VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

PROBLEMATIKA BEZDRÁTOVÝCH SÍTÍ

WIRELESS NETWORK ASPECTS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — LUKÁŠ KLEIN
AUTHOR

VEDOUCÍ PRÁCE — Ing. JIŘÍ KŘÍŽ, Ph.D.
SUPERVISOR

BRNO 2011

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2010/2011
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Klein Lukáš

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Problematika bezdrátových sítí

v anglickém jazyce:

Wireless Network Aspects

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

BARKEN, L. Wi-Fi: jak zabezpečit bezdrátovou síť. vyd. 1. Brno: Computer Press, 2004. ISBN 80-251-0346-3.
BRISBIN, S. Wi-fi: postavte si svou vlastní wi-fi síť. vyd. 1. Praha: Neocortex, 2003. ISBN 80-86330-13-3.
KÖHRE, T. Stavíme si bezdrátovou síť Wi-Fi. vyd. 1. Brno: Computer Press, 2004. ISBN 80-251-0391-9.
PUŽMANOVÁ, R. Bezpečnost bezdrátové komunikace: Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. vyd. 1. Brno: Computer Press, 2005. ISBN 80-251-0791-4.
ZANDL, P. Bezdrátové sítě WiFi: Praktický průvodce. vyd. 1. Brno: Computer Press, 2003. ISBN 80-7226-632-2.

Vedoucí bakalářské práce: Ing. Jiří Kříž, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2010/2011.

L.S.

Ing. Jiří Kříž, Ph.D. Ředitel ústavu	doc. RNDr. Anna Putnová, Ph.D., MBA Děkan fakulty

V Brně, dne 31.05.2011

Abstrakt

Tato bakalářská práce se zabývá problematikou bezdrátových sítí. Vysvětluje základní pojmy a dělení bezdrátových sítí. Dále popisuje mezinárodní standard IEEE 802.11 a jeho rozšíření. Detailně se věnuje zabezpečení bezdrátových sítí včetně bezpečnostních doporučení pro jednotlivé skupiny sítí.

Klíčová slova

Bezdrátová síť, WLAN, WiFi, IEEE 802.11, SSID, WEP, WPA, WPA2, bezpečnost bezdrátových sítí

Abstract

This Bachelor's thesis deals with the issue of wireless networks. It explains basic terms and classification of wireless networks. It also describes the international standard IEEE 802.11 and its extensions. Closed attention is given to the security of wireless networks including safety recommendations for each group of networks.

Key words

Wireless network, WLAN, WiFi, IEEE 802.11, SSID, WEP, WPA, WPA2, security of wireless networks

Bibliografická citace práce

KLEIN, L. *Problematika bezdrátových sítí*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2011. 53 s. Vedoucí bakalářské práce Ing. Jiří Kříž, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 30.5.2011 ……

Poděkování

Chtěl bych poděkovat vedoucímu práce panu Ing. Jiřímu Křížovi, Ph.D. za cenné rady a udávání směru při psaní této práce.

Obsah

1. Úvod

Dostupnost připojení k Internetu je dnes naprostou samozřejmostí. Jen málo lidí žijících v dnešní moderní společnosti si už dokáže svůj život bez Internetu představit. Konektivita se stala fenoménem. Bezdrátové sítě mají na tomto fenoménu velký podíl. Asi jen málokdo si v počátcích používání bezdrátových sítí, kdy nacházely uplatnění výhradně ve velkých podnicích, dokázal představit jejich rychlé a masové rozšíření do soukromého sektoru, ke kterému brzy došlo. Nejprve byly bezdrátové sítě dobrou alternativou pro připojení míst, na která nevedly telefonní linky. Později získaly ještě mnohem větší popularitu díky přínosu, jaký měly pro komfort uživatelů. Tato popularita sílila ruku v ruce s tím, jak se zlevňoval hardware s bezdrátovou technologií. Právě onen komfort je důvodem, proč dnes používáme bezdrátové sítě ve většině firem, domácností a dokonce i na mnohých veřejných prostranstvích.

V posledních letech se rozšiřuje paleta přístrojů podporujících bezdrátové sítě i mimo notebooky a mobilní telefony, kde je to prakticky již standardem. Bezdrátovou konektivitu podporují stále častěji televize a audiosystémy, ale také už není výjimkou ani u mikrovlnné trouby a dalších běžných domácích spotřebičů. Důvodem je opět již zmíněný komfort. Uživatelé mohou snadno propojit jednotlivé přístroje v domácnosti a sdílet různá data, přehrávat video uložené v počítači na televizi ve vedlejší místnosti nebo pomocí mobilního telefonu zapnout vytápění bytu či spustit robotický vysavač.

Masové rozšíření bezdrátových sítí však sebou nese i mnohá úskalí. Jedním z nich je například jistá přehlcenost používaných rádiových pásem. Tím nejdůležitějším je však bezpečnost. S oblibou bezdrátových sítí totiž roste i riziko zneužití dat, která jsou v těchto sítích dostupná. Je proto velmi důležité dbát na správné zabezpečení bezdrátových sítí a vždy přizpůsobit své chování důvěryhodnosti konkrétní sítě.

2. Cíl práce

Cílem mé bakalářské práce je vysvětlit základní termíny, které souvisejí s problematikou bezdrátových sítí. Postupně bude probrána topologie sítí a referenční modely, na základě kterých sítě fungují. Dále pak popíši možné způsoby přenosu dat bez použití kabelů. Podrobně budou rozebrány standardy rádiových bezdrátových sítí a zvláštní pozornost bude věnována zabezpečení těchto sítí.

V části, která se zabývá analýzou současného stavu je popsána výchozí situace firmy a podmínky, za kterých firma pracuje nyní. Zaměřuji se na nedostatky tohoto řešení a prostor pro zlepšení.

Při samotném návrhu řešení výchozí situace jsou zohledněny možnosti budoucích prostor v souvislosti s napojením na stávající podnikovou síť. Dále je také brán ohled na požadavky firmy vycházející z postřehů z praxe. Mezi hlavní požadavky patří snadná údržba sítě, bezpečnost a efektivita. Dále pak je řešení vypracováno s ohledem na stanovený rozpočet.

3. Teoretická východiska práce

3.1. Základní pojmy

Obecně lze pojmem počítačová síť označit spojení minimálně dvou stanic, tedy počítačů. Nejčastěji se v praxi můžeme setkat se spojeními založenými na technologii ethernet.

3.1.1. Referenční model ISO / OSI

V počátcích budování počítačových sítí, tedy někdy v polovině 70. let, se začaly na trhu objevovat produkty několika světových výrobců, kteří přišli s vlastními metodami a technologiemi. Tento fakt sebou jako nepříjemný důsledek přinesl proprietárnost jednotlivých produktů – tedy skutečnost, že jednotlivé produkty nebyly vzájemně kompatibilní. Situace na trhu si vynutila potřebu vyvinout síťovou architekturu, která by byla otevřená a široce dostupná, což by umožnilo zbavit se závislosti na jediném výrobci a nutnosti udržovat jakýsi systém dvorních dodavatelů. Byla zde potřeba otevřít trh konkurenci a umožnit tak kombinovaná řešení od různých výrobců. [8]

Takovouto nezávislou síťovou architekturu nakonec vypracovala mezinárodní standardizačí organizace ISO (*International Standards Organization*). Z původního záměru vytvořit jednotný standard pro fungování všech otevřených systémů, tedy vlastně všech počítačů nehledě na to, zda jsou to uzly zapojené do nějaké sítě či nikoliv, nakonec sešlo. Pozornost ISO byla tedy od fungování samotných počítačů zaměřena spíše na komunikaci mezi nimi. Na začátku 80. let tak vznikl referenční model otevřené komunikace – OSI (*Open System Interconnection*) jako standard ISO 7498 pro propojování heterogenních počítačových systémů. Tento model definuje podmínky, při jejichž dodržení mohou libovolní účastníci přenosu komunikovat mezi sebou navzájem po sériové sběrnici. Tento model není závislý na žádném firemním řešení, jedná se o otevřený model. [8] [11]

Referenční model ISO / OSI je sedmivrstvový a každá vrstva má svou přesně definovanou funkci a poskytuje předem popsané služby. Vrstvy jsou rozděleny do dvou

bloků po třech a mezi nimi je tzv. přizpůsobovací vrstva, která má vyrovnávat rozdíly mezi možnostmi bloku nižších vrstev a potřebami bloku vyšších vrstev. [11]

Dále stručně popíši význam jednotlivých vrstev a princip fungování OSI modelu. Každá vrstva je schopna komunikovat pouze se sousední vrstvou, tedy tou bezprostředně hierarchicky pod a nad sebou. To znamená, že každá vrstva využívá služeb své bezprostředně nižší vrstvy, sama plní své úkoly a výsledek poskytuje své bezprostředně vyšší vrstvě. [8]

Fyzická vrstva

Jako jediná nemá žádnou bezprostředně nižší vrstvu. Jejím úkolem je přenos jednotlivých bitů k přímým sousedům, tedy k uzlům, ke kterým vede přímé spojení. Fyzická vrstva zajišťuje korektnost přenosu jednotlivých bitů, tzn. má na starosti to, aby je příjemce spolehlivě rozpoznal. Význam jednotlivých bitů však fyzická vrstva neřeší a ani jej není schopna rozpoznat. Jejím hlavním úkolem je kódování, časování a synchronizace. Prvky, které pracují na úrovni fyzické vrstvy jsou opakovače (*repeater*) a rozbočovače (*hub*). [11]

Linková vrstva

Linková vrstva realizuje přenos datových bloků pomocí fyzické vrstvy. Tyto bloky se nazývají rámce (*frames*). Linková vrstva zajišťuje rozpoznání začátku a konce každého rámce a taky jeho jednotlivých částí, jako např. hlavičky a adres, které obsahuje. Adresace je zajištěna pomocí MAC adresy, která je vázána na síťovou kartu a měla by být celosvětově unikátní. Lze ji však softwarově změnit. V takovém případě by však měla přesto být zachována její jedinečnost v rámci jednoho síťového segmentu. MAC adresa je tvořena 48 bity. Její první polovina je identifikátorem výrobce a druhá zajišťuje unikátnost. [9] [11]

Síťová vrstva

Síťová vrstva také přenáší data po blocích, ty se zde však nazývají pakety (*packets*). Adresace je zde uvažována na úrovni síťového prostředí. Adresy jsou logické. Nejsou už tedy generovány podle nějakého klíče při výrobě zařízení a uživatel je může měnit. Sestávají opět ze dvou částí. První část určuje síť, ve které se zařízení nachází a druhá část pak odkazuje na samotné zařízení. Hlavním úkolem síťové vrstvy je tedy

směrování neboli nalezení vhodné cesty k příjemci dat. O výběr nejvhodnější cesty od odesílatele k příjemci se starají směrovače (*routery*). [9] [10] [11]

Transportní vrstva

Úkolem transportní vrstvy je zajistit, aby tři vrstvy pod ní byly schopny splnit požadavky vyšších vrstev na spolehlivost a kvalitu přenosu. Požadavky se nejčastěji týkají různých úrovní spolehlivosti pro konkrétní typy přenosů a také charakteru přenosu, který může být spojovaný nebo nespojovaný. Spolehlivostí se myslí postup při výpadcích přenosu či výskytