu antény. Nízký výkon má za následek výpadky a krátký dosah sítě, velký výkon zase nelze použít kvůli státem nastaveným limitům.

Charakteristika protokolu 802.11g je napsána v následující tabulce č. 4.

Tabulka 4 - Charakteristika protokolu 802.11g (převzato z [2], str. 114)

Schválen	Červen 2003
Radiofrekvenční technologie	DSSS a OFDM
Frekvenční spektrum	2,4 GHz
Kódování	Barker 11 a CCK
Modulace	DBPSK a DQPSK
Přenosové rychlosti	1, 2, 5,5 a 11 Mb/s s modulací DSSS, 6, 9, 12, 18, 24, 36, 48, 54 Mb/s s modulací OFDM
Nepřekrývající se kanály	1, 6, 11

2.5 Protokol 802.11n

Protokol 802.11n je oproti ostatním standardům poměrně novým, jeho vznik se datuje do roku 2009. Jak to u každého nového standardu bylo, i tento byl navrhnut za účelem zvýšení rychlosti přenosu dat na bezdrátových místních sítích LAN. Jeho teoretické přenosové rychlosti se pohybují od 54 Mb/s až k 600 Mb/s, což je znatelně více, než bylo doposud u variant a, b, g. Změny se tentokrát dočkala i šířka jednotlivých kanálů, nový protokol nepracuje nejen šířkou 20 MHz, ale dokáže i dva sousedící kanály sdružovat. Proto je šířka jednotlivých kanálů pro vyšší rychlosti přenosu rovna 40 MHz. [22]

Navíc protokol 802.11n je prvním svého druhu, který dokáže komunikovat ve dvou frekvenčních pásmech, a to jak v pásmu 2.4 GHz, tak i na nižších frekvencích pásma 5 GHz. Toto je také důvod, proč je také prvním protokolem, který je kompatibilní nejen s protokoly 802.11 b/g, ale i s 802.11a.

Novinkou, proč dokáže protokol 802.11n komunikovat ve vysokých rychlostech a navíc v obou pásmech je, že jedno zařízení používá k odesílání i přijímání dat více antén. Tato technologie se označuje jako MIMO (Multiple-Input, Multiple-Output). MIMO umožňuje také pracovat ve full-duplexním režimu, což starší protokoly díky jedné anténě neuměly.

Technologie MIMO[4] existuje ve třech typech, předběžném kódování, prostorovém multiplexování, anebo v kombinovaném kódování. První zmíněná metoda využívá více vysílacích antén k tvorbě jednoho, za to silnějšího signálu. Druhý způsob pro změnu využívá své antény k paralelnímu vysílání. Celkový počet datových proudů je tak roven

[4] Ačkoliv je problematika technologie MIMO zajímavá, jeho znalost pro splnění níže uvedených úloh není nutná. Případné informace o této technologii jsou dostupné například na http://www.ece.ualberta.ca/~HCDC/mimohistory.html

minimálnímu počtu antén schopných přenosu na obou stranách komunikace. Pokud má tedy vysílací strana 4 antény, zatímco přijímací 2, lze využít přenosu pouze po dvou datových proudech.

Z minulého odstavce je patrné, že různá zařízení mohou mít různý počet antén. Navíc, na jednom zařízení může být i jiný počet antén určených k odesílání a k přijímání dat. V dokumentaci se pro označení počtu antén používá styl AxB. První číslo (A) značí počet antén nebo datových proudů určených k vysílání. Druhé číslo pak vyjadřuje počet datových proudů k přijímání. Většina bezdrátových zařízení v sítích WLAN má obvykle dva nebo tři datové proudy pro oba směry vysílání. Dle zmíněné notace existují hlavně také typy 2x2, 3x3 nebo také 2x3. Na následujících řádcích je shrnuta charakteristika protokolu 802.11n:

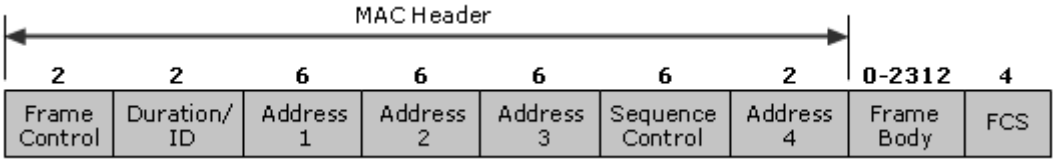
Tabulka 5 - Charakteristika protokolu 802.11n

Schválen	2009
Radiofrekvenční technologie	OFDM MIMO
Frekvenční spektrum	2,4 nebo 5 GHz
Modulace	BPSK, QPSK, 16-QAM, 64-QAM
Přenosové rychlosti	7,2, 14,4, 21,7, 28,9, 43,3, 57,8, 65, 72,2 pro 20 MHz kanál; 15, 30, 45, 60, 90, 120, 135, 150 pro 40 MHz kanál
Nepřekrývající se kanály	1, 6, 11, záleží na použití 20 MHz nebo 40Mhz kanálů

2.6 Hlavičky rámců v bezdrátové síti

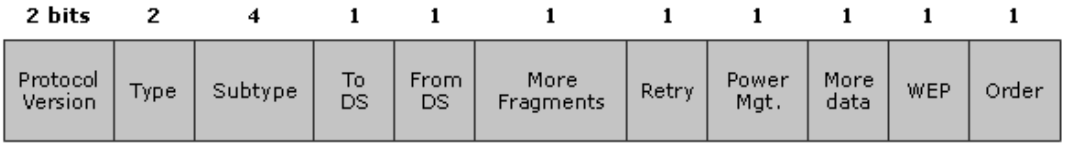
Každý rámec v síti, ať už v metalické, nebo v bezdrátové, musí být zaopatřen určitou hlavičkou. Za hlavičkou následuje tělo rámce a po něm kontrolní sekvence. Podle hlavičky (MAC Header) ostatní zařízení nejen poznají, kde vlastně rámce poslal, ale také komu jsou určena. Jedná se o podobnou analogii, jakou využívají poštovní balíky. Každý takovýto balík má také napsáno, kdo ho odeslal, komu ho posílá a k tomu ještě řadu dalších dodatkových informací. Tělo rámce (Frame Body) již obsahuje přímo data, které zařízení posílá. V poštovní analogii by se jednalo o vnitřek balíku. Poslední částí rámce je tzv. frame check sequence (FCS). Jedná se o kontrolní součet vytvořený z celého rámce, podle kterého adresát pozná, jestli mu rámec přišel celý a bez chyb, nebo jestli se někde po trase vyskytla chyba a má odesílatele požádat o znovu zaslání daného rámce. [4]

Na následujícím obrázku (obr. číslo 8) je zobrazen jeden bezdrátový rámec. Nad každou částí rámce je tučným číslem napsána její velikost v bytech. [4]



Obrázek 8 - Hlavička bezdrátového rámce (převzato z [4])

Počáteční pole (Frame Control) slouží k identifikaci typu rámce a poskytnutí nezbytných informací k tomu, aby mohl být rámec cílovou stanicí zpracován. Toto pole veliké 2 byty se skládá z několika dalších částí, jejichž obsah se maličko liší u každého druhu rámce. Na obrázku 9 je pole Frame Control detailně zobrazeno. Na rozdíl od obrázku 8, zde je velikost polí psána v bitech. Jelikož je velikost většiny velký jen 1 bit, mohou jednotlivé části obsahovat hodnoty 0 nebo 1. [4]



Obrázek 9 - Detailní pohled na pole Frame Control (převzato z [4])

Frame Control se tedy skládá z následujících položek:

- **Protocol Version** – Informuje, jaké verze protokolu 802.11 je daný rámec. Cílová stanice se pak může rozhodnout, zda danou verzi protokolu podporuje a rámec bude zpracovávat dál anebo ho zahodí.
- **Type a Subtype** – Tyto dvě položky říkají, k čemu tento rámec vlastně slouží. Existují 3 hlavní typy rámců, a těmi jsou rámce pro kontrolu, rámec obsahující data a rámec sloužící ke správě (control, data, management). Každý typ má ještě další různé podtypy (Subtype).
- **To DS a From DS** – Další dvě položky slouží k tomu, aby oznámily, zda daný rámec putuje do (To DS) distribučního systému anebo z něho ven (From DS). Obě tyto položky se používají jen u rámců typu data. Odesílatel zapíše hodnotu 1 do pole, které je pravdivé.
- **More Fragments** – Toto pole cílové stanici oznamuje, zda má ještě očekávat další rámce tohoto stejného typu (hodnota 1). Odesílatel tím tak informuje, že musel zprávu rozdělit a adresát s ní nemá nic dělat, dokud neposkládá všechny části dohromady. V případě, že se jedná o samotný nebo poslední rámec, má pole hodnotu 0.
- **Retry** – Hodnota 1 v tomto poli znamená, že odesílatel daný rámec posílá již minimálně podruhé.
- **Power Management** – Tato položka říká, zda je stanice v aktivním módu (hodnota 0), či v módu režimu nízké spotřeby (hodnota 1).
- **More Data** – Používá se v případě, kdy přístupový bod informuje stanici, která je v režimu nízké spotřeby, že pro něho má ještě další rámce, které mu plánuje poslat.

Druhým případem použití je pro informování přístupových bodů, že zařízení bude posílat ještě další multicastové/broadcastové rámce. V těchto případech má pole hodnotu 1, jinak 0.

- **WEP** – Značí, zda je (hodnota 1) anebo není (hodnota 0) rámec šifrován.
- **Order** – Říká, zda je nutné všechny přijaté rámce zpracovávat popořadě (hodnota 1), či nikoliv (hodnota 0).

Druhou položkou hlavičky bezdrátového rámce je Duration/ID. Která z těchto hodnot bude použita, je určeno typem rámce. Duration znamená, jak dlouho má dané zařízení pozastavit vysílání, aby se předešlo kolizím na síti. ID značí číslo stanice připojené k přístupovému bodu, který rámec posílal. [4]

Dalších několik polí v hlavičce se týká adres. Existuje 5 typů, které se do rámců mohou zapsat, ale platí, že v jednom rámci mohou být obsaženy jen 4. Jaké to budou, to závisí na typu rámce (viz Frame Control - Type and Subtype). Za zmínku také stojí, že klasická ethernetová hlavička používaná na metalických kabelážích obsahovala adresy jen dvě, a to zdrojovou (source address) a cílovou (destination address). [4]

- **BSS Identifier (BSSID)** – Pokud je tato adresa využita v rámci, který vysílá přístupový bod, jedná se o MAC adresu jeho samotného. Pokud je toto pole použito v IBSS (Independent Basic Service Set) přímo klientskou stanicí, jedná se o náhodně vytvořenou adresu stanicí, která klasické BSSID supluje.
- **Destination Address (DA)** – Pod pojmem cílová adresa se myslí MAC adresa zařízení, kterému je rámec určen.
- **Source Address (SA) –** Zdrojovou adresou se myslí MAC adresa zařízení, které rámec odeslalo.
- **Receiver Address (RA) –** MAC adresa zařízení, které má daný rámec převzít a následně ho poslat směrem k cílové stanici (určenou polem Destination Address - DA).
- **Transmitter Address (TA) –** Toto pole udává MAC adresu zařízení, které daný rámec vyslalo do bezdrátové sítě.

Posledním polem hlavičky je tzv. sequence control. Jeho úkolem je číslování fragmentovaných rámců tak, aby je později bylo možné poskládat zase do původního stavu.

Po hlavičce v rámci následují již samotná data. Jejich maximální velikost je však 2312 bytů, čili ne závratně veliká. Proto, pokud chce zařízení poslat data větší, musí je rozložit do více rámců. Tento proces je znám jako fragmentování. [3], [4]

Rámec je pak zakončen pomocí tzv. kontrolní sekvence rámce (frame check sequence FCS). Odesílatel spočítá kontrolní součet rámce a vepíše ho do této kolonky. Po přijetí celého rámce si pak příjemce vytvoří svůj kontrolní součet podle stejných pravidel, jako předtím odesílatel. Následně oba součty porovná a jsou-li shodné, přišel rámec

v nezměněné podobě. Pokud nejsou, rámec byl někde na cestě porušen a je nutné odesílatele zažádat o zaslání znovu. [3], [4]

2.7 Shrnutí protokolů 802.11

Na předchozích stránkách byly zmíněny nejčastěji používané protokoly na bezdrátových sítích LAN. Všechny varianty využívaly dvou nelicencovaných pásem, a to buď 2,4 GHz anebo 5 GHz. Na prvním operuje původní protokol 802.11 a jeho dva doplňky, 802.11b a 802.11g. Na druhém, 5 GHz pásmu, je pak založen standard 802.11a. Nový protokol, 802.11n, dokáže operovat na obojích pásmech a tím se z něj stává jediný, který je zpětně kompatibilní se všemi výše zmíněnými standardy.

Jelikož se obor informatiky vyvíjí opravdu rychle, bylo nutné, aby se jednotlivé standardy rychle přizpůsobovaly době. Firmy si již totiž začínaly vyvíjet své technologie pro rychlejší přenos dat po bezdrátových sítích. Proto bylo nutné zavést mezinárodní standardy, aby jednotlivá zařízení od odlišných firem spolu mohly stále komunikovat.

Původní protokol zvládal přenosovou rychlost rovnou pouhým 1-2 Mb/s. Postupně se však pomocí jiných modulací signálu dokázala rychlost přenosu zvýšit až na 54 Mb/s u verze g. Touto verzí se vyrovnaly přenosové rychlosti na obou pásmech. Varianta 802.11g je však zpětně kompatibilní jak s původní verzí protokolu, tak i se standardem 802.11b. Z tohoto důvodu standard 802.11a začal postupně upadat.

Stručné shrnutí a porovnání bezdrátových protokolů je zobrazeno v tabulce 6.

Tabulka 6 - Porovnání protokolů IEEE 802.11

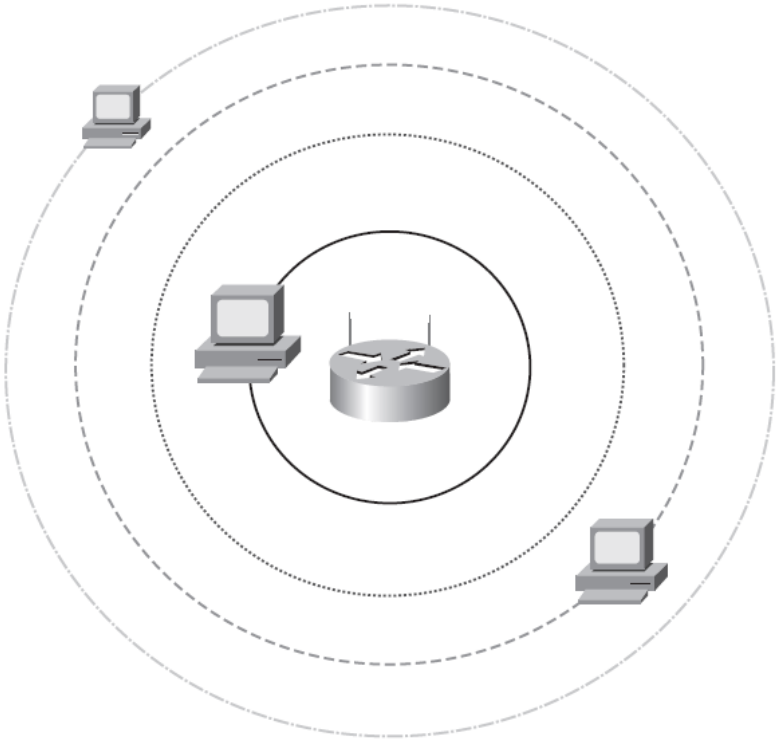
Standard	Rok vydání	Pásmo [GHz]	Podporované rychlosti [Mb/s]	Modulace
IEEE 802.11	1997	2,4	1, 2	DSSS, FHSS
IEEE 802.11a	1999	5	6, 9, 12, 18, 24, 36, 48, 54	OFDM
IEEE 802.11b	1999	2,4	802.11+ 5,5 a 11	DSSS
IEEE 802.11g	2003	2,4	802.11b + 6, 9, 12, 18, 24, 36, 48, 54	OFDM
IEEE 802.11n	2009	2,4 nebo 5	7,2, 14,4, 21,7, 28,9, 43,3, 57,8, 65, 72,2, 15, 30, 45, 60, 90, 120, 135, 150	MIMO OFDM

3 Faktory ovlivňující bezdrátové přenosy

Jedním ze základních faktorů, který se od kvalitní bezdrátové sítě očekává, je její spolehlivost. Při výskytu problému se signálem u kabelových sítí obvykle stačí zkontrolovat, zde není kabeláž poškozena. U bezdrátových sítí je nutné však nutné prozkoumat vícero faktorů, které mohou signál buď pohltit anebo odrazit. Proto se následující kapitoly budou věnovat základním věcem, které musí každý administrátor brát v úvahu, než síť začne konstruovat.

3.1 Modely Path Loss a Free Path Loss

Základními modely při určování ztráty signálu založené na vzdálenosti komunikujících zařízení se nazývají tzv. Path Loss. Signál, který každá anténa vyzařuje do prostoru, je vlastně vlněním. Každá taková vlnu vypadá pro představu obdobně, jako když vhodíme kámen do jezera. Vlny čím více postupují od středu, tím více se zmenšují, až po určité vzdálenosti bez cizího zavinění zcela vymizí. Odtud pochází výraz Free z názvu Free Path Lost. Z toho vyplývá, že čím blíže ke zdroji vlnění jsme, tím vyšší signál máme. Tato věta ale platí především v ideálních podmínkách. V reálném světě signál po své cestě potká poměrně dost překážek, od kterých se různě odráží. Na následujícím obrázku číslo 10 je zobrazen vysílač v podobě Wi-Fi routeru a tři klientská zařízení, která se na něho připojují. Síla vysílaného signálu je zobrazena kružnicemi, přičemž čím slabší signál je, tím více děr se na ní objevuje. [cisco 56]



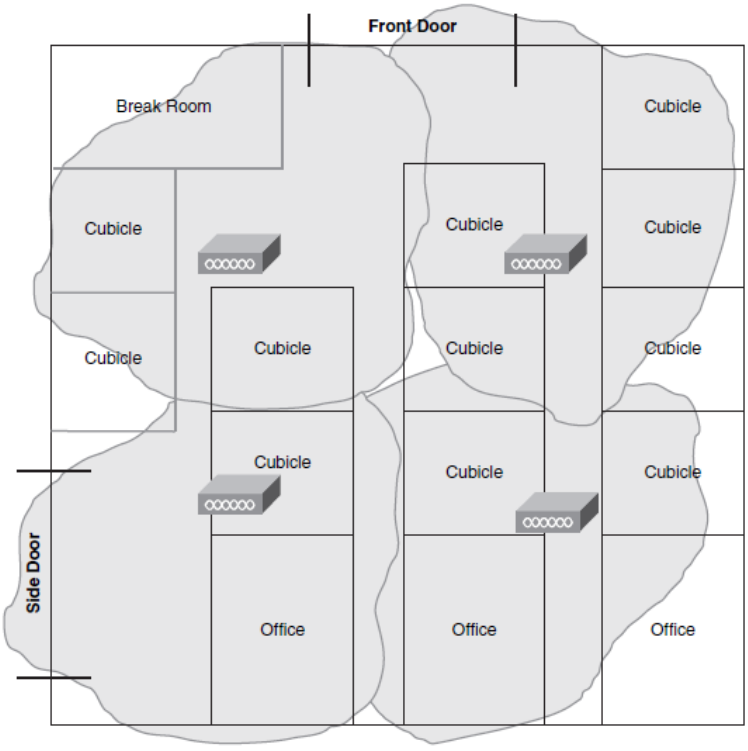
Obrázek 10 - Model Free Path Loss (převzato z [2])

3.2 Pohlcování vln

Jak již bylo řečeno, signál se přenáší ve formě vln. Každá vyzářená vlna však časem ztrácí na intenzitě, až zcela vymizí. Jak již bylo zmíněno, takto se vlnění chová jen v otevřeném prostoru, kde se mu do cesty nepostaví žádné překážky. Tento případ je ale dosti ojedinělý, protože Wi-Fi routery bývají obvykle umísťovány v budovách a tudíž ne vždy na sebe komunikující zařízení vidí přímo. A jelikož ne vždy je každé místnosti a na každé chodbě access point, častokrát musí signál k cíli procházet skrze zdi.

Každá překážka, která se vlně postaví do cesty, pohltí část její energie. Tím se sníží amplituda, energie, kterou vlna ještě má. Pokud musí tedy vlnění čelit mnoha překážkám nebo třeba i jedné velké, může se celá její energie ztratit, pohltit, a vlnění tak zcela zmizet. Při pohlcování vln navíc vzniká teplo. Tento jev se využívá u mikrovln. Mikrovlnná trouba vytváří vlny, které se nechávají pohltit jídlem, a díky teplu vzniklému z pohlcení, se jídlo postupně ohřívá.

Díky pohlcování signálu mohou s komunikací na síti nastat nemalé problémy. Může se stát, že signál, který dostatečně pokrýval celou prázdnou místnost, ji už po nastěhování nábytku pokrývat celou nebude. Příklad takovéto situace je zobrazen na následujícím obrázku číslo 11.

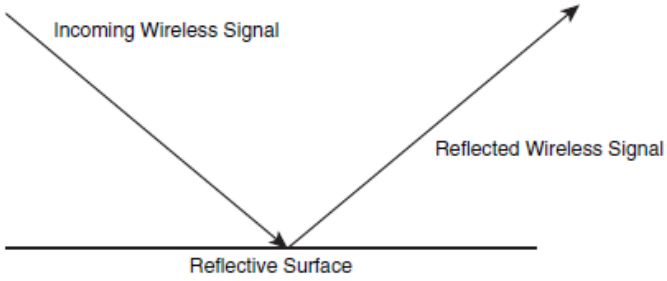


Obrázek 11 – Příklad pohlcování signálu (převzato z [2])

3.3 Odrazy signálu

Kromě výše zmíněného pohlcování ještě existují další faktory, které mohou signál zkreslit, či jinak znehodnotit. Jedním z problémů, který může nastat, je odraz signálu. Tento jev je podobný odrazu světla, akorát vlny ke svému odražení nutně nepotřebují jen skla a zrcadla, mohou je odrazovat i jiné objekty. Názorný příklad odražení signálu od reflexního povrchu pod stejným úhlem, pod jakým dopadl, je znázorněn na obrázku číslo 12.

U odrazů je důležité vědět, že ne každý materiál dokáže odrazit vlnění o všech frekvencích. Je tedy možné, že signál na 5 GHz frekvenci bude procházet v pořádku, zatímco 2.4 GHz signál se od objektu odrazí a dojde k jeho následné interferenci.

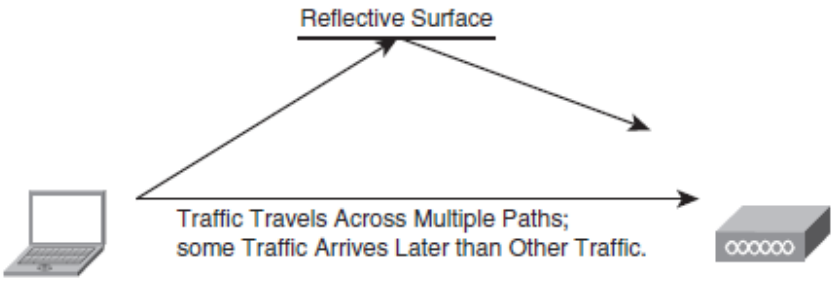


Obrázek 12 - Problém s odrazem (převzato z [2])

3.4 Problém vícecestnosti

Problém s vícecestností je úzce spjat s odrazem signálu. Ve výše uvedeném příkladu se vlny odrážely proti sobě tak, že docházelo buď k interferenci anebo k úplné ztrátě signálu. V praxi však ne všechny vlny musí putovat po stejné trase. Je možné, že se jedna část signálu odrazí od stěny, zatímco druhá k cíli půjde přímo. Výsledkem je, že pořadí, ve kterém vysílač data posílá, nemusí být nutně stejné, jako pořadí, ve kterém data přicházejí k přijímači. Tento případ je znázorněn na obrázku 13.

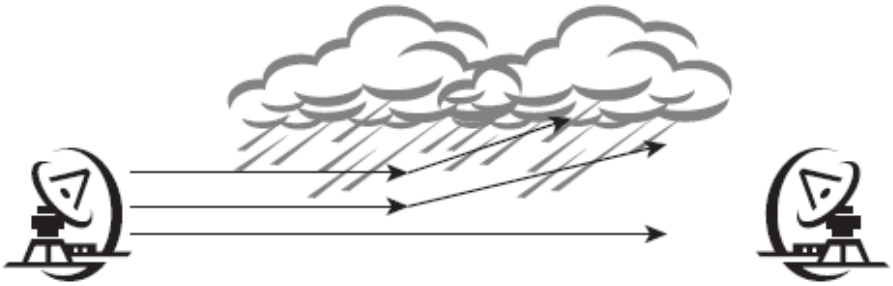
Druhou vlastností vícecestnosti je, že se jedna vlna signálu může odrazem opozdit natolik, že do cíle dorazí s opačnou fází, než jeho další vlna. Výsledkem je, že se vlny navzájem vyruší a vznikne tak nulový signál.



Obrázek 13 - Problém vícecestnosti (převzato z [2])

3.5 Rozptýlení signálu

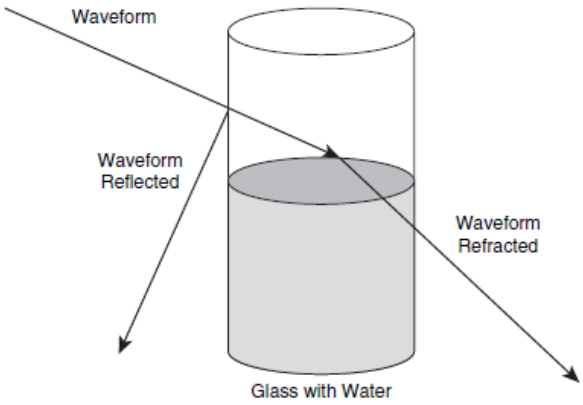
Rozptýlení je dalším faktorem, který může negativně ovlivnit kvalitu výsledného signálu. Dochází k němu, pokud je signál vysílán do mnoha směrů zároveň. Vlny se rozkládají o objekty, které mají reflexní povrch bez ostrých hran. Mezi takovéto povrchy patří třeba částice prachu ve vzduchu, či vodě. V malém množství kapky nedokážou závažně poškodit kvalitu přenosu. Jiná situace ale nastává v případě většího počtu kapek, čili za deště, či bouřky. Tento případ je znázorněn na obrázku 14. Signál pak může být zcela rozptýlen a komunikace bezdrátových zařízení narušena. Stejně jako u odrazů, vlnění o různých frekvencích podléhá rozptylu jinak.



Obrázek 14 - Rozptyl bezdrátového signálu (převzato z [2])

3.6 Lom signálu

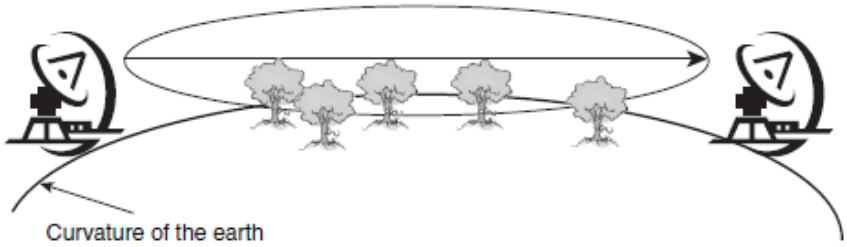
Lom vzniká, pokud vlnění přechází z jednoho prostředí do jiného, které má odlišnou hustotu a ve kterém se vlnění pohybuje jinak rychle. Různými prostředími, kterými může signál procházet, pak mohou být třeba vzduch, sklo, či voda. Pokud se vlnění šíří vzduchem, následně narazí na sklenici vody, část signálu se od její hrany odrazí. Zbytek signálu poté pokračuje skrz hranu sklenice, ale následně se láme o hladinu vody. Vlnění pak prochází skrz sklenici pod jiným úhlem, než pod kterým na ni dopadlo. Tento problém je zobrazen na obrázku 15.



Obrázek 15 - Problém s lomem (převzato z [2])

3.7 Problém přímé viditelnosti

Při tvorbě sítí, zvláště těch, které propojují větší vzdálenosti pomocí směrových antén, se často používá pojem *„přímá viditelnost“*. Tento pojem však neznamená jen, že dvě zařízení na sebe musí přímo vidět, tzn., že na úsečce začínající u prvního zařízení a končící u druhého, nesmí být překážka. Cesta signálu, tedy vlnění, se ale nepohybuje po přímce; rozšiřuje se okolo středového bodu a naopak zužuje u krajních bodů. U dvou bodů, které se propojují na velké vzdálenosti, se navíc další překážkou stává zakřivený povrch planety Země. Z obrázku 16 je patrné, že i když na sebe 2 zařízení přímo vidí, signál musí na své cestě překonat i různé další překážky, zejména, co se terénu týče.



Obrázek 16 - Směrové antény a LOS s překážkami (převzato z [2])

4 Zabezpečení bezdrátových sítí

Bezdrátové sítě se stávají fenoménem dnešní doby. Uživatel již nemusí každé zařízení fyzicky připojovat do sítí, tedy nosit sebou kabel a hledat volnou přípojku. S přibývající oblibou Wi-Fi sítí se však také zvedl počet pokusů o nabourávání těchto sítí. U metalických sítí však bylo nutné, aby byl útočník do sítě fyzicky připojen. V případě bezdrátových sítí mu však stačí, že je v dosahu některého vysílače, metalický kabel a místo k připojení tak již nepotřebuje.

Přenos dat po bezdrátových sítích je vázán normami 802.11, které byly výše popsány. Bohužel z hlediska bezpečnosti však tedy nelze zajistit úplnou bezpečnost spojení na fyzické vrstvě. Jakým způsobem bude daná síť komunikovat, je z důvodu veřejného přístupu útočníkovi známé. Proto je nutné řešit zabezpečení přenosu i na vyšších vrstvách.

4.1 Obecné druhy útoků

Na následujících řádcích budou stručně popsány některé typy útoků na bezdrátové sítě. Některé mají za úkol zisk citlivých dat ze systému, jiné zase znemožnění komunikace jednotlivých zařízení. Náročnost těchto útoků jak na uživatele, tak na zařízení, se značně liší. K uskutečnění některých stačí pozměnit jeden paket, zatímco k provozu jiné je potřeba paketů tisíce.

4.1.1 Hardwarové útoky a útoky na fyzické vrstvě

Sice na nejnižší vrstvě modelu ISO/OSI nelze zajistit stoprocentní bezpečnost přenosu, je však nezbytné, aby se i na ní vykonaly určité bezpečnostní kroky. I v případě kvalitních ochran na vyšších vrstvách však stále existují jiné možnosti, jak síť znepřístupnit anebo se dostat k citlivým datům. Jedním z příkladů může být umístění vysílače do místnosti, kam má útočník volný přístup. V případě chabých ochran nepadnutého zařízení pak může útočník změnit parametry dané sítě, či si zjistit, jak jsou data k přenosu kódována. Pokud by se snažil síť jen znepřístupnit, stačilo by, kdyby odpojil vysílač z elektrické sítě.

4.1.2 Falšování identity zdroje

Tento útok je také znám pod anglickým názvem *address spoofing*. Jeho princip takový, že si útočník nejprve zjistí, jaké zařízení mají do sítě přístup. Pokud se mu pak povede získat jejich adresu (ať MAC nebo IP), může pak zkusit na zakázaném zařízení změnit adresu svých vysílaných paketů tak, aby vyhovovala podmínkám napadené sítě. V případě úspěchu se pak útočník tváří pro síť jako důvěryhodný klient, jehož adresu odcizil. Možné dopady na zisk citlivých údajů, či modifikování parametrů sítě se pak liší podle toho, za jak moc důvěryhodné zařízení se maskuje. Nejvíce škody by napáchal, pokud by se mu povedlo se takto do sítě připojit jako administrátor, tato možnost však bývá často blokována. [3], [23]

4.1.3 Man in the middle attack

Do našeho jazyka se tento útok volně překládá jako „muž uprostřed“. Princip je takový, že podvodník umístí do sítě zařízení, které se vydává za jedno z důvěryhodných. Nechá pak klienty na sebe napojit a zprostředkovává jim stejné služby, jako původní důvěryhodné zařízení. Na rozdíl od něho však odposlouchává, co za data si dané strany vyměňují. V případě, že se klient bude snažit přistoupit k nezabezpečené službě, například FTP serveru, posílá heslo v paketech nezašifrované. Útočící zařízení ho pak lehce odposlechne. [3], [23]

4.1.4 Útoky na přístupová hesla (slovníkové útoky)

Pravděpodobně nejrozšířenější a nejběžnější útok, který se používá na všech typech sítí, jak na metalických, tak na bezdrátových. Stále se ještě stává, že lidé v síti používají slabá hesla spočívající jen v několika písmenech. V horším případě navíc tzv. slovníková hesla, čili taková slova, která se dají lehce uhádnout. Útočník pak zkouší heslo buď postupně tipovat (brutal force) anebo ho získat pomocí trojských koňů, či pomocí phisingu. Phishing je metoda odhalení hesla tím, že se útočník vydává za administrátora a nezkušený pracovník mu pak heslo napíše sám. Druhou možností je vytvořit webovou stránku obdobnou oficiální, kde se uživatel pokusí přihlásit a tím heslo podvodníkovi též poskytne.

Tento útok je však nebezpečný, i pokud selže v zisku hesla. Jednou z možných obran proti brutal force útokům je, že se účet po několika špatných pokusech o přihlášení zablokuje. Útočník pak tedy může takto zablokovat většinu účtů v systému. [3], [23]

4.1.5 Útoky prostřednictvím odposlechu

Jedná se o podobný útok typu man in the middle. Útočník se však nevydává za důvěryhodné zařízení, ale umístí své někam doprostřed firemní sítě, například místo opakovače. Může pak nejen odposlouchávat, co jednotlivá zařízení na obou stranách vysílají, ale taky posílaná data likvidovat. Z dat, která získá, pak může získat přístup k citlivým místům sítě. [3]

4.1.6 Útoky vedoucí k odmítnutí služby

Tento typ útoku je poměrně známý útok pod anglickým názvem *Denial of Service (DoS)*. Na rozdíl od výše zmíněných metod, tato nemá za účel zisk zneužitelných dat. Jeho cílem je znemožnit zařízením na síti jejich vzájemnou komunikaci. Jednou z metod útoku je ta, kdy útočník bombarduje access point tolika pakety, kolika jen dokáže. Tímto ho pak zahltí natolik, že nebude stíhat odpovídat ostatním. Druhou možností je, že útočník bude stále vysílat tak, aby docházelo k interferenci jednotlivých vlnění a ostatní zařízení tak zůstanou přehlušena. [3], [23]

Varianta *Distributed Denial of Service (DDoS)* je založena na této metodě. Její princip je stejný naprosto shodný, ale k provedení nevyužívá pouze jedno útočící zařízení, ale oběť bombarduje z pokud možno co nejvíce stran. [3], [23]

4.2 Autentizace

Pod pojmem autentizace v počítačových sítích se rozumí proces spočívající v tom, že některé zařízení (např. access point) ověřuje přístup klienta do své sítě. Ověřování činí dle administrátorem nastavených kritérií a dotazujícímu se klientovi buď přístup umožní, anebo zamítne.

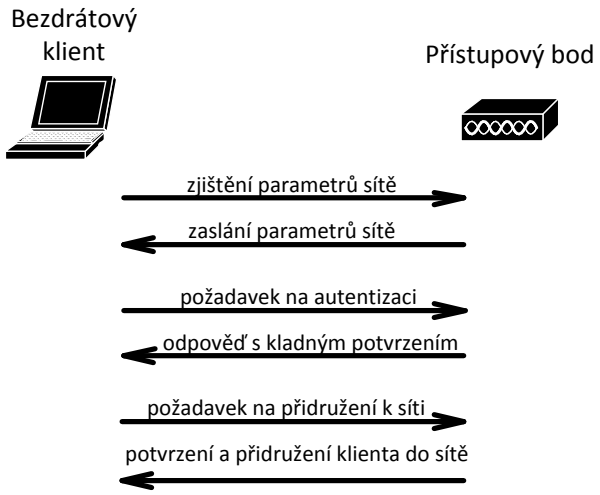
Nejjednodušším typem autentizace je identifikace pomocí přístupových hesel, popř. uživatelského jména a hesla. Nevýhodou je nutnost volit složitá neslovníková hesla, které jsou náchylné k zapomenutí. Častokrát se pak může stát, že složité heslo si uživatel radši někam zaznamená a útočníkovi pak dává možnost, dané heslo přečíst. Tato studie se bude zabývat právě touto, v praxi nejčastěji používanou metodou.

Druhou možností je autentizace pomocí klíčenek, čipových karet a podobných hardwarových předmětů. Tento způsob je sice složitější na prolomení než pouhé heslo, ale zase pro změnu nastává problém v případě, kdy předmět uživatel ztratí anebo mu ho útočník odcizí.

Třetí a asi nejsložitější metodou na zfalšování je autentizace pomocí otisků prstů, hlasu, či struktury duhovky oka. Nevýhodou této metody je značná cena zařízení, které tuto metodu dokážou kvalitně používat.

4.2.1 Otevřená autentizace

Princip otevřené autentizace je lehký. Každému zařízení, které zažádá o připojení do sítě, je odpovězeno kladně. Proces je tedy takový, že klient vyšle autentizační požadavek přístupovému bodu, který mu následně odpoví potvrzením dotazu a zařízení si zaregistruje. Klient poté vyšle požadavek na přidružení do sítě. Celý postup je znázorněn na obrázku 17. Otevřená autentizace je bezpečností metodou operující na druhé vrstvě. Prakticky se využívá především v hotspotech. Příkladem takovýchto míst mohou být internetové kavárny, či restaurace. Na těchto místech obvykle není nutné k připojení k Internetu znát jakékoliv heslo.



Obrázek 17 – Přidružení klienta k síti při otevřené autentizaci (volně převzato z [2])

4.2.2 Autentizace Wired Equivalent Privacy – Pre Shared Key (WEP-PSK)

Metoda WEP-PSK je velmi dobře známá pod českým jménem autentizace pomocí předem sdíleného klíče. Na rozdíl od otevřené autentizace tato metoda nevpustí do sítě každého, kdo požádá. Přístup je povolen pouze tomu, kdo zná určitou sekvenci znaků – určitý klíč. Jiný způsob ověření identity uživatele, například pomocí účtů, WEP nedokáže. Administrátor tak například nemá možnost zjistit, který zaměstnanec je napojen ke kterému přístupovému bodu. Navíc velkým bezpečnostním nedostatkem je, že klíč není používán jen pro ověření přístupu do sítě, ale je základem veškerého dalšího šifrování vzájemné komunikace. Toto kódování zpráv je založeno na proudové šifře RC4.

Proces připojení klienta do sítě tímto způsobem je veden ve čtyřech krocích: [2]

1. Klient pošle autentizační požadavek na přístupový bod.
2. Přístupový bod mu odpoví nezašifrovanou zprávou obsahující text výzvy.
3. Klient zašifruje text výzvy podle uživatelem nastaveného WEP klíče. Daný text vloží do nového autentizačního požadavku a ten pošle zpět na přístupový bod.
4. Přístupový bod klientův požadavek dešifruje. Pokud bude dešifrovaný text shodný s původní zprávou, pošle zpět klientovi kladnou odpověď a do sítě ho vpustí. V opačném případě požadavek zamítne.

Ačkoliv se to na první pohled nemusí zdát, tak z hlediska bezpečnosti se tato metoda nedá považovat za dostačující. Důvodem pro toto tvrzení je, že útočník může zachytit nezašifrovanou zprávu s výzvou a poté následně klientovu zašifrovanou odpověď. Tyto údaje mu postačují na to, aby v relativně krátké době dokázal odvodit, pomocí jaké sekvence se data šifrují. Tím se mu do ruky dostane WEP klíč a pomocí něho se následně může do sítě bez problému připojit.

Druhým nedostatkem protokolu je, že přenášená data jsou šifrována pomocí inicializačního vektoru a původního WEP klíče, který se za celou dobu přenosu nemění. Vyjma samotných dat a jejich kontrolního součtu, tak jedinou proměnnou ve vzorci zůstává inicializační vektor, který je dlouhý 24 bitů. Díky této velikosti existuje maximálně 2^24 = 16777216 hodnot, kterých může vektor nabývat. Toto číslo se může zdát dosti velké, ale opak je pravdou. Při běžném provozu na síti se kapacita rychle vyčerpá a inicializační vektory se tak začnou opakovat. Pokud tedy útočník budou dostatečnou dobu odposlouchávat síť, povede se mu zachytit více paketů, které jsou šifrovány pomocí stejného vektoru. To mu pak postačí, aby klíč dokázal dešifrovat. Proto se dnes WEP používá jen tam, kde nelze implementovat složitější metodu (například WPA/WPA2).

Samotný WEP klíč může být různě dlouhý. U všech druhů však platí, že prvních 24 bitů je vyhrazeno pro inicializační vektor (IV). Zbývající bity tvoří již samotný klíč. Čím více bitů je použito, tím déle musí útočník síť odposlouchávat a tím více času mu prolomení hesla zabere.

Původní klíč měl délku 64 bitů (40 bitů pro samotný klíč). Tento klíč lze zapsat buď jako sekvenci 10 hexadecimálních znaků (pomocí znaků 0-9, A-F) anebo 5 znaků z ASCII tabulky (jeden znak je zapsán jako 8 bitů, 5x8 = 40).

Další variantou je klíč dlouhý 128 (104 použitelných) bitů. Tato sekvence se dá zapsat jako 26 hexadecimálních znaků, či 13 tisknutelných znaků z ASCII tabulky.

Poslední používanou délkou WEP klíče je 256 bitů (232 použitelných). Těchto 232 bitů lze zapsat pomocí 58 hexadecimálních symbolů, či 29 znaků.

4.2.3 Filtrování MAC adres

Poměrně jednoduchou metodou autentizace je filtrování dle MAC adres. Jako první krok musí administrátor nastavit povolené, či zakázané, MAC adresy na přístupovém bodu. Poté kdykoliv se klient pokusí připojit do sítě, přístupový bod přečte z rámce zdrojovou MAC adresu a porovná ji se svým seznamem. Dle toho se rozhodne, zda rámec potvrdí, či nikoliv. Velkou nevýhodou však je, že zfalšovat a změnit MAC adresu zařízení není složité. Stačí tedy útočníkovi zjistit, jaké adresy mají přístup do sítě a svoji podle toho pozměnit. [18]

4.3 Pokročilé metody autentizace a šifrování

Výše zmíněné metody využívaly pro kontrolu věrohodnosti uživatelů pouze sdílené heslo, případně MAC adresu. Z hlediska bezpečnosti však tyto metody nejsou zcela dostačující. Proto se zpravidla ve větších podnicích využívá možnosti ověření klienta pomocí AAA (Authentication, Authorization, and Accounting) serveru. Při této metodě musí klient předložit svůj veřejný klíč (obvykle certifikát) přístupovému bodu, který jej následně pošle zmíněnému AAA serveru a nechá ho rozhodnout, zda je klient důvěrný, či nikoliv.

4.3.1 Infrastruktura veřejných klíčů a digitální certifikáty

Pro vysvětlení principu funkce veřejných klíčů je dobré uvést příklad z reálného života. Pokud často cestujeme autem, občas se nám přihodí, že narazíme na policejní hlídku, která nás vyzve k tomu, abychom předložili svůj občanský průkaz a řidičské oprávnění. Tuto identifikaci nám však neposkytl on sám, ale třetí strana, které příslušník police důvěřuje, a to v tomto případě státní orgán České republiky. Kdyby mu třeba student předložil svoji žákovskou knížku, či index, které vystavují školy, či univerzity, příslušník by ji odmítl, protože těmto organizacím nedůvěřuje. Analogický stejný je příklad, kdyby nás k předložení totožnosti vyzval náhodný člověk na ulici, který by se nám ničím neprokázal (například policejním odznakem). To bychom zase my nedůvěřovali jemu. [7], [9]

Obdobně jako občanský průkaz obsahuje například jméno a příjmení osoby, i digitální certifikát má jisté náležitosti. Mezi nejdůležitější patří uživatelské jméno, veřejný

klíč (a jeho použité kódování), platnost vydání, sériové číslo a dodatečné informace o vydavateli a samotném certifikátu. [6], [7], [9]

Z hlediska počítačových sítí je princip ověření velmi podobný. Každý klient musí vlastnit veřejný klíč - certifikát, který mu dává oprávnění do sítě vstoupit. Tyto certifikáty obvykle vydávají tzv. certifikační autority (CA). Příkladem mohou být autority VeriSign, Thawte, ipsCA a Comodo). Společnosti si ale účtují poměrně vysoké poplatky za vydání certifikátu. Naopak bezplatné zaregistrování poskytuje například autorita CAcert. Poslední možností je, když si server podepíše certifikát sám. Takto si však certifikát může podepsat každý, kdežto certifikační autority musí ze zákona například zjišťovat, zda je společnost zapsána v obchodním rejstříku. Proto z hlediska důvěryhodnosti je dobré, aby společnosti využily některé z placených certifikačních autorit[7], [8], [9]

Dalším problémem jak bezplatných, tak samo-sebou podepsaných certifikátů je, že jim operační systémy přímo nedůvěřují. Musí si je tedy uživatelé klientských zařízení přidat do vlastního úložiště certifikátů. [7], [9]

4.3.2 Autentizační standard 802.1x

Standard 802.1x se původně používal u klasických pevných sítí. Jeho úkolem bylo zablokování fyzického přístupu do počítačové sítě. U bezdrátových sítí plní stejnou úlohu, zablokuje veškerou komunikaci každému novému připojenému zařízení až do té doby, než se úspěšně autorizuje u AAA serveru. Jediný druh komunikace, který mu povolí, je pomocí protokolu EAP. Protokol EAP existuje ve dvou typech, prvním je EAPoL (EAP over LAN) a druhým EAPoWLAN (EAP over WLAN).

Aby se klientské zařízení mohlo připojit do sítě, musí obsahovat tzv. žadatele (neboli prosebníka, anglicky supplicant). V dnešní době je tento supplicant součástí všech moderních operačních systémů. Postup autentizace pak začíná tím, že stanice pošle svoji žádost o přístup spolu se svoji identitou (certifikátem) pomocí zmíněného protokolu EAP autentizačnímu zařízení, obvykle přístupovému bodu. Ten pomocí protokolu RADIUS přepošle žádost na autentizační server (AAA server), který podle svého seznamu povolených uživatelů rozhodne, zda na požadavek odpoví kladně, či přístup do sítě pro dané zařízení zamítne.

Celý postup autentizace se dá shrnout takto: (převzato z[2], Bezdrátové sítě Cisco, str. 335)

1. Klient se přidruží k přístupovému bodu.
2. Klient přijme autentizační požadavek.
3. Klient vrátí autentizační odpověď.
4. Klient přijme požadavek na přidružení.
5. Klient odešle odpověď přidružení.

Jakmile proběhne otevřená autentizace, může libovolná ze stran zahájit proces 802.1x. V této fázi je „port“ nadále blokován pro uživatelský provoz a probíhají následující děje:

1. Žadatel pošle pověření autentizačnímu zařízení.
2. Přístupový bod odešle autentizační informace na server pomocí paketu RADIUS.
3. Data protokolu RADIUS jsou vrácena z autentizačního serveru a přístupový bod je předá zpět klientovi.
4. Během komunikace klient a přístupový bod odvodí unikátní klíče relace.
5. Server RADIUS odešle zpět klientovi zprávu o úspěšném přístupu spolu s klíčem WEP relace.
6. Přístupový bod udržuje klíč WEP relace, který používá při komunikaci.
7. Přístupový bod předá klientovi klíč WEP relace spolu s klíčem WEP pro všesměrové nebo vícesměrové vysílání.
8. Klient a přístupový bod mohou šifrovat provoz pomocí klíčů WEP relace.

Přístupový bod uchovává klíč WEP relace, aby mohl šifrovat komunikaci s klientem a chránit tím připojení. Přístupový bod odesílá klíč WEP pro všesměrové nebo vícesměrové vysílání, protože každý klíč WEP relace je jedinečný. Pokud tedy klient pomocí něj zašifroval všesměrové nebo vícesměrové vysílání, mohl by zprávu přečíst pouze přístupový bod.

4.3.3 Autentizační server

Pro správnou činnost procesu 802.1x je důležité, aby autentizační server, žadatel, i přístupový bod podporovaly metodu EAP. Pod pojmem autentizační server se dá představit nejen volně dostupný server RADIUS, ale může jím být i server ACS (Cisco Secure Access Control Server). Pokud síť obsahuje řadič, je nutné na něm nastavit IP adresu daného autentizačního serveru a také sdílený tajný klíč (heslo), které se bude pro proces používat.

4.3.4 Extensible Authentication Protocol (EAP)

Zatímco standard 802.1x předepisuje, jaké jednotlivé kroky má obsahovat celý proces přidružení a následné autorizace klientů, tak EAP již konkrétně popisuje, jak mají vypadat rámce, pomocí kterých se žadatel dorozumívá s autentizačním serverem.

Celkem pro všechny druhy sítí existuje zhruba 40 různých EAP metod. Navíc však ještě existuje několik způsobů zapouzdření rámců EAPu. Mezi nejznámější patří namátkou PEAP, LEAP, EAP-TLS, EAP-MD5, EAP-PSK nebo EAP-FAST.

Základní postup posílání uživatelských pověření pomocí protokolu EAP zahrnuje kroky:

1. Klient požádá o přístup.
2. Autentizační zařízení se klienta dotáže na jeho identitu.
3. Klient poskytne důkaz.
4. Klient dostane odpověď od serveru.

4.4 Pokročilé šifrovací metody

Předcházející kapitoly se věnovaly připojování klientů do sítě a jejich následné autentizaci. V případě, že tyto kroky proběhly úspěšně, stane se klientské zařízení členem takovéto počítačové sítě a může na ní normálně komunikovat s ostatními zařízeními. Z důvodu bezpečnosti a jako prevence před útočníky se však i postup autentizace musí šifrovat. Na bezdrátových sítích je totiž poměrně snadné odposlechnout vzájemnou komunikaci klienta a přístupového bodu. Útočník se však nemusí pokusit do sítě jen surově nabourat, může jen nenápadně přihlížet a poslouchat, jaké důvěrné data si dané zařízení po vlnách bezdrátové sítě posílají. Proto je nejen nutné zabezpečit autentizaci zařízení, ale také jakoukoliv následující komunikaci. Předešle zmíněná metoda WEP tyto podmínky splňuje, ovšem na druhou stranu velmi trpí tím, že je lehko prolomitelná. Proto se postupem času vyvinuly důmyslnější a silnější šifry, jako je třeba zabezpečení WPA (Wi-Fi Protected Access) a WPA2 (Wi-Fi Protected Access 2).

4.4.1 WPA (Wi-Fi Protected Access)

Vzhledem k prolomení zabezpečení typu WEP, Wi-Fi Alliance musela rychle vytvořit jiné, bezpečnější zabezpečení. Začala tak pracovat na dodatku k bezdrátovým sítím 802.11i. Jelikož bylo nutné na prolomení WEP zareagovat rychle, vydala tak roku 2003 třetí koncept svého 802.11i pod názvem WPA a dále pracovala na tvorbě důmyslnější metody, WPA2. Hlavním problémem, kterému Wi-Fi Alliance čelila, bylo, že v počítačích po celém světě již zdárně fungovalo mnoho síťových karet, ale i přístupových bodů, které metodu WEP využívaly. Musela tak vymyslet nový druh zabezpečení, které by vyřešil bezpečnostní díru, ale zároveň nepotřeboval zasáhnout do hardware již stávajících zařízení. Tuto úlohu se členům Alliance povedlo zvládnout a tak ke správnému fungování WPA většinou postačí upgradovat pouze software, tzv. firmware. Na rozdíl od klasickéhoWEP, WPA poskytuje dva autentizační režimy:

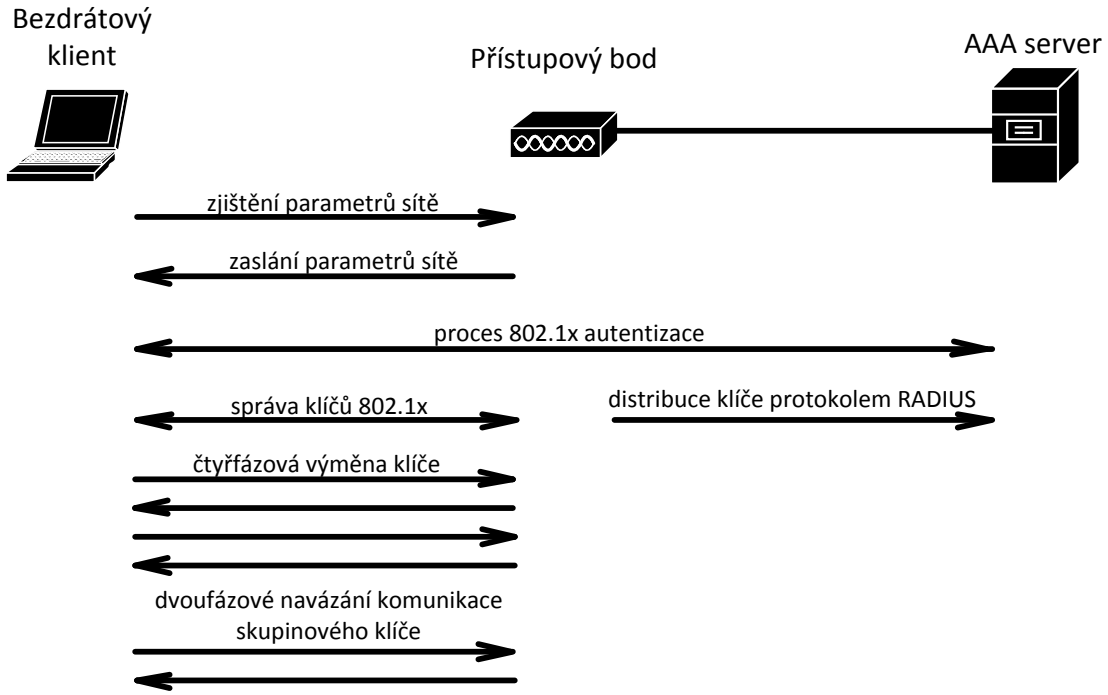
- **Podnikový režim (WPA-Enterprise)** – standard WPA v podnikovém režimu vyžaduje autentizační server. Při autentizaci a distribuci klíčů se používá protokol RADIUS a uplatňuje se také protokol TKIP s volitelným šifrováním AES.

- **Osobní režim (WPA-Personal)** – standard WPA v osobním režimu pracuje s předem sdílenými klíči. Tato možnost je proto slabší, a proto se s ní spíše setkáte v prostředí domácích sítí. Díky absenci RADIUS serveru je konfigurace osobního režimu o dost snazší než podnikového.

Zabezpečení WEP používá pro šifrování svého klíče algoritmus RC4. Jelikož se tento klíč po celou dobu spojení klienta a přístupového bodu nemění, je statický. WPA již svůj klíč po určitém čase dynamicky mění. K těmto změnám využívá protokol TKIP (Temporal Key Integrity Protocol). Nedostatkem tohoto protokolu je však to, že kvůli kompatibilitě se starším hardware je stále založený na šifře RC4. Plusem WPA je, že díky dynamické změně klíče odpadly některé druhy útoků (WEP key recovery attack). Bohužel však některé stále zůstaly. Vzhledem k mnoha způsobům, jak lze šifru RC4 prolomit se v dnešní době (rok 2012) TKIP nepovažuje za bezpečný protokol. Proto byl protokol WPA

doplněn o možnost použití šifrování AES, jakožto náhrady za TKIP. Kvůli větší výpočetním nárokům ale nešel AES úspěšně použít na starších zařízeních.

Na následujících řádcích bude popsán proces autentizace WPA, který je shrnut na obrázku 18.



Obrázek 18 - Autentizace WPA-Enterprise (volně převzato z [2])

Tento postup autentizace je už poměrně náročný. Pro potřeby níže uvedených laboratorních cvičení ho však není nutné znát nazpaměť. Z toho důvodu bude na následujících řádcích uveden jen ve zkrácené podobě.

Prvním krokem autentizace je, že se klient dotáže přístupového bodu, jaký bezpečnostní režim využívá. Poté, co mu autentizační zařízení odpoví, začne klasický proces 802.1x zmíněný v kapitole 4.3.2. V případě úspěšné autentizace si AAA server odvodí svůj hlavní klíč (PMK, Pairwise Master Key) a pošle ho přístupovému bodu. Stejný klíč je odvozen na straně klienta. PMK zůstává v platnosti po celou dobu relace. [2]

Následujícím krokem procesu je čtyřfázové navázání komunikace, kdy klient a přístupový bod dospějí k novému klíči, tzv. PTK (Pairwise Transient Key). Tento klíč potvrzuje sdílený klíč PMK, nastaví dočasný klíč pro šifrování zpráv, autentizuje vyjednávané parametry a vytvoří podklad pro klíče v další fázi, která se nazývá dvoufázové navázání komunikace skupinového klíče. [2]

Proces autentizace dále pokračuje dvoufázovým navázáním komunikace skupinového klíče. V tomto kroku si klient s autentizačním zařízením vyjednají klíč GTK (Group Transient Key), který slouží k dešifrování přenosů všesměrového (broadcast) a vícesměrového (multicast) vysílání. Klíč GTK se vytváří na základě náhodného čísla a obdobně jako TK klíče, nezůstává stále stejný, mění se tehdy, když vyprší jeho platnost nebo když se klient odpojí od sítě. [2]

4.4.2 WPA 2 (Wi-Fi Protected Access 2)

V červnu roku 2004 byl schválen dodatek k standardu 802.11 s názvem 802.11i, který je spíše známý pod názvem WPA2. Jedním z cílů autorů staršího WPA bylo, aby se nový protokol dal poměrně lehce nasadit do již stávajících sítí, bez nutnosti obměny a nákupu nových zařízení. Kompletní dodatek 802.11i se požadavky na hardware nijak neomezuje. Právě kvůli použití důmyslnější šifry AES potřebuje hardware o něco silnější, než předešlé varianty, které využívaly slabší šifrování RC4. Tato změna šifrování znamenala opuštění protokolu TKIP, a zavedení nové a bezpečnější metody AES/CCMP (Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code Protocol). Od protokolu TKIP se upustilo hlavně proto, že se hackerům povedlo nalézt způsob, jak ho prolomit. Obě zmíněné metody využívají k šifrování inicializační vektor (IV) a hodnoty MIC, ale nově AES/CCMP inicializační vektor po každém bloku šifry prodlužuje. [10], [11]

Standard 802.11i nebyl napsán přímo pro potřeby starších zařízení, ba naopak, ke svoji správné a rychlé funkčnosti potřeboval, aby na přístupových bodech byly silnější procesory. Problémem však mohl nastat, kdyby se do sítě chtěl připojit klient se slabším zařízením, či mobilním telefonem, který zabezpečení WPA2 nepodporuje. Proto na kvalitnějších přístupových bodech existuje možnost zabezpečení typu WPA+WPA2. Pak se novější zařízení připojují klasicky pomocí nového WPA2 a klienti, kteří ho nepodporují, mají možnost využít staršího a stále ještě poměrně bezpečného WPA. [13]

5 Odchytávání provozu na bezdrátových sítích

V dobách, kdy bezdrátové sítě ještě neexistovaly, musel se útočník nejprve do sítě fyzicky připojit, aby poté mohl odposlouchávat data, či s ní jinak manipulovat. S rozrůstající oblibou Wi-Fi sítí se tato situace pro hackery výrazně zjednodušila. Dnes již stačí, aby se přiblížil na dosah některé bezdrátové síti, a může se pokusit ji odposlouchávat, či zkoušet prolomit heslo.

Nejjednodušším místem pro odposlech jsou takzvané hotspoty. Příkladem takových může být Internetová kavárna, herny, či obdobné podniky. Z hlediska zabezpečení se často útočník může přihlásit do sítě bez znalosti hesla (díky otevřené autentizaci) a ani následná komunikace jeho, ani ostatních klientů, není nikterak šifrována. Takový ráj pro hackery naštěstí většina firemních a snad už ani domácích sítí neposkytuje. Útočník tak musí nejprve zjistit, jakým způsobem jsou data šifrována, a až poté zahájit samotný odposlech.

Prolomení šifry WEP není nikterak zdlouhavá záležitost a proto se ho v dnešní době nedoporučuje používat. Protokol WPA je na prolomení o dost těžším. Stále ale existují možnosti, jak se přes něho dostat. Ovšem v případě volby dlouhého a složitého hesla samotné prolomení trvá poměrně značnou dobu. Nejnovější protokol 802.11i, známý jako WPA2, nebyl prozatím ještě prolomen (rok 2012) a tak se považuje za bezpečný. [13], [14]

5.1 Potřebné vybavení

Kdysi dávno, v dobách pevných sítí, potřeboval útočník počítač, síťový kabel a nějaký způsob, jak se fyzicky připojit do sítě. V dnešní době postačí některé bezdrátové zařízení, obvykle laptop, a pouze se k dané síti přiblížit. Zvláštností síťových adaptérů je to, že ne každý je pro odposlech stejně dobrý. Naopak, existují karty, které jsou pro odposlouchávání dosti nevhodné anebo celý proces značně prodlužují. Druhou věcí, která funkce karty značně modifikuje, je její chipset a použité ovladače. Pro to, než se tato studie bude věnovat samotnému odposlechu, je dobré znát režimy, ve kterých je Wi-Fi karta schopna pakety zachytávat:

- normální
- monitorující
- promiskuitní

Normální režim využívají karty ve většině případů. Jde o takový, kdy zachytává rámce buďto určené jen jí samotné, anebo rámce určené všem poslané všesměrovým vysíláním (broadcast). V tomto režimu tedy nelze zachytávat rámce ze sítě, do které nemá uživatel přímý přístup. A i v případě, kdy se zařízení připojí k přístupovému bodu, nedokáže odposlechnout data, které jsou určeny jinému zařízení.

Monitorující režim je ze všech tří nejlepším a přímo určeným pro odposlouchávání. Karty přepnuté do tohoto módu dokážou zachytit veškeré pakety, které se v jejím dosahu vysílají. Navíc tuto činnost provozují i bez asociace s přístupovým bodem.

Promiskuitní režim obvykle pro odposlechnutí komunikace postačuje, není však tak výhodný, jako výše zmíněný. Stejně jako předcházející karta dokáže zachycovat rámce určené jí i zbytku sítě. Rozdílem však je, že se do této sítě musí nejprve napojit.

Poslední věcí, která se u různých karet a použitých ovladačů odlišuje, je možnost využití tzv. packet injection (injektování paketů). Jde o metodu, kdy lze komunikaci na síti ovlivňovat přímým vkládáním a vysíláním paketů, obvykle použitých v předcházející relaci. Přímo pro odposlech dat není však nutné injektování paketů použít. Značně to však urychlí práci, pokud je na síti slabý provoz. Útočník tak může uměle zvýšit provoz, díky kterému nachytá více paketů, a tím i více inicializačních vektorů a rychleji tak odhadne přístupové heslo.

5.2 Potřebné programové vybavení

Většina vybavení určených k zisku hesla byla v minulosti dostupná jen na operačním systému Linux. Dokonce vznikly i některé speciální linuxové distribuce, které se touto problematikou zabývají. Příkladem takových jsou BackTrack a Wifislax. Postupem času se ale začaly objevovat klony linuxových aplikací, spustitelné na OS Microsft Windows.

Pro prolomení předem sdíleného klíče WEP jsou potřeba programy na uskutečnění následujících kroků: [14]

1. zjištění dostupných sítí v okolí, SSID a další parametry sítě (síla signálu, mac adresa přístupového bodu, typ používaného zabezpečení)
2. programy pro monitorování a zachycení šifrovaného provozu na síti
3. analýza získaných dat a výpočet předem sdíleného klíče

Mezi programy, které zjišťují parametry sítě a jsou navíc dostupné volně ke stažení, patří NetStumbler[5] a inSSIDer[6]. Obě tyto aplikace jsou dostupné jak pro MS Windows, tak i pro uživatele linuxů.

Pro monitorování a analýzu dat slouží programy Wireshark[7] anebo CommView for Wi-Fi[8]. Prvně zmíněná aplikace se používá pro monitorování datového toku na pevných sítích již řadu let. Po aplikaci některých pluginů ji však lze použít i pro odposlech na Wi-Fi sítích. Druhý program, ačkoliv není vydáván pod licencí GNU/GPL, je určen přímo

[5] Pro více informací viz http://www.netstumbler.com/
[6] Pro více informací viz http://www.metageek.net/products/inssider/
[7] Pro více informací viz http://www.wireshark.org/
[8] Pro více informací viz http://www.tamos.com/products/commwifi/

pro bezdrátové sítě a i v testovací verzi dokáže odposlechnout data bez dalších pluginů. Navíc mezi jeho funkce patří export logů do formátu Wiresharku, tudíž nachytané data lze pak pomocí Wiresharku analyzovat.

Vypočtení klíče ze získaných dat lze provést jedním programem z balíku nástrojů aircrack-ng[9]. Tento balík ale obsahuje poměrně dost dalších aplikací sloužících k revizi bezdrátových sítí. Jejich popis je dostupný z webových stránek programu či ze stránek Wikipedie[10].

[9] Více informací viz http://www.aircrack-ng.org/
[10] Soupis programů aircrack-ng je dostupný na http://en.wikipedia.org/wiki/Aircrack-ng

6 Laboratorní úlohy

Na následujících stránkách bude popsáno několik laboratorních cvičení, které mají za úkol procvičit teoretické znalosti, které byly výše popsány. Úlohy jsou většinou situovány pro použití na zařízeních od firmy Cisco, popř. TPLink, či ZyXEL. Proto pokud při řešení úloh bude třeba využít HW od jiných firem, může se postup mírně lišit a bude nutné zadání daných úloh poupravit.

Vzhledem k faktu, že se obor informatiky velmi rychle zdokonaluje a technika rychle zastarává, jsou úlohy psané v co nejobecnějším smyslu tak, aby nebyly vázány pouze na jeden typ HW. Proto by jejich splnění nemělo činit potíže ani s použitím jiných zařízení, než kterou jsou uvedeny. V případech, kdy to jen bylo alespoň částečně možné, je použit obdobný hardware jako v programu Cisco Packet Tracer, aby bylo možné splnění úloh i mimo drahé laboratoře. Bohužel pomocí programu nelze vždy stoprocentně simulovat realitu, a proto splnění úloh v laboratoři je více než doporučeno. Pro pořádek je u každé úlohy napsáno, zda by ji šlo ve výše zmíněném programu splnit, či ne.

V zadání každé úlohy je popsáno, jaká obecná zařízení jsou potřebné. V následující závorce je pak uvedeno, jaký hardware byl při tvorbě skutečně použit. Stejný popis je pak také využit u úloh, kdy je potřeba pro splnění úlohy implementovat speciální software.

6.1 Úloha č. 1 – Propojení 2 bezdrátových zařízení pomocí Wi-FI routeru

Toto cvičení je základem všech dalších. Jeho cílem je propojení dvou bezdrátových klientů pomocí Wi-Fi routeru. Jelikož není použit žádný druh zabezpečení, tak by připojení klientů nemělo činit žádné potíže. Pro splnění úlohy je potřeba nastavit základní parametry sítě (SSID, režim, IP adresa) a také umět nastavit IP adresu na síťové rozhraní klientů.

V této i následujících úlohách se počítá s tím, že student má znalost alespoň základních principů sítí (příkladem může být činnost DHCP). Dále úloha počítá se znalostmi nabytými v kapitolách a podkapitolách 1.5 Rozdělení sítí podle IEEE 802.11 a 2 Standard 802.11.

V základní verzi této laboratorní práce není použit žádný pokročilý hardware ani software, proto ji lze splnit nejen ve specializované počítačové laboratoři, ale i v domácím prostředí, či v Cisco Packet Traceru. Modifikace úlohy je ale možné splnit pouze v reálném prostředí. Pro splnění modifikací je nutné mít nainstalovaný program inSSIDer[11], který slouží k zobrazení okolních Wi-Fi sítí a měření síly jejich připojení.

Zadání první úlohy je k dispozici na vytisknutí v příloze A. Řešení pak v příloze H.

[11] Program je dostupný z http://www.metageek.net/products/inssider/

6.2 Úloha č. 2 – Základní nastavení zabezpečení bezdrátové sítě

Toto cvičení je nadstavbou předcházejícího. Hlavním úkolem studentů je vylepšit zapojení o zavedení základních bezpečnostních mechanismů. Studenti tak implementují protokol WEP a následně pak osobní WPA2. Navíc musí rozhodnout, zda je bezpečnější, aby přístupový bod své SSID vysílal, či nikoliv.

Úloha předpokládá, že student úspěšně zvládl předcházející cvičení a prostudoval čtvrtou kapitolu Zabezpečení bezdrátových sítí a volitelně 5tou kapitolu věnovanou Odchytávání provozu na bezdrátových sítích. V ní je uvedeno, jak je zabezpečení typu WEP náchylné na odposlech.

Cvičení opět není náročné na použitý hardware ani software – ty jsou navíc stejné jako v předcházející úloze. Proto je pro správné splnění úlohy jedno, zda ji student vykoná v reálném prostředí, či Cisco Packet Traceru.

Zadání druhé úlohy je k dispozici na vytisknutí v příloze B. Řešení pak v příloze I.

6.3 Úloha č. 3 – Zamezení přístupu do sítě pomocí filtrování MAC adres

Druhá úloha byla věnována bezpečnostním protokolům. Další metodou, která se využívá zároveň s protokoly, je filtrování MAC adres. Pomocí nich lze nastavit, jaké zařízení se do sítě mohou nebo naopak nemohou napojit.

Cvičení opět předpokládá, že před ním student úspěšně zvládl obě předchozí. Z materiálů je dobré prostudovat pouze podkapitolu 4.2.3 Filtrování MAC adres. K tomu se předpokládá, že student zná, jak a kde se dá zjistit MAC adresa bezdrátové karty jeho klienta.

Z hlediska použitého hardware přibyl další klient. Tudíž ke zdárnému splnění je potřeba vlastnit už 3. Jiný náročný hardware ani software potřeba není. Je ovšem potřeba dbát na volbu Wi-Fi routeru. Některé levnější varianty nemusí metodu filtrování dle MAC adres podporovat. V případě nutnosti lze tuto úlohu splnit i v Cisco Packet Traceru.

Zadání třetí úlohy je k dispozici k vytisknutí v příloze C. Řešení pak v příloze J.

6.4 Úloha č. 4 – Správa přístupu pomocí AAA serveru

Druhé a třetí cvičení se dotýkaly bezpečností politiky. Následující cvičení má za úkol vysvětlit základní problematiku správy účtů skrz RADIUS server. Ačkoliv nastavení AAA serveru má poměrně velkou řadu možností, úloha se bude věnovat pouze těm

základním, ale za to nejvíce používaným. V programu Packet Tracer nelze ani použít. Modifikace této úlohy se týká nasazení AAA serveru v reálném prostředí.

Úloha předpokládá, že je student obeznámen s podkapitolou 4.3 Pokročilé metody autentizace a šifrování. Následně pak také s kapitolou 4.4 Pokročilé šifrovací metody. Z obou kapitol je nutné znát, jakým způsobem pracuje AAA server typu RADIUS a také protokol WPA2.

Při plnění této úlohy v základní verzi musí student vlastnit 1 počítač s nainstalovaným Cisco Packet Tracerem[12]. Pokud program nevlastní, stále může splnit modifikaci. Pro ni je potřeba mít Wi-Fi router, který podporuje podnikový typ protokolu WPA. Navíc je potřeba mít jeden počítač s nainstalovaným RADIUS serverem (při plnění úlohy byl využit TekRADIUS) a doporučení je i mít nainstalovaný program RADTest.

Zadání čtvrté úlohy je k dispozici k vytisknutí v příloze D. Řešení pak v příloze K.

6.5 Úloha č. 5 – Prolomení klíče WEP protokolu

Následující úloha si klade za úkol ukázat, jak jednoduše lze prolomit a získat přístup do sítě, když administrátor využil autentizační protokol WEP. Úkony popsané se týkají frekvenčního pásma 2.4 GHz. Při použití pásma 5 GHz je nutné některé kroky postupu poupravit.

V kapitole 4.2.2 Autentizace Wired Equivalent Privacy – Pre Shared Key (WEP-PSK) jsou nedostatky této autentizační metody popsány. Další kapitolou týkající se prolomení WEP je 5 Odchytávání provozu na bezdrátových sítích. Obě tyto kapitoly je doporučeno prostudovat.

Z důvodu potřeby pokročilého software nelze úloha vypracovat v programu Cisco Packet Tracer. Navíc vzhledem k náročnosti některých úkonů je lepší úlohu vypracovávat v pokročilé laboratoři, než v domácím prostředí. Na bezdrátovém klientovi, který bude použit jako útočník, je nutné mít síťovou kartu nastavenou tak, aby podporovala monitorovací režim[13]. Režim vkládání paketů (packet injection) není vyžadován, urychlí však práci.

Zadání páté úlohy je k dispozici k vytisknutí v příloze E. Řešení pak v příloze L.

[12] Cisco Packet Tracer lze stáhnout ze stránek Cisco Akademie pouze v případě, že jste jejím studentem. Případné informace o tomto programu lze zjistit na http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html

[13] Ne každá síťová karta tyto režimy podporuje. U některých karet navíc různé ovladače podporují různé režimy.

6.6 Úloha č. 6 – Odchytávání provozu na bezdrátové síti

V předcházejícím cvičení bylo předvedeno, jak lze prolomit síť, která je zabezpečena slabým šifrováním typu WEP. Tato úloha má za úkol předvést, jak lze s pomocí klíče monitorovat celou síťovou komunikaci. Student má za úkol odposlechnout nešifrovaný provoz mezi bezdrátovým klientem a FTP serverem.

Pro splnění úlohy je dobré prostudovat kapitolu 5 Odchytávání provozu na bezdrátových sítích. Dále je dobré být obeznámen s možnostmi programu CommView, případně s Wiresharkem.

K zapojení z minulého cvičení nově přibyl FTP server. Toho je možno do sítě umístit buď jako program běžící na dalším počítači, případně lze využít služeb některého dostupného na Internetu. Řešení této úlohy předpokládá instalace vlastního TYPSoft FTP serveru. Z důvodu využití pokročilých technik nelze úlohu splnit v Cisco Packet Traceru a ani se nedoporučuje absolvování v domácím prostředí. Předpokladem pro správné vyřešení je, že útočníkův počítač obsahuje takovou síťovou kartu tak, která podporuje monitorovací režim. Zadání šesté úlohy je k dispozici k vytisknutí v příloze F. Řešení pak v příloze M.

6.7 Úloha č. 7 – Problém vícera sítí pracujících na stejném kanálu

V kapitole číslo 2 Standard 802.11 bylo zmíněno, že se sítě operující na frekvenčním pásmu 2.4 GHz značně ovlivňují. Následně pak dochází k poruchám síťové komunikace. Úloha si klade za úkol dokázat, na kolik je důležité využívat různých a od sebe vzdálených kanálů tak, aby se sítě negativně ovlivňovat nemohly. V praxi to však vždy jednoduše zařídit nelze. Není neobvyklé, že v panelových domech bývá u sebe i více jak 10 bezdrátových sítí.

Pro splnění toho cvičení je dobré prostudovat výše zmíněnou druhou kapitolu. Také je dobré mít alespoň základní znalosti z třetí kapitoly věnované Faktorům ovlivňujícím bezdrátové přenosy.

Schéma zapojení této úlohy je velmi unikátní. Je potřeba využít minimálně dvou Wi-Fi routerů a dvou i více klientů. Čím více se jich však do sítě přidá, tím lépe se problém přeplněnosti pásma ukáže. Navíc všechny zařízení je potřeba umístit tak, aby nebyly posazeny přímo vedle sebe. Například dobrým tahem je jejich rozmístění do různých místností. Dbejte však na to, že některé režimy 802.11 mají dosah poměrně dosti veliký a na malých vzdálenostech tak přeslechy netrpí. Pokud budou zařízení od sebe vzdáleny pouze metr, pravděpodobně se to na výsledcích měření nepromítne. Z hlediska programového vybavení stačí pouze příkazová řádka a příkaz ping. Volitelné je mít nainstalovaný program inSSIDer, který vám ukáže, jak moc silný signál od Wi-Fi routerů máte. Modifikace úlohy se věnují problému pohlcování signálu pomocí různých překážek.

Zadání sedmé úlohy je k dispozici k vytisknutí v příloze G. Řešení pak v příloze N.

Závěr

V teoretické části bakalářské práce byly představeny základní principy a vlastnosti bezdrátových sítí. První sepsaná kapitola se již přímo týkala taxonomie počítačových sítí. Popsány byly sítě typu WPAN, WLAN, WMAN a WWAN.

V pořadí druhé kapitole byl důraz kladem na nejpoužívanější standardy, které se na sítích používají. Tyto standardy vydává 11. pracovní skupina organizace IEEE. Popsány jsou typy 802.11a, b, g, n. Krom těchto standardů jsou ještě popsány hlavičky bezdrátových rámců. U každé varianty protokolu IEEE 802.11 je uveden souhrn jejich vlastností. Kapitola je zakončena porovnáním těchto čtyřech standardů.

Následující kapitola popsala principy faktorů, které signály bezdrátových sítí ovlivňují. Mezi popsaná témata patří modely free path loss, princip rozptýlení, pohlcování a odrazování signálů. Jedno ze cvičení se tématiky ztráty signálu zaobírá.

Čtvrtá teoretická kapitola se věnovala problému bezpečnosti. Toto téma je v dnešní době velmi důležitým. V kapitole jsou popsány bezpečností protokoly WEP, WPA a WPA2 a 802.1x. Kromě nich se tato část bakalářské práce věnuje i různým formám útoků, které v dnešní době útočníci využívají.

Praktická část byla tvořena přímo praktickými úlohami. První úlohy měly za úkol naučit studenty, jakým způsobem vybudovat jednoduchou síť a následně ji zabezpečit jak pomocí postaršího protokolu WEP, tak i novějšího WPA. Třetí úloha navíc obohatila předchozí o filtrování dle MAC adres. Poslední cvičení věnované zabezpečování sítí ukázalo, jak lze na síti využít AAA serveru typu RADIUS.

Další dvě cvičení se částečně věnují problému bezpečnosti také. Ovšem z opačného hlediska. Tentokrát je úkolem síť se zabezpečením typu WEP prolomit. Následně pak odposlechnout komunikaci bezdrátového klienta spolu s FTP serverem. Z těchto nešifrovaných dat pak pro útočníky není problém použité uživatelské jméno a heslo přečíst.

Bohužel z důvodu veliké rozsáhlosti bylo do práce zařazeno pouze sedm úloh. Kdybych měl v budoucnu možnost práci rozšířit, pokusil bych se některé další úlohy zaměřit např. na využití řadičů v sítích LAN. Tyto cvičení by ale nešlo splnit v normálních podmínkách, ale v pokročilé laboratoři.

Použité zdroje

[1] PÁV, Miroslav, Jan SYŘÍNEK a Jana HOŠKOVÁ. *CCNA Exploration - Základy sítí* [online]. Plzeň, 2011, 2011-10-10 [cit. 2012-07-21]. Registrační číslo projektu: CZ.1.07/1.1.12/01.0004. Dostupné z: http://nidv.mysh.cz/data/resources/ccna_exploration_1_tisk_%5B9141179%5D.pdf

[2] CAROLL, Brandon James. *Bezdrátové sítě Cisco*: *Autorizovaný výukový průvodce*. Martin Babarík, Jakub Goner, David Krásenský. Brno: Computer Press, 2011. ISBN 978-80-251-2884-8.

[3] PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, bluetooth, GPRS či 3G. Vyd. 1. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.

[4] How 802.11 Wireless Works. MICROSOFT. *Windows Server | Deploy, Manage, Troubleshoot* [online]. 28. 3. 2010 [cit. 2012-08-01]. Dostupné z: http://technet.microsoft.com/en-us/library/cc757419%28v=ws.10%29.aspx

[5] GEIER, Jim. 802.11 Beacons Revealed. QUINSTREET INC. *Wi-Fi Planet – The Source for Wi-Fi Business and Technology* [online]. 2002 [cit. 2012-07-28]. Dostupné z: http://www.wi-fiplanet.com/tutorials/print.php/1492071

[6] *Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů*

[7] DOLEŽAL, Dušan. Co to je digitální certifikát. *Interval.cz* [online]. 21. 1. 2003 [cit. 2012-07-24]. Dostupné z: http://interval.cz/clanky/co-to-je-digitalni-certifikat/

[8] SSL Certificates powered by VeriSign. VERISIGN. *Symnatec Authentication Services Powered by VeriSign* [online]. 2012 [cit. 2012-08-08]. Dostupné z: https://www.verisign.com/products-services/index.html

[9] Public key certificate. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2012-08-08 [cit. 2012-08-08]. Dostupné z: http://en.wikipedia.org/wiki/Public_key_certificate

[10] CCMP. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2012-04-07 [cit. 2012-08-01]. Dostupné z: http://en.wikipedia.org/wiki/CCMP

[11] The Weakness of TKIP Encryption. In: JAIZANUAR. *Extra Reading Materials* [online]. 20.1.2010 [cit. 2012-08-01]. Dostupné z: http://blogs.iium.edu.my/jaiz/2010/01/20/the-weakness-of-tkip-encryption/

[12] Comparison between WPA and WPA2. SECURITY PRODEDURE. *SecurityProcedure.com | Information System Auditing Resources* [online]. 2008 [cit. 2012-08-01].
Dostupné z: http://www.securityprocedure.com/comparison-between-wpa-and-wpa2

[13] Wi-Fi Protected Access. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 6. 8. 2012 [cit. 2012-08-08].
Dostupné z: http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

[14] Prolomení WEP. In: KERSLAGER, Milan. *Hlavní strana – Milan Kerslager* [online]. 2011, 22. 11. 2011 [cit. 2012-08-08].
Dostupné z: http://www.pslib.cz/ke/Prolomen%C3%AD_WEP

[15] LEHEMBRE, G. Wi-Fi security - WEP, WPA and WPA2 [online]. 2005 [cit. 2012-08-03].
Dostupné z: http://www.hsc.fr/ressources/articles/hakin9wi_/hakin9 wi_ EN.pdf

[16] WLAN Radio Frequency Design Considerations. CISCO. *Cisco Systems, Inc.* [online]. San Jose, 2012 [cit. 2012-08-03]. Dostupné z: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/RFDesign.htmlomiscuous-mode

[17] Wireless network. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2012-08-08 [cit. 2012-08-08].
Dostupné z: http://en.wikipedia.org/wiki/Wireless_network

[18] BLACKWELL, Gerry. MAC Filtering for Your Wireless Network. QUINSTREET. *Wi-Fi Planet - The Source for Wi-Fi Business and Technology* [online]. 10. 2. 2011 [cit. 2012-07-15]. Dostupné z: http://www.wi-fiplanet.com/tutorials/article.php/3924486/MAC-Filtering-for-Your-Wireless-Network.htm

[19] Wireless LAN. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2012-07-30 [cit. 2012-08-08].
Dostupné z: http://en.wikipedia.org/wiki/Wireless_LAN

[20] Basic Service Set. ZIFF DAVIS. *IT Wiki* [online]. 11.10. 2007 [cit. 2012-06-24].
Dostupné z: http://it.toolbox.com/wiki/index.php/Basic_Service_Set

[21] HELTZEL, Paul. Ad-Hoc vs. Infrastructure. PEARSON EDUCATION, Informit. *InformIT: The Trusted Technology Source for IT Pros and Developers* [online]. Indiana, 17. 10. 2003 [cit. 2012-08-08]. Dostupné z: http://www.informit.com/articles/article.aspx?p=101591&seqNum=2

[22] MITCHELL, Bradley. Wireless Standards - 802.11b 802.11a 802.11g and 802.11n. BOUT.COM. A PART OF THE NEW YORK TIMES COMPANY. *Networking - Computer and Wireless Networking Basics - Home Networks Tutorials* [online]. 2012 [cit. 2012-08-08]. Dostupné z: http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm

[23] FIEDLER, Petr a Zdeněk BRADÁČ. Zabezpečení bezdrýtových sítí WiFi (IEEE 802.11b,g). *Automa*: *časopis pro automatizační techniku* [online]. Praha: FCC Public, 7. 10. 2004 [cit. 2012-08-05]. ISSN 1210-9592. Dostupné z: http://www.odbornecasopisy.cz/index.php?id_document=32563

[24] MIMO History. HCDC LABORATORY. *HCDC* [online]. Edmonton, 2010 [cit. 2012-08-11]. Dostupné z: http://www.ece.ualberta.ca/~HCDC/mimohistory.html

[25] Cisco Networking Academy. Cisco akademie: materiály pro výuku CCNA [online]. [cit. 2012-08-11]. Dostupné z: http://www.cisco.com/web/learning/netacad/index.html

Příloha A – Zadání laboratorní úlohy číslo 1

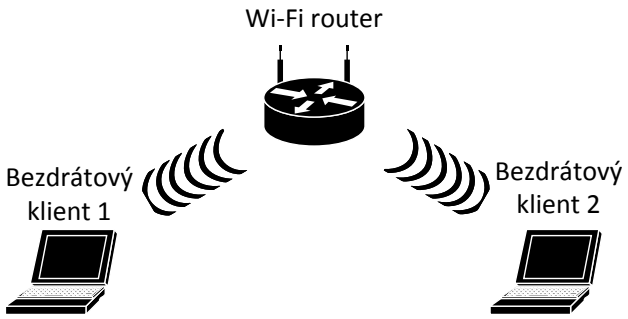
Cíl

Cílem tohoto cvičení je propojení dvou bezdrátových klientů pomocí Wi-Fi routeru.

Potřebná zařízení obecně (přesný název použitého hardware)

- 1x Wi-Fi router (Linksys WRT 300N)
- 2x bezdrátový klient (2x ASUS M51V se systémem Windows 7 / Ubuntu 12.04)
- 1x ethernetový kabel (křížený ethernetový kabel CAT 5.5)

Schematický obrázek zapojení sítě



Pokyny

Název sítě, do které se zařízení budou napojovat, nastavte na „Cviceni-WLAN“. Dále síť uzpůsobte tak, aby se do ní mohly připojit jednak novější zařízení, ale i klienti, kteří nové režimy nepodporují. Tudíž na prvním místě ve výběru módu vyberte takový, který podporuje co možná nejvíce režimů, a tím alespoň částečně zohledňujte zpětnou kompatibilitu. Na síti prozatím nekonfigurujte žádné bezpečnostní mechanismy.

Na zařízeních nastavte IP adresy podle následující tabulky

zařízení	IP adresa	maska podsítě
bezdrátový klient č. 1	192.168.0.1	255.255.255.0
bezdrátový klient č. 2	192.168.0.2	255.255.255.0
Wi-Fi router	192.168.0.200	255.255.255.0

Náznak postupu vypracování úlohy

- Pomocí síťového kabelu se připojte k Wi-Fi routeru.
- Vyresetujte nastavení Wi-Fi routeru tak, aby byl v továrním nastavení.
- Nakonfigurujte na něm parametry podle pokynů v zadání.
- Nastavte na obou klientech IP adresy jejich WLAN sítě.
- Odpojte síťový kabel mezi klientem a Wi-Fi routerem.
- Vyzkoušejte, zda spolu mohou oba klienti komunikovat pomocí příkazu ping.

Otázky k dané úloze

1) Kolika BSA nebo ESA je tato síť tvořena?

   _____

2) Je bezpodmínečně nutné na přístupovém bodu nastavovat DHCP pro funkčnost této sítě?
   - Ano
   - Ne

3) Jaký režim (jaký mód) ze standardů 802.11 pro síť zvolíte?

   _____

4) Jak bude vypadat výpis příkazu „ipconfig“ na prvním bezdrátovém klientu? Vypište jen tu část, která se týká WLAN sítě.
   - Místní IPv6 adresa v rámci propojení: _____
   - Adresa IPv4: _____
   - Maska podsítě: _____
   - Výchozí brána: _____

5) Jak bude vypadat výpis příkazu „ping 192.168.0.2“ spuštěný z prvního bezdrátového klienta?

_____

_____

_____

_____

Příloha B – Zadání laboratorní úlohy číslo 2

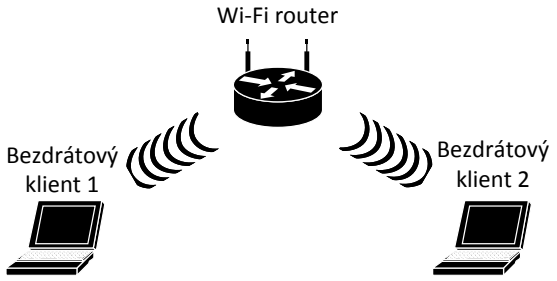
Cíl

Cílem tohoto cvičení je vyzkoušení několika bezpečnostních mechanismů, které se dají na bezdrátové síti aplikovat. Jmenovitě jde o nasazení protokolů WEP a WPA2.

Potřebná zařízení obecně (přesný název použitého hardware)

- 1x Wi-Fi router (Linksys WRT 300N)
- 2x bezdrátový klient (2x ASUS M51V se systémem Windows 7 / Ubuntu 12.04)
- 1x ethernetový kabel (křížený ethernetový kabel CAT 5.5)

Schematický obrázek zapojení sítě



Pokyny

Název bezdrátové sítě nastavte na „Cviceni-WLAN“ a nechte ji fungovat ve standardním režimu mixed(b+g+n). Vysílání jména sítě nakonfigurujte tak, aby to pro celou síť bylo co možná nejbezpečnější. Z hlediska autentizace nastavte režim nejprve na WEP a jako klíč zvolte „3a3b544a564453612950763c6b“. [14] Následně po vyzkoušení funkčnosti sítě zkuste zvolit takový režim WPA2, kde Wi-Fi router obstarává autentizaci přímo sám. Z možností šifer vyberte tu silnější, kterou zastaralý WEP podporovat nemohl. Heslo zvolte z následující tabulky takové, aby bylo co možná nejbezpečnější proti hackerským útokům.

abcd	A123BCD	Cba8!JLO54*z
planeta*	heslo	UPCE!
Hardware	E2!op4*	102567813

[14] Klíč lze buď manuálně zadat, nebo vygenerovat např. na http://www.andrewscompanies.com/tools/wep.asp

Na zařízeních nastavte IP adresy podle následující tabulky

zařízení	IP adresa	maska podsítě
bezdrátový klient č. 1	192.168.0.1	255.255.255.0
bezdrátový klient č. 2	192.168.0.2	255.255.255.0
Wi-Fi router	192.168.0.200	255.255.255.0

Náznak postupu vypracování úlohy

- Nastavte parametry bezdrátové sítě, zatím nekonfigurujte žádné bezpečnostní mechanismy.
- Vyzkoušejte, zda oba klienti mohou na sebe dosáhnout pomocí příkazu ping.
- Nastavte parametry WEP a poupravte nastavení bezdrátových sítí na klientských zařízeních.
- Vyzkoušejte, zda síť funguje, a následně zodpovězte níže vypsané otázky, které se tohoto bezpečnostního protokolu týkají.
- Poté přepněte síť do režimu WPA2, přizpůsobte nastavení klientů, vyzkoušejte funkčnost sítě a zodpovězte otázky, které se WPA2 týkají.

Otázky k dané úloze

1) Jak na Wi-FI routeru nastavíte vysílání SSID do prostoru (SSID Broadcast) a proč?
    - Zapnutý (Enabled)
    - Vypnutý (Disabled)

---

2) Jakou velikost WEP klíče musíte nastavit, aby bylo možné použít klíč ze zadání a proč?

---

3) Je bezpečnější využít WEP klíč o délce 40(64)bit nebo 104(128)bit a proč?

---

4) Jaký režim WPA2 zvolíte a z jakého důvodu?

---

5) Jaký druh šifrování vyberete pro režim WPA2 a z jakého důvodu?

---

6) Které heslo z tabulky 8 pro síť v režimu WPA2 použijete a proč?

Příloha C – Zadání laboratorní úlohy číslo 3

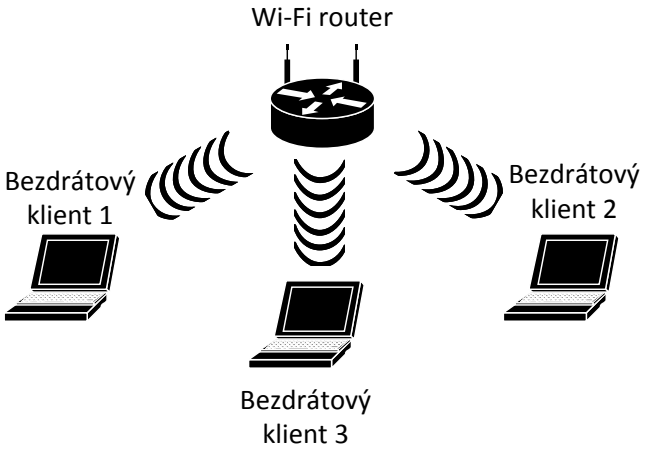
Cíl

Cílem úlohy je vyzkoušení metody filtrování klientů podle MAC adres. V průběhu plnění cvičení si vyzkoušíte jak filtrování povolených, tak nepovolených zařízení.

Potřebná zařízení obecně (přesný název použitého hardware)

- 1x Wi-Fi router (Linksys WRT 300N)
- 3x bezdrátový klient (3x ASUS M51V se systémem Windows 7 / Ubuntu 12.04)
- 1x ethernetový kabel (křížený ethernetový kabel CAT 5.5)

Schematický obrázek zapojení sítě



Pokyny

SSID této bezdrátové sítě nastavte na „Cviceni-WLAN“. Režim nechte nastaven stále na mixed(b+g+n). Na Wi-Fi routeru nevyužívejte služeb DHCP serveru. Z hlediska zabezpečení využijte metodu WPA2-Personal se šifrováním AES a heslem „BezdratovaSit*“ (pro tuto úlohu není náročné heslo nezbytně nutné). Následně pomocí prvního filtru MAC adres zablokujte přístup klienta číslo 3 do této sítě. Po zodpovězení níže položených otázek tento filtr odeberte a nastavte nový (druhý filtr), který naopak povolí přístup do sítě zařízením číslo 1 a 3.

Na zařízeních nastavte IP adresy podle následující tabulky

zařízení	IP adresa	maska podsítě
bezdrátový klient č. 1	192.168.0.1	255.255.255.0
bezdrátový klient č. 2	192.168.0.2	255.255.255.0
bezdrátový klient č. 3	192.168.0.3	255.255.255.0
Wi-Fi router	192.168.0.200	255.255.255.0

Náznak postupu vypracování úlohy

- Wi-Fi router nastavujte pomocí síťového kabelu. Pro testování funkčnosti sítě však tento kabel odpojujte.
- Nakonfigurujte základní parametry sítě Wi-Fi routeru podle zadání.
- Zjistěte si MAC adresy všech tří bezdrátových klientů a vyplňte je do níže uvedené tabulky. Nezapomeňte, že potřebujete zjistit MAC adresu bezdrátového rozhraní WLAN, ne ethernetové LAN karty.
- Nastavujte MAC filtr tak, aby byl ve správném režimu (povolení/blokování).
- Vyzkoušejte funkčnost sítě a zodpovězte níže uvedené otázky, poté filtr zrušte.
- Nakonfigurujte MAC filtr tak, aby odpovídal druhému ze zadání (povolení/blokování) a následně do něho zapište správné adresy.

Otázky k dané úloze

1) Do následující tabulky napište MAC adresy bezdrátových zařízení.

zařízení	MAC adresa Wi-Fi karty
bezdrátový klient č. 1	
bezdrátový klient č. 2	
bezdrátový klient č. 3	

2) Vyberte, která zařízení spolu mohou komunikovat po aplikování prvního MAC filtru.
    - první klient s druhým klientem
    - druhý klient s třetím klientem
    - první klient s třetím klientem
    - Wi-Fi router s prvním klientem
    - Wi-Fi router s druhým klientem
    - Wi-Fi router s třetím klientem

3) Vyberte, která zařízení spolu mohou komunikovat po aplikování druhého MAC filtru.
    - první klient s druhým klientem
    - druhý klient s třetím klientem
    - první klient s třetím klientem
    - Wi-Fi router s prvním klientem
    - Wi-Fi router s druhým klientem
    - Wi-Fi router s třetím klientem

Příloha D – Zadání laboratorní úlohy číslo 4

Cíl

Cílem čtvrté úlohy je úspěšné připojení klienta do sítě za použití účtu a hesla, které je spravovány AAA serverem. Základní verze úlohy je splnitelná v programu Cisco Packet Tracer. V modifikaci zadání je cílem zprovoznit RADIUS server v reálném prostředí.

Potřebné zařízení pro splnění v PT (přesný název použitého hardware)

- 1x počítač s nainstalovaným Packet Tracerem (ASUS M51V s OS Windows 7 s programem Cisco Packet Tracer verze 5.3.2.0027)

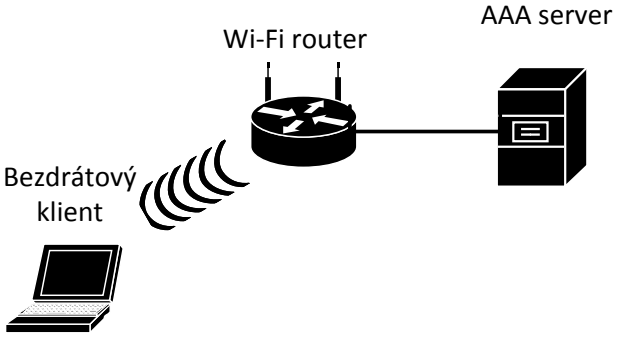
Potřebné fyzické zařízení obecně (název v PT / reálném prostředí)

- 1x Wi-Fi router (Linksys WRT 300N / ZyXEL P660HW-T3 v2)
- 1x AAA server (Server-PT / ASUS M51V s OS Windows 7)
- 1x bezdrátový klient (Labtop-PT s Linksys WPC300N / ASUS M51V s OS Win7)
- 1x přímý ethernetový kabel

Potřebné programové vybavení pro splnění modifikace zadání

- RadTest 2.6
- TekRADIUS LT

Schematický obrázek zapojení sítě



Pokyny

Zapojte všechna zařízení podle výše zmíněného schématu a následně jim nastavte statické IP adresy dle níže uvedené tabulky. Wi-Fi router uzpůsobte tak, aby jeho bezdrátová síť „Cviceni-WLAN“ pracovala v režimu Mixed (802.11bgn) a také, aby posílala v majákových rámcích (beacon frames) své SSID. Dále využijte podnikového režimu WPA2 se sdíleným tajemstvím „sdileneTajemstvi“. Na Serveru-PT využijte jen službu RADIUS serveru. Klienta tohoto serveru pojmenujte „Linksys“ a uživatele „uziv1“ s heslem „cisco1“. Bezdrátovou síť nechte fungovat v režimu AES, v případě neúspěchu využijte TKIP.

Na zařízeních nastavte IP adresy podle následující tabulky

zařízení	IP adresa	maska podsítě
labtop	192.168.0.1	255.255.255.0
server	192.168.0.10	255.255.255.0
Wi-Fi router	192.168.0.200	255.255.255.0

Náznak postupu vypracování úlohy

- Na pracovní plochu vložte Labtop-PT a Server-PT a Linksys WRT300N.
- Propojte Wi-Fi router spolu se serverem pomocí přímého kabelu.
- Na labtopu zvolte správnou síťovou kartu (modul).
- Wi-Fi router nastavte podle zadání. Využijte přitom GUI rozhraní routeru. Rozhodněte se, zda využijete šifrování typu AES, či TKIP.
- Na Serveru zakažte ty služby, které ke své funkci nepotřebuje.
- V nastavení RADIUS serveru zvolte správně klienta i typ serveru.
- V nastavení RADIUS serveru přidejte nového uživatele dle zadání.
- Na labtopu zvolte desktopovou aplikaci PC Wireless a v ní záložku profil. Vytvořte nový se jménem „profil 1“. Využijte možnosti Advanced Setup pro úplnou konfiguraci. Pokud máte problém se šifrováním AES, změňte na labtopu v záložce Config- Wireless-Encryption Type šifrování na TKIP.

Modifikace

Stejnou síť, kterou jste konfigurovali dle původního zadání, převeďte do reálných podmínek. Pro RADIUS server zvolte program TekRADIUS LT a pro jeho otestování před nasazením do sítě program RadTest 2.6.

AAA server nechte pracovat na portech 1812 (autentizace) a 1813 (správa účtů). U uživatele nastavte atribut Check-User-Password roven heslu uvedeném v zadání. Dále pak nastavte atribut Success-Reply-User-Password na hodnotu úplně stejnou, jako jste

právě napsali do Check. Protokol PEAP nastavte na EAP-MD5. Zbytek uživatelů a klientů RADIUSu (tj. přístupových bodů) nezapomeňte správně nastavit dle původního zadání. Kvůli testování přidejte mezi klienty i adresu samotného serveru (tzn. adresu sama sebe).

V programu RadTest vytvořte novou úlohu. Údaje nastavte dle zadání. V kolonce Addition Packet přidejte nový a vložte do něho 2 atributy. User-Name s hodnotou „uziv1“ a User-Password s hodnotou „cisco1“. Následně zkuste úlohu spustit a tím ověřit, zda RADIUS server funguje. Pokud ano, přejděte k nastavení Wi-Fi routeru a síť poté otestujte.

Otázky k dané úloze

1) Jak nastavíte možnost SSID broadcast na Wi-Fi routeru?

    - Enabled
    - Disabled

2) Na jakém portu v základní verzi komunikuje Wi-Fi router s RADIUS serverem?

    _____

3) Doplňte následující informace týkající se nastavení Wi-Fi routeru.
    - Security mode: _____
    - Encryption: _____
    - RADIUS server: _____
    - RADIUS port: _____
    - Shared Secret: _____
    - Key Renewal: _____

4) Jak budete vypadat záznam o klientovi na AAA serveru?

Client name	Client IP	Server type	Key

5) Napište, jaké uživatele a s jakým heslem bude AAA server obsahovat.

UserName	Password

Příloha E – Zadání laboratorní úlohy číslo 5

Cíl

Cílem tohoto cvičení je prolomení protokolu WEP. Postup a pokyny v této úloze jsou situovány pro použití na 2.4 GHz pásmu. Pokud budete chtít použít pásmo 5 GHz, musíte některé kroky poupravit.

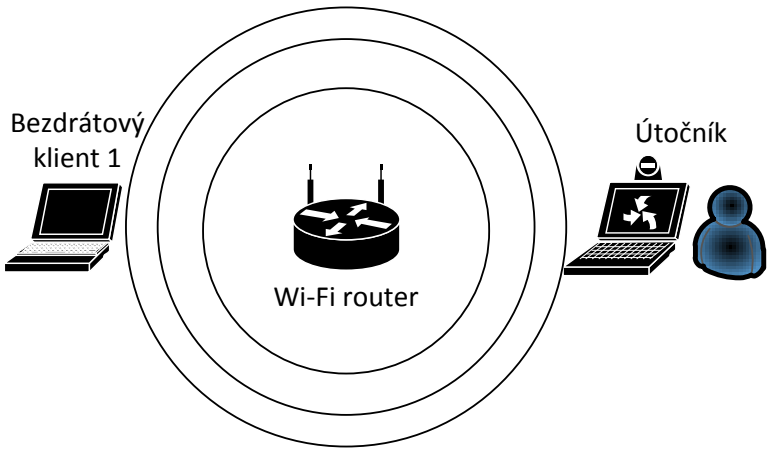
Potřebná zařízení obecně (přesný název použitého hardware):

- 1x Wi-Fi router (Tenda Router W311R+ pracující v pásmu 2.4 GHz)
- bezdrátový klient (ASUS M51V se systémem Windows 7)
- bezdrátový klient v roli útočníka s wi-fi kartou podporující monitorovací režim (ASUS M51V s wi-fi kartou Intel Wi-Fi Link 5100 AGN)
- připojení k Internetu (není nezbytné)
- 1x ethernetový kabel (křížený ethernetový kabel CAT 5.5)

Potřebné programové vybavení na počítači útočníka:

- CommView for Wi-Fi[15]
- AirCrack-ng[16]

Schematický obrázek zapojení sítě



[15] Program lze stáhnout na http://www.tamos.com/products/commwifi/
[16] Program lze stáhnout na http://www.aircrack-ng.org/

Pokyny

Nastavte síť tak, aby byla pojmenována „Tenda“ a okolí o svém SSID informovala. Síť ponechte pracovat na kterémkoliv režimu pracujícím na 2.4 GHz pásmu. Kanál však vyberte s číslem 2[17]. Zabezpečte síť tak, aby využívala protokolu WEP-PSK. Heslo zadejte „aaaaa“, popř 6161616161[18] v šestnáctkové podobě. Poté nastavte prvního klienta tak, aby se mohl napojit k síti. Spusťte na něm v příkazovém řádku příkaz „ping 10.0.0.10 –t“ pro udržení provozu na síti. Alternativou může být připojení a následné surfování po Internetu. Pro urychlení celé operace je počet zachycených paketů klíčový.

Na útočníkově počítači nainstalujte programy CommView for Wi-Fi a AirCrack ng. V případě potřeby upgradněte ovladače wi-fi karty tak, aby podporovala monitorující režim. V aplikaci CommView nastavte zachytávání pouze datových paketů[19]. V nastavení logování zvolte automatické ukládání do adresáře „C:\dev\“. Pravidla pokročilého zachytávání uzpůsobte tak, aby program zachytával pakety se vzorcem „ftype=2 and wep=1“. Následně začněte sledovat síť na Vámi zvoleném kanálu a také ve Vámi zvoleném režimu.

Po nějakém čase, kdy CommView nachytá dostatek paketů a vyčlení určité množství [20]inicializačních vektorů, využijte vestavěného Log View a otevřete v něm automaticky uložené logy paketů. Ty následně vyexportujte ve formátu Wireshark do adresáře „C:\dev\log\“. Následně pomocí programu AirCrack-ng nechte z daného souboru dešifrovat heslo. Program se spouští souborem Aircrack-ng GUI.exe.

Na zařízeních nastavte IP adresy podle následující tabulky

zařízení	IP adresa	maska podsítě
bezdrátový klient č. 1	10.0.0.1	255.255.255.0
útočník (klient č.2)	----------	----------
Wi-Fi router	10.0.0.10	255.255.255.0

[17] Pro pásmo 5 GHz nutno upravit na kanál s jiným číslem. Každopádně pro zjednodušení situace vyberte takový kanál, na kterém momentálně žádná jiná síť nepracuje.
[18] Pro tuto úlohu není podstatné, jak složité heslo zvolíte.
[19] Ve většina verzí programu postačí nechat zatrhnuté pouze Capture Data Packets v záložce Rules.
[20] Toto množství nelze přesně definovat. Doporučuje se odchytit alespoň 150 000 paketů a mít 5000 IV.

Otázky k dané úloze

1) Jaký režim (jaký mód) a kanál jste ze standardů 802.11 pro síť zvolili?

_____

2) Kolik paketů jste potřebovali pro získání hesla?

_____

3) Kolik inicializačních vektorů (IV) bylo pro dešifrování hesla potřeba?

_____

Příloha F – Zadání laboratorní úlohy číslo 6

Cíl

Toto cvičení je nadstavbou předchozího. Po zisku WEP klíče lze již bezproblémově odposlechnout veškerý síťový provoz. V tomto případě komunikaci FTP serveru a jeho klienta. Cílem úlohy je přečtení dat z paketů a vyčtení uživatelského jména a hesla, která uživatel použit k přihlášení na FTP server.

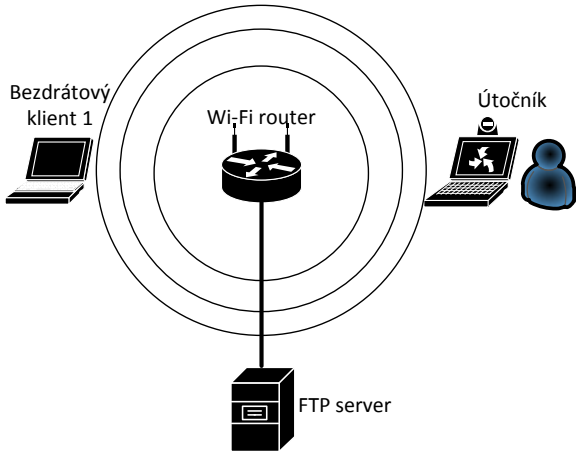
Potřebná zařízení obecně (přesný název použitého hardware)

- 1x Wi-Fi router (Tenda Router W311R+ pracující v pásmu 2.4 GHz)
- bezdrátový klient (ASUS M51V se systémem Ubuntu 12.04)
- bezdrátový klient v roli útočníka s wi-fi kartou podporující monitorovací režim (ASUS M51V s wi-fi kartou Intel Wi-Fi Link 5100 AGN)
- FTP server (ASUS M51V s TYPSoft FTP server v 1.10)
- připojení k Internetu (není nezbytné)

Potřebné programové vybavení na počítači útočníka

- CommView for Wi-Fi, případně Wireshark

Schematický obrázek zapojení sítě



Pokyny

Nejprve na zařízeních nainstalujte potřebný software a nastavte IP adresy dle níže uvedené tabulky. Na FTP serveru vytvořte uživatele „uzivatel“ s heslem „mojeheslo“. Bezdrátovou síť nakonfigurujte tak, aby pracovala v režimu 802.11 mixed (b/g/n) a své SSID „Tenda“ vysílala do okolí. Z hlediska bezpečnosti použijte protokol WEP s klíčem „aaaaa“, popř. 6161616161 v šestnáctkové podobě. Síťovou kartu útočníka nastavte tak, aby podporovala monitorovací režim. Na útočníkově počítači nastavte v programu CommView stejný WEP klíč, jaký je na Wi-Fi routeru.[21] V nastavení pravidel nechte odposlouchávat FTP porty 20 a 21 v obou směrech[22].

Na útočníkově počítači zapněte odposlouchávání této bezdrátové sítě. Poté se z bezdrátového klienta přihlaste k FTP servru a vytvořte na něm adresář „adresar“. Následně analyzujte výsledná data z programu CommView.

Na zařízeních nastavte IP adresy podle následující tabulky

zařízení	IP adresa	maska podsítě
FTP server	10.0.0.1	255.255.255.0
bezdrátový klient č. 1	10.0.0.2	255.255.255.0
útočník (klient č. 2)	--------	--------
Wi-Fi router	10.0.0.10	255.255.255.0

Otázky k dané úloze

V následujících otázkách vypisujte jen čisté textové znaky. Paznaky neopisujte.

1) Napište alespoň dva FTP příkazy, či zprávy, které se Vám podařilo z dat paketů odposlechnout.

_____

_____

2) Vypište příkaz, kterým posílá klient serveru uživatelské jméno.

_____

3) Jak v paketu vypadá příkaz posílající serveru heslo?

_____

4) Z jakého uživatelského portu posílá klient serveru data?

_____

[21] Lze nastavit v Settings – WEP/WPA keys. Klíč byl zjištěn v minulém cvičení.
[22] Lze nalézt v záložce Rules - Ports

Příloha G – Zadání laboratorní úlohy číslo 7

Cíl

Cílem této úlohy je dokázání, že se vícero sítí operujících v pásmu 2.4 GHz negativně ovlivňuje.

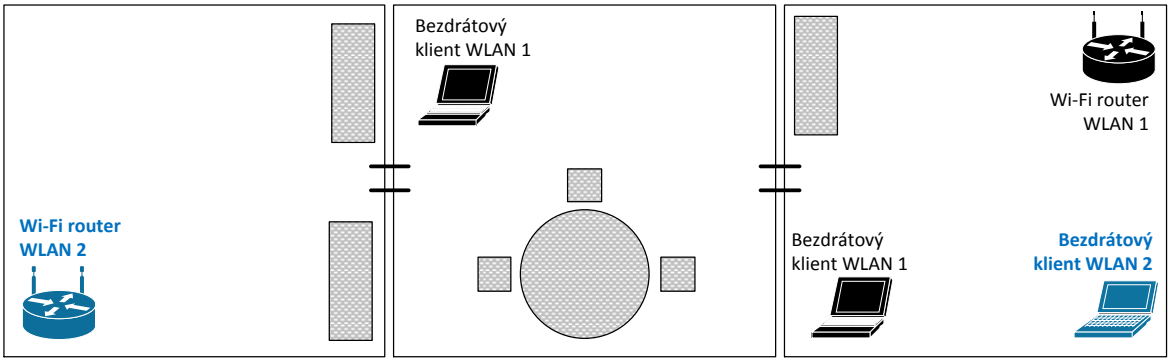
Potřebná zařízení obecně (přesný název použitého hardware)

- 2 a více Wi-Fi routerů pracujících v 2.4 GHz pásmu (Tenda Router W311R+, ZyXEL P660HW-T3 v2)
- 2 a více bezdrátových klientů (ASUS M51V se OS Ubuntu 12.04, 2x ASUS M51V s OS Win 7)

Potřebné programové vybavení

- inSSIDer (není ke splnění nezbytně nutný)

Schematický obrázek zapojení sítě



Pokyny

Jednotlivá zařízení je potřeba umístit v poměrně velké vzdálenosti od sebe. Pokud by byly v jedné místnosti, pravděpodobně by sítě moc omezeny nebyly. Schematický obrázek zapojení ukazuje případ, jak byli klienti rozmístěni při tvorbě této úlohy. Z hlediska parametrů sítě je pouze důležité, aby všechny pracovaly na stejném 2.4 GHz pásmu. Sítě nechte pracovat v režimu 802.11n, popř. 802.11g[23].

První test spočívá v tom, že nakonfigurujete vysílání všech sítí na stejný kanál (např. 6). Pomocí příkazu „ping IP_adresa -l 1400 -f -t“ otestujte propustnost sítě.

[23] Mějte na paměti, že protokol 802.11n má kratší dosah, než jeho předchůdci. Pokud použijete protokol 802.11b, může se stát, že při nízkém provozu na síti se signály příliš ovlivňovat nebudou.

Pro druhý test nakonfigurujte sítě tak, aby jedna operovala na kanálu číslo 1, druhá na 6, případně třetí na 11. Opět pomocí stejného příkazu ping otestujte síť a výsledky obou měření zaneste do níže uvedených tabulek.

Modifikace zadání

Na síti vyzkoušejte různé standardy 802.11. Prozkoumejte v praxi, jak daleko signál při kterém použitém typu dosáhne, jak moc náchylné na okolní podmínky jsou a jakých přenosových rychlostí dosáhnou. Druhou modifikací je vyzkoušení, jaké předměty signál pohlcují. Pro názornost vyzkoušejte vložit Wi-Fi router do papírové krabice, či kovového rámu. Na kvalitě signálu se tyto podmínky znatelně projeví.

Na zařízeních nastavte IP adresy podle následující tabulky

zařízení	IP adresa	maska podsítě
bezdrátový klienti WLAN 1	192.168.0.x	255.255.255.0
bezdrátový klienti WLAN 2	10.0.0.y	255.255.255.0
Wi-Fi router č. 1	192.168.0.202	255.255.255.0
Wi-Fi router č. 2	10.0.0.10	255.255.255.0

Otázky k dané úloze

1) Jaké režimy a bezpečnostní protokoly jste ve Vašich sítích zvolili?

- WLAN síť 1 _____
- WLAN síť 2 _____
- WLAN síť 3 _____

2) Vypište celkové statistiky příkazu ping, zavolaného z klienta **první** WLAN a směrovaného na jeho Wi-Fi router, který pracoval na **kanálu 6**.

Pakety: odeslané: _____, přijaté: _____, ztracené_____ (ztráta ____ %)

Přibližná doba do přijetí odezvy v milisekundách.
Minimum = _____ ms, maximum = _____ ms, průměr = _____ms

3) Vypište celkové statistiky příkazu ping, zavolaného z klienta **druhé** WLAN a směrovaného na jeho Wi-Fi router, který pracoval na **kanálu 6**.

Pakety: odeslané: _____, přijaté: _____, ztracené_____ (ztráta ____ %)

Přibližná doba do přijetí odezvy v milisekundách.
Minimum = _____ ms, maximum = _____ ms, průměr = _____ms

4) Vypište celkové statistiky příkazu ping, zavolaného z klienta **první** WLAN a směrovaného na jeho Wi-Fi router, který pracoval na **kanálu 1**.

Pakety: odeslané: _____, přijaté: _____, ztracené_____ (ztráta ____ %)

Přibližná doba do přijetí odezvy v milisekundách.
Minimum = _____ ms, maximum = _____ ms, průměr = _____ms

5) Vypište celkové statistiky příkazu ping, zavolaného z klienta **druhé** WLAN a směrovaného na jeho Wi-Fi router, který pracoval na **kanálu 6** (případně **11**).

Pakety: odeslané: _____, přijaté: _____, ztracené_____ (ztráta ____ %)

Přibližná doba do přijetí odezvy v milisekundách.
Minimum = _____ ms, maximum = _____ ms, průměr = _____ms

6) Porovnejte Vámi naměřené výsledky a odhadněte, proč některé spoje vykazovaly ztráty a vyšší přenosové rychlosti, než ostatní.

_____

_____

7) Kolik různých BSA a ESA obsahují tyto sítě? Vypište i kteří klienti se ke které přidružují.

_____

_____

_____

Příloha H – Řešení laboratorní úlohy číslo 1

Některé odpovědi v této úloze závisí na továrním nastavení Wi-Fi karet v labtopech, proto odpovědi uvedené níže se Vašem případě budou velice pravděpodobně lišit. Pro správnost však stačí, že je zachován stejný formát takovéto odpovědi. Pro zjednodušení, ty možnosti, které se pravděpodobně budou odlišovat, jsou označeny hvězdičkou (*).

Odpovědi na otázky:

1) Kolika BSA nebo ESA je tato síť tvořena?

   Síť je tvořena pouze jednou BSA.

2) Je bezpodmínečně nutné na přístupovém bodu nastavovat DHCP pro funkčnost této sítě?

   ~~o Ano~~
   o Ne

3) Jaký režim (jaký mód) ze standardů 802.11 pro síť zvolíte?

**Mixed (b+g+n) – popř. jakýkoliv jiný mixed mód.*

4) Jak bude vypadat výpis příkazu „ipconfig“ na prvním bezdrátovém klientu? Vypište jen tu část, která se týká WLAN sítě.
   - Místní IPv6 adresa v rámci propojení: ** fe80::557f:8fb4:cb4e:9b55%12*
   - Adresa IPv4: *192.168.0.1*
   - Maska podsítě: *255.255.255.0*
   - Výchozí brána: *192.168.0.200 – není nutné zadat*

Jak bude vypadat výpis příkazu „ping 192.168.0.2“ spuštěný z prvního bezdrátového klienta?

**Odpověď od 192.168.0.2: bytes=32 time=2ms TTL=128*

**Odpověď od 192.168.0.2: bytes=32 time=5ms TTL=128*

**Odpověď od 192.168.0.2: bytes=32 time=1ms TTL=128*

**Odpověď od 192.168.0.2: bytes=32 time=2ms TTL=128*

Příloha I – Řešení laboratorní úlohy číslo 2

Odpovědi na otázky:

1) Jak na Wi-FI routeru nastavíte vysílání SSID do prostoru (SSID Broadcast) a proč?
   - ~~Zapnutý (Enabled)~~
   - Vypnutý (Disabled)

Pro útočníka je těžší hackovat síť, kterou ihned nevidí než tu, která se prezentuje okolí.

2) Jakou velikost WEP klíče musíte nastavit, aby bylo možné použít klíč ze zadání a proč?

104(128)bit. Zadaný klíč obsahuje 26 HEX cifer, 40(64)bit podporuje pouze 10HEX cifer.

3) Je bezpečnější využít WEP klíč o délce 40(64)bit nebo 104(128)bit a proč?

104(128)bit. Je těžší prolomit delší klíč než kratší.

4) Jaký režim WPA2 zvolíte a z jakého důvodu?

Osobní režim WPA2-PSK (Personal). Podnikový (Enterprise) využívá AAA serveru.

5) Jaký druh šifrování vyberete pro režim WPA2 a z jakého důvodu?

AES. Jedná se o bezpečnější (ale také výpočetně náročnější) šifru než zastaralý TKIP.

6) Které heslo z tabulky 8 pro síť v režimu WPA2 použijete a proč?

*Cba8!JLO54*z . Jedná se o heslo, ve kterém se nachází malá i velká písmena, číslice a i speciální znaky. Heslo „E2!op4*“ je méně bezpečné, protože obsahuje menší počet znaků.*

Příloha J – Řešení laboratorní úlohy číslo 3

Některé odpovědi v této úloze závisí na továrním nastavení Wi-Fi karet v labtopech, proto odpovědi uvedené níže se Vašem případě budou velice pravděpodobně lišit. Pro správnost však stačí, že je zachován stejný formát takovéto odpovědi. Pro zjednodušení, ty možnosti, které se pravděpodobně budou odlišovat, jsou označeny hvězdičkou (*). MAC adresy vyplněné v následující tabulce mohou být psány i v jiném formátu. Příkladem může být „00E0.8F60.3891“.

Odpovědi na otázky:

1) Do následující tabulky napište MAC adresy bezdrátových zařízení.

zařízení	**MAC adresa Wi-Fi karty**
bezdrátový klient č. 1	**00:60:47:78:6D:3D*
bezdrátový klient č. 2	**00:90:0C:67:9E:49*
bezdrátový klient č. 3	**00:E0:8F:60:38:91*

2) Vyberte, která zařízení spolu mohou komunikovat po aplikování prvního MAC filtru.
   - o první klient s druhým klientem
   - ~~o druhý klient s třetím klientem~~
   - ~~o první klient s třetím klientem~~
   - o Wi-Fi router s prvním klientem
   - o Wi-Fi router s druhým klientem
   - ~~o Wi-Fi router s třetím klientem~~

3) Vyberte, která zařízení spolu mohou komunikovat po aplikování druhého MAC filtru.
   - ~~o první klient s druhým klientem~~
   - ~~o druhý klient s třetím klientem~~
   - o první klient s třetím klientem
   - o Wi-Fi router s prvním klientem
   - ~~o Wi-Fi router s druhým klientem~~
   - o Wi-Fi router s třetím klientem

Příloha K – Řešení laboratorní úlohy číslo 4

Odpovědi na otázky:

1) Jak nastavíte možnost SSID broadcast na Wi-Fi routeru?

   - Enabled
   - ~~Disabled~~

2) Na jakém portu komunikuje Wi-Fi router s RADIUS serverem?

   1645

3) Doplňte následující informace týkající se nastavení Wi-Fi routeru.
   - Security mode: *WPA2 Enterprise*
   - Encryption: *AES (TKIP)-dle toho, co si student zvolil*
   - RADIUS server: *192.168.0.10*
   - RADIUS port: *1645*
   - Shared Secret: *sdileneTajemstvi*
   - Key Renewal: *3600*

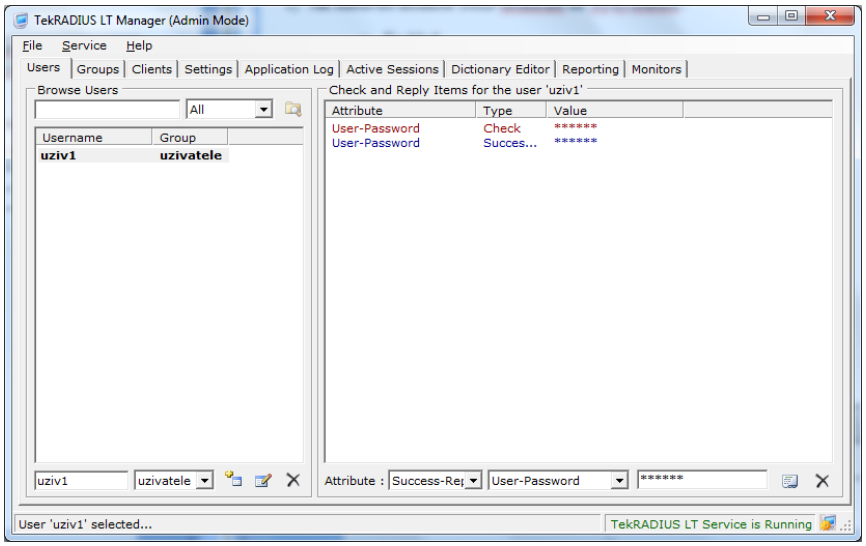
4) Jak budete vypadat záznam o klientovi na AAA serveru?

Client name	Client IP	Server type	Key
Linksys	*192.168.0.200*	*Radius*	*sdileneTajemstvi*

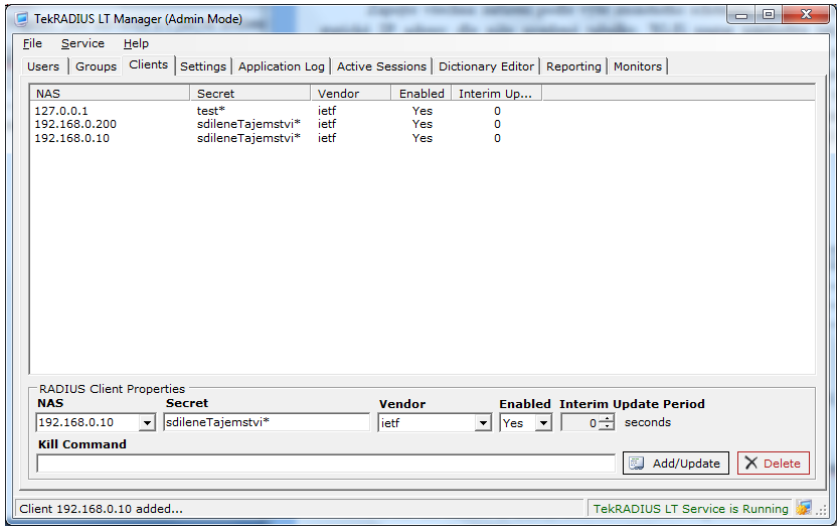
5) Napište, jaké uživatele a s jakým heslem bude AAA server obsahovat.

UserName	Password
uziv1	*cisco1*

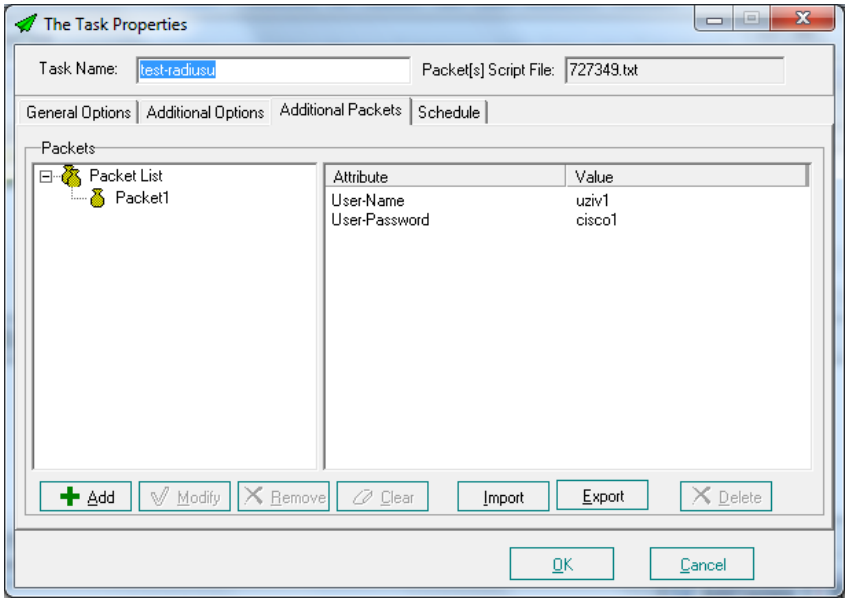
Nastavení uživatelů v TekRADIUS LT



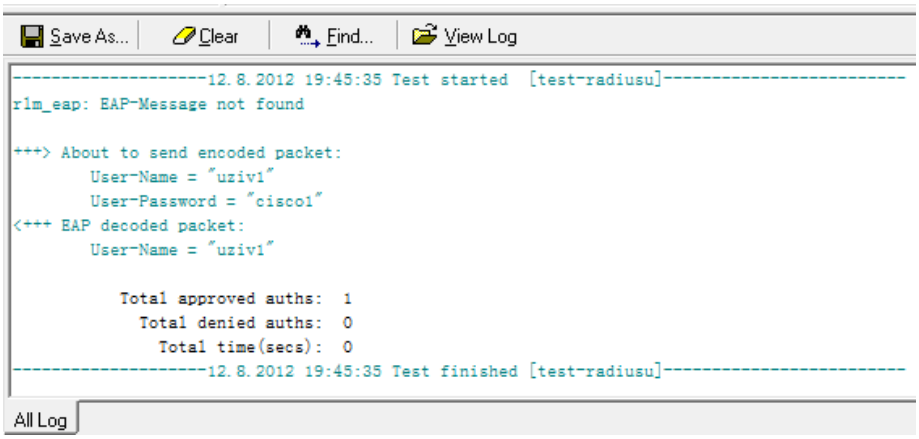
Nastavení klientů v TekRADIUS LT



Nastavení paketů v RadTestu



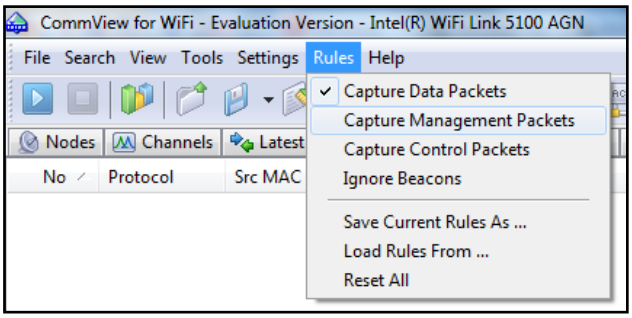
Ověření připojení klienta v RadTestu



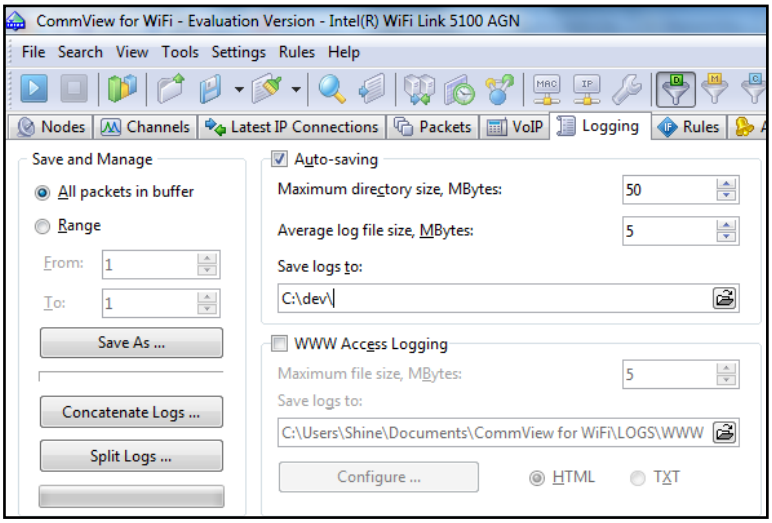
Příloha L – Řešení laboratorní úlohy číslo 5

Na následujících obrázcích je zobrazeno nastavení programu CommView for Wi-Fi.

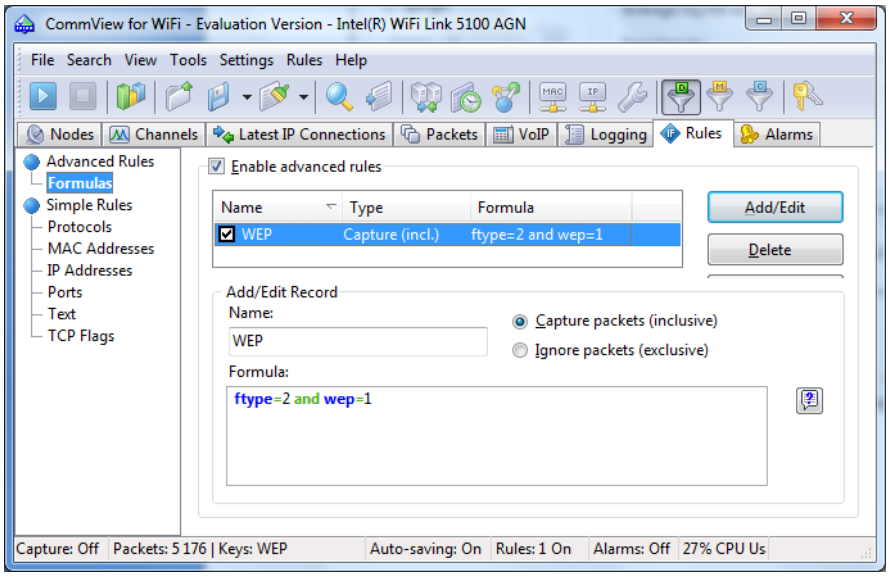
Nastavení zachytávání datových paketů.



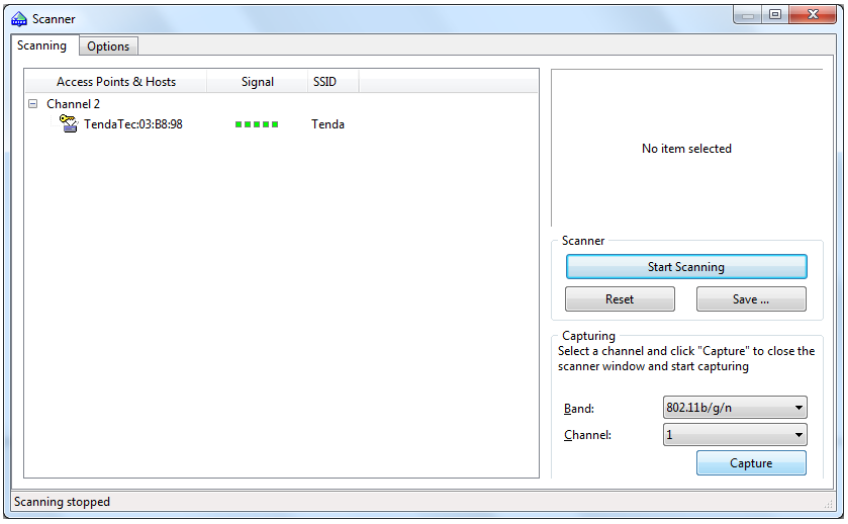
Nastavení logování.



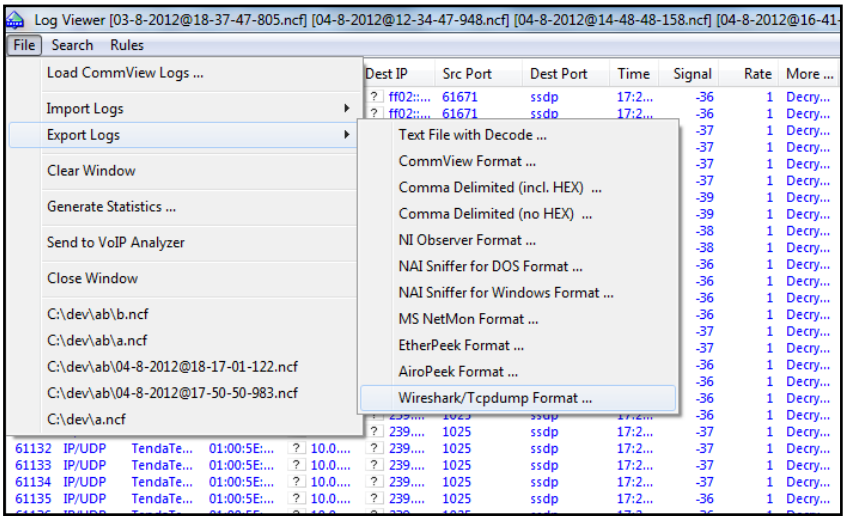
Nastavení pokročilých pravidel zachytávání.



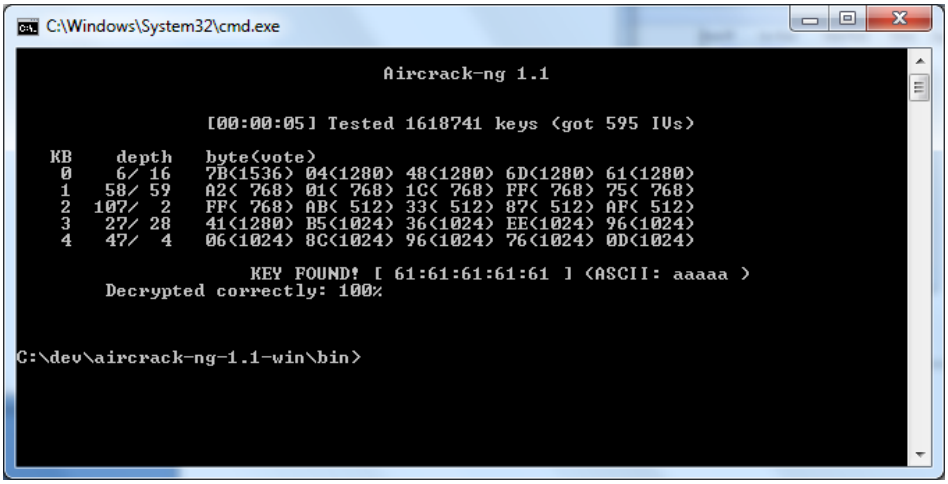
Po stisknutí CTRL+S a vyhledání sítě následné spuštění zachytávání paketů.



Po zachycení dostačeného množství paketů stiskněte CTRL+L. V oknu otevřete soubory s logy. Pakety vyexportujte ve formátu Wireshark.



Vyobrazení nalezení WEP klíče k této síti.



V následujících odpovědích jsou hvězdičkou (*) označeny ty, které se budou při každém jiném pokusu o prolomení hesla lišit.

Odpovědi na otázky:

Jaký režim (jaký mód) ze standardů 802.11 jste pro síť zvolili?

**802.11 b/g/n mixed mode*

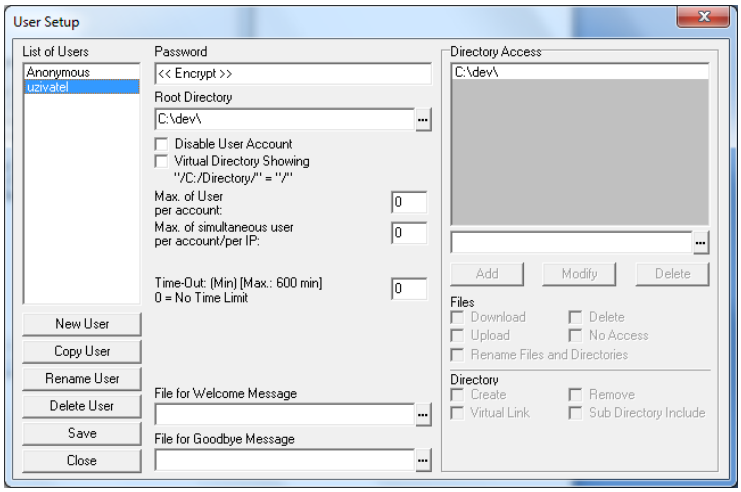
Kolik paketů jste potřebovali pro získání hesla?

**61154*

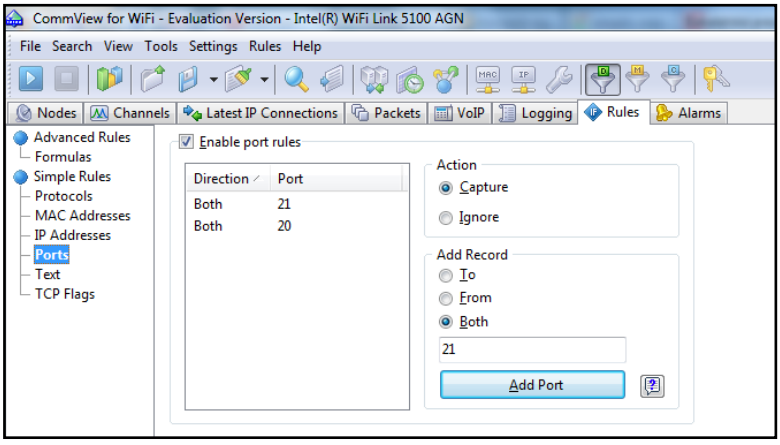
Kolik inicializačních vektorů (IV) bylo pro dešifrování hesla potřeba?
**595*

Příloha M – Řešení laboratorní úlohy číslo 6

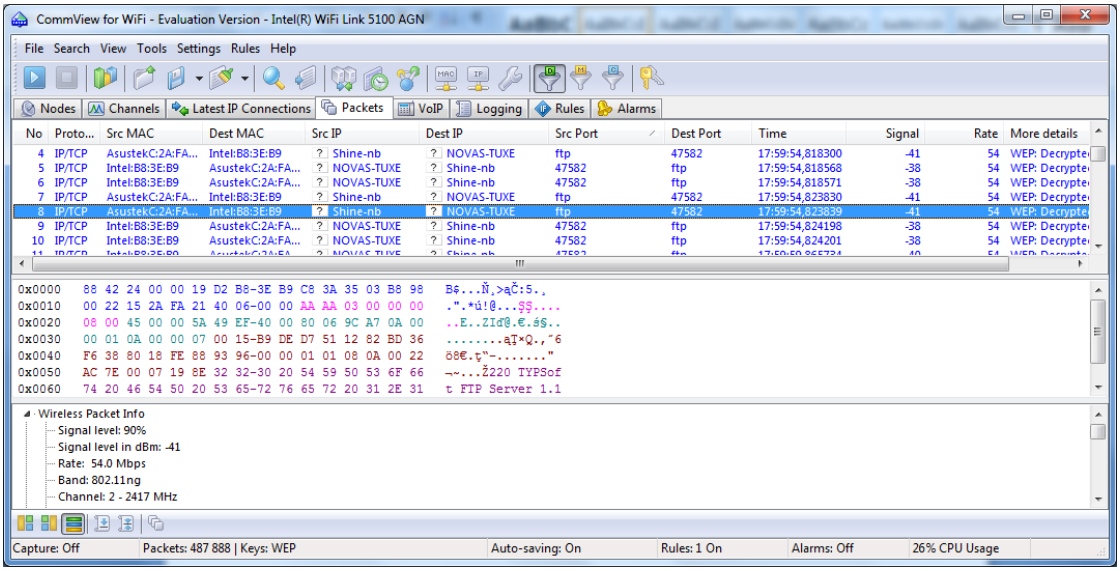
Jedno z mnohých nastavení TYPSoft FTP Server.



Nastavení programu CommView.

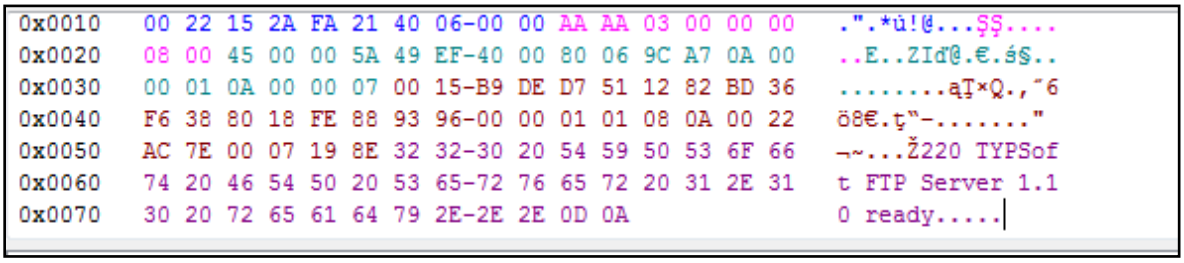


Vyobrazení zachycených paketů.

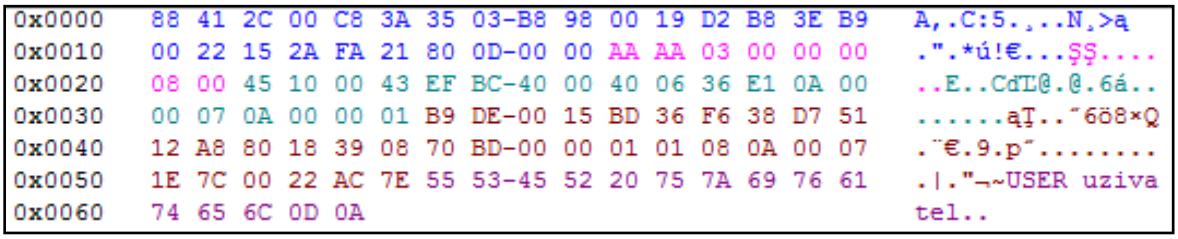


Odpovědi na otázky:

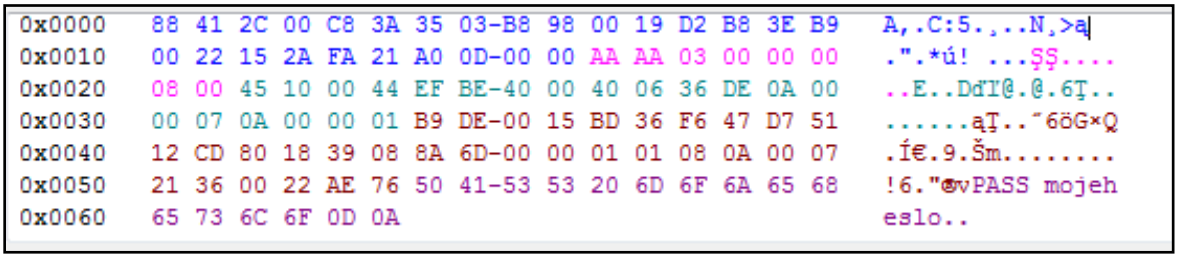
Některé z možných příkazů a zpráv jsou „TYPSoft FTP Server 1.1 ready.“, „User uzivatel“, „PASS mojeheslo“, „MKD adresar“, popř. „Quit“ nebo „Good bye“.



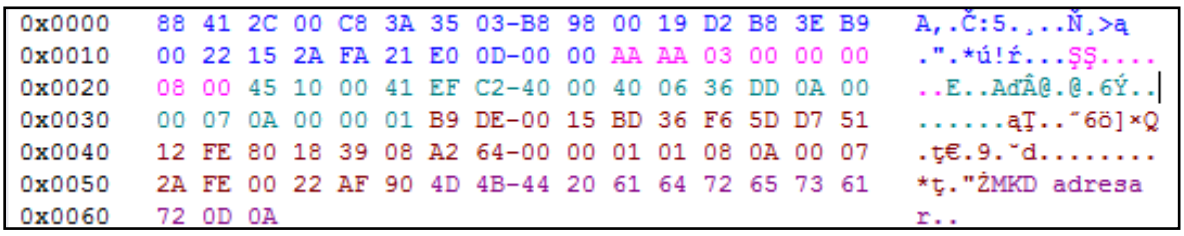
Vypište příkaz, kterým posílá klient serveru uživatelské jméno.



Jak v paketu vypadá příkaz posílající serveru heslo?

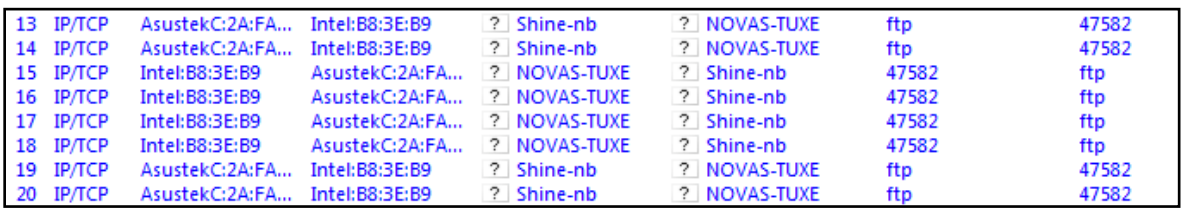


Paket, který vytvářel adresář se jménem „adresar“.



Z jakého uživatelského portu posílá klient serveru data?

**V tomto případě 47582. S každou relací se číslo uživatelského portu mění.*



Příloha N – Řešení laboratorní úlohy číslo 7

Otázky k dané úloze

1) Jaké režimy a bezpečnostní protokoly jste pro Vaše sítě zvolili?

   - WLAN síť 1 *802.11g s WPA2-Personal*
   - WLAN síť 2 *802.11n s WPA2-Personal*

2) Vypište celkové statistiky příkazu ping, zavolaného z klienta **první** WLAN a směrovaného na jeho Wi-Fi router, který pracoval na **kanálu 6**.

   Pakety: odeslané: *220*, přijaté: *220*, ztracené: *0* (ztráta *0* %)

   Přibližná doba do přijetí odezvy v milisekundách.
   Minimum = *2* ms, maximum = *39* ms, průměr = *3* ms

3) Vypište celkové statistiky příkazu ping, zavolaného z klienta **druhé** WLAN a směrovaného na jeho Wi-Fi router, který pracoval na **kanálu 6**.

   Pakety: odeslané: *198*, přijaté: *191*, ztracené: *7* (ztráta *3* %)

   Přibližná doba do přijetí odezvy v milisekundách.
   Minimum = *3* ms, maximum = *1005* ms, průměr = *42* ms

4) Vypište celkové statistiky příkazu ping, zavolaného z klienta **první** WLAN a směrovaného na jeho Wi-Fi router, který pracoval na **kanálu 1**.

   Pakety: odeslané: *198*, přijaté: *198*, ztracené *0* (ztráta *0* %)

   Přibližná doba do přijetí odezvy v milisekundách.
   Minimum = *2* ms, maximum = *43* ms, průměr = *5* ms

5) Vypište celkové statistiky příkazu ping, zavolaného z klienta **druhé** WLAN a směrovaného na jeho Wi-Fi router, který pracoval na **kanálu 6** (případně **11**).

Pakety: odeslané: _192_, přijaté: _191_, ztracené__1__ (ztráta _0_ %)

Přibližná doba do přijetí odezvy v milisekundách.
Minimum = __4__ ms, maximum = _110_ ms, průměr = __11_ms

6) Porovnejte Vámi naměřené výsledky a odhadněte, proč některé spoje vykazovaly ztráty a vyšší přenosové rychlosti, než ostatní.

Komunikace klienta a Wi-Fi routeru, kteří jsou blízko u sebe (případ WLAN 1), není tolik ovlivněna ani provozem ostatních zařízení, ani četnými překážkami. Pro druhou síť platí přesný opak.

7) Kolik různých BSA a ESA obsahují tyto sítě? Vypište i kteří klienti se ke které přidružují.

Každý přístupový bod poskytuje jednu BSA. Tudíž síť postavená dle schematického obrázku obsahuje 2 BSA. Na BSA Wi-Fi routeru č. 1 se napojují dva klienti, na BSA č. 2 pouze jeden.

Jelikož přístupové body nejsou mezi sebou propojeny, pro síť platí BSA=ESA. Tzn síť obsahuje 2 ESA, kde na první působí dva klienti a na druhé pouze jeden.