# Datová Bezpečnost bezdrátové komunikace v rámci vnitřních podnikových sítí

Date security wirelles communication in terms of inside copany network

Miroslav Píša

Bakalářská práce
2008

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav aplikované informatiky
akademický rok: 2007/2008

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Miroslav PÍŠA** |
| Studijní program: | **B 3902 Inženýrská informatika** |
| Studijní obor: | **Informační technologie** |
| Téma práce: | **Datová bezpečnost bezdrátové komunikace v rámci vnitřních podnikových sítí** |

Zásady pro vypracování:

1. **Analyzujte informační zdroje vhodné pro řešení problematiky bezdrátové komunikace a vnitřních sítí.**
2. **Stanovte metody bezpečné komunikace a porovnejte je.**
3. **Zvolte vhodnou metodu a proveďte její implementaci.**
4. **Vyhodnoťte pozitiva a negativa zvolené implemetace.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:


1. **BARKEN,Lee. Wi-Fi : Jak zabezpečit bezdrátovou síť. 1. vyd. Brno : Computer Press, 2004. ISBN 80-251-0346-3.**
2. **PUŽMANOVÁ, Rita . Bezpečnost bezdrátové komunikace : jak zabezpečit Wi-Fi,Bluetooth, GPRS, či 3G. 1. vyd. Brno : ComputerPress, 2005. ISBN 80-251-0791-4.**
3. **ZANDL, Patrick. Bezdrátové sítě Wi-Fi -- Praktický průvodce. 1. vyd. Brno : ComputerPress, 2003. ISBN 80-722-6632-2.**
4. **KÖHRE, Thomas . Stavíme si bezdrátovou síť Wi-Fi, 1. vyd. Brno : ComputerPress, 2004. ISBN 80-251-0391-9.**
5. **SVĚT SÍTÍ [online] dostupný z WWW: [http://www.svetsiti.cz]**
6. **SECURITY-PORTAL.CZ [online] dostupný z WWW: [http://www.security-portal.cz]**


Vedoucí bakalářské práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a statistiky

Datum zadání bakalářské práce: **20. února 2008**

Termín odevzdání bakalářské práce: **5. května 2008**

Ve Zlíně dne 20. února 2008

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
*děkan*

doc. Ing. Ivan Zelinka, Ph.D.
*ředitel ústavu*

## ABSTRAKT

Práce řeší informační a datovou bezpečnost uvnitř firemní sítě z pohledu bezdrátové komunikace. První, teoretická část, krátce seznámí čtenáře se základy bezdrátových počítačových sítí. Dále se věnuje aktuálním bezpečnostním rizikům a typům útoků na bezdrátovou síť. Jako poslední jsou podrobně popsány jednotlivé způsoby zabezpečení bezdrátové sítě. V druhé, praktické části, je uvedeno srovnání jednotlivých bezpečnostních metod, praktická doporučení pro zabezpečení bezdrátové sítě a metody, kterými lze dosáhnout bezpečné firemní sítě. V závěru práce je uvedena praktická implementace.


Klíčová slova: bezdrátová síť, zabezpečení, přístupový bod, autentizace, WEP,WPA, AES, SSID


## ABSTRACT

This study deal with informational and data safeguard within the company´s network on the part of wireless communication. First, the theoretical part of this study shortly appryses the basics of the wireless networks to the readers. Next it applys oneself to actual safety risks and describes kinds of attacks on the wireless network. Last this study describes each method of safeguard of the wireless networks in detail. In the second, practical part of this study is introduced comparison of these methods of safeguard, then practical references to protection the wireless networks and methods which are able to achieve the secure of company´s network. In the final section of this study is introduced the practical implementation.


Keywords: wireless network, security, access point, authetication, WEP,WPA, AES, SSID

# PODĚKOVÁNÍ

Chtěl bych poděkovat mému vedoucímu, panu Doc.Mgr. Romanu Jaškovi, Ph.D., za cenné rady a připomínky při vypracovávání této bakalářské práce. Rád bych také poděkoval rodičům a přátelům, kteří mě podporovali při psaní této práce a při celém mém studiu.


Prohlašuji, že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně 9.5.2008

…….
Podpis diplomanta

# OBSAH

# ÚVOD

Převážná většina firem dnes využívá výhod, které jim výpočetní technika nabízí a elektronická komunikace se stala samozřejmostí. V každé větší firmě dnes již mají počítačovou sít připojenou k světové síti internet. Firemní síť slouží k přenosu dat, hlasu, obrazu. Dá se říct že bez výpočetní techniky a firemní sítě by žádná větší firma neměla šanci existovat a konkurovat ostatním.

Od dob realizace prvních firemních počítačových sítí již uplynul nějaký čas. První sítě byly realizovány pomocí koaxiálního kabelu, pak přišla na řadu kroucená dvojlinka a v posledních letech dochází k značnému rozvoji sítí bezdrátových. Ty sesebou přinesly větší míru pohodlí pro uživatele a také osvobození od kabelu a síťové zásuvky. Z pohledu síťového administrátora však představují starost navíc.

Spolu s pohodlím a mobilitou, které bezdrátová síť představují, představují i veliké riziko z pohledu zabezpečení přenášených dat. Data, která putují takovou sítí nám doslova „létají pod nosem“ a může je zachytit každý, kdo bude v dosahu signálu a kdo k tomu bude mít příslušné vybavení. Bezpečnost interních firemních dat bývá při budování počítačové sítě prioritou číslo jedna a protože dlouhou dobu neexistoval opravdu spolehlivý způsob zabezpečení pro bezdrátovou síť, pronikly bezdrátové sítě do firemní sféry mnohem později než například do soukromé, kde nejsou bezpečnostní požadavky až takové. I při velkém rozmachu, stále převážná většina firem dává z bezpečnostních důvodů přednost metalickým rozvodům před bezdrátovou sítí..

V první, teoretické části, bych chtěl seznámit čtenáře s tím co je to bezdrátová síť, jaká sebou přináší rizika a jak se dá zabezpečit.

První kapitola se věnuje bezdrátovým sítím obecně, specifikaci 802.11, frekvenčním pásmům na kterých se lokální bezdrátové sítě realizují, jednotlivým komponentám bezdrátových sítí a topologiím.

Druhá kapitola se věnuje bezpečnostním rizikům bezdrátových sítí, způsobům jak mohou být napadeny a nástrojům které jsou k takovýmto útokům využívány.

Poslední kapitolu teoretické části pojednává o jednotlivých zabezpečovacích mechanizmech bezdrátových sítí.

V druhé, praktické, části práce se nachází srovnání jednotlivých bezpečnostních standardů. Dále jsem uvedl doporučení, jak zabezpečit bezdrátové sítě z pohledů různého stupně bezpečnostního rizika, a metody, kterými lze dosáhnout bezpečné firemní sítě. Jako poslední jsem provedl praktickou implementaci bezpečnostního standardu na přístupový bod a nastavil jsem klienta, kterého jsem k tomuto přístupovému bodu připojil.

# I. TEORETICKÁ ČÁST

# 1 BEZDRÁTOVÁ SÍŤ, WI-FI

Bezdrátové sítě se velice rychle ujaly nejprve pro hlasovou komunikaci, jako doplněk a postupně i náhrada pevných telefonních přípojek. Mobilní (digitální) sítě (GSM/GPRS/EDGE a 3G) se staly nedílnou součástí života každého z nás, takže dnes si většina uživatelů už svůj soukromý ani pracovní život bez mobilního telefonu nedokáže představit.

Komfort volání „bez drátů“ se zalíbilo také počítačové veřejnosti a začaly se pilně vyvíjet specifikace primárně datových bezdrátových sítí, které by nahradily pevné sítě nejprve v lokálním měřítku. Tak vznikly bezdrátové lokální sítě, WLAN, s jejichž dnes nejpopulárnějším typem: Wi-Fi (IEEE 802.11b). WLAN byly ve svém počátku principiálně naprosto odlišné od mobilních sítí a nespolupracovaly s nimi. WLAN byly určeny pro datovou komunikaci, mobilní sítě pro hlasovou komunikaci. Ač v obou případech bezdrátové sítě, WLAN omezovaly pohyb uživatele v rámci dosahu přístupového bodu, zatímco mobilní sítě podporovaly plnou mobilitu uživatele.

S rostoucí zálibou v bezdrátových zařízeních, mobilních telefonech, PDA, laptopech a jejich funkcích, se také rozvíjela podpora jejich vzájemné komunikace např. pro synchronizaci dat, adresářů apod. Taková komunikace se týká především zařízení daného uživatelem, takže se začaly vyvíjet specifikace pro osobní bezdrátovou komunikaci a jako první se objevil Bluetooth. Původně průmyslovou specifikaci nakonec převzal mezinárodní institut IEEE a rozpracoval ještě několik dalších projektů bezdrátových osobních sítí (WPAN, 802.15). [2]

Bezdrátové sítě jsou pro firmy i domácí uživatele neuvěřitelně atraktivní, protože poskytují značnou míru pružnosti a svobody, která vyplývá ze ztráty závislosti na fyzické kabeláži. Fyzické připojení je klaustrofobií. Bezdrátová technologie vám nabízí sobodu přesouvat se podle chuti. A co se stane, pokud budete chtít přestěhovat počítač z jednoho stolu na jiný? Ve světě metalických kabelů musíte stěhovat nejenom počítač , ale i jeho síťové připojení. A co když na novém místě ethernetová zásuvka není? Budete muset najit volný port v přepínači a skrz stěny tahat kabely.Bezdrátové prostředí otevírá nové možnosti a příležitosti.Nemusíte se o nic starat, pokud přenesete počítač z jedné místnosti do druhé, nemusíte se zabývat tím, kde jsou a nejsou volné ethernetové porty. Bezdrátové lokální sítě dnes nabízejí kavárny, hotely, letiště a další místa, kde mohou návštěvníci použít své přenosné počítače či PDA, přečíst si poštu či surfovat na internetu.[1]

WiFi (Wireless Fidelity) je bezdrátová, síť určená primárně k náhradě kabelového ethernetu v bezlicenčním pásmu, které je dostupné prakticky v celém civilizovaném světě. Hlavní výhodou této technologie je její nízká cena, způsobená mimo jiné tím, že certifikovaná zařízení jsou k dispozici ve velkých sériích. Protože požadavky na certifikaci zařízení jsou běžně dostupné a norma 802.11b dokonce volně k dispozici na webu, existují řádově desítky (možná již stovky) různých výrobců, počínaje NoName přidružená výroba věznice v Šen Čou a konče velkými korporacemi typu CISCO Systems, 3Com nebo Microsoft.

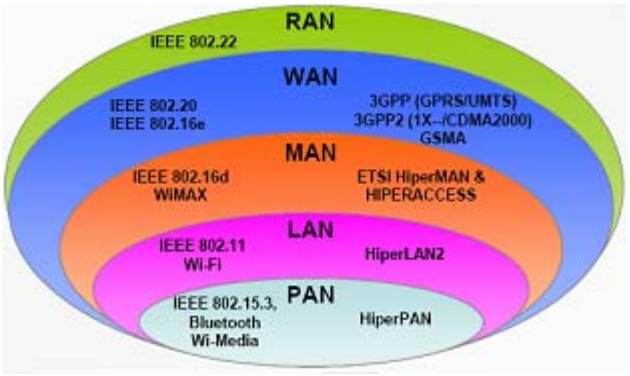
Cena a možnosti jednotlivých krabic na trhu se přirozeně velmi liší, nicméně jejich interoperabilita je zabezpečena právě logem WiFi. [5]

## 1.1 Standard IEEE 802

IEEE (The Institute of Electrical and Electronics Engineers) je největší profesní a standardizační organizace na světě, založená roku 1884, jejíž aktivity mimo pořádání konferencí a vydávání odborných časopisů zahrnují přípravu a vydávání komunikačních a síťových standardů.[7] IEEE sdružuje přes 350 000 elektroinženýrů a informatiků v cca 150 zemích ve všech světadílech. IEEE vydává více než 100 titulů odborných periodik a řadu knih (25% světové produkce odborné literatury v elektrotechnice a informatice pochází z IEEE), pořádá konference a všemožně podporuje rozvoj oboru.[6]

IEEE 802, standardizační výbor zabývající se problematikou lokálních sítí byl vytvořen v roce 1980 a je tvořen několika podvýbory. Bezdrátovou komunikací se zabývají :

- **IEEE 802.11** : Bezdrátové lokální sítě (WLAN, Wireless Local Area Network)
- **IEEE 802.15** : Bezdrátové osobní sítě (WPAN, Wireless Personál Area Network,)
- **IEEE 802.16** : Bezdrátové městské sítě (WMAN, Wireless Metropolitan Area Networks)
- **IEEE 802.20** : Širokopásmový mobilní přístup (MBWA, Mobile Broadband Wireless Access, 2002)
- **IEEE 802.22** : Oblastní bezdrátové sítě (WRAN, Wireless Regional Area Network)




*Obr. 1. Bezdrátové standardy [9]*

### 1.1.1 IEEE 802.11

Standard IEEE 802.11 byl schválen v roce 1997 jako první světový bezdrátový standard pro lokální sítě. Skupina která se zabývala jeho vývojem byla založena už roku 1990. Původní specifikace definovala síť v pásmu 2,4 GHz s rychlostmi přenosu 1 a 2 Mbit/s, brzy se však stala nedostačující a tak bylo v rámci tohoto standardu vytvořeno několik podskupin, které tento standard doplňují nebo rozšiřují. Jejich vytváření pokračuje dodnes.

- **802.11a** : Bezdrátové sítě pracující na frekvenci 5 GHz, což má za následek zlepšení ze strany interferencí, ovšem slabinou je zpětná kompatibilita se sítěmi 802.11 b a 802.11g. Oproti 802.11b a g má povolen větší vyzařovací výkon, lze jej tudíž použít na větší vzdálenosti. Rychlost přenosu se pohybuje kolem 20 Mbit/s (1999).
- **802.11b** : Tuto specifikaci dnes používá většina Wi-Fi zařízení. Definuje bezdrátové sítě pracující na frekvenci 2,4 GHz s teoretickou přenosovou rychlostí až 11 Mbit/s. Tento podstandard je nejvíce spojován se skratkou Wi-Fi (1999).
- **802.11c** : Definuje práci síťových mostů v bezdrátových sítích. V podstatě jde o doplněk standardu 802.1D (2003).
- **802.11d** : tzv. „*Globální harmonizační standard*“, Definuje požadavky na fyzickou vrstvu k uspokojení regulačních domén nepokrytých existujícími standardy. Liší se v povolených frekvencích, vyzařovacích výkonech a propustnosti signálu. Specifikace eliminuje nutnost vývoje a výroby specifických produktů pro různé země (2001).[10]

- **802.11e** : Doplňuje podporu pro kvalitu služeb (*Quality of Service*, QoS) pro zajištění přenosu hovorového signálu, obrazu apod. IEEE 802.11e doplňuje sítě definované IEEE 802.11a/b/g. Doplněk navíc zajišťuje zpětnou kompatibilitu se zařízeními, které nejsou podporou pro QoS vybaveny (2003). [11]
- **802.11f** : Doplněk IEEE 802.11F vylepšuje mechanismus předávání stanic (*Roaming*) při přechodu mezi dvěma rádiovými kanály nebo z jedné sítě do sousední s připojením k jinému přístupovému bodu. Protokol IAPP (*Inter-Access Point Protocol*) umožňuje spolupráci přístupových bodů od různých výrobců. (2003). [11]
- **802.11g** : Jde o obdobu 802.11a, ovšem je specifikován pro sítě pracující v pásmu 2.4GHz. Maximální přenosová rychlost je zvýšena až na 54Mbit/s. Zajišťuje zpětnou kompatibilitu se standardem 802.11b (2003).
- **802.11h** : Standard rozšiřuje 802.11a o evropské podmínky pro použití bezdrátových sítí v pásmu 5GHz mimo budovy. Zavádí dynamický výběr kanálu (*Dynamic Channel Selection*) a řízení vysílacího výkonu (*Transmit Power Control*) (2003).
- **802.11i** : zlepšuje zabezpečení bezdrátových sítí 802.11 použitím AES (*Advanced Encryption Standard*) šifrování namísto WEPu. Produkty certifikované pro tento standard budou označeny WPA (Wi-Fi Protected Access) (2004).
- **802.11j** : Doplněk pro použití pásma 4,9 – 5 GHz pro multimediální služby v bezdrátových sítích. Používá se zatím pouze v Japonsku (2004).
- **802.11x** : Neformální obecné označení kteréhokoli z doplňujících standardů 802.11
- **802.11X** : Bezpečnostní standard bezdrátových i metalických sítí založený na autentifikaci a filtrování portů při přístupu k síti. Běžně nesprávně označován jako 802.11x.

**Doposud neschválené standardy :**

- **802.11k** : Doplněk pro zefektivnění využití přenosového média na základě měření kvality jednotlivých kanálů, šumu, zahlcení a vzájemného rušení. Na základě těchto informací dojde k optimalizaci nastavení klientů a ke konfiguraci sítě tak, aby se dospělo k co největší kvalitě spoje.[11]

- **802.11.l** : Rezervováno a nebude použito.
- **802.11m** : Kontrola dokumentů vydaných ostatními skupinami a oprava případných nesrovnalostí a chyb v původních specifikacích.
- **802.11n** : Skupina IEEE 802.11n studuje různé možnosti nastavení parametrů fyzické vrstvy a MAC podvrstvy pro zvýšení datové propustnosti. Mezi tyto možnosti patří použití více antén, změny kódovacích schémat a změny MAC protokolů. Aktuální cíl skupiny je přenosová rychlost minimálně 100 Mbit/s nad MAC vrstvou. Navíc má IEEE 802.11n zajistit vyšší dosah se zachováním co největší rychlosti a zvětšit odolnost proti rušení.[11]
- **802.11o** : Rezervováno a nebude použito.
- **802.11p** : Podpora připojení stanic umístěných v pohyblivých prostředích (auta,vlaky…) k pevným přístupovým bodům.
- **802.11q** : Rezervováno a nebude použito.
- **802.11r** : Specifikace pro rychlé přesuny uživatelů mezi přístupovými body (*Roaming*)
- **802.11s** : Standard pro samoorganizující se bezdrátové mesh sítě. Používá tzv. „Multi-hopping“, každý klient je zároveň i přístupovým bodem a naopak.
- **802.11u** : Doplněk organizující spoluprácí se sítěmi mimo standardy 802.
- **802**.**11v** : Vytváří jednotné rozhraní pro management zařízení v bezdrátové síti. Stanice budou moci provádět funkce managementu zahrnující monitoring a konfiguraci buď centralizovaně, nebo distribuovaně prostřednictvím mechanismu na druhé vrstvě.[11]
- **802.11w** : Rozšíření stávající MAC vrstvy o mechanismy na podporu integrity dat, autenticity zdroje dat, utajení dat a ochrany před útoky typu replay pro vybrané rámce určené pro management. Cílem je zvýšení zabezpečení rámců pro management.[11]

## 1.2 Frekvenční pásma bezdrátových sítí 802.11

Na rozdíl od řady jiných bezdrátových standardů běží 802.11 na „volné“ části rádiového spektra. To znamená, že pro vysílání a komunikaci není potřeba žádná licence. Volnými částmi rádiového spektra, které využívá 802.11 (a Wi-Fi), jsou pásma 2,4GHz a 5 GHz. Tato volná spektra využívá také mnoho domácích zařízení, jako například mikrovlnné trouby a bezdrátové domácí telefony. [12]

V různých zemích světa se však využívá různý frekvenční rozsah. V některých státech jako např. USA je zakázáno používat určité části frekvenčního spektra z důvodu rušení jiných zařízení pracujících na těchto frekvencích. Česká republika se však drží evropské konvence ETSI která dává k dispozici plné frekvenční spektrum.

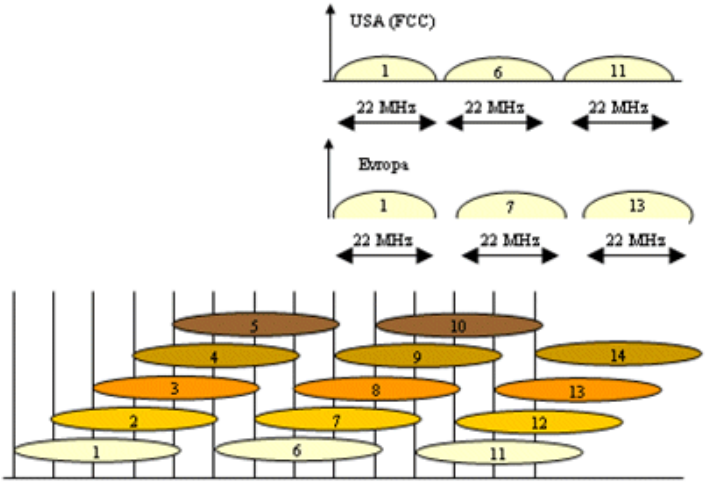
### 1.2.1 Frekvenční pásmo 2,4 GHz

Bezdrátové sítě 802.11b/g pracují v pásmu 2,4 GHz, což ovšem znamená frekvenční rozsah 2,4 GHz až 2,4835 GHz, tedy pásmo široké 83,5 MHz. Jelikož technologie 802.11b potřebuje ke své činnosti kanál o šířce 22MHz, bez překrývání by se do tohoto rozsahu vešly pouze 3 kanály. V praxi se však používá 14 částečně se překrývajících kanálů. Mezi jednotlivými kanály je odstup 5MHz, přenos na 2 sousedních kanálech je tedy možný, nedosahuje však takových kvalit jako v případě 2 nepřekrývajících se kanálů. V praxi, pokud je to tedy možné, je lepší při budování sítě zvolit kanál, který se co nejméně překrývá se sousedními sítěmi. Následující tabulka (Tab. 1) zobrazuje jednotlivé kanály a jejich použití ve světě.

*Tab. 1. Frekvenční rozsahy kanálů a jejich využití v různých zemích*

| Kanál | Frekvence [GHz] | USA,Kanada | Evropa | Japonsko |
|---|---|---|---|---|
| 1 | 2401-2423 | x | x | x |
| 2 | 2406-2428 | x | x | x |
| 3 | 2411-2433 | x | x | x |
| 4 | 2416-2438 | x | x | x |
| 5 | 2421-2443 | x | x | x |
| 6 | 2426-2448 | x | x | x |
| 7 | 2431-2453 | x | x | x |
| 8 | 2436-2458 | x | x | x |
| 9 | 2441-2463 | x | x | x |
| 10 | 2446-2468 | x | x | x |
| 11 | 2451-2473 | x | x | x |
| 12 | 2456-2478 | --- | x | x |
| 13 | 2461-2483 | --- | x | x |
| 14 | 2466-2488 | --- | | x |

Evropské státy, kromě Francie (10 a 11 kanál) a Španělska (10-13 kanál), se drží konvence ETSI, která dovoluje používat plné frekvenční spektrum. V ČR , a ve většině ostatních Evropských zemí, je povoleno vybrat pro provoz bezdrátových sítí 3 vzájemně se nepřekrývající kanály, tedy na kanálech 1, 7 a 13. V USA je situace obdobná, ovšem tam se jedná o kanály 1, 6 a 11. Z následujícího obrázku (Obr. 2) je patrné že v USA jsou mezi sousedními kanály mnohem menší odstupy.



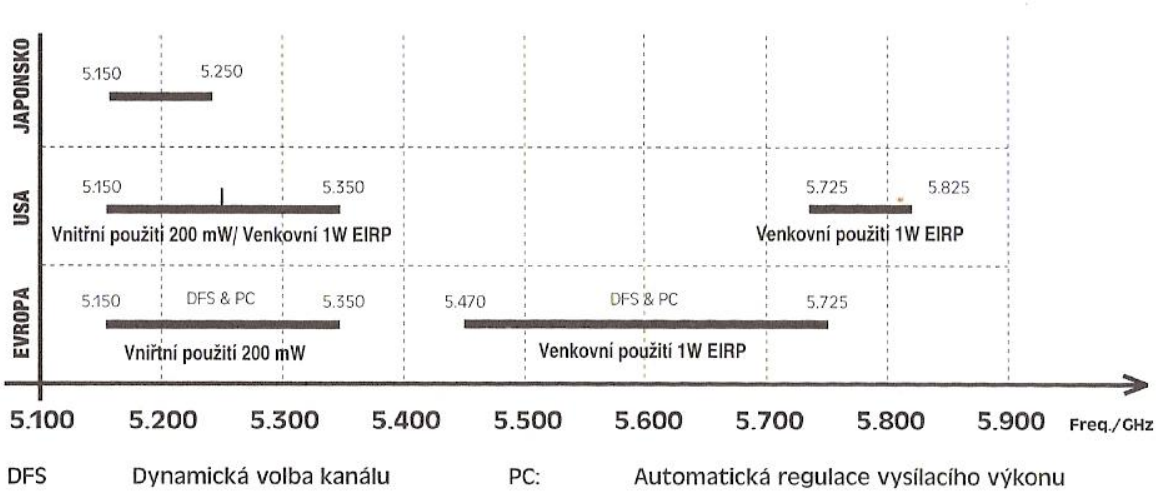

*Obr. 2. Frekvenční kanály v pásmu 2,4 GHz [13]*

### 1.2.2 Frekvenční pásmo 5 GHz

Frekvenční pásmo 5 GHz je podstatně širší než 2,4 GHz, zatím však nedošlo ke shodě při jeho uvolňování a využití mezi americkou organizací FCC a evropským regulačním orgánem EU. Původní návrhy na standard 802.11a totiž nebraly v úvahu fakt, že v jiných zemích než je USA se pásmo 5GHz využívá pro jiné účely. Standard 802.11a dělí spektrum podle výstupního výkonu na 3 rozsahy :

- **5,150-5,250 GHz** : 4 kanály s max. vysílacím výkonem 40mW
- **5,250-5,350 GHz** : 4 kanály s max. vysílacím výkonem 200mW
- **5,47 - 5,725 GHz** : 4 kanály s max. vysílacím výkonem 800mW

Rozdíly ve využití jednotlivých kanálů mezi Evropou, USA a Japonskem jsou vidět na následujícím obrázku (Obr. 3).




*Obr. 3. Využití pásma 5 GHz ve světě [3]*

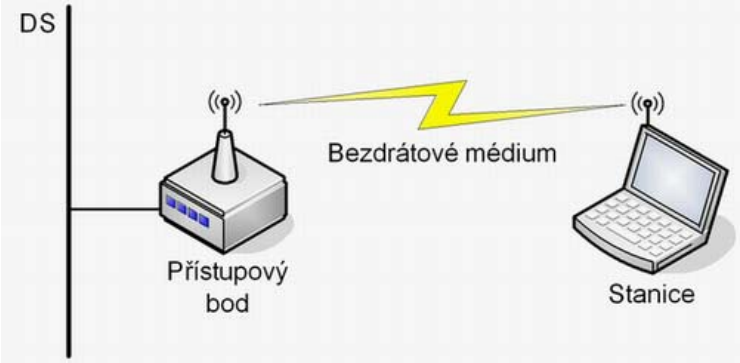
## 1.3 Komponenty sítě

Každá ze sítí 802.11 obsahuje čtyři hlavní druhy fyzických komponent :

- Distribuční systém
- Přístupový bod (access point)

- Bezdrátové médium
- Stanice

V praxi lze tyto čtyři komponenty shrnout do dvou nebo tří, protože bezdrátové médium je funkcionalitou využívanou stanicí i přístupovým bodem a distribuční systém (kabelová síť) není potřeba v případě, když od bezdrátové sítě neočekáváme propojení do jiné sítě a má sloužit pouze k zajištění komunikace mezi bezdrátově připojenými stanicemi. [3]




*Obr. 4. Komponenty sítě 802.11*

### 1.3.1 Distribuční systém

Distribuční systém je logickou komponentou bezdrátové sítě. Jakmile je síť tvořena více přístupovými body, je třeba zajistit jejich vzájemnou komunikaci pomocí distribučního systému. Standard 802.11 přímo nespecifikuje, jak má být distribuční systém realizován, určuje pouze jaké má poskytovat funkce.

V naprosté většině komerčních systémů je distribuční systém řešen jako kombinace síťového mostu a distribučního média, jímž je páteřní síť používaná pro přenášení dat mezi přístupovými body. [3]

### 1.3.2 Přístupový bod

Jde o přemostění mezi kabelovou a bezdrátovou sítí a ačkoli poskytuje i celou řadu dalších funkcí, funkce mostu mezi bezdrátovou a kabelovou částí je nejdůležitější. [3]

### 1.3.3 Bezdrátové médium

Bezdrátové médium je pro sítě WLAN tímtéž, co kabeláž pro sítě kabelové. Bezdrátové médium je nosičem dat při přesunu dat od stanice ke stanici. Mohli bychom říci, že tím

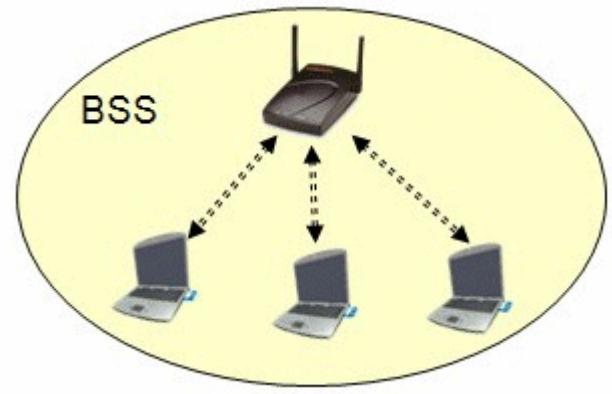
médiem je vzduch, což je ovšem nesmysl (ostatně sítě WLAN fungují i ve vzduchoprázdnu). Bezdrátovým médiem rozumí 802.11 dvě radiové frekvence (2,4 a 5 GHz) a málo využívanou infračervenou fyzickou vrstvu.

### 1.3.4 Stanice

Stanicí se v bezdrátové síti rozumí jakékoli zařízení které se dokáže do sítě připojit, Notebook, PDA, počítač. Podmínkou není ani mobilita připojeného zařízení. Příkladem mohou být firemní bezdrátové sítě tam, kde není možnost instalace síťové kabeláže. V takových případech se nemusí řešit, zda se uživatel do sítě připojuje s notebookem, nebo stolním počítačem, který nikam nepřenáší.

## 1.4 Architektura WLAN

Základní stavební blok 802.11 sítě označujeme jako Basic Service Set (BSS), tedy základní soubor služeb. Jde o skupinu stanic, které spolu komunikují. Tato společná komunikace probíhá v území vymezeném průnikem dosahu těchto stanic a takovéto území nazýváme Basic Service Area (BSA). [3]




*Obr. 5. Basic Service Set (BSS) [13]*

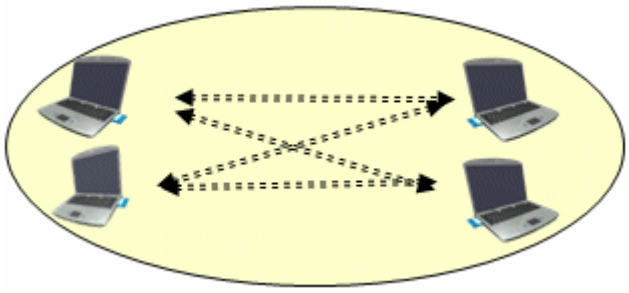
Bezdrátové sítě mohou pracovat ve dvou základních režimech. Je to buď režim IBSS (Independed Basic Service Set), též označovaný jako režim Ad-hoc. V tomto případě se klienti spojují přímo mezi sebou navzájem. Druhým režimem je BSS/ESS (Basic Service Set/Extended Service Set) neboli režim infrastruktury. V těchto sítích se využívá centrálních přístupových bodů (Access Point).

### 1.4.1 IBSS (Ad-hoc) režim

Sítě Ad-hoc se někdy rovněž nazývají nezávislé sítě, to z toho důvodu, že jednotlivé stanice v takové síti spolu komunikují přímo, podle potřeby, a tedy nezávisle na nějakém prostředníkovi. Z toho vyplývá, že pokud spolu stanice chtějí komunikovat, musí být ve vzájemném rádiovém dosahu. Pro menší síť s několika stanicemi vzdálenými pár metrů od sebe je to vhodné komunikační schéma, ale je zřejmé, že sítě s více počítači, nebo sítě v členitějších a rozlehlejších prostorách, kde princip vzájemného radiového dosahu nemůže být vždy zajištěn, takto realizovat nelze.

Nejčastější použití sítí Ad-hoc je propojení několika počítačů z nějakého specifického důvodu a na omezený čas – kupříkladu LAN party, nárazová výměna dat atd. [3]

Avšak bezpečnostní dopady tohoto uspořádání jsou samozřejmě zcela zásadní. Pro připojení do sítě Ad-hoc stačí znát použitý kanál a SSID. V tomto režimu sice lze použít i WEP, nicméně specifikace WPA už sítě IBSS neošetřuje a jejich zabezpečení tak bude řádně vyřešeno až s příchodem standardu 802.11i. [1]

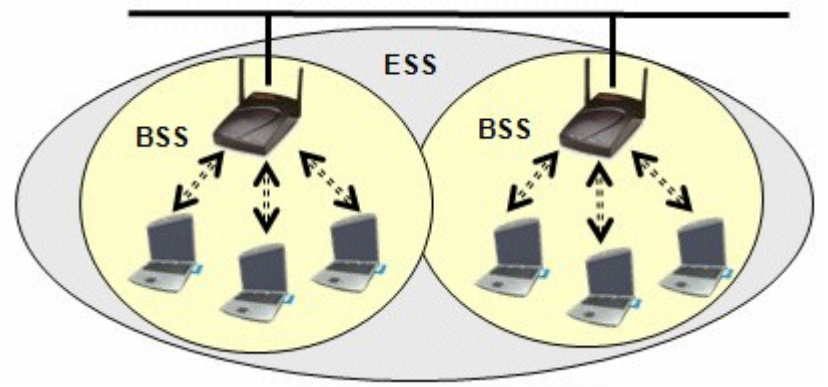


*Obr. 6. Síť v režimu IBSS (Ad-hoc) [13]*

### 1.4.2 BSS/ESS režim (sítě s infrastrukturou)

Jednoduše řečeno, BSS je prostě AP připojené k metalické infrastruktuře, například Ethernetu. Jednotlivé bezdrátové stanice se připojují k centrálnímu přístupovému bodu a veškerý provoz (dokonce i přímý provoz mezi klienty) se směřuje přes AP.

ESS (Extended Service Set) jsou dvě nebo více BSS, propojené nějakým distribučním systémem, například Ethernetem. BSS a ESS porovnává následující obrázek (Obr. 7.).




*Obr. 7. Wifi síť ESS složená z buněk BSS [13]*

V tomto režimu AP funguje jako most mezi metalickou a bezdrátovou sítí. V závislosti na typu a nastavení se může chovat skutečně jako „hloupý“ most na druhé síťové vrstvě, anebo může fungovat mnohem chytřeji jako směrovač, zajišťovat překlad adres (NAT), přidělování adres (DHCP) a další. Volba AP tedy v každém případě závisí na tom, jak plánujete infrastrukturu sítě.

V režimu infrastruktury je významným bezpečnostním rizikem neoprávněný přístup ke vzdálené správě AP. Útočník, který získá přístup ke správě zařízení, bude moci zobrazit/změnit klíče protokolů WEP/WAP, bude moci ovlivnit jiná nastavení, což může vést k porušení ochrany dat a k útokům DoS. [1]

# 2 SOUČASNÁ BEZPEČNOSTNÍ RIZIKA

Podobně jako většina ostatních přínosných technologií jsou i bezdrátové sítě zranitelné vůči různým hrozbám. Bezdrátové technologie se ovšem naštěstí dále vyvíjejí a dnes již máme řadu možností, jak tyto sítě zabezpečit. [14]

## 2.1 Bezdrátové „Válečné hry“

Jednou jeden londýnský autor, Ben Hammersley, něco nového psal a chtěl si dát v kavárně přes ulici šálek kávy a možná i něco zakousnout. Nainstaloval si tedy doma bezdrátový přístupový bod a měl přesně to, co chtěl. A jako dobrák od kosti dal vědět všem sousedům, kteří tak dostali bezdrátový přístup do Internetu. Této dobrosrdečnosti kupodivu nikdo nevyužil, do hry ale vstoupil jistý jeho známý, Matt Jones, který vymyslel a na webových stránkách vystavil několik nových „mezinárodních“ symbolů, z nichž by lidé poznali, že se někde poblíž nachází bezdrátový přístupový bod. Kouskem křídy načmáral tyto symboly na obrubník před kavárnou a jako první tak provedl „WarChalking“.

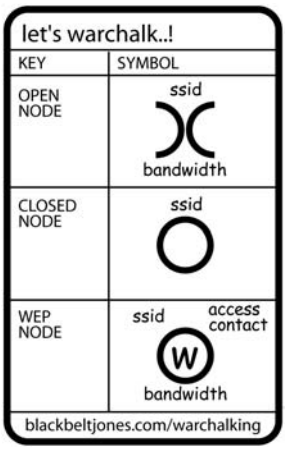
Krátce poté, co Matt zveřejnil tyto své symboly na Internetu, se informace rychle rozšířila a našedvojice dala vzniknout internetovému fenoménu, který s sebou nese zlověstné názvy jako WarChalking, WarSpying, WarSpamming a WarDriving. Všechno jsou to pojmy, kterými útočníci popisují své aktivity a jsou nedílnou součástí vývoje bezdrátového přístupu k sítím. [14]

Z právního hlediska ovšem nejsou tyto „War… činnosti“ nezákonným jednáním, a to jak v České republice, tak třeba i v USA, jedná-li se pouze o zjišťování volně dostupných informací o síti, aniž by síť byla jakkoli využita nebo v ní byly prováděny jakékoli další změny, kopírována data apod. Pokud ovšem dotyčná osoba vstoupí do sítě za účelem odcizení dat, služeb, zachycování komunikace, nebo zneužívání počítačových prostředků, může se jednat to trestný čin.

### 2.1.1 WarChalking

Tímto pojmem se označuje praxe, kdy si „hackeři“ vzájemně sdělují místa, v nichž se dá zadarmo připojit do podnikové či soukromé bezdrátové sítě. Symboly navíc označují, jestli je přístupový bod „otevřený“ nebo „uzavřený“, a jaké zabezpečení v něm funguje (Obr. 8).

Z pohledu bezpečnosti je krajně nepravděpodobné, že bychom opravdu viděli tento symbol někde na chodníku. Pokud ale není bezdrátová síť správně zabezpečená, má velkou šanci se objevit na vhodné internetové mapě a někdo ji dříve nebo později zneužije. [14]




*Obr. 8. Symboly pro WarChalking*

### 2.1.2 WarDriving

Metoda motorizovaného „válečného nájezdu“ WarDriving znamená pro hackera velmi snadné hledání otevřených bezdrátových sítí a zároveň obrovské zvětšení dosahu takového „špizování“. Základní princip je docela jednoduchý – dotyčný se prostě někde pohybuje v autě a hledá bezdrátové sítě. Technika je zajímavá mimo jiné i díky pozičním systémům GPS, které se snadno dají napojit k notebooku a napájet přímo z automobilu. WarDriving je pak hodně přesné a díky většímu prostorovému záběru auta má i větší naději na úspěch.

[14]

### 2.1.3 WarFlying

Technika „válečných náletů“ WarFlying byla zaznamenána snad jen dvakrát, ale je velice zajímavá. Jde zkrátka o hledání bezdrátových sítí z letícího letadla. Přístup k vhodnému malému letadlu a potřebnému vybavení má ale jen málokdo, takže i nadále bude zaznamenaných případů určitě podstatně méně než WarDriving. Vzhledem k omezenému dosahu bezdrátových sítí se letadlo musí pohybovat ve výšce pod 500metrů. Nálety metodou WarFlying byly poprvé zaznamenány v australském Perthu.[14]

### 2.1.4 WarSpamming

Hromadnou, nevyžádanou poštu neboli spam už někdy dostal asikaždý, je doslova shoubou internetu i každé poštovní schránky. Pro autory spamu je ovšem stále obtížnější šířit své zprávy, neboť se objevují země které postavily rozesílání spamu mimo zákon a existují i organizace, které zveřejňují IP adresy původu spamu. Není tedy nic jednoduššího než si najít nezabezpečenou bezdrátovou síť, připojit se k mailserveru a začít rozesílat. Jde ovšem o velmi závažný problém, neboť odesílatel je zodpovědný za obsah zprávy a je velice snadno identifikovatelný. Firma nebo i jednotlivec se tak nevědomky může velice rychle dostat do problémů a díky novým zákonům o nevyžádané poště může vše skončit i u soudu. WarSpamming se bude pravděpodobně i nadále rychle rozvíjet, neboť spammeři mají stále těžší život. [14]

### 2.1.5 WarSpying

Jde o poměrně nový jev, který útočí na bezdrátové obrazové sítě. Jde o vyhledávání nezabezpečených zdrojů videosignálu na frekvencích bezdrátových sítí. Nejčastějším zdrojem jsou X10 kamery. Ve městech bývají často takovým zdrojem bezpečnostní kamery.

## 2.2 Hrozby a útoky na WLAN

Ohrožení bezdrátových sítí má nejrůznější podobu – někdo se může připojit k bezdrátovému přístupovému bodu bez oprávnění, anebo může pomocí vhodného nástroje odposlouchávat pakety přímo „ze vzduchu“. Řada uživatelů bezdrátových sítí nemá přitom nejmenší tušení, jakým nebezpečím se při pouhém zapojení přístupového bodu do pevné sítě vystavují. [14]

Většina metod se odvíjí od faktu, že oblast pokrytí bezdrátovou sítí nejsme schopni fyzicky kontrolovat a zamezit tak pohybu nežádoucích osob. [3]

### 2.2.1 Nesprávně konfigurované AP

Nesprávné konfiguraci přístupových bodů bychom sice měli být schopni zabránit, jinak ale představují významnou díru do bezpečnosti bezdrátové sítě WLAN. Řada přístupových bodů tak podle prvotní, tovární konfigurace otevřeně vysílá své SSID všem oprávněným uživatelům. Někteří síťoví administrátoři pak SSID nesprávně používají v roli hesla pro

ověření oprávněnosti uživatele. Protože ale SSID se vysílá nesměrově, znamená tato konfigurace velmi závažnou chybu. Případný vetřelec se může SSID velice snadno zmocnit a vydávat se za právoplatného uživatele sítě. [14]

### 2.2.2 Odposlech

Bezdrátová komunikace probíhá formou vysílání rádiových vln a proto můžeme pouhým naslouchánim přenosů snadno odposlechnou všechny nešifrované zprávy. Na rozdíl od pevných sítí LAN není totiž uživatel bezdrátové sítě omezen jen na vlastní prostory firmy ani na jeden přístupový bod. Dosah bezdrátové sítě LAN se může pohybovat i daleko za obvodové zdi kancelářské budovy, kde tím pádem umožňuje i neoprávněný přístup z veřejných míst jako je parkoviště nebo kancelář firmy. Útočníkovi, který se chce dostat na nechráněný přístupový bod, tak úplně stačí být v jeho dosahu, a nepotřebuje žádné speciální vědomosti či vybavení.

Pomocí vhodné aplikace pro „odposlech paketů“(packet sniffer) není problém sledovat veškerý provoz, který prochází určitým ethernetovým připojením (ať už vede do pevné nebo bezdrátové sítě). Takovýto nástroj zachycuje veškeré pakety, jenž prochází přes jedno nebo několik spojení v síti Ethernet, a umožňuje jejich pozdější kontroly. Odposlechové aplikace vezmou paket, analyzují jej a zjistí jeho datovou zátěž. Jednou z největších hrozeb je zde zcela jednoznačně krádež identity právoplatného, oprávněného uživatele. [14]

### 2.2.3 Rozluštění WEP klíče (WEP Cracking)

Luštění klíče WEP je oblíbenou metodou útočníků. K rozluštění klíče je zapotřebí mezi 5 a 10 miliony paketů a útočník spoléhá na to, že po celou dobu, kdy je budete zachytávat, WEP klíč nezměníte. Útočníci mají k dispozici open source programy jako AirSnort nebo WEPCrack a stačí jim zachytávat komunikaci mezi přístupovým bodem a klientem. [3]

### 2.2.4 Zjištění MAC adresy (MAC attack)

Adresa MAC pro připojení na přístupový bod se zjišťuje stejně, jako se dekóduje WEP klíč. Pokud není v síti WEP aktivováno, stačí útočníkovi zachytávat komunikaci mezi přístupovým bodem a klientem a vyhledat hlavičku MAC adresy a tu si pak přečíst. Pokud je WEP používán, musí útočník nejdříve dekódovat WEP, v tomto případě mu ale

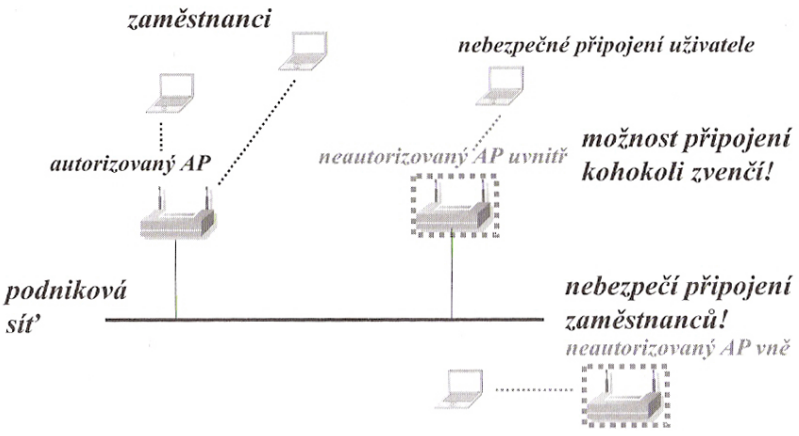
postačuje i offline analýza zachycených datových rámců. V okamžiku, kdy útočník získá MAC adresu, může ji podstrčit své klientské kartě a vystupovat jako oprávněný uživatel. [3]

### 2.2.5 Falešná zařízení

Z hlediska WLAN jsou velice nebezpečná neautorizovaná, falešná zařízení (ve skutečnosti to může být jak hardware, tak software), kterými mohou být nejen AP, ale také počítače. Falešný AP(rouge AP) je jakýkoli neautorizovaný AP v organizaci. A může se jednat o „přátelské“ i nepřátelské úmysly, protože mnohdy zaměstnanci přinesou svůj AP bez přemýšlení. Naneštěstí CIO často vůbec nevědí o WLAN ve svých organizacích. Zejména malé AP (pro domácí uživatele) jsou nebezpečná v podnikových sítích, protože negenerují žádnou komunikaci s jinými AP, takže je lze jen obtížně detekovat (i na Ethernetu). [2]

Jeden ředitel jisté velké technologické společnosti prý nedávno řekl, že „nejhůře se proti bezdrátovým hrozbám zabezpečuje taková síť, která nemá vůbec žádný bezdrátový přístup“(nebo něco takového). Tím měl namysli, že i když firma do své sítě nezakoupí a nenainstaluje žádné bezdrátové zařízení, neznamená to ještě, že tam žádné takové zařízení není. [14]

Je důležité si uvědomit, že neautorizovaný AP může a nemusí být připojen k podnikové síti, aby napáchal škody (Obr. 9 ). Falešný AP vně budovy může nezabezpečeného uživatele přimět k přidružení, a narušitel se tak může dostat k důležitým datům. Připojení AP k podnikové síti už vyžaduje porušení i dalších bezpečnostních pravidel, třeba fyzického přístupu, proto se toho spíše dopouštějí sami zaměstnanci než útočníci zvenčí.




*Obr. 9. Neautorizované AP [2]*

### 2.2.6 Útok typu muž uprostřed (man-in-the-middle)

Útoky typu „muž uprostřed“ jsou charakteristické tím, že hacker vstoupí mezi přístupový bod a klienta a přeruší veškerý provoz mezi nimi. Hacker zachytává a dekóduje data přenášená mezi přístupovým bodem a klientem během asociačního procesu. Takto získá základní informace o klientovi i přístupovém bodu, jako jsou IP adresy obou zařízení, asociační ID klienta a SSID přístupového bodu. S těmito informacemi může být hacker schopen vytvořit podvržený přístupový bod blíže uživateli (na jiném kanálu) a změnit připojení uživatele na tento podvržený přístupový bod. Data, která na tento přístupový bod přijal, zaznamenává a také přeposílá na skutečný přístupový bod, takže jak klient, tak skutečný přístupový bod se domnívají, že spolu přímo komunikují, zatímco ve skutečnosti jejich komunikaci zprostředkovává a především zachytává „muž uprostřed“. Hacker se takto dostává ke všem datům včetně hesel atd. [3]

U bezdrátových sítí se tento typ útoku provádí podobnými metodami jako u pevných sítí, ale útočník může být od oblastní sítě značně daleko. Útok „Muž uprostřed“ lze provádět na fyzické nebo spojové vrstvě WLAN. Falešný přístupový bod (jako neautorizovaný AP útočník nejčastěji použije softwarový AP na kartě ve svém laptopu nebo i PDA) má šanci tehdy, pokud klienti nemají přednastavený kmitočet, na kterém pracují. Pokud ho mají, musel by útočník překonat legitimní AP na jeho vlastním kmitočtu. V opačném případě klientské karty detekují neautorizovaný AP na kanálu odlišném od současně používaného a automaticky se k němu přidružují, jakmile se spojení s legitimním AP zhorší nebo úplně zmizí. Main-in-the-middle se nemusí nutně vydávat za přístupový bod, může nahradit jednoho z oprávněných klientů. Narušiteli to ušetří práci, protože nemusí svoje zařízení nastavit jako AP. Navíc útočníkovi při rychlém útoku proti jednomu klientskému zařízení nehrozí odhalení, protože nevyvolá stížnosti uživatelů o logování. [2]

### 2.2.7 Útok s cílem odmítnutí služby: DoS (Denial of Service)

Útoky DoS nepatří v pravém slova smyslu mezi průniky do sítě, jde vlastně jen o vyřazení sítě z provozu. Útočník zahltí přístupový bod nesmyslnými daty ve velkém množství. Přístupový bod se snaží tato data vyhodnotit a dojde k jeho zahlcení nebo zahlcení přenosového pásma. To zpomalí nebo zcela znemožní připojení ostatních uživatelů. Útok

DoS bývá zlomyslným vtípkem náctiletých pitomečků, kteří zjistili, že takto lze mnohdy příliš jednoduše někomu uškodit. V horším případě útok DoS předchází útokům typu Man-in-the-middle, kdy má za cíl odpojit uživatele od skutečného přístupového bodu a umožnit přepojení na podvržený přístupový bod. [3]

Mezi útoky DoS patří :

- **jamming** – zahlcení sítě neužitečnými rámci, případně silné zarušení sítě (specifické zařízení může být založeno na bázi mikrovlnné trouby).
- **záplava rámců pro odpojení ze sítě** – rozšířený útok může vést k obtížnému opětovnému přidružení k síti.
- **falešné chybové autentizační rámce** – klient může mít následně problém s opětovným přidružením k síti.
- **chybějící šifrování a ochrana integrity pro rámce managmentu** (platí i v případě 802.11i) – útočník může podvrhnout rámce typu deasociace nebo deautentizace stanice nebo AP, a tím zablokovat nebo zpozdit legitimní pakety.
- **přeplnění bufferu AP pro rámce pro pridružení a autentizaci** – hrozí přetečení vyrovnávací paměti u AP a spadnutí AP při velkém množství ustavených spojení nebo požadavků na autentizaci.
- **specifické nastavení WLAN** – na základě nastavení úspory energie při napájení (útočník může falšovat rámce s TIM, Trafic Indication Map, informující spící klienty o příchozích datech pro ně), nebo režim RTS/CTS (na základě upřednostnění – útočník zaplavuje síť rámci RTS s nastaveným polem trvání na dlouhou dobu, takže blokuje médium pro autorizaci klienty, kteří na základě rámců CTS pro útočníka musí čekat). [2]

### 2.2.8 Slovníkový útok (Dictionary Attacks)

Tento útok je založen na využití slovníku pro útok na uživatelská jména a hesla. Útočník posílá výzvu na odezvu zaheslovaného protokolu a snaží se za pomoci databáze běžně používaných přihlašovacích jmen a hesel prolomit šifru. Jakmile se mu podaří odhalit správnou kombinaci, získává plný přístup do bezdrátové sítě. Na pomoc hackerům přichází open source programy a databáze hesel a přihlašovacích jmen, které není těžké z Internetu získat. Velkou výhodou pro nás je, že jsou zaměřeny převážně na anglofonní uživatele

a jen zřídka akceptují českou realitu. Login *honza* a heslo *lucinkaslunicko* se tedy v takovém slovníku pravděpodobně nenajde, což je jistou útěchou pro administrátory sítě.

### 2.2.9 Session Hijacking

Někdy je hacker schopen nejenom přenášená data odposlouchávat, ale také do nich vložit své vlastní informace – může tak „nasednout“ do přenosu dat a odesílat informace, které se tváří jako původní z klienta nebo přístupového bodu. Tak může přesměrovat provoz z legitimního zařízení na sebe.

### 2.2.10 Nástroje pro prolomení WLAN

Nyní bych chtěl uvést několik nástrojů, které lze s úspěchem použít k provedení některého z výše uvedených útoků. Teoreticky sice mají tyto programy sloužit administrátorům ke správě a obsluze jejich bezdrátové sítě a jako takové se i prezentují, mnohem častěji však slouží spíše útočníkům k činnostem přesně opačným.

#### *NetStumbler*

NetStumbler je malý freewarový nástroj běžně stáhnutelný na internetu, který dokáže zjistit zajímavé „tajné“ informace :

- Identifikátor SSID bezdrátového přístupového bodu
- MAC adresu přístupového bodu
- Sílu signálu nalezeného přístupového bodu a jestli tento přístupový bod používá WEP
- Kanál, na kterém přístupový bod vysílá a mnoho dalšího.

NetStumbler rozešle na všech kanálech nesměrové vysílání a čeká na odpověď. Jestliže bezdrátový přístupový bod podle své konfigurace odpovídá nesměrovým rozesíláním svého SSID, pak si jej NetStumbler zaznamená. NetStumbler se však dokáže napíchnout na bezdrátové přístupové body podle normy 802.11b a na některé 802.11a. Jednou z nejlepších funkcí nástroje NetStumbler je možnost vyhledávání přístupových bodů ve spojení s notebookem a integrovanou jednotkou GPS. [14]

### *Ethereal*

Program Ethereal patří k nejpoužívanějším síťovým snifferům na světě. Jde opět o program, který je zdarma a lze ho běžně stáhnout na internetu. Je dostupný ve verzích pro většinu známých platforem (MS Windows 98-XP, všechny významné linuxové distribuce, Apple Mac Os X, BeOS, atd…). Jde o zcela pasivní nástroj, to znamená, že dokáže pakety zachytávat a zobrazovat jejich obsah, ne však je vytvářet, měnit nebo odesílat. Také nedokáže na zachytávanou komunikaci nijak reagovat. Program Ethernal tedy dokáže zachytávat data ze síťové komunikace a nebo je číst ze souboru, který vytvořil jiný program. Zachycená data pak mohou být analyzována prostřednictvím grafického rozhraní, nebo prostřednictvím TTY-módu. Za pomocí programu Ethernal lze detekovat a analyzovat přes 400 síťových protokolů. [15]

### *AirSnort*

Program AirSnort se objevil v roce 2001. Myšlenka „sbírání paketů“ a prolomení jejich šifrovací ochrany nebyla ničím novým a bezpečnostní odborníci už nějakou dobu o slabých stránkách protokolu WEP věděli. V nástroji AirSnort tak dostali hackeři obě funkce (odposlech a prolomení šifer) pohodlně dohromady. Jedinou jeho nevýhodou je, že pracuje na linuxové platformě. [14]

Program AirSnort pasivně monitoruje provoz na síti a shromažduje pakety. Jakmile jich nasbírá dostatečné množství, asi 5 – 10 miliónů, provede výpočet WEP klíče. To při dnešních rychlostech procesorů trvá jen několik málo sekund.

# 3 ZABEZPEČENÍ WLAN

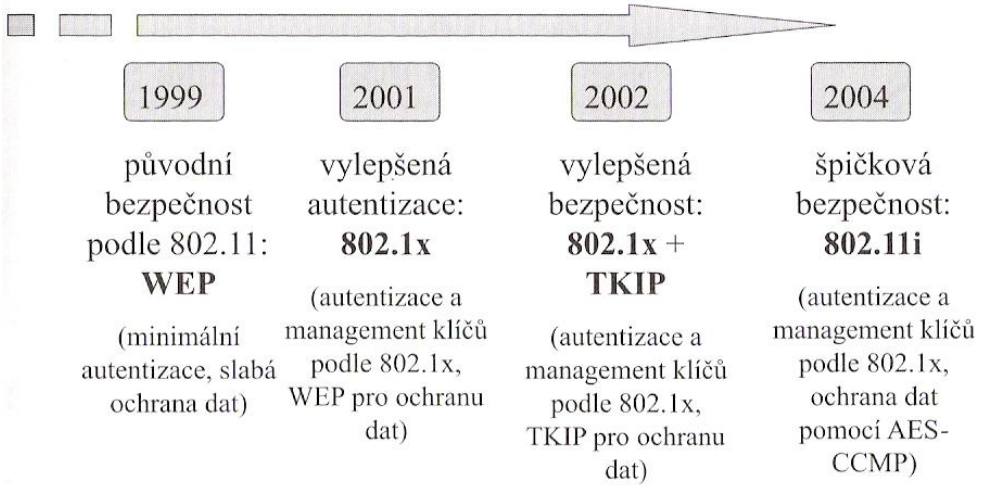
Bezpečností sítě se rozumí minimalizace zranitelných míst síťových prostředků. Ochranu v síti vyžadují:

- **Informace a data** (včetně dat spojených s bezpečnostními opatřeními, např. hesla).
- **Služby** přenosu a zpracování dat.
- **Zařízení**
- **Uživatelé**

Ohrožení komunikačního systému zahrnuje zničení, poškození, modifikaci, ukradení či ztrátu informací, případně zdrojů, odhalení soukromé informace, nebo přerušení služeb. K ohrožení může docházet neúmyslně nebo úmyslně („útoky“), zvenčí i zevnitř.[2]

Bezdrátové sítě, Wi-Fi, nemají žádnou implicitně zabudovanou bezpečnost (implicitní je otevřený přístup k přístupovému bodu sítě), ale nabízejí zabezpečení jako nedílnou volitelnou možnost. Přesto mnohé firemní WLAN stále pracují zcela nezabezpečené, jak ukazují výsledky aktivit jako *warwalking, wardrivinng* nebo vizuálně dokreslené *warchalking.* [2]

Od začátku implementace WLAN se pracuje na jejich lepším zabezpečení a v dnešní době jsou již k dispozici mechanismy, které dokáží zabezpečit WLAN i pro použití v nejpřísnějších podmínkách (např. vládní instituce). Vývoj řešení bezpečnosti WLAN je naznačen na obrázku (Obr. 10.).




*Obr. 10. Vývoj podpory zabezpečení WLAN [2]*

Bezpečnostní prvky v normě 802.11a/b/g se zaměřují pouze na autentizaci, šifrování a integritu dat. Autorizace není součástí specifikace a musí se provádět externími mechanismy (např. mechanismem pro řízení přístupu 802.1x). [2]

## 3.1 SSID

Přístupový bod vysílá implicitně identifikátor SSID (Service Set Identifier) každých několik sekund v takzvaném majákovém rámci (beacon frame). Takto může oprávněný uživatel snadno najít správnou síť, ale zároveň se do ní dostane i neoprávněný hacker. Právě díky této funkci dokáže většina softwarových detekčních nástrojů najít bezdrátovou síť bez předchozí znalosti SSID. [14]

Hodnotu parametru SSID v síti je třeba považovat za první úroveň zabezpečení. Ve své základní, tovární, podobě nemusí SSID poskytovat žádnou ochranu proti neoprávněnému přístupu k síti, pokud jej ale změníme na hůře uhodnutelný text, nedostanou se vetřelci do sítě tak snadno.

*Tab. 2. Výchozí hodnoty SSID u některých výrobců*

| Výrobce | Výchozí hodnota SSID |
|---|---|
| 3Com | 101,comcomcom |
| Addtron | WLAN |
| Cisco | Tsunami, WaveLAN Network |
| Compaq | Compaq |
| Dlink | WLAN |
| Intel | 101, 195, xlan, intel |
| Linksys | Linksys, wireless |
| Lucent/Cabletron | RoamAbout |
| NetGear | Wireless |
| SMC | WLAN |
| Symbol | 101 |
| Teletronics | any |
| Zcomax | any, mello, Test |
| Zyxel | Wireless |
| Ostatní | Wireless |

Podrobný seznam SSID od všech výrobců, a dokonce i výchozí logovací jména a hesla k dalším síťovým zařízením, jsou dostupné na internetu. [14]

Vedle SSID se používá také ESSID (Extend Service Set Identification), který slouží jako jedna ze základních technik pro řízení přístupu klientů do WLAN. ESSID je hodnota

naprogramovaná do AP pro identifikaci sítě (subnet), v níž se AP nachází. ESSID se nevysílá, takže přidružení do WLAN je povoleno pouze autorizovaným stanicím, které hodnotu identifikátoru znají. Síť používající ESSID se oprávněně označuje jako uzavřená. [2]

## 3.2 Filtrování MAC adres

Metoda filtrování fyzických adres MAC představuje další možnost zabezpečení sítí nad normou 802.11b. Adresa MAC síťové karty je 12ciferné hexadecimální číslo, které je jedinečné mezi všemi síťovými kartami na světě. Protože svoji adresu MAC má i každá bezdrátová karta sítě Ethernet, můžeme v přístupovém bodu snadno omezit povolení přístupu jen pro jistou množinu oprávněných zařízení a kohokoli cizího tak snadno vykázat ze sítě.

Filtrování adres MAC není ale bohužel úplně bezpečné, a plně se na ně spoléhat by bylo hrubou chybou.[14]

Problém je totiž v tom, že řada bezdrátových karet mívá ovladač, který uživateli umožňuje MAC adresu změnit. Existují i jiné nástroje, které umožňují měnit MAC adresu. Protože se zdrojová a cílová adresa posílají nešifrovaně (a to i v případě použití WEP), může útočník jednoduše odposlechnout hodnoty povolených MAC adres a pak svou bezdrátovou kartu nastavit tak, aby používala takovouto platnou adresu. Když se karta tváří jako karta s povolenou MAC adresou, bude AP přesvědčeno, že jde o legitimní provoz. [1]

Kromě rizika falšování MAC adres se ve větších sítích stává neudržitelná administrace seznamu autorizovaných adres. Udržovat evidenci MAC adres všech karet, které ve vaší společnosti pořizujete nebo vyřazujete, a udržovat tento seznam aktualizovaný na všech AP, to je příliš mnoho práce v jakémkoli prostředí. [1]

## 3.3 WEP

WEP není a ani neměl být žádným bezpečnostním algoritmem. Jeho úlohou nebyla ochrana dat ani před skriptovými amatéry, ani před inteligentnějšími útočníky, kteří se v síti zajímají o důvěrné údaje. Protokol WEP není postaven jako nějaká zvlášť pevná bašta, ale pouze zajišťuje, abychom si přechodem z pevné sítě „do vzduchu“ nesnížili bezpečnost dat (proto se také většinou vykládá jako Wired Equivalent Privaci, tedy „míra

soukromí, ekvivalentní s pevnou sítí“). Problém je, že mnozí lidé vidí v jeho zkratce písmeno „E“ jako „Encryption“, šifrování. Úkolem WEP je vyřešit slabší zabezpečení bezdrátového přenosu oproti klasické pevné síti, to znamená, že *s protokolem WEP jsou data stejně bezpečná, jako na pevné, ale nešifrované síti typu Ethernet.* To je všechno a tečka. [14]

### 3.3.1 Princip činnosti WEP

WEP funguje na symetrickém principu, kdy se pro šifrování a dešifrování používá stejný algoritmus i totožný statický klíč. Nejčastější (a nejslabší) 40-bitový klíč pro ověření totožnosti (autentizaci) je stejný pro všechny uživatele dané sítě (sdílený klíč) a klienti jej využívají spolu se svou adresou MAC pro autentizaci vůči přístupovému bodu.

Šifrování přenášených dat se provádí 64-bitovým klíčem, který je složen z uživatelského klíče a dynamicky se měnícího vektoru IV (Initialization Vector). WEP používá šifrovací algoritmus RC4.

V závislosti na výrobci může nabízet silnější zabezpečení ve formě 128-bitového šifrování (sdílený klíč má délku 104 bitů, vektor poté 24 bitů). [16]

### 3.3.2 Autentizace

WEP používá symetrický postup, tedy pro šifrování a dešifrování se používá stejný algoritmus i stejný klíč. Autentizace se provádí buď **otevřeně** (open system), nebo na základě **sdíleného klíče** (shared key).

- **Otevřená autentizace** není založena na žádném prověřování identifikačních údajů klienta. Ten pouze pošle svoji identifikaci přístupovému bodu a na základě tohoto požadavku jej přístupový bod přidruží. V rámci otevřené autentizace se může jakýkoli klient přidružit k přístupovému bodu.
- **Autentizace sdíleným klíčem** používá 40bitový uživatelský klíč, který je statický a stejný pro všechny uživatele dané sítě. Ve skutečnosti se ověřuje totožnost síťové karty, nikoli uživatele, což je jedna z hlavních slabin autentizace v rámci WEP.

Autentizace se provádí pouze jednostranně, nikoli vzájemně. Klienti nemají možnost žádat přístupový bod, aby se autentizoval.

Zvolený režim autentizace nemá přímou souvislost s šifrováním dat. [2]

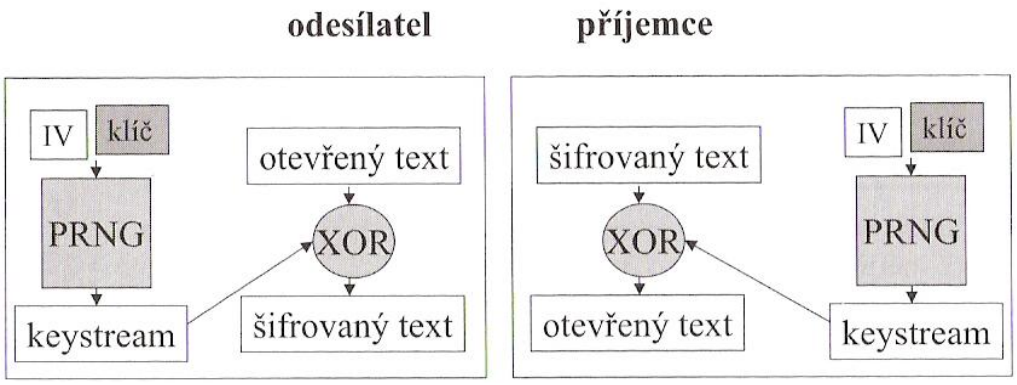
### 3.3.3 Šifrování

Informace o tom, že se používá šifrování WEP, je naznačená v záhlaví MAC rámce, nastavením bitu *Protecte Frame* v poli řízení rámce. Šifrování přenášených dat mezi klientem a přístupovým bodem se provádí 64bitovým nebo 128bitovým klíčem, který je složen z uživatelského (tajného) klíče v délce 40 respektive 104 bitů a dynamicky se měnícího inicializačního vektoru IV (*Initialization Vector*), vždy v délce 24 bitů. IV generuje vysílací strana, použije jej pro vytvoření šifry a současně jej pošle v otevřené formě jako součást záhlaví každého paketu. Příjemce použije IV přijatého rámce pro spojení se sdíleným WEP klíčem a provede dešifrování přijatých dat. [2]

### 3.3.4 Šifra RC4

WEP používá RC4, symetrickou proudovou šifru vyvinutou v roce 1987 Ronaldem Rivestem (*Ron's Code No.4*). RC4 byla ve své době (konec 90. let) zvolena pro zabezpečení WLAN kvůli jednoduchosti implementace přímo do hardwaru síťového adaptéru, která má jen zanedbatelný dopad na výkonnost zařízení u většiny adaptérů. Proudová šifra umožňuje z klíče pevné délky vytvořit šifrovací proud (*cipher stream*) tak, aby bylo možné otevřený text libovolné délky (každému bitu textu odpovídá jeden bit šifry). RC4 dovoluje klíč o délce do 256 bitů, 802.11 pro WEP zvolilo délku 40 bitů.

RC4 pracuje jako generátor pseudonáhodných čísel (*PRNG, PseudoRandom Number Generator*), jehož základem je jedinečná kombinace tajného klíče a IV (Obr. 11.). Tajný klíč zůstává stejný, mění se periodicky jen IV. Výsledná pseudonáhodná posloupnost nul a jedniček se pro zašifrování spojí s otevřeným textem (daty) prostřednictvím logické funkce XOR. Dešifrování probíhá opět prostřednictvím funkce XOR použité na šifrovaný tok a zašifrovaný text. Funkce XOR totiž umožňuje opětovným použitím na výsledek získat původní hodnotu (RC4(X) XOR X XOR Y = RC4(Y)), proto hovoříme o RC4 jako o symetrické šifře. Jak uvidíme dále, právě tato vlastnost činí RC4, a tedy celý WEP, velice náchylným na útoky, a to i při částečné znalosti obsahu paketu ze strany útočníka.




*Obr. 11. Šifrování RC4 [2]*

## 3.4 IEEE 802.1x a EAP

O 802.1x se mnohdy hovoří různě: jako o bezpečnostní normě, protokolu, nebo dokonce autentizační metodě. Může se proto zdát, že 802.1x je samospasitelné řešení bezpečnosti (nejen v bezdrátových sítích). Skutečnost je poněkud méně optimistická, ale v každém případě je tato norma – novější než normy pro WLAN – při správné implementaci schopna přispět k lepšímu zabezpečení WLAN. Je třeba předeslat, že 802.1x nenahrazuje WEP, ale pracuje jako jeho nadstavba, a to pouze pro řízení přístupu.

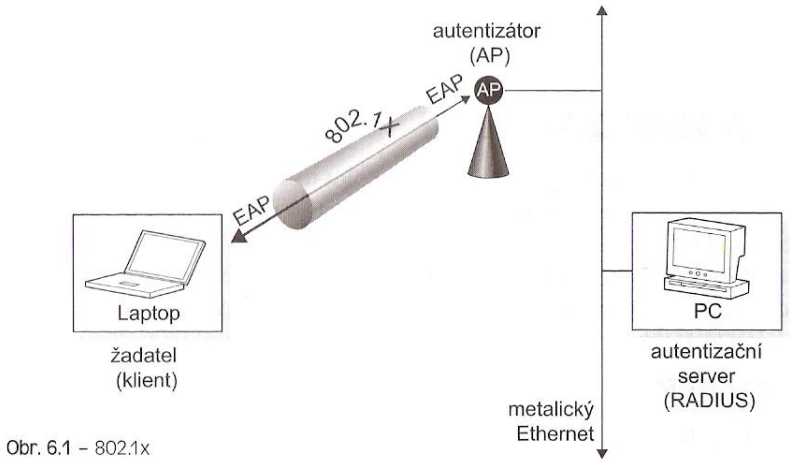
IEEE 802.1x (Port Based Network Access Kontrol, 2001) je obecný bezpečnostní rámec pro LAN, zahrnující autentizaci uživatelů, integritu zpráv (šifrování) a distribuci klíčů. Autentizace se v případě WLAN realizuje na úrovní logických portů přístupového bodu (každá bezdrátová stanice komunikuje s jedním logickým portem AP na základě přidružení se k WLAN). Protokol 802.1x má za cíl blokovat přístup k segmentu lokální sítě pro neoprávněné uživatele. 802.1x slouží jako transport na spojové vrstvě pro zprávy autentizačního protokolu vyšší vrstvy (EAP). [2]

Protokol EAP byl původně vytvořen jako rozšíření protokolu PPP (Point-to-Pint Protocol, používaný u vytáčených připojení a některých DSL modemů, autentizuje pouze na základě jména a hesla). Základním cílem bylo vytvořit obecnou platformu pro různé autentizační metody. Jinak řečeno, jde o PPP se „zásuvnými“ autentizačními moduly. Díky tomu můžete uživatele autentizovat tak, jak se vám zlíbí. Můžete používat hesla, certifikáty, tokeny, PKI, čipové karty, Kerberos (autentizační protokol), biometriky, (cokoliv jiného na co si vzpomenete), a tak dále. Otevřený standard zajišťuje, že kdykoliv v budoucnu budete moci metody zabezpečení zlepšit, protože jako nový typ EAP bude možno použít mechanismy, které dnes ještě ani neznáme. [1]

802.1x má 3 základní komponenty :

- **Žadatel** : Uživatel nebo klient, požadující přístup k síti.
- **Autentizátor** : „Muž uprostřed“, přepínač nebo AP, povolující nebo blokující provoz.
- **Autentizační server** : Systém udržující autentizační informace, typicky server RADIUS.

[1]



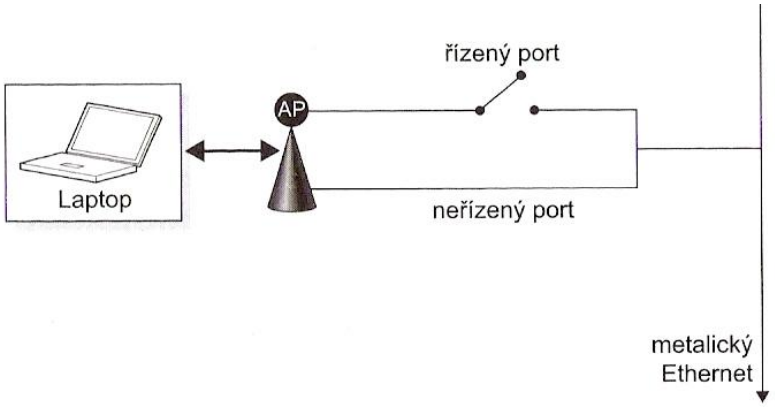

*Obr. 12. Komponenty 802.1x [1]*

Princip řízení přístupu je jednoduchý: jakmile chce klient získat přístup k LAN, autentizátor zablokuje veškeré síťové prostředky a služby pro klienta vyjma autentizačního serveru. Tak se klient musí nejprve autentizovat, než získá přístup do sítě.

Přístupové body tedy musí umožnit komunikaci po EAP pro klienta ještě před vlastní autentizaci. Proto se používá model tzv. duálního portu (Obr. 14.), kdy autentizátor podporuje dva porty:

- **Neřízený** (uncontrolled) – filtruje veškerý provoz kromě rámců EAP.
- **Řízený** (controlled) – pro veškerý provoz autentizovaného/autorizovaného klienta.

[2]




*Obr. 13. Řízený a neřízený port [1]*

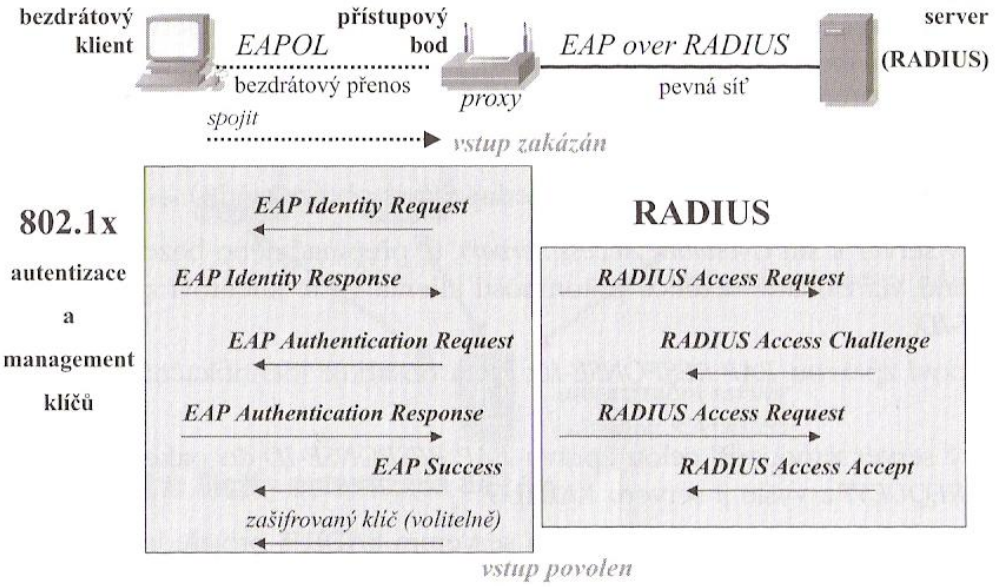
### 3.4.1 Autentizace 802.1x

Autentizaci ve WLAN zprostředkovává přístupový bod pro klienty na základě jejich výzvy pomocí lokálního přístupového seznamu. Pouze ověřený uživatel má možnost přístupu k bezdrátové síti. Komunikace za účelem autentizace se ve skutečnosti skládá ze dvou částí: mezi klientem a přístupovým serverem a mezi přístupovým serverem a autentizačním serverem. Přístupový server je pouhým prostředníkem, který předává příslušné zprávy mezi klientem a serverem a zpět.

Postup při autentizaci 802.1x je následující (Obr. 15.) :

- přístupový server k síti (Network Access Server), tj. přepínač nebo bezdrátový přístupový bod, na základě detekce přítomnosti klienta vyšle klientovi zprávu EAP REQUEST-ID.
- Klient odpoví zprávou EAP RESPONSE-ID, která obsahuje identifikační údaje uživatele.
- přístupový server zapouzdří celou zprávu EAP RESPONSE-ID do paketu RADIUS ACCESS_REQUEST a vyšle ji serveru RADIUS.
- zprávy EAP jsou posílány mezi klientem a serverem RADIUS prostřednictvím přístupového serveru: mezi klientem a AP jsou zapouzdřeny jako EAPOL a mezi AP a autentizačním serverem jako pakety RADIUS.

- server RADIUS odpoví zprávou obsahující povolení/zákaz přístupu pro daného klienta do sítě : RADIUS ACCESS_ACCEPT/DENY, která v sobě obsahuje informaci EAP SUCCESS/FAILURE, kterou přístupový server přepošle klientovi.
- v případě povolení přístupu (SUCCESS) je příslušný (logický) port přístupu do sítě (přes který autentizace probíhala) otevřen pro data daného uživatele, která je na základě úspěšného výše popsaného procesu považován za utentizovaného.




*Obr. 14. Autentizace podle 802.1x [2]*

Po úspěšné autentizaci následuje fáze správy klíčů, kdy přístupový bod distribuuje šifrovací klíče autentizovaným stanicím, a to prostřednictvím zprávy EAPOL-Key. Tato zpráva se může použít pro distribuci obou typů klíče. Zpráva se nepotvrzuje, takže při její ztrátě nebude mít žadatel a autentizátor stejné klíče a následná komunikace neproběhne v pořádku. Pak se musí provést autentizace celá znovu.

V rámci procesu autentizace se generují dvě sady klíčů (128 bitových) :

- **párové klíče** (*pairwise*) jedinečné pro spojení mezi přístupovým bodem a klientem – zajištění spoje a překonání stejného klíče pro všechny u WEP, **PMK** (*Pair wise Master Key*) je jedinečný pro relaci mezi žadatelem a autentizačním serverem.

- **skupinové klíče** (*groupwise*) sdílené všemi stanicemi v jedné buňce 802.11 – používané pro šifrování skupinové komunikace (*multicast*).

[2]

### 3.4.2 Autentizační metody protokolu EAP

V současné době protokol EAP podporuje desítky metod autentizace. Následujících pět patří mezi ty nejrozšířenější. Od zvolené metody se odvíjí jak náročnost její implementace, tak i bezpečnost celého řešení. Některé metody se instalují snáze, jiné jsou zase mnohem bezpečnější. Zvolenou metodu autentizace EAP musí podporovat všechny tři komponenty systému – žadatelé, autentizátoři i autetizační server. [1]

- **EAP-MD5 –** Metoda EAP-MD5 se při odesílání autentizačních informací na server RADIUS opírá o haš (otisk) MD5, vytvořený z uživatelského jména a hesla. Tato metoda nezajišťuje žádnou správu klíčů ani nenabízí dynamické generování klíčů WEP, a proto vyžaduje statické klíče WEP, má proto jistá omezení :
  - ♦ Protože není k dispozici žádné dynamické generování klíče WEP, neznamená protokol EAP oproti WEP žádné vyšší zabezpečení; útočníci mohou i nadále odposlouchávat síť a snadno dešifrovat klíč WEP.
  - ♦ EAP-MD5 nenabízí žádné prostředky, kterými by si klientské zařízení ověřilo, že vysílá informace do správného přístupového bodu; klient tak může mylně vysílat i do pirátského přístupového bodu.

  Znamená to, že EAP-MD5 nenabízí oproti samotnému standardu 802.1x žádné funkce navíc, a proto se ze všech metod EAP považuje za nejméně bezpečnou.
- **LEAP -** Metodu EAP-Cisco Wireless (označovavá častěji jako LEAP) vyvinula na základě normy 802.1x firma Cisto a je základem velké části oficiálně schválené verze EAP. Podobně jako EAP-MD5 i metoda LEAP od klientského bezdrátového zařízení přebírá uživatelské jméno a heslo, a předává je k autentizaci na server RADIUS. Firma Cisto doplnila kromě požadavků samotné normy i další podporu a přinesla tak do metody vyšší bezpečnost :
  - ♦ Metoda LEAP provádí autentizaci klienta; pro každé klientské připojení se dynamicky generují jednorázové klíče WEP. To znamená, že každý klient

bezdrátové sítě pracuje s jiným dynamicky vygenerovaným klíčem, který nikdo nezná – dokonce ani samotný uživatel.

- ♦ LEAP podporuje jednu funkci protokolu RADIUS, kterou jsou časové limity komunikačních relací; to znamená, že se klient musí každých několik minut přihlásit znovu. Uživatel ale naštěstí nemusí dělat nic zvláštního. Přidáme-li k této funkci dynamické klíče WEP, budou se v důsledku toho klíče WEP měnit tak často, že se útočníkům nepodaří je včas prolomit.
- ♦ LEAP provádí vzájemnou autentizaci, tedy *klienta vůči přístupovému bodu* i naopak *přístupového bodu vůči klientu*; tím se vytváří ochrana proti instalaci pirátských přístupových bodů do sítě.

U autentizační metody LEAP je v současné době známo jediné omezení; pro autentizaci klientů i přístupového bodu se používá protokol MS-CHAPv1, který obsahuje známá zranitelná místa.

- **EAP-TLS –** Metodu EAP-TLS vyvinula firma Microsoft a její popis je uveden v dokumentu RFC 2176. Namísto kombinace uživatelského jména a hesla provádí tato metoda autentizaci pomocí certifikátů X.509; informace veřejného klíče v PKI se zde do EAP přenášejí pomocí zabezpečení transportní vrstvy. Podobně jako LEAP nabízí i verze EAP TLS dvě důležité funkce:
  - ♦ Dynamické generování jednorázového klíče WEP
  - ♦ Vzájemná autentizace zařízení

  A mezi nevýhody metody EAP-TLS patří :
  - ♦ Pro jeho činnost je nutný protokol PKI, který ale většina firem neprovozuje.
  - ♦ Je možné využít také službu Microsoft Aktive Direktory a server certifikátů, tato změna je však obtížná.
  - ♦ Pokud v síti běží adresářové služby Open LDAP nebo Novell Directory Services, potřebujeme mít také server RADIUS, opět ale platí, že ne každý má k němu okamžitý přístup.
  - ♦ Jestliže máme implementovánu PKI s certifikáty VeriSign, nejsou u ní k dispozici všechna pole požadovaná metodou EAP-TLS.

Tuto metodu má smysl uvádět do provozu jen v případě, že se při její implementaci budeme přesně držet doporučení firmy Microsoft.

- **EAP-TTLS –** Autentizační metodu EAP-TTLS zavedla firma Funk Software, a to jako alternativu k výše popsané EAP-TLS. Bezdrátový přístupový bod se i zde musí autentizovat vůči klientu pomocí serverového certifikátu, ale uživatelé odesílají pro přihlášení jen uživatelské jméno a heslo. Tyto přihlašovací údaje pak EAP-TTLS předává k ověření pomocí libovolného mechanismu výzvy a odpovědi, určeného administrátorem (PAP, CHAP, MSCHAPv1, MS-CHAPv2, PAP/totenová karta, nebo EAP). Jedinými nedostatky této metody je:

  - Je o něco méně bezpečná ne dvojité certifikáty EAP-TLS
  - Přesně stejným způsobem pracuje i nově vyvíjený standard firem Microsoft a Cisco – „chráněná“ verze Protecte EAP (PEAP)

[14]

- **PEAP -** Protokol PEAP používá protokol TLS (Transport Level Security) k vytvoření zašifrovaného kanálu mezi ověřovaným klientem protokolu PEAP, například počítačem v bezdrátové síti, a ověřovatelem protokolu PEAP, například server RADIUS. Protokol PEAP neurčuje metodu ověřování, ale poskytuje další zabezpečení ostatních protokolů ověřování EAP, například protokolu EAP-MSCHAPv2, který může pracovat prostřednictvím zašifrovaného kanálu protokolu TLS poskytnutého protokolem PEAP. Protokol PEAP lze použít jako metodu ověřování u klientských počítačů bezdrátové sítě s ověřovacím standardem 802.11, nikoliv však u klientů virtuální privátní sítě (VPN) nebo jiných klientů vzdáleného přístupu.

  Protokol PEAP poskytuje následující funkce rozšiřující protokol EAP a síťové zabezpečení:

  - Ochrana vyjednávání metody protokolu EAP mezi klientským počítačem a serverem prostřednictvím kanálu protokolu TLS.
  - Podpora fragmentace a nového sestavování zpráv, což umožňuje použít typy protokolu EAP, které tyto funkce neposkytují.

- Možnost ověřování serverů IAS a serverů RADIUS klienty bezdrátové sítě. Protože tyto servery také ověřují klienty, dochází k vzájemnému ověřování.

- Ochrana před zavedením neautorizovaných bezdrátových přístupových bodů (WAP) během ověřování certifikátu poskytnutého klientskému počítači protokolu EAP serverem služby IAS. Hlavní tajný klíč protokolu TLS vytvořený ověřovatelem a klientem protokolu PEAP navíc není s přístupovým bodem sdílen. Díky tomu není přístupový bod schopen zprávy chráněné protokolem PEAP dešifrovat.

- Rychlé obnovení připojení protokolu PEAP zkracující dobu zpoždění mezi požadavkem klienta na ověření a odpovědí serveru IAS nebo serveru RADIUS. Protokol PEAP umožňuje klientům bezdrátové sítě přesunovat se mezi přístupovými body bez nutnosti opakování požadavku na ověření. Tato funkce snižuje požadavky na prostředky klienta i serveru.

Proces ověřování pomocí protokolu PEAP mezi klientem a ověřovatelem tohoto protokolu se skládá ze dvou fází. Během první fáze je vytvořen zabezpečený kanál mezi klientem a ověřujícím serverem protokolu PEAP. V druhé fázi dojde mezi klientem a ověřovatelem protokolu EAP k ověřování pomocí protokolu EAP.

[17]

## 3.5 WPA

31. října 2002 ohlásila Wi-Fi aliance protokol WPA, což je v zásadě kompromisní řešení, protože některé části specifikace 802.11i už byly hotovy (například 802.11y a TKIP, tedy Temporary Key Integrity Protocol), zatímco jiné ještě ne (například AES, Advanced Encryption Standard a zabezpečená deautentizace a disasociace).

Logika, kterou se Wi-Fi asociace řídila, byla prostá: Nemůžeme čekat do doby, než dojde k ratifikaci 802.11i, což se stane přinejlepším za rok nebo dva[1], takže vezmeme to, co už je

[1] Ke schválení došlo v roce 2004

hotovo a vydáme to hned. WPA je tak podmnožinou 802.11i, kterou lze implementovat prostřednictvím aktualizace softwaru a firmwaru. Řeší jak šifrování (TKIP), tak řízení přístupu (802.1x). Z bezpečnostního pohledu mají tyto technologie značný význam, protože řeší řadu slabin a bezpečnostních děr protokolů WEP a 802.11. [1]

Pro WPA je potřeba :

- Přístupový bod s podporou pro WPA.
- Bezdrátová karta s ovladači pro WPA.
- Klient s podporou WPA v operačním systému.

WPA tvoří následující 3 složky :

- **Temporary Key Integrity Protocol** (TKIP): používá 40bitový klíč jako WEP (s RC4), ale mění jej pro každý paket a brání se tak proti útoku hrubou silou, navíc se zdvojnásobila délka IV na 48 bitů.
- **Message Integrity Check** (MIC): přenos je chráněn proti narušení, integrita dat zajištěna (ochrana proti falešným přístupovým bodům).
- **Extensible Authentication Protocol** (EAP): vzájemná autentizace uživatele i sítě (ochrana proti falešným přístupovým bodům) a distribuce klíčů.

[2]

### 3.5.1 TKIP

Mechanismus TKIP zlepšuje šifrování prostřednictvím tří hlavních prvků:

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

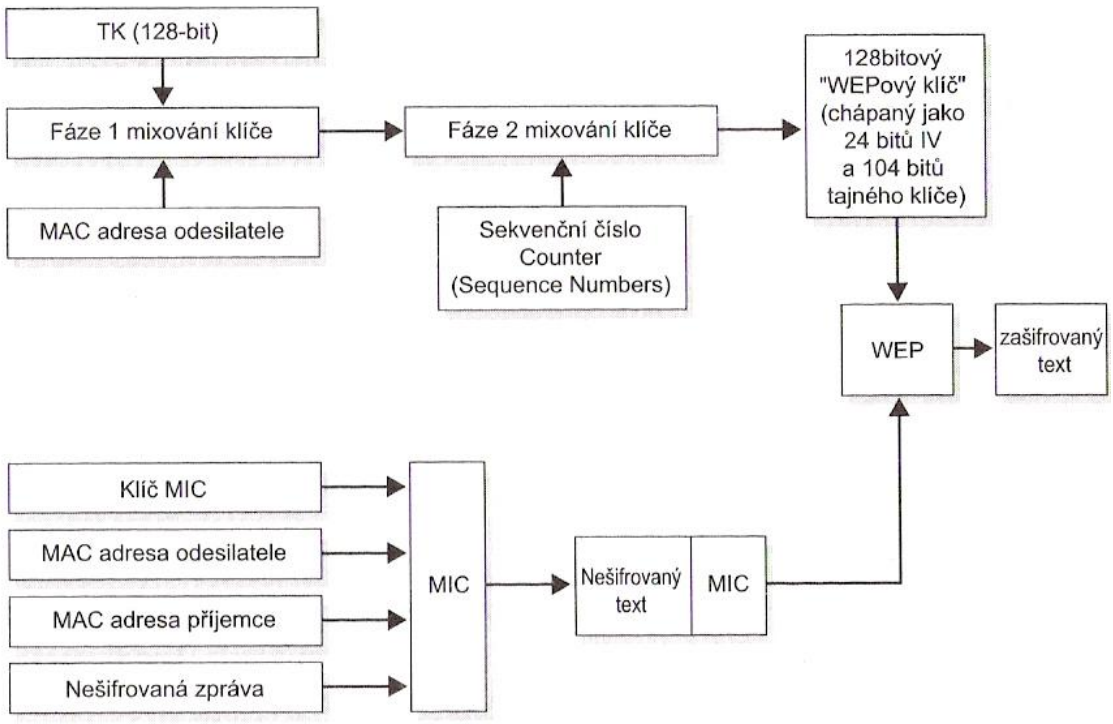
V zásadě představuje TKIP pouze dočasnou opravu protokolu WEP. Kvůli zachování zpětné kompatibility s velkým počtem stávajících instalovaných hardwarových zařízení byly při jeho návrhu učiněny různé kompromisy. Představuje však řešení všech známých problémů protokolu WEP.

Připomeňme si, že problém původního návrhu protokolu WEP spočíval v tom, že hodnota IV se jednoduše připojila k tajnému klíči a předala se generátoru RC4.

U TKIP klient začíná s dvěma klíči – 128bitovým šifrovacím klíčem a 64bitovým klíčem pro zajištění integrity, které získá bezpečnými mechanismy v průběhu iniciální komunikace protokolem 802.1x. Šifrovací klíč se označuje jako TK, Temporary Key. Klíč pro zajištění integrity se označuje jako klíč MIC, Message Integrity Code. V první fázi se provede XOR mezi MAC adresou odesilatele a hodnotou TK, čímž vzniká klíč označovaný jako Fáze 1 (někdy též „mezilehlý klíč“). Klíč Fáze 1 se mixuje se sekvenčním číslem a vzniká tak klíč Fáze 2, pro přenos jediného paketu. Výstup druhé fáze se předává mechanismu WEP jako standardní 128bitový WEPový klíč (ted IV + tajný klíč). Zbytek procesu už probíhá jako klasická transakce protokolem WEP.

Rozdíly spočívají v tom, že v důsledku první fáze už nepoužívají všichni klienti stejný WEPový klíč, a v důsledku druhé fáze už neexistuje korelace mezi hodnotou IV (v tomto případě sekvenčním číslem) a samotnou klíčovací sekvencí. Tento proces se nazývá Fiestelova šifra a navrhli ji Doug Whiting a Ron Rivest.

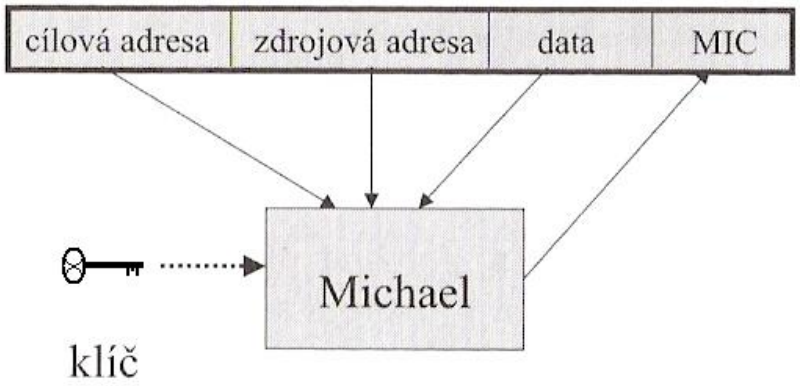
[1]




*Obr. 15. Šifrování mechanismem TKIP [1]*

### 3.5.2 MIC

Pro zajištění integrity zpráv se používá kód MIC (Message Integrity Code). MIC ke každému rámci přidává digitální podpis, čímž zamezuje útoku typu *main-in-the-middle*, kdy by útočník mohl odchytit paket na jeho cestě k příjemci, změnit ho a poslat dál. Digitální podpis se automaticky vypočítá (na základě datové části rámce a zdrojové a cílové MAC adresy, pořadového čísla paketu a náhodné hodnoty) a zabuduje do datové části rámce a následně je celý rámec zašifrován (Obr. 17.)




*Obr. 16. Výpočet MIC [2]*

Na straně příjemce se nejprve zkontrolují hodnoty IV, CRC a ICV, než se zkontroluje samotný MIC. Pokud je MIC v nepořádku, téměř jistě to svědčí o aktivním útoku. Při odhaleném útoku na integritu zprávy se okamžitě přestanou používat aktivní klíče a po minutě dojde k překličování.

Kontrola integrity zprávy se provádí pomocí MIC, který se připojuje ke zprávě a získává se z dat a adres zprávy prostřednictvím funkce přezdívané Michael. Kontrolní součet MIC nahrazuje jednoduchý a nebezpečný vektor ICV používaný u WEP. MIC představuje rovnováhu mezi bezpečností a spotřebou výpočetních zdrojů a implementační náročnost.

MIC má na rozdíl od ICV dvojnásobnou délku a pro jeho vytvoření se používá jednocestná funkce nad některými poli záhlaví a daty rámce. Je odolná vůči útokům, které vyly úspěšné u ICV, jako záměny bitů, falšování záhlaví. Neodolá ovšem některým útokům typu DoS.

## 3.6 802.11i (WPA2)

V lednu roku 2001 byla v institutu IEEE sestavena úkolová skupina *i* za účelem zlepšení autentizace dat standardu 802.11 a bezpečnosti šifrování. Jako reakci na korporátní zájem o bezdrátovou bezpečnost vydala Wi-Fi Alliance (asociace pro propagaci a certifikaci Wi-Fi) v dubnu roku 2003 doporučení. Rovněž si však byly vědomi, že zákazníci by si nebyli ochotni vyměnit své stávající zařízení.

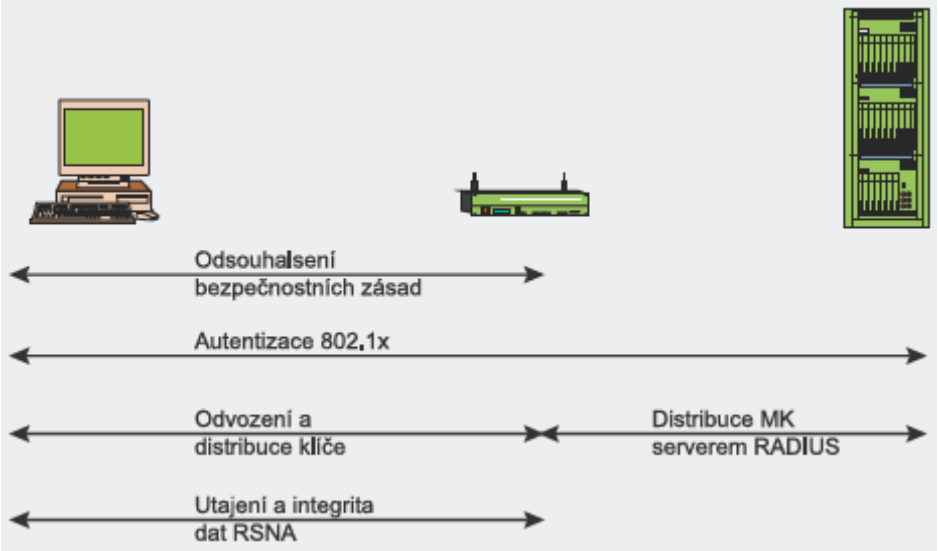
V červnu 2004 bylo schváleno konečné vydání standardu 802.11i, který dostal od asociace Wi-Fi Alliance komerční název WPA2. Standard IEEE 802.11i přinesl takové základní změny jako oddělovaní autentizace uživatele od vynucování integrity a soukromí zprávy, tudíž poskytuje stabilní a škálovatelnou bezpečnostní architekturu vhodnou nejen pro domácí sítě ale i velké podnikové systémy. Nová architektura pro bezdrátové sítě nese označení RSN (*Robust Security Network*) a používá autentizaci 802.1X, silnou distribuci klíčů a nové mechanismy k zajištění integrity a soukromí.

I když architektura RSN je složitější, nabízí bezpečná a škálovatelná řešení pro bezdrátovou komunikaci. Ve většině případech akceptuje RSN pouze zařízení s podporou RSN, nicméně IEEE 802.11i definuje také architekturu TSN (*Transitional Security Network*), do které lze zahrnout jak systémy RSN, tak systémy WEP, což umožní uživatelům včas aktualizovat své zařízení Pokud procedura autentizace nebo asociace použitá mezi stanice využívá 4-fázový handshake, asociace se označuje jako RSNA (*Robust Security Network Association*).

Sestavení bezpečného komunikačního kontextu se skládá ze čtyř fázi (Obr. 18.):

- odsouhlasení bezpečnostních zásad.
- autentizace 802.1X.
- odvozování a distribuce klíče.
- utajení a integrita dat RSNA.

[18]

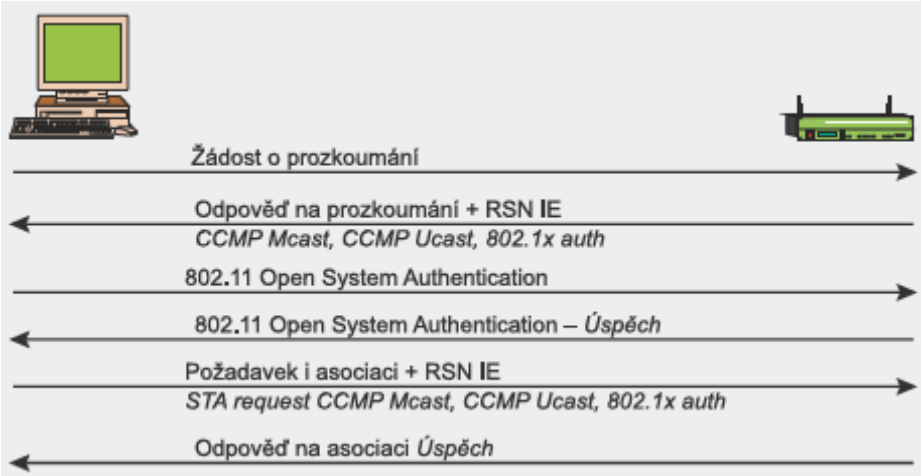



*Obr. 17. Jednotlivé fáze standardu 802.11i [18]*

### 3.6.1 Odsouhlasení bezpečnostních zásad

První fáze vyžaduje, aby se komunikující strany dohodly na bezpečnostních zásadách, které budou používat. Bezpečnostní zásady podporované přístupovým bodem jsou oznámeny ve zprávě *Beacon* nebo *Probe Respond* (následující *Probe Request* od klienta). Poté následuje standardní otevřená autentizace (stejně jako v sítích TSN, kde je autentizace vždy úspěšná). Odezva klienta je obsažena ve zprávě *Association Request*, jejíž platnost je ověřeně pomocí *Association Response* z přístupového bodu. Informace o bezpečnostní zásadě se zašlou v poli RSN IE (*Information Element*) a popisují:

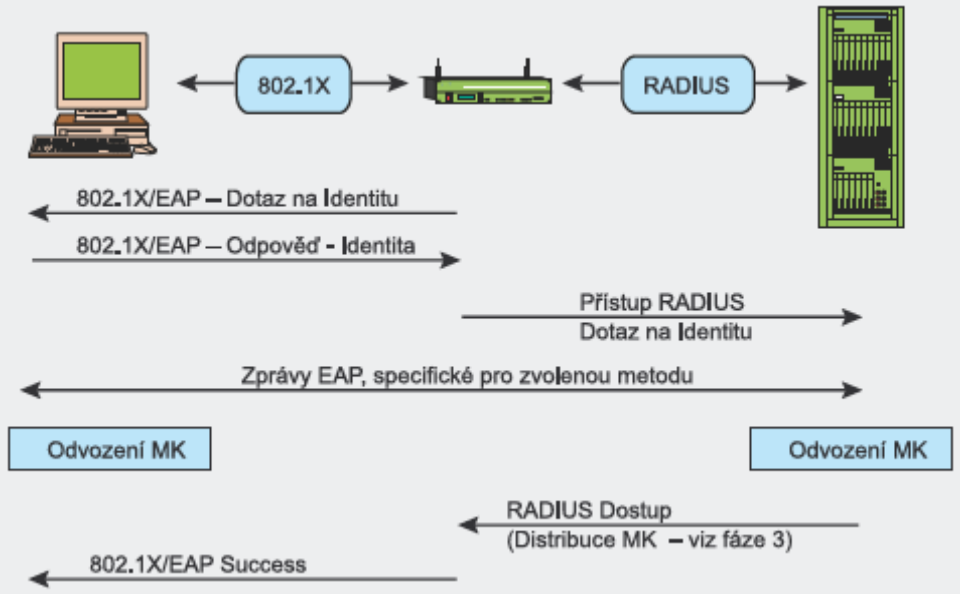
- podporované autentizační metody (802.1X, PSK (Pre-Shared Key)).
- bezpečnostní protokoly pro provoz dílčího vysílání – unicast (CCMP, TKIP a podobně) – sada šifer po dvojicích.
- bezpečnostní protokoly pro provoz skupinového vysílání – multicast (CCMP, TKIP a podobně) – skupinová sada šifer.
- podporu před-autentizace, která v rámci hladkého předání umožňuje uživatelům provést před-autentizaci před přepnutím na přístupový bod stejné sítě.




*Obr. 18. Odsouhlasení bezpečnostních zásad [18]*

### 3.6.2 Autentizace

Druhou fází je autentizacace 802.1X založená na protokolu EAP a dříve odsouhlasené specifické autentizační metodě: EAP/TLS s certifikáty klienta a serveru (vyžadující infrastrukturu veřejného klíče), EAP/TTLS nebo PEAP pro hybridní autentizaci (s certifikáty vyžadovanými pouze pro servery) a tak dále. Autentizace 802.1X se zahájí, když si přístupový bod vyžádá údaje o identitě klienta s odezvou klienta obsahující upřednostňovanou autentizační metodu. Poté proběhne výměna vyhovujících zpráv mezi klientem a autentizačním serverem, aby se vygeneroval společný master klíč (MK). Na konci procedury se z autentizačního serveru na přístupový bod zašle zpráva *Radius Accept* obsahující MK a konečnou zprávu *EAP Success* pro klienta.

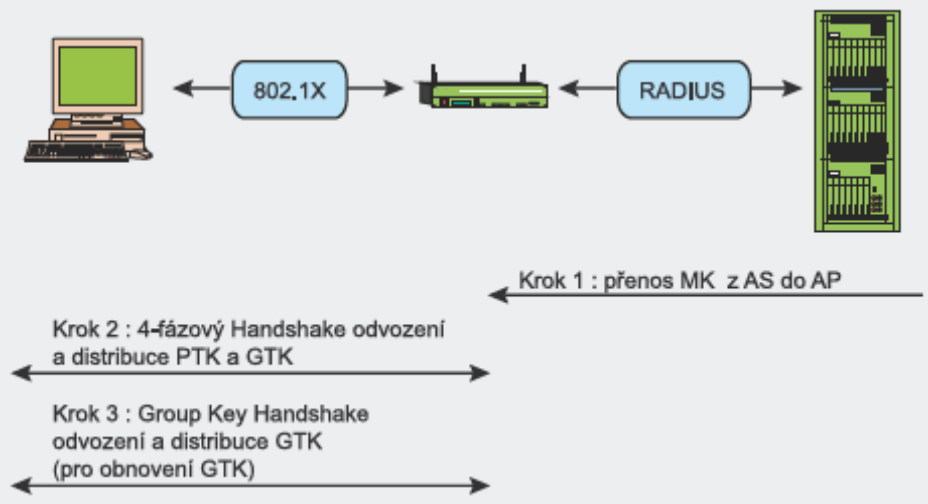



*Obr. 19. Autentizace 802.11i [18]*

### 3.6.3 Hierarchie klíčů a distribuce

Bezpečnost připojení značně závisí na bezpečnosti klíčů. V RSN má každý klíč omezenou životnost a celková bezpečnost se zajišťuje pomocí kolekce různých klíčů, které jsou hierarchicky uspořádané. Jakmile se po úspěšné autentizaci stanoví bezpečnostní kontext, vytvoří se dočasné (relační) klíče, které se pravidelně aktualizují, dokud se bezpečnostní kontext nezavře. Generování a výměna klíčů je cílem třetí fáze. V průběhu odvozování klíče nastanou dva handshaky (viz Obrázek 7):

- *4-Way Handshake* pro odvození PTK (*Pairwise Transient Key*) a GTK (*Group Transient Key*)
- *Group Key Handshake* pro obnovení GTK.
- Odvození PMK (*Pairwise Master Key*) závisí na používané autentizační metodě:
- Používá-li se PSK (*Pre-Shared Key*), PMK = PSK. PSK se generuje z hesla, které tvoří více slov či shluků znaku (od 8 do 63 znaků) nebo 256bitového řetězce a poskytuje řešení pro domácí sítě a malé podniky, které nemají autentizační server.
- Používá-li se autentizační server, PMK se odvodí z autentizace 802.1X MK.




*Obr. 20. Odvození a distribuce klíče [18]*

K šifrování nebo kontrolu integrity se však nikdy nebude používat samotný PMK, slouží totiž pro generování dočasného šifrovacího klíče – u provozu unicast to je PTK (*Pairwise Transient Key*). Délka PTK je odvislá od šifrovacího protokolu: 412 bitů u TKIP a 384 bitů u CCMP. PTK se skládá z několika přidělených dočasných klíčů:

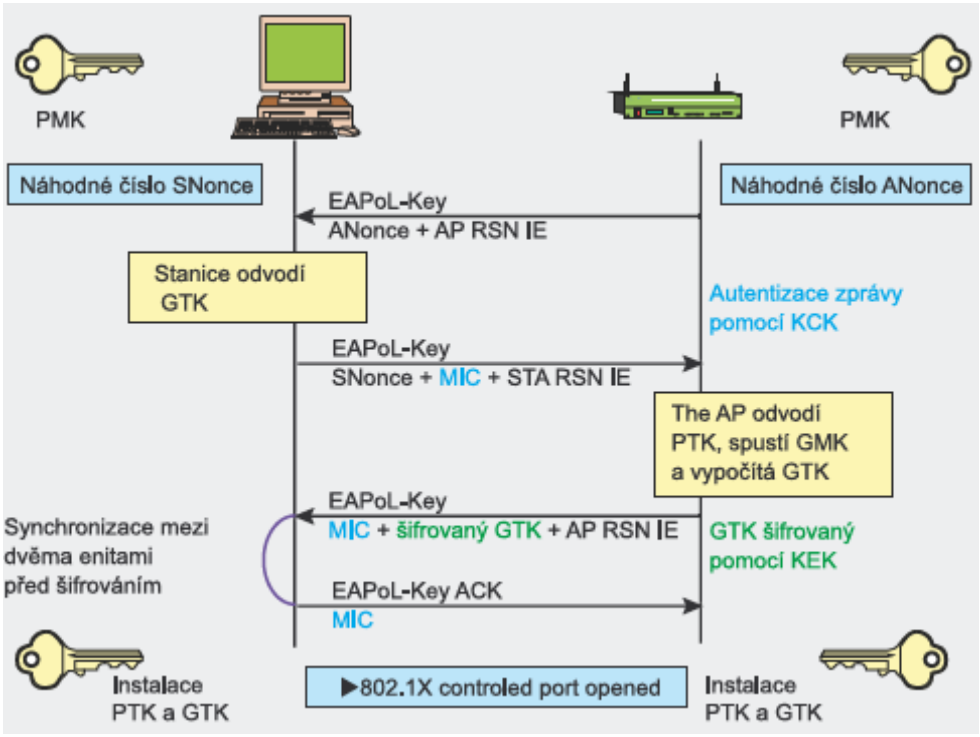
- KCK (*Key Confirmation Key* – 128 bitů): Klíč pro autentizační zprávy (MIC) během *4-Way Handshake* a *Group Key Handshake*,
- KEK (*Key Encryption Key* – 128 bitů): Klíč pro zajištění utajení dat během *4-Way Handshake* a *Group Key Handshake*,
- TK (*Temporary Key* – 128 bitů): Klíč pro šifrování dat (používaný TKIP a CMMP),
- TMK (*Temporary MIC Key* – 2x64 bitů): Klíč pro autentizaci dat (pracuje s ním pouze algoritmus Michael s TKIP). Přidělený klíč se používá na každé straně komunikace.

*4-Way Handshake* spuštěný přístupovým bodem umožňuje:

- potvrdit, že klient zná PMK,
- odvodit nový PTK,
- instalovat klíče šifrování a integrity,
- šifrovat přenos GTK,

- potvrdit výběr sady šifer.

Mezi klientem a přístupovým bodem se v průběhu *4-Way Handshake* vymění čtyři zprávy EAPOL-Key. Tento proces je znázorněn na Obrázku 22.




*Obr. 21. 4-Way Handshake [18]*

PTK se odvodí z PMK, pevného řetězce, MAC adresy přístupového bodu, MAC adresy klienta a dvou náhodných čísel (*ANonce* a *SNonce* generovaných autentizátorem a supplicantem v uvedeném pořadí). První zprávu spustí přístupový bod výběrem náhodného čísla *ANonce* a jeho zasláním supplicantu bez šifrování zprávy nebo jiné ochrany před zfalšováním. Supplicant generuje své vlastní náhodné číslo *SNonce* a nyní může vypočítat PTK a odvozené dočasné klíče, takže pomocí klíče KCK zašle *SNonce* a klíč MIC vypočítaný z druhé zprávy. Jakmile autentizátor obdrží druhou zprávu, může vytáhnout *SNonce* (protože zpráva není šifrována) a vypočítat PTK a odvozené dočasné klíče. Nyní může ověřit hodnotu MIC ve druhé zprávě a tudíž se ujistit, že supplicant zná PMK a má správně vypočítaný PTK a odvozené dočasné klíče.

Třetí zpráva zaslaná autentizátorem supplicantu obsahuje GTK (šifrované pomocí klíče KEK), odvozené z náhodného GMK a *GNonce* (podrobnosti viz Obrázek 10) spolu s MIC vypočítaným ze třetí zprávy pomocí klíče KCK. Když supplicant obdrží zprávu, v rámci

zajištění, že autentizátor zná PMK a má správně vypočítaný PTK a odvozené dočasné klíče, se ověří hodnota MIC.

Poslední zpráva potvrzuje dokončení celého handshake a udává, že supplicant nyní nainstaluje klíč a spustí šifrování. Při přijetí instaluje autentizátor, jakmile ověří hodnoty MIC, své klíče. Tudíž mobilní zařízení a přístupový bod získaly, vypočítaly a nainstalovaly šifrovací klíče a nyní jsou schopny komunikovat prostřednictvím bezpečného kanálu pro provoz dílčího a skupinového vysílání.

Provoz skupinového vysílání, nebo-li multicast, je chráněn jiným klíčem – GTK (*Group Transient Key*), který se generuje z master klíče s názvem GMK (*Group Master Key*), pevného řetězce, MAC adresy přístupového bodu a náhodného číslo *GNonce*. Délka GTK závisí na šifrovacím protokolu – u TKIP má 256 bitů a u CCMP má 128 bitů. GTK se dělí na dočasné klíče:

- GEK (*Group Encryption Key*): Klíč pro šifrování dat (používá ho protokol CCMP pro autentizaci a šifrování a protokol TKIP),
- GIK (*Group Integrity Key*): Klíč pro autentizaci dat (používá ho pouze algoritmus Michael s protokolem TKIP).

Mezi klientem a přístupovým bodem se v průběhu *Group Key Handshake* vymění dvě zprávy *EAPOL-Key*. Tento handshake využívá dočasné klíče generované v průběhu *4-Way Handshake* (KCK a KEK). Tento proces je znázorněn na Obrázku 11.

*Group Key Handshake* je potřeba pouze k deasociaci hostitele a k obnovení GTK na požadavek klienta. Výběrem náhodného čísla *GNonce* a vypočítáním nového GTK spustí autentizátor první zprávu. Zašle supplicantu šifrovaný GTK (pomocí KEK), pořadové číslo GTK a kód MIC vypočítaný z této zprávy pomocí KCK. Jakmile supplicant zprávu obdrží, MIC se ověří a je možné GTK dešifrovat.

Druhá zpráva potvrzuje dokončení *Group Key Handshake* zasláním pořadového čísla GTK a kódu MIC vypočítaného na této druhé zprávě. Při přijetí autentizátor instaluje nový GTK (po ověření hodnoty MIC).

### 3.6.4 Utajení a integrita dat RSNA

Všechny dříve generované klíče se používají v protokolech podporující utajení a integritu dat RSNA:

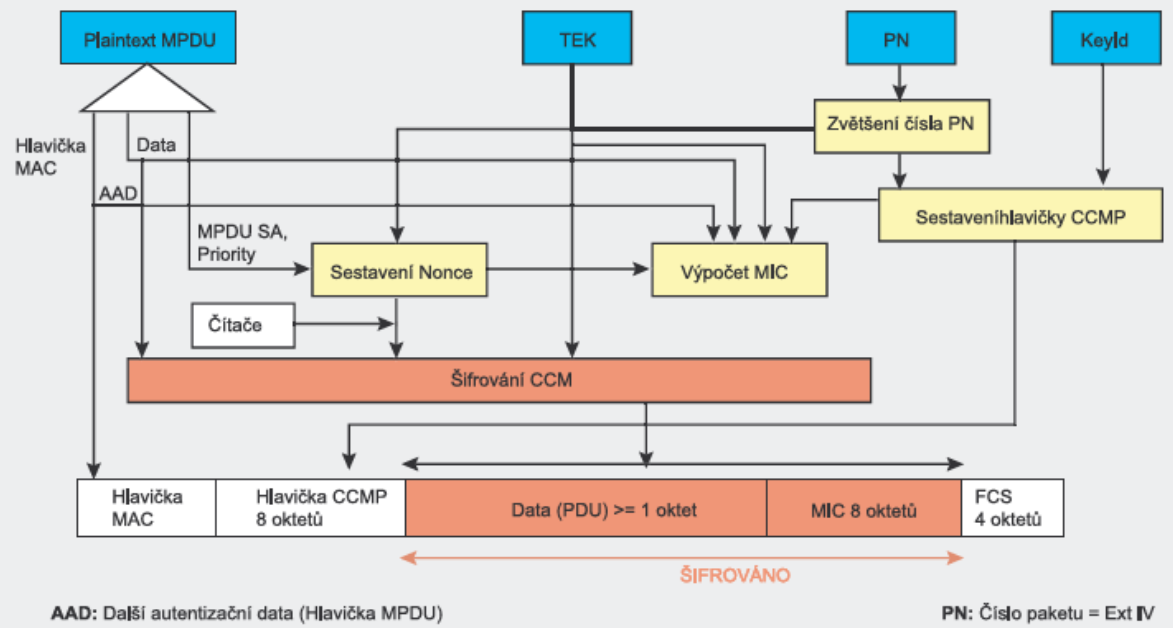
- TKIP (*Temporal Key Hash*).
- CCMP (*Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol*).
- WRAP (*Wireless Robust Authenticated Protocol*).

Dříve, než si tyto protokoly podrobně vysvětlíme, je třeba pochopit důležitý koncept : rozdíl mezi MSDU (*MAC Service Data Unit*) a MPDU (*MAC Protocol Data Unit*). Obojí se odvolává na jediný paket dat, ale MSDU představuje data před fragmentací, kdežto MPDU představuje více datových jednotek po fragmentaci. Rozdíl je důležitý v šifrování protokolů TKIP a CCMP, jelikož v TKIP se MIC vypočítá z MSDU, kdežto v CCMP se vypočítá z MPDU.

- **Protokol TKIP** viz. 3.5.1
- **Protokol CCMP** je založen na skupině blokových šifer AES (*Advanced Encryption Standard*) v jejich provozním režimu CCM s klíčem a bloky o délce 128 bitů. AES představuje pro protokol CCMP totéž, čím je RC4 pro protokol TKIP, avšak na rozdíl od TKIP, jehož záměrem bylo přizpůsobit se stávajícímu hardwaru WEP, CCMP nepředstavuje žádný kompromis, nýbrž zcela nový návrh protokolu. Protokol CCMP vytváří kód MIC pomocí režimu čítače a metody autentizace zprávy označované jako *Cipher Block Chaining* (CBC-MAC). Rovněž byly přidány určité zajímavé funkcionality, například použití jediného klíče k šifrování a autentizaci (s různými inicializačními vektory) nebo pokrývání nešifrovaných dat pomocí autentizace. Protokol CCMP přidává k MPDU 16 bajtů: 8 bajtů pro hlavičku CCMP a 8 bajtů pro MIC. Hlavička CCMP je nešifrované pole obsažené mezi hlavičkou MAC a šifrovanými daty obsahující 48bitové PN (*PacketNumber* = rozšířený IV) a *Group Key KeyID*. Pro každou následnou MPDU se PN zvýší o hodnotu jedna. K získání konečného kódu MIC o velikosti 64 bitů (konečný kód MIC je 128bitový blok, jelikož dolních 64 bitů se vyřadí) využívá výpočet MIC algoritmus CBC-MAC, který šifruje počáteční nonce blok (vypočítaný z polí *Priority*, zdrojové adresy MPDU a zvýšeného PN) a XORy následných bloků. Následně se kód MIC připojí k nešifrovaným datům pro šifrování AES v režimu čítače. Čítač se sestaví z nonce, které se podobá nonce

MIC, ale má zvláštní pole čítače s výchozí hodnotu 1, které se zvýší pro každý blok.

- **Protokol WRAP,** který je rovněž založen na AES, používá režim OCB (*Offset Codebook Mode*) autentizovaného šifrovacího schématu (šifrování a autentenizace se provede v jediném výpočtu). Pracovní skupina IEEE 802.11i nejprve vybrala režim OCB, ale posléze se kvůli problémům s duševním vlastnictvím a možným licenčním poplatkům od něj upustilo. Následně byl přijat protokol CCMP jako povinný.




*Obr. 22. Šifrování protokolu CCMP*

# II. PRAKTICKÁ ČÁST

# 4 POROVNÁNÍ METOD ZABEZPEČENÍ

## 4.1 WEP vs. WPA vs. WPA2

Jak jsem již uvedl v teoretické části, protokol WEP nebyl konstruován jako bezpečnostní algoritmus, ale pouze jako prostředek pro zachování nedostupnosti dat při přechodu z metalické části sítě do bezdrátového vysílání. Bylo tedy jen otázkou času, kdy se najdou první způsoby, jak tento způsob zabezpečení obejít. Přesto však poskytuje určitou míru zabezpečení a méně zkušený nebo nezkušený útočník si nedokáže s jeho prolomením tak snadno poradit.

Protokol WEP obsahuje velké množství dnes již obecně známých zranitelných míst, které se snažily vyřešit následné šifrovací algoritmy, WPA a WPA2.

Prvním slabým článkem protokolu WEP je samotný inicializační vektor IV. Jeho rozsah 24bitů mu dává $2^{24}$ kombinací což je 16 777 216. Toto číslo se může zdát na první pohled dostatečně velké, vezmeme-li však potaz hustotu síťového provozu a fakt, že ne všechny hodnoty ze zmíněného rozsahu jsou pro šifrování vhodné, je jasné, že čísla se velice brzy začnou opakovat.

V návaznosti na první uvedenou slabinu protokolu WEP je vhodné uvést problém šifrovacího algoritmu RC4, který je u protokolu WEP použit. Samotná šifra RC4 problém nepředstavuje, tím je až způsob, jakým byla u protokolu WEP použita. Jelikož se jako šifrovací klíč používá inicializační vektor IV a ten se, jak sem již uvedl, může po čase začít opakovat, a tím dojde k porušení jednoho ze základních pravidel při šifrování.

Další slabé místo tvoří jednostranná autentizace u protokolu WEP. Uživatel, který se připojí do sítě chráněné protokolem WEP, nemá jistotu, že AP, ke kterému se připojil, je skutečně autorizované. Útočník, který předem rozluštil WEP klíč tak může snadno podstrčit neautorizovaný AP.

Výše popsané nedostatky však neznamenají, že je protokol WEP nepoužitelný. Rozhodně je lepší než nic, a pro sítě s nízkým bezpečnostním rizikem je naprosto dostačující a jeho implementaci zvládnou i méně zkušení živitelé.

Protokol WPA představuje pouze dočasné řešení před uvedením normy 802.11i, i tak však představoval velký krok kupředu v zabezpečení bezdrátové komunikace. Novinkami, které zavedl, byla oboustranná autentizace 802.1x a šifrovací protokol TKIP. Jeho primárním

úkolem bylo řešení hlavních nedostatků protokolu WEP a to se také povedlo. Zavedl dynamické generování klíčů, kontrolu integrity zpráv a číslování paketů. Stále však používá mechanismu RC4 stejně jako WEP. Jednou z největších výhod WPA byla též zpětná kompatibilita s již používanými zařízeními, takže k jeho implementaci stačilo pouze aktualizovat firmware.

Norma IEEE 802.11i, označovaná též jako WPA2, byla vydána v roce 2004. Primárně se zaměřuje na autentizaci a utajení datových rámců a přinesla protokol CCMP a blokový šifrovací algoritmus AES. O autentizaci a zprávu klíčů se stará protokol 802.1x. AES je považován za dostatečně bezpečný algoritmus, používá 128, 192 nebo 256 bitové klíče.

Následující tabulka znázorňuje použité metody zabezpečení pro jednotlivé způsoby zabezpečení :

*Tab. 3. Porovnání použitých bezpečnostních metod u WEP, WPA a WPA2*

| | **WEP** | **WPA** | **WPA2** |
|---|---|---|---|
| **Autentizace** | otevřená | 802.1x (EAP-MD5, EAP-TLS, PEAP) | 802.1x (EAP-MD5, EAP-TLS, PEAP) |
| **Šifrování** | statický WEP | TKIP/CKIP | AES |

*Tab. 4. Porovnání odolnosti WEP, WPA a WPA2 vůči útokům*

| | **WEP** | **WPA** | **WPA2** |
|---|---|---|---|
| **Útok :** | **Odolnost :** | | |
| Na integritu a důvěrnost dat, Man-In-The-Middle | Dobrá | Lepší | Nejlepší |
| Falešná autentizace | Nic moc | Nejlepší | Nejlepší |
| Na slabý klíč | Nic moc | Nejlepší | Nejlepší |
| Falšované pakety | Minimální | Nejlepší | Nejlepší |
| Falešný přístupový bod | Minimální | Lepší | Lepší |

Z tabulky (Tab. 4.) vyplývá, že v porovnání protokolů WEP, WPA a WPA2 poskytuje nejsilnější zabezpečeni protokol WPA2. Proto je v sítích s vysokými bezpečnostními požadavky vhodná implementace tohoto bezpečnostního protokolu.

# 5 ZABEZPEČENÍ BEZDRÁTOVÉ SÍTĚ V PRAXI

## 5.1 Navržení bezpečnostních zásad pro WLAN

Při implementaci zabezpečení do bezdrátové sítě bychom měli vzít v potaz účel, ke kterému bude síť využívána a kde ji realizujeme. Obecně totiž platí, že čím větší chceme bezpečnost, tím větší náklady budeme muset investovat do zařízení.

Je jasné, že pokud chceme zabezpečit malou domácí síť, která bude sloužit pouze pro bezdrátové připojení k internetu a pořádání herních LAN párty, není ji potřeba zabezpečovat těmi nejdokonalejšími prostředky, které budou náročné nejen po finanční stránce, ale také po stránce administrační. Jiná situace ovšem nastává, pokud jde o bezdrátovou síť ve firmě, kde hrozí únik citlivých dat, zneužití osobních údajů aj. Zde se již vyplatí do zabezpečení investovat a udržovat ho aktuální.

Bezdrátové sítě lze podle stupně bezpečnostního ryzika rozdělit do tří základních skupin :

- Domácí a SOHO sítě – nízká bezpečnostní rizika
- Malé kanceláře a vzdálený přístup – střední bezpečnostní rizika
- Firemní sítě – vysoké bezpečnostní ryzika

### 5.1.1 Nízká bezpečnostní rizika – domácí a SOHO sítě

Domácí sítě a sítě malých kanceláří SOHO (small office / home office) představují neatraktivní cíl pro hackery, protože infiltrovat se do takové sítě zpravidla nepředstavuje větší zisk, než zdarma přístup k internetu, cena dat v takových sítích je pro útočníka nulová. Takovéto sítě jsou velmi citlivé na cenu a na nároky na administraci – uživatelé požadují co nejjednodušší administraci a nízkou cenu.

Zabezpečení takové sítě se zaměřuje především na odstranění základních a snadno odhalitelných chyb v zabezpečení tak, aby se potenciálnímu útočníkovi nevyplatilo zabezpečení prolamovat, protože by to znamenalo příliš mnoho práce za tak hubený výsledek.

**Doporučené kroky zabezpečení :**

- **Aktualizace firmware –** proveďte aktualizaci ihned po zakoupení AP a pravidelně kontrolujte dostupnost nových updatů

- **Aktivace WEP –** zvolte nejvyšší možné zabezpečení WEP, má sice svoje slabiny ale je lepší jak nic a méně zkušené útočníky odradí.
- **Změna SSID / zrušení vysílání SSID** – změňte SSID než jaké má AP nastaven z výroby, volte takové názvy, které neodpovídají názvu firmy, jménu nebo adrese. Pokud je to možné, vypněte vysílání SSID úplně. Win. XP a některé programy jej sice i tak dokáží zachytit, ale méně zkušeného útočníka to opět zmate.
- **Filtrace MAC adres** – MAC adresa síťové karty lze sice změnit, ale ne každý ví jak na to a v kombinaci s WEP šifrováním tvoří slušné zabezpečení.
- **Používat firewall** – oddělte přístup z WLAN do Internetu firewalem, abyste zamezily průnikům z Internetu. Pokud vlastníte nějaká citlivá data, oddělte je také nějakou formou firewallu od bezdrátové sítě.
- **Co nejdříve přejít na WPA** – v dnešní době dostupné na téměř všech AP, poskytuje větší míru zabezpečení a jeho aktivace je stejně jednoduchá jako u WEP šifrování.

### 5.1.2 Střední bezpečnostní rizika – malé kanceláře a vzdálený přístup

- **Aktualizace firmware**
- **Aktivujte WEP**
- **VPN** – Pokud je to možné, používejte přístupové body s podporou IPSec, které mohou zajistit zabezpečený tunel mezi koncovým uživatelem a přístupovým bodem. VPN může poskytovat silné zabezpečení!
- **Access point** – Zabezpečte přístup k administraci přístupového bodu dobrým heslem a pravidelně jej měňte. Ujistěte se, že u všech bodů jste změnily výrobcem přednastavená hesla, jsou profláknutá a snadno je lze dohledat!
- **Pozor na SNMP** – možnost administrace přístupových bodů pomocí protokolu SNMP přináší jistá rizika. Protokol SNMP původně přenášel hesla nekódovaně a až od SNMP v3 jsou bezpečně kódovaná. Pokud si nejste jisti, jakou verzi váš AP používá, raději SNMP administraci zakažte.

- Měňte často WEP klíče a další hesla. Pokud je uživatelům zasíláte e-mailem, používejte pro zakódování programy typu PGP, hesla po síti neposílejte v nezakódované podobě
- Zajistěte patřičnou fyzickou bezpečnost síťových prvků. Přístupové body umísťujte vysoko na zeď, nikoli na stůl, kde se k nim každý nepozorovaně dostane. Nezapomínejte na to, že mnoho přístupových bodů je možné resetováním uvést do továrního nastavení a zrušit tak heslo.

### 5.1.3 Vysoké bezpečnostní rizika – firemní sítě

Pro bezdrátové firemní sítě je zpravidla vyžadována stejná míra zabezpečení a podpory služeb, jako u firemního Ethernetu. Proto pro ně platí vše, co tu již bylo uvedeno a k tomu ještě něco navíc :

- **Monitoring podvržených přístupových bodů** – mějte přehled o tom, kolik a kde umístěných přístupových bodů ve vaší síti je. Použijte programy nebo speciální analyzery sítě a občas projděte vaši bezdrátovou síť a hledejte, zda vám nepřibyl nějaký podvržený přístupový bod. Nezapomínejte na to že nemusí jit a hackera, kdo ho tam dal.
- **Access controler** – Přístupové body nabízejí velmi nedostatečnou autentizaci. Přemýšlejte o tom, zda by nebylo dobré zařadit do sítě nějaký *access controler*, tedy zařízení nabízející možnost autentizaci vůči serveru RADIUS. I některé přístupové body autentizaci vůči RADIUS nebo LDAP serveru již podporují, případně lze dokoupit samotný *access controler*. EAP a 8O2.1X poskytnou další zabezpečení
  a autentizaci, v případě ještě vyšších nároků můžete používat pro autentizaci i digitální certifikáty.
- **Pokrytá oblast** – Minimalizujte vysílání signálu mimo oblast firmy, tam kam je běžný veřejný přístup. Parkoviště, parčík před firmou jistě nemusí být pokryté signálem. Používejte sektorové antény a směrujte je tak, aby pokrývaly vnitřní a veřejnosti nepřístupné prostory firmy. V případě nutnosti utlumte signál přístupových bodů v rozích budovy tak, aby síť nebyla zachytitelná mimo budovu.

- **Bezdrátová zóna** – efektivní možnost, jak zabezpečit firemní síť proti točníkům z bezdrátové sítě, je vytvoření bezdrátové zóny. Přístupové body vyčleňte do DMZ (demilitarizovaná zóna sítě) a vytvořte bezdrátovým uživatelům tunel do sítě pomocí VPN.
- **DHCP** – Většina bezdrátových sítí má výrobně nastaveno automatické přidělování IP adres pomocí DHCP. DHCP ovšem není schopno odlišit oprávněného uživatele od hackera, a tak kdokoliv, kdo zná správné SSID, může dostat přidělenou IP adresu z DHCP serveru. Vypnutím automatického přidělování IP adres můžete značně minimalizovat možnost, že by hacker zjistil správnou IP adresu. Nezapomeňte změnit přednastavený rozsah IP adres – mnoho bezdrátových směšovačů přiděluje adresy počínaje rozsahem 192.168.0.1 a to je to první, co hacker zkouší.

  Rozsahy IP adres pro vnitřní sítě :

  - **10.0.0.0 – 10.255.255.255**
  - **172.16.0.0 – 172.31.255.255**
  - **192.168.0.0 – 192.168.255.255**

## 5.2 Prostředky k bezpečné firemní síti

### 5.2.1 Bezpečnostní studie

Bezpečnostní studie tvoří první krok při řešení problematiky informační bezpečnosti. Jejím cílem je zmapovat situaci v organizaci, najít všechna důležitá aktiva, určit jejich důležitost pro firmu a odhalit největší bezpečnostní chyby. Nedílnou součást tvoři i návrh základních nápravných opatření.

Tato bezpečnostní studie se obecně nemusí týkat jen síťového řešení ve firmě. Jelikož na bezpečnost jako takovou by se mělo pohlížet komplexně, měla by se týkat většího spektra oblastí, a to :

- Fyzická bezpečnost
- Personální bezpečnost
- **Bezpečnost IT**

- Logická bezpečnost
- Legislativní otázky

Takováto bezpečnostní studie by měla tvořit podklad pro definování Bezpečnostní politiky firmy včetně Bezpečnostní politiky firemní sítě.

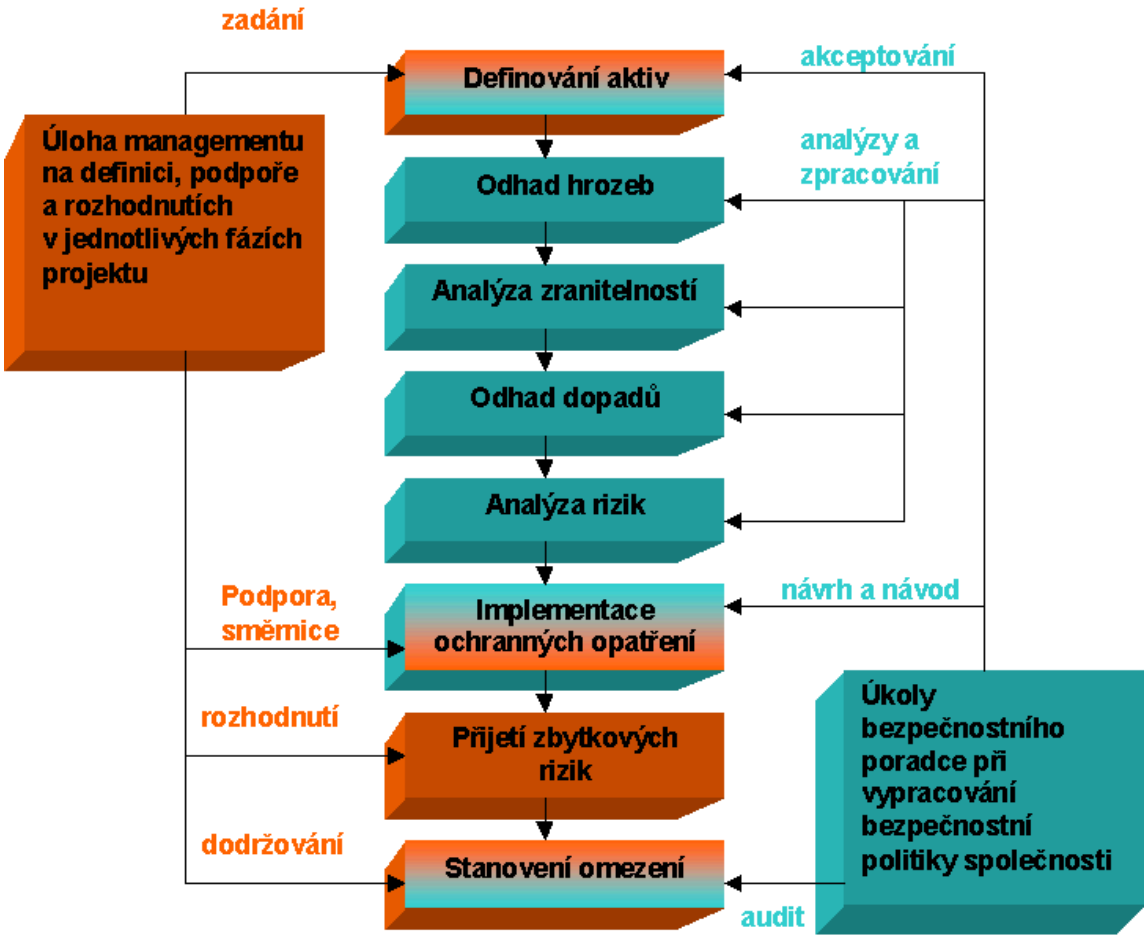
### 5.2.2 Bezpečnostní politika firemní sítě

Bezpečnostní politika by měla tvořit základ při budování a provozu každé firemní sítě a každý správce sítě by měl vyžadovat její důsledné dodržování.

Bezpečnostní politika je obecně založena na principu rozpoznání autorizovaného a neautorizovaného chování. Dohodnutá bezpečnostní politika se implementuje za použití různých mechanismů, které slouží k prevenci, detekci nebo nápravě. Bezpečnostní politika podnikové sítě musí podporovat cíle celého podniku, musí být jasně definovaná jako součást organizačního řízení a odpovědnosti musí být jasně deklarovány. Politiku je třeba také periodicky prověřovat, nejlépe externími zdroji. Současně musí být použité bezpečnostní prostředky i nákladově efektivní, s vědomím, že 100% zabezpečení nelze nikdy dosáhnout. Bezpečnostní politika musí být také naplnitelná a použitelná zaměstnanci, proto při její přípravě musí být brán ohled na potřeby všech podnikových oddělení.[2]

Bezpečnost WLAN nelze oddělit od celkového řešení bezpečnosti sítě. Nejde jen o zabezpečení bezdrátové komunikace, ale o řešení bezpečnosti na všech vrstvách síťové architektury, od fyzického zabezpečení po virtuální privátní sítě či SSL. [2]

Při vypracovávání bezpečnostní politiky se postupuje v následujících korcích :




*Obr. 23. Postup při vypracovávání bezpečnostní politiky*

Výsledkem je návrh a implementace ochranných opatření, vypracování směrnic, pravidel a postupů zacházení s datovými aktivy v organizaci.

Takto zpracovaná bezpečnostní politika může být již podkladem při posuzování organizace dle zákona č.148/1998 Sb. o ochraně utajovaných skutečností .

### 5.2.3 Bezpečnostní audit WLAN

Jedinou účinnou možností, jak ověřit zabezpečení WLAN a předejít případným útokům, je podívat se na síť očima hackera. Dnes již existuje řada firem, které nabízejí vyhotovení bezpečnostního auditu bezdrátové sítě. Z výsledné zprávy pak lze snadno vyčíst kde jsou slabá místa a na které aspekty zabezpečení je třeba se zaměřit. Pro názornost uvádím ve stručnosti jeden z možných postupů při takovém auditu :

1. **zjištění autorizovaných přístupových bodů** – prostřednictvím prostředků pro sledování inventáře vytvořit mapu AP pod vlastní správou.

2. **analýza síťového provozu** – rámce 802.11, otevřený datový přenos (např. protokoly Telnet, POP, IMAP, http, FTP, IRC, IM posílají nejen data, ale i identifikační údaje uživatelů v otevřené formě), autentizační protokoly, DHCP (dojednávání zapůjčení IP adres v sobě má řadu informací potenciálně zajímavých pro útočníka, samozřejmě včetně IP adresy samotné pro krádež identity), směrovací protokoly (informace mohou útočníkovi sdělit logickou topologii sítě), Syslog a NTP. Protokoly jako STP, NEJBIOS nebo SNP síť zbytečně zahlcují a mohou znamenat bezpečnostní slabinu. Provoz mimo pracovní dobu (možné zneužívání WLAN po pracovní době).
3. **přidružení k WLAN a detekování monitorů** – detekce všech dostupných sítí, odlišení vlastní od cizí, prověření nebezpečí přidružení k cizí (sousední) síti (únik citlivých informací, možnost propojení s vlastní podnikovou sítí).
4. **identifikace přítomných klientů** – ne každý klient je detekovatelný prostřednictvím pasivního monitoru.
5. **využití slabých míst ve WLAN** – v aktivní fázi testování je potřeba nalézt potenciálně nebezpečné klienty a zjistit, jaké útoky na nich lze spáchat.
6. **přechod z WLAN do další části sítě** – připojení AP do přepínače podnikové sítě dává útočníkům mnoho možností rozšířit útok prostřednictvím průniku z WLAN do celé podnikové sítě. Obranou je firewall oddělující WLAN od zbytku sítě – přímý útok proti ní nebývá úspěšný, a navíc vede k zachycení IDS a zaznamenání útoků (útočník ale může přejít na útok na vyšší vrstvě síťové architektury).
7. **prověřit pravidla filtru mezi bezdrátovou a pevnou sítí**

### 5.2.4 monitorování WLAN

Řada výrobců nabízí prostředky pro monitorování média, které jsou součástí centralizovaného managementu bezdrátových sítí. Monitorováním lze detekovat neautorizované přístupové body a upozornit na ně správce dané sítě. Zjištění, zda někdo neodposlouchává WLAN, je velmi obtížné, ale se znalostí odlišností různých běžně dostupných prostředků pro odposlouchávání (např. NetStumbler) je lze podle jejich vzorku restování sítě (probing) při dostatečném počtu vysílaných paketů odhalit, alespoň co do existence.

**Monitorování WLAN by se mělo integrovat do monitorování provozu celé podnikové sítě !**

WLAN analyzátory pro podrobné sledování provozu potřebují specializované ovladače pro umožnění režimu RFMON (Radio Frequency Monitoring) na adaptéru 802.11. Analyzátory mohou pracovat ve skenovacím režimu, kdy postupně přecházejí mezi více kanály nebo SSID. První případ se hodí pro detekci rádiového dění v okolí, zatímco druhý pak poskytuje podklady pro podrobnou analýzu a řešení problémů. Analyzátory samozřejmě nemusejí sbírat veškerý provoz: prostřednictvím filtrů je lze nastavi na sběr paketů podle zdroje, cíle nebo protokolu, případně je možné nastavit určitý vzorec provozu, na základě něhož se uvedou do provozu (např. v případě nového přístupového bodu). Snímaný provoz lze využít při monitorování v reálném čase, nebo se může ukládat do vyrovnávací paměti či do souboru pro pozdější zkoumání.

Nasnímaný provoz lez zpracovávat mnoha způsoby :

- sumárně pro přístupový bod, stanici nebo kanál
- dekódování obsahu paketů prostřednictvím čitelných hodnot polí v paketu
- s použitím mapování zobrazení jmen místo numerických adres
- filtrace informací z nasbíraných dat
- rekonstrukce relací TCP nebo aplikačních dialogů
- zobrazení statistik (tabulek nebo grafů) využití sítě, chybovosti apod.
- vytváření map pro zobrazení vazeb a toků mezi uzly v síti
- generování poplašných zpráv jako varování při neočekávaném provozu či potenciálních problémech
- poskytování analýzy vázané na konkrétní protokol na základě varovných signálů a doporučení

Analyzátory vykovávají další funkce související s plánováním a správou WLAN :

- **analýza spektra** - identifikace jiných než 802.11 signálů.
- **stumbling** – odhalení WLAN prostřednictvím pouhého sledování *beacons*, pomocí GPS upřesnění jejich umístění.

- informace o **potenciálních neautorizovaných/nových AP.**
- **záznam signálu a rušení** ve vazbě na místo.
- snímání provozu na **vzdálených místech** (*probes*) jako podklad pro IDS.
- **Dekódování zašifrovaného provozu** v případě zadání klíčů.
- Řešení problémů WLAN prostřednictvím aktivní práce analyzátoru v síti jako klienta

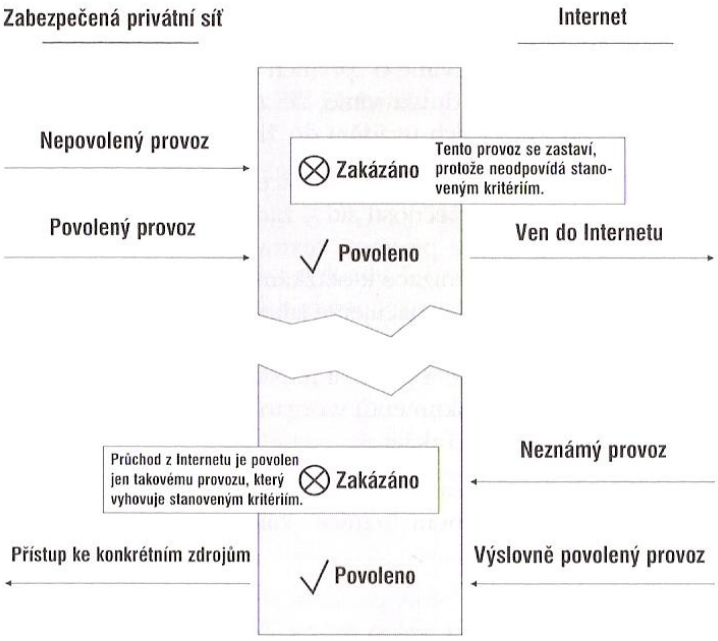
Generace prostředků monitorování WLAN

- **přenosné skenery** – jednoduché zařízení, ve větším rozsahu ovšem obtížně hledají falešné AP nebo klientská zařízení v pohybu. Vhodné pro ukázku a management, nikoli pro dlouhodobý, průběžný monitoring.
- **distribuované (optimalizované) senzory** – lepší než běžné AP, umožňují detekci AP a zařízení, detekci narušení, monitorování politiky, základní podávání zpráv.
- **hybridní řešení** – distribuované senzory s korelací na straně pevné sítě: vztahy a vazby, znalost chování zařízení a aplikací, dolování dat, nalezení i transientních zařízení na nečekaných kmitočtech.

### 5.2.5 Firewall

Firewall kontroluje síťový provoz, který vstupuje do některého z jeho rozhraní, a aplikuje na něj takzvaná *pravidla*, na základě nich pak v podstatě daný provoz buďto povolí, nebo zamítne. Firewall provádí filtrování příchozího i odchozího provozu (Obr. 13.). Stejně jako přístupové seznamy (ACL) mohou firewally filtrovat síťový provoz podle zdrojové a cílové IP adresy, podle protokolu, a dále podle stavu pojení. Firewall může také do svých protokolů zaznamenávat pokusy o spojení, které se shodují s jistými pravidly a které v síti vedou k vyvolání výstrahy či „poplachu“. A nakonec firewall umožňuje také překlady síťových adres z vnitřních privátních IP adres na veřejné IP adresy (NAT).

Firewall je dnes implementován ve většině routerů a tak je dobré ho mít aktivovaný. Může totiž zabránit většině útoků z internetu. Pokud je podniková WLAN napojená na metalickou, ke které jsou připojeny servery obsahující citlivé informace, je též dobré oddělit ji firewallem. Pokud se totiž útočník dostane do vaší WLAN, neznamená to ještě, že překoná firewall a dostane se tak k požadovaným datům. [14]




*Obr. 24. Princip funkce Firewallu [14]*

# 6 IMPLEMENTACE ZVOLENÉHO ŘEŠENÍ

## 6.1 Popis použitých zařízení

Firemní bezdrátová síť bývá zpravidla pouze prodloužením ethernetu a slouží zaměstnancům k přístupu do sítě. Toto řešení velkou mobilitu připojených uživatelů. Pro modelovou studii sem se rozhodl použít AP od firmy SMC, které bude simulovat přístupový bod, a jako klienta notebook od firmy HP. Abych docílil funkčního spojení, připojil jsem AP k routeru od firmy CC&C, na kterém byl aktivován server DHCP.

### 6.1.1 Přístupový bod SMC WEBT-G

Toto zařízení je možné provozovat buď v režimu klient, nebo v režimu Access Point, který má vestavěnou funkci Repeateru (opakovače) s podporou přes WDS. Velmi snadno je tak možné umístěním dalšího SMCWEBT-G zařízení do sítě (do místa pokrytého signálem od prvního AP), připojit i klienty v místech, kam signál od prvního SMCWEBT-G již nedosáhne a pokrýt signálem veškeré prostory v domě či firmě. SMCWEBT-G je postavené na Atheros čipsetu a zabezpečení je možné prostřednictvím 64/128 bit WEP nebo WPA či WPA2 (TKIP/AES). Pro zvýšení bezpečnosti je také možné zakázat (skrýt) vysílání SSID a použít funkci filtrování MAC adres. Nastavení se provádí přes webové rozhraní.


*Obr. 25. AP SMCWEBT-G*

**Technické parametry :**

- Chipset: AP51 SoC/Atheros 2316 (108M)
- Podporované režimy: Acces Point / Repeater (Bridge) / Klient (v režimu klient obslouží zařízení za sebou pouze 1 MAC adresu)
- Druh modulace: DSSS, OFDM
- Protokol: 802.11b + g/108Mbps
- Pracovní frekvence: 2, 400 až 2, 4835 GHz
- Rychlost: SMC 108G, 54Mpbs, aut. snižování na 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 Mbps
- Provedení: externí
- Porty: 1 x LAN 10/100 Mbps,
- Anténa: 1 x externí odnímatelná anténa + 1 x interní anténa
- Výkon: 15dBm +- 1dBm
- Citlivost: 802.11b: -90dBm, 802.11g: -88dBm @6Mbps, -70dBm@54Mbps
- IP adresa + heslo: 192.168.2.25 (smcadmin)

### 6.1.2 Intel PRO/Wireless 2200BG v notebooku HP nx6110

Jde o MiniPCI kartu určenou pouze pro notebooky s Centrino technologií a spolu s nejnovějšími ovladači podporuje všechna dostupná zabezpečeni dle standardu 802.11. Karta je integrována v notebooku HP nx6110 s os. Windows XP. K nastavení připojení je použit program Intel PROSet/Wireless v.10.1.0.6.

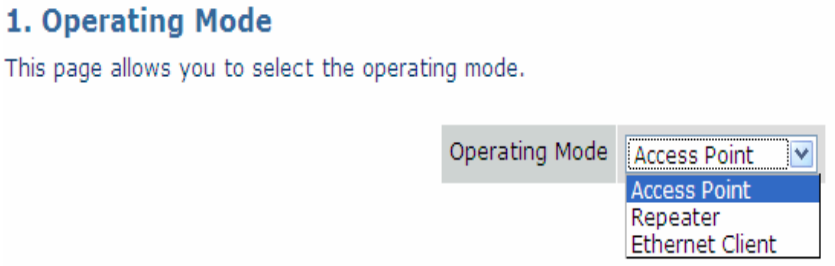
*Obr. 26. MiniPCI Intel PRO/Wireless 2200BG*

**Technické specifikace :**

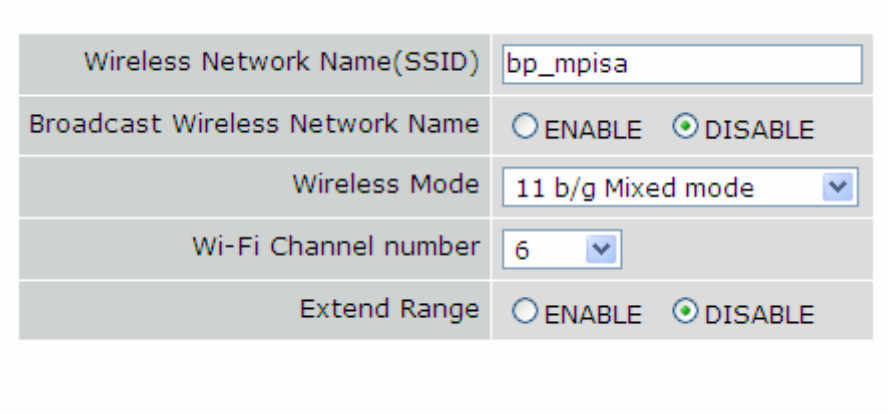
- Protokol 802.11bg
- Frekvence 2,4 GHz
- Podpora kanálu 1-13, 14 pouze pasivně

## 6.2 Nastavení přístupového bodu

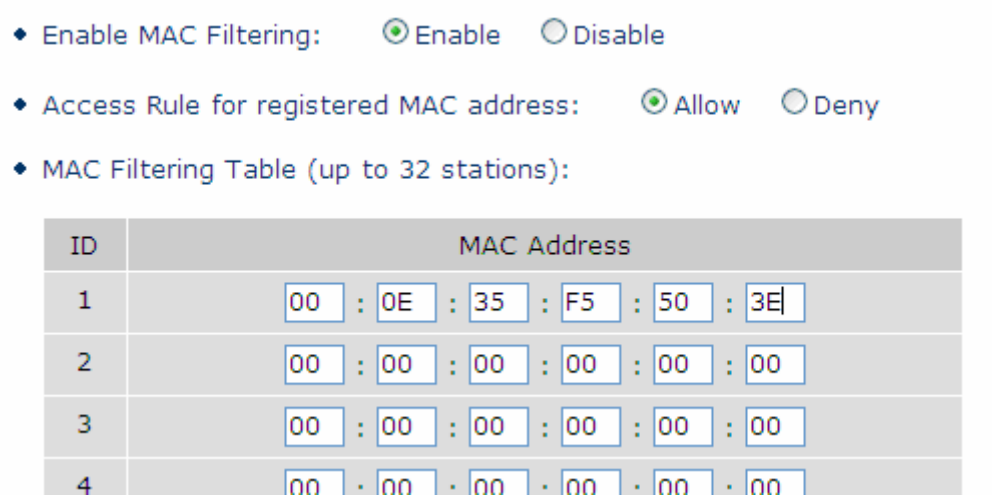
Zařízení MSC WEBT-G jsem nastavil do režimu AccessPoint (Obr. 27.), jako SSID jsem zadal hodnotu bp_mpisa a vypnul jsem jeho veřejné vysílání, kanál jsem nastavil na 6 (Obr. 28.). Aktivoval jsem filtr MAC adres (Obr. 29.) a zabezpečení WPA2 (Obr. 30.). Jelikož jsem neměl k dispozici autetifikační server RADIUS, zvolil jsem šifrování WPA2-osobní s použitím PSK, abych mohl vytvořit funkční připojení (Obr. 31.). Pro názornost uvádím i možnost nastavení AP na autentifikaci 802.1X a s použitím serveru RADIUS (Obr. 32.).



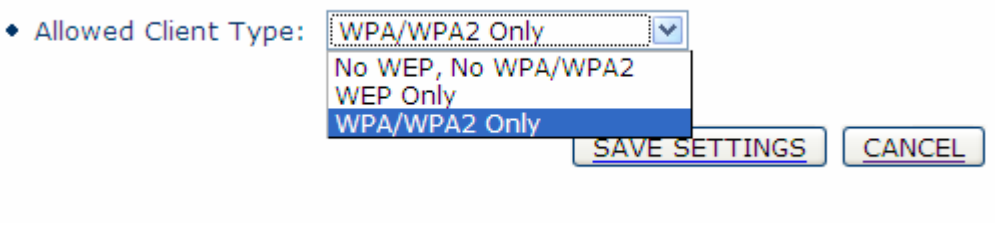

*Obr. 27. Nastavení operačního módu*



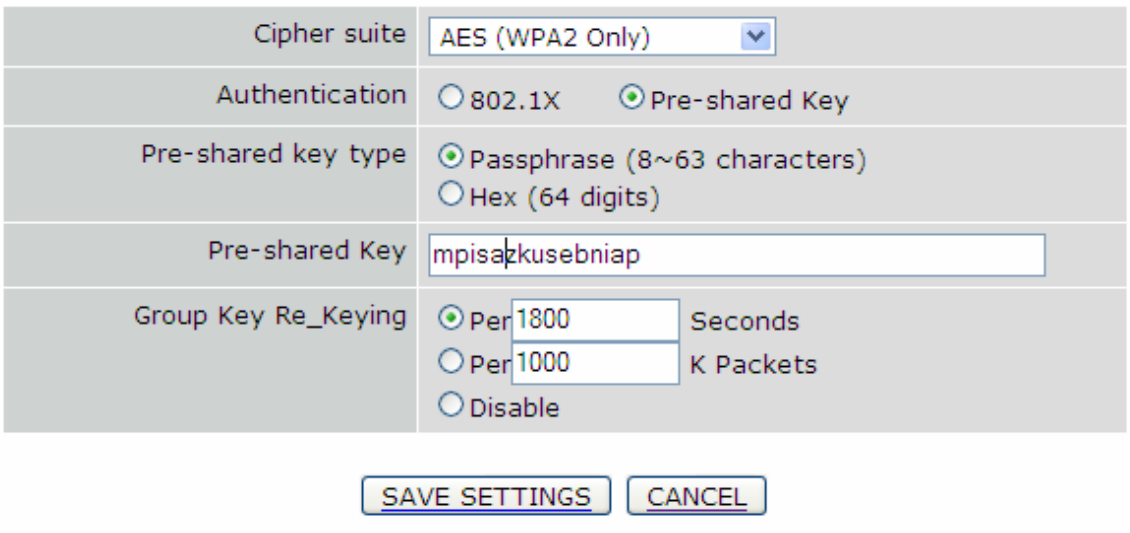

*Obr. 28. Nastavení SSID a vysílacího kanálu*



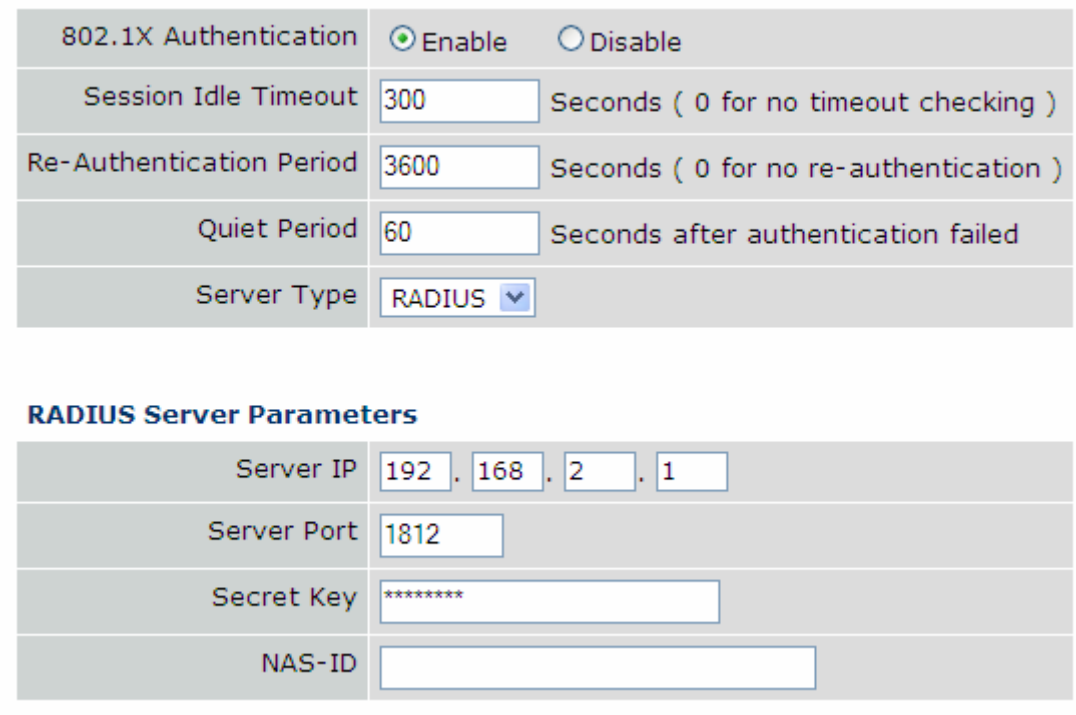

*Obr. 29. Nastavení filtrovaní MAC adres*




*Obr. 30. Aktivace zabezpečení*



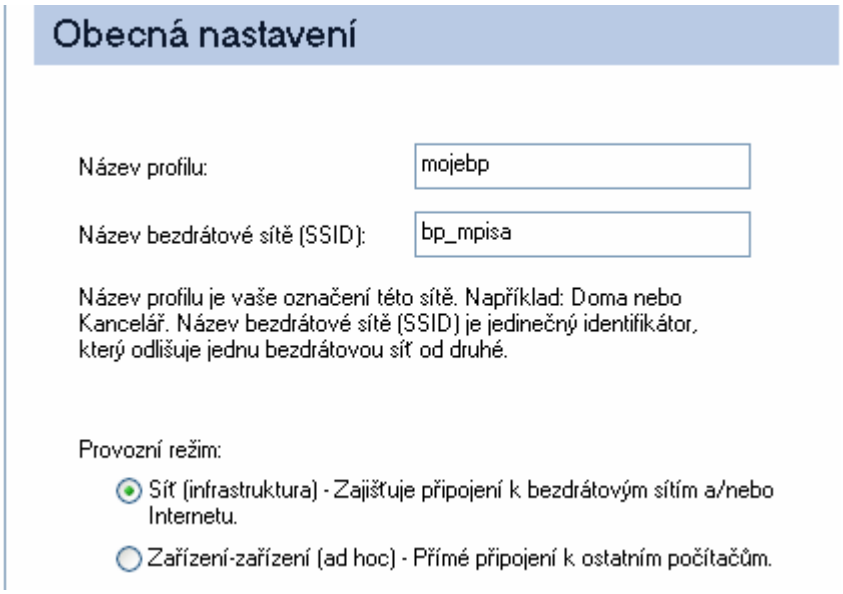

*Obr. 31. Nastavení šifrování WPA2-PSK*



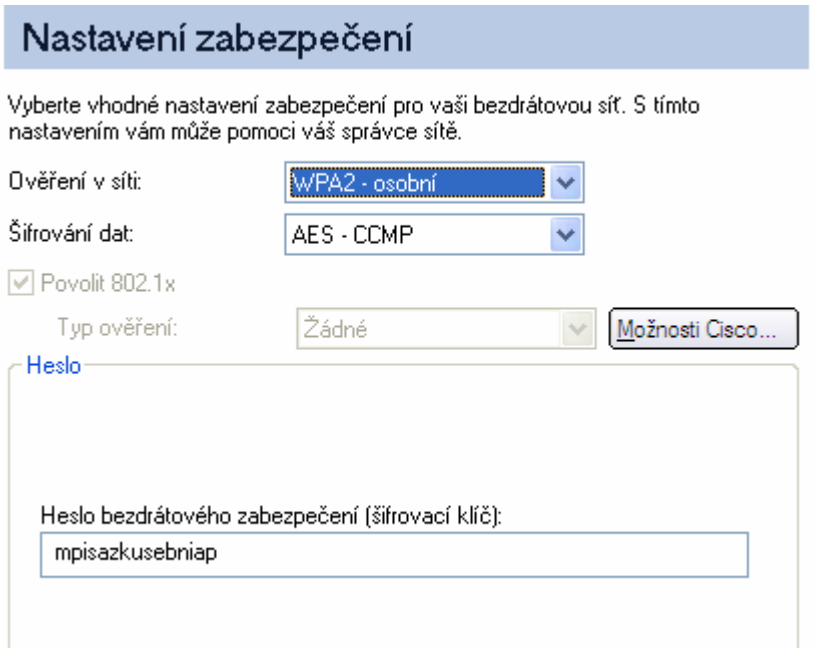

*Obr. 32. Možnost aktivace autentizace 802.1X*

## 6.3 Nastavení uživatele

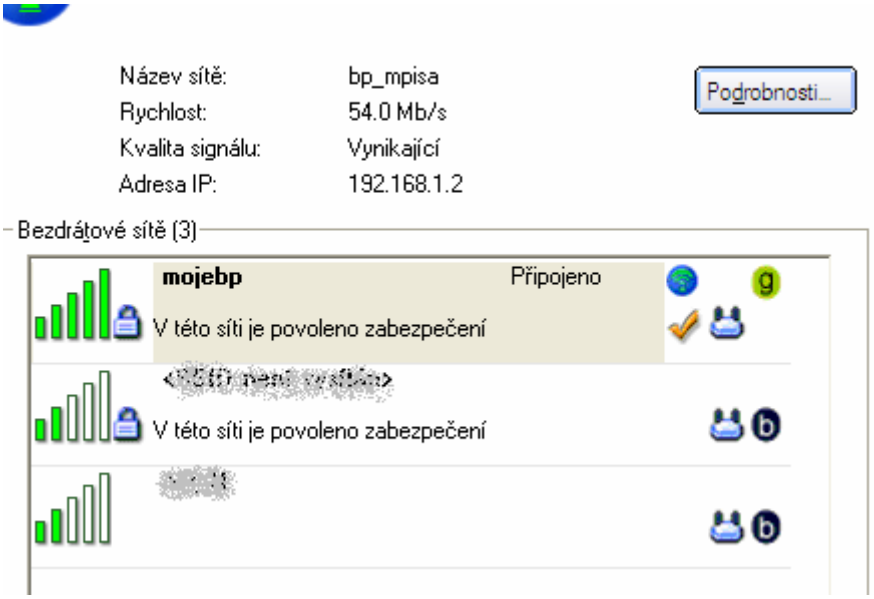
Po spuštění programu Intel PROSet/Wireless jsem vytvořil nový profil „moje BP“. Jelikož jsem na AP deaktivoval vysílání SSID, bylo nutné je zadat SSID ručně (Obr. 33). Po odkliknutí tlačítka Další program sám rozpoznal použitý zabezpečovací protokol a stačilo už jen zadat klíč PSK (Obr. 34). Po vytvoření profilu se počítač bez problémů připojil k AP a byla mu přiřazena platná IP adresa. Tím bylo vytvořeno funkční spojení (Obr. 35.). Pro názornost uvádím i možnost pro připojení k AP s aktivovanou autentizaci 802.1X metodou PEAP (Obr. 36.).



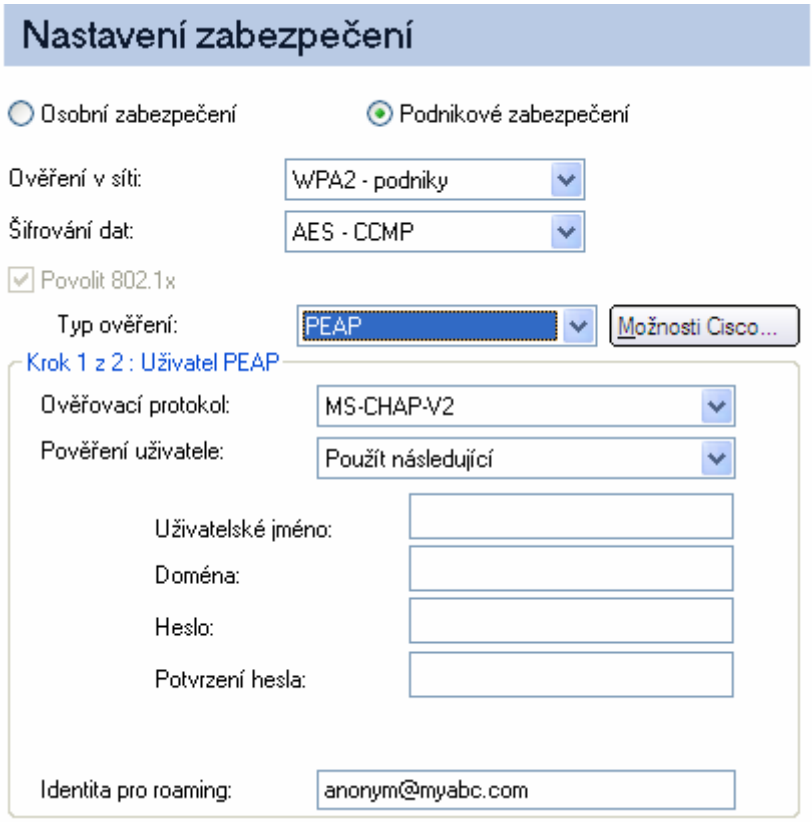

*Obr. 33. Vytvoření nového profilu*




*Obr. 34. Zadání klíče PSK pro zabezpečení WPA2-osobní*




*Obr. 35. Funkční připojení k síti bp_mpisa*




*Obr. 36. Možnosti nastavení pro WPA2-podniky*

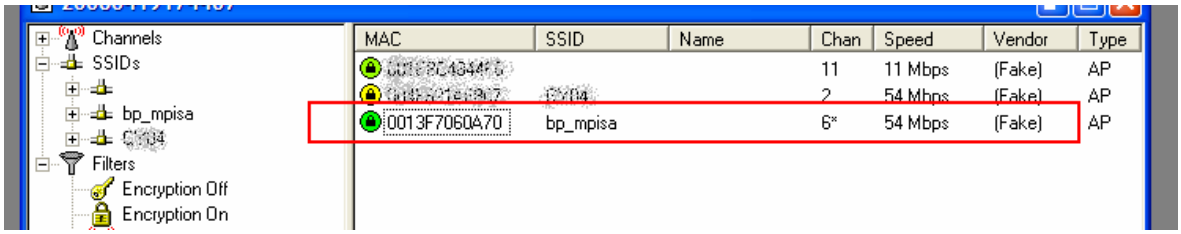
## 6.4 Vyhodnocení zvolené implementace

Pro praktickou jsem vybral zabezpečení protokolem WPA2 s šifrování AES. Jelikož jsem neměl k dispozici autentizační server RADIUS, zvolil jsem metodu bez autentizace 802.1X, pouze s využitím klíče PSK, tzv. WPA2-osobní. Dále jsem na AP vypnul veřejné vysílání SSID a aktivoval jsem filtr MAC adres. Po nastavení přístupového bodu a klienta bylo vytvořeno funkční spojení.

Zvolené zabezpečení považuji za dostačující v případě menších firemních sítí, které z bezpečnostního hlediska nevyžadují nutně použití autentifikačního serveru. Neposkytuje však tak vysokou míru zabezpečení jako při použiti autentifikace 802.1X, která je momentálně nejbezpečnějším dostupným protokolem. Jeho implementace však již vyžaduje určitý stupeň odbornosti, obzvláště co se týče autentifikačního serveru.

Deaktivace vysílání SSID považuji za samozřejmost pro každou bezdrátovou síť, ta je pak na první pohled nerozeznatelná, ovšem ne pro speciální nástroje jako např. NetStumbler (Obr. 37.).

Použití filtru MAC má v tomto případě spíše ilustrativní formu a při použití protokolu WPA2 není nutností. Větší význam má spíše v kombinaci s protokolem WEP.




*Obr. 37. Výpis zachycených sítí v programu NetStumbler*

# ZÁVĚR

Bezdrátové sítě se v poslední době těší stále větší oblibě a postupně nahrazují sítě metalické. Z pohledu využití ve firmě sebou přináší větší komfort, mobilitu a dostatečné přenosové rychlosti. V současné době dochází ke stálému zdokonalování a já osobně vidím v bezdrátových sítích budoucnost počítačových sítí. Jejich implementace je snadná a jejich využití se nabízí i všude tam, kde není možné realizovat kabelové rozvody.

Tato práce se zabývá bezdrátovými sítěmi z pohledu bezpečné komunikace uvnitř firemních sítí. Dnes již bezdrátové sítě nabízí několik způsobů jak je zabezpečit před případným útokem či vniknutí, od těch nejjednodušších až po ty nejdokonalejší. Jejich podrobnému popisu jsem se věnoval v praktické části této práce. Uvedl principy jejich činnosti, míru zabezpečení kterou představují i jejich nedostatky.

Musíme si však uvědomit že dokonalé zabezpečená bezdrátová síť podstatě neexistuje. Každý nový a dokonalejší způsob zabezpečení představuje pro útočníky výzvu k nalezení slabého místa a následnému prolomení takovéhoto zabezpečení. A je pravdou že k tomu dříve nebo později vždy dojde. To ovšem neznamená že není možné mít ve firmě bezpečnou bezdrátovou síť.

V zájmu každé firmy by měla být dostatečná ochrana interních dat. Stále se ovšem dají nalézt nezabezpečené bezdrátové firemní sítě, nebo sítě s naprosto nedostatečným zabezpečením. To že při instalaci bezdrátového přístupového bodu technik aktivuje šifrování WEP a jako heslo zvolí první slovo, které ho napadne, to ještě neznamená že je síť bezpečná, spíše naopak. Takovéto sítě přímo vybízí k tomu aby je někdo napadnul a prolomit WEPový klíč již dnes zvládne téměř každý kdo se aspoň trochu vyzná v počítačových sítích, ostatně návod lze bez problémů nalézt na internetu.

Ve druhé kapitole praktické části jsem uvedl několik metod a doporučení, s jejichž pomocí lze firemní síť efektivně zabezpečit. Vypracování bezpečnostní studie, bezpečnostní politiky a bezpečnostního auditu obstará odborná firma. Správce sítě pak na jejich základě může vytvořit optimálně zabezpečenou nepředimenzovanou firemní síť.

V závěru praktické části jsem provedl praktickou implementaci bezpečnostní metody na přístupový bod SMC WEBT-G konfiguraci klientské síťové karty tak, aby bylo možné se k tomuto přístupovému bodu připojit.

# SUMMARY

The wireless networks have been enjoying high popularity and they have been substituting the metallic networks. On the part of their using in companies, the wireless networks have been bringing with themselves bigger comfort, mobility, and sufficient bit rates. At present they have continually been improving and that is why I see the future in the wireless computers networks. Their implementation is easy and their using is also offered wherever there it is not possible to realize the cable wiring.

This paper deals with the wireless networks on the part of secure communication within company´s networks. Today the wireless networks have already been offering several methods how to make them safe against possible attacking or breaking in, from the easiest to the most perfect one. I describe these methods in detail in a practical part of this study. I introduce their working principles and factors of safety which also represent their shortages.

We must realize that there are no perfect wireless networks, they essentially do not exist. Every new and better method of safeguard of the wireless networks against an attacker represents a challenge to find weak points and ensuing breaking through this safeguard. And it is true that it will happen sooner or later. That of course means that it is not possible to have safe wireless network in a company. Sufficient protection of internal data should be in the interest of each company. But it is also possible to find unsecure wireless networks in a company or networks with absolutely insufficient safeguard. The technician activates WEP coding when installing the wireless access point, he chooses the first word that comes to his mind for a password. It does not mean yet that the network is secure. Rather vice-versa. Such networks directly challenge to be attacked and today almost everybody who knows at least a little bit about computer networks is able to break through a WEP´s key. Moreover everybody can find the instructions without a problem on the Internet.

In the second part of the practical part I introduce several methods and references which are efficiently able to secure company´s network. A specializing firm will take charge of working up the safety study, security policy and safety audit. Then on the basis of this a server administrator can make an optimally protected and not overfilled company´s network.

In the final section of the practical part I provide the implementation of a protective method concerning the SMC WEBT-G access point in practice. With the help of configuration of a client net card, it was possible to get a connection to the access point.

# SEZNAM POUŽITÉ LITERATURY

[1] BARKEN, Lee. *Jak zabezpečit bezdrátovou síť Wi-Fi*. Jiří Veselský. 1. vyd. Brno : Computer Press, 2004. 176 s. ISBN 80-251-0346-3.

[2] PUŽMOVÁ, Rita. *Bezpečnost bezdrátové komunikace : Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. 1. vyd. Brno : Computer Press, 2005. 184 s. ISBN 80-251-0791-4.

[3] ZANDL, Patrick. *Bezdrátové sítě Wi-Fi : Praktický průvodce*. 1. vyd. Brno : Computer Press, 2003. 204 s. ISBN 80-7226-632-2.

[4] KÖHRE, Thomas. *Stavíme si bezdrátovou síť Wi-fi*. Marek Šiller. 1. vyd. Brno : Computer Press, 2004. 296 s. ISBN 80-251-0391-9.

[5] ŘEHÁK, Jan. Co je to WiFi : úvod do technologie. *Hw.cz* [online]. 2003 [cit. 2008-02-24]. Dostupný z WWW: <http://hw.cz/Produkty/Ethernet/ART915-Co-je-to-WiFi---uvod-do-technologie.html>.

[6] *IEEE CS : Československá sekce IEEE* [online]. 27.2.2008 [cit. 2008-02-27]. Dostupný z WWW: <http://www.ieee.cz/>.

[7] *Svět sítí : Slovníček pojmů a zkratek* [online]. c2000-2008 [cit. 2008-02-27]. Dostupný z WWW: <http://svetsiti.cz/slovnik.asp?Chr=I>.

[8] *IEEE 802 :IEEE 802 LAN/MAN Standards Committee* [online]. [2000] , 25.2.2008 [cit. 2008-03-01]. Angličtina. Dostupný z WWW: <http://www.ieee802.org/>.

[9] REMER, Jiří. Mobilní technologie v českých organizacích. *Mobile & Wireless Solutions* [online]. 2007 [cit. 2008-03-03]. Dostupný z WWW: <http://www.mobilewireless.cz/files/Remr_MWS07.pdf>.

[10] IEEE 802.11. *Wikipedie : otevřená encyklopedie* [online]. 2008 [cit. 2008-03-03]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/IEEE_802.11>.

[11] PRAVDA, Ivan. Přehled doplňků standardu IEEE 802.11. *Access server* [online]. 2005 [cit. 2008-03-03]. Dostupný z WWW: <http://access.feld.cvut.cz/view.php?nazevclanku=&cisloclanku=2005113002>.

[12] DAVIS, Harold. *Bezdrátové sítě Wi-Fi : Průvodceúplného začátečníka*. Karel Voráček. 1. vyd. Praha : Grada Publishing, 2006. 376 s. ISBN 80-247-1391-8.

[13] PETERKA, Jiří. Báječný svět počítačových sítí : seriál, PC World. *E-archiv : archiv článků a přednášek Jiřího Peterky* [online]. 2005-2007 [cit. 2008-03-15]. Dostupný z WWW: <http://www.earchiv.cz/i_bajecnysvet.php3>.

[14] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. David Krásenský. 1. vyd. Brno : Computer Press, 2005. 344 s. ISBN 80-251-0417-6.

[15] PINTÉR, Dominik. Průvodce programem ethereal. *Root.cz* [online]. 2006 [cit. 2008-03-16]. Dostupný z WWW: <http://www.root.cz/clanky/pruvodce-programem-ethereal-1/>.

[16] PUŽMOVÁ, Rita. Bezpečnost WLAN podle IEEE. *Lupa : server o českém internetu* [online]. 2002 [cit. 2008-03-30]. Dostupný z WWW: <http://www.lupa.cz/clanky/bezpecnost-wlan-podle-ieee/>.

[17] Protokol PEAP. *MicrosoftTechNet : Microsoft Windows Server TechCenter* [online]. 2005 [cit. 2008-04-07]. Dostupný z WWW: <http://technet2.microsoft.com/windowsserver/cs/library/3e94a25d-8922-4935-b248-540aa6b8c5101029.mspx?mfr=true>.

[18] LEHEMBRE, Guillaume. Bezpečnost Wi-Fi – WEP, WPA a WPA2. *Hackin9 : IT Security Magazine* [online]. 2006, č. 1 [cit. 2008-04-10]. Dostupný z WWW: <http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf>.

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| AES | Advanced Encryption Standard |
| AP | Acccess Point |
| BSS | Basic Service Set |
| BSSID | Basic Service Set Identifier |
| CBC | Cipher Block Chaining |
| CCMP | Counter mode - CBC Message authentication Protocol |
| CRC | Cyclic Redundancy Check |
| CTS | Clear To Send |
| DHCP | Dynamic Host Configuration Protocol |
| DoS | Denial of Service |
| DSL | Digital Subscribe Line |
| DSSS | Direct Sequence Spread Spectrum |
| EAP | Extensible Authentication Protocol |
| EAPOL | Extensible Authentication Protocol Over LAN's |
| EAP-TLS | EAP - Transport Layer Security |
| EAP-TTLS | EAP - Tunneled Transport Layer Security |
| ESS | Extended Service Set |
| ESSID | Extended Service Set IDentifier |
| GEK | Group Encryption Key |
| GIK | Group Integrity Key |
| GMK | Group Master Key |
| GTK | Group Transient Key |
| HTTP | HyperText Transport Protocol |
| CHAP | Challenge Authentication Protocol |
| IDS | Intrusion Detection Systém |
| IEEE | Institute of Electrical and Electronics Engineers |

| | |
|---|---|
| IV | Initialization Vector |
| KCK | Key Confirmation Key |
| KEK | Key Encryption Key |
| MAC | Media Access Control |
| MAC | Message Authentication Code |
| MD5 | Message Digest |
| MIC | Message Integrity Check |
| MK | Master Key |
| MPDU | Mac Protocol Data Unit |
| MSDU | MAC Service Data Unit |
| NAT | Network Address Translation |
| OCB | Offset Codebook Mode |
| OFDM | Orhtogonal Frequency Division Multiplex |
| PDA | Persondal Digital Assistant |
| PKI | Publik Key Infrastructure |
| PMK | Pairwise Master Key |
| PN | Packet Number |
| PPP | Point to Point Protocol |
| PRNG | Pseudo Random Number Generator |
| PSK | Pre-Shared Key |
| PTK | Pairwise Transient Key |
| RADIUS | Remote Authentication Dial-In User Service |
| RC4 | Ron's Code No. 4 |
| RSN | Robus Security Network |
| RSN IE | RSN Information Element |
| RSNA | Robus Security Network Association |
| RTS | Request To Send |

| | |
|---|---|
| RTS | Ready To Send |
| SNMP | Simple Network Managment Protocol |
| TIM | Trafic Indication Map |
| TK | Temporary Key |
| TKIP | Temporal Key Integrity Protocol |
| TMK | Temporary MIC Key |
| TSN | Transitional Security Network |
| VPN | Virtual Private Network |
| WEP | Wired Equivalent Privacy |
| Wi-Fi | Wireless Fidelity |
| WLAN | Wireless Local Area Network |
| WPA | Wi-Fi Protected Access |

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK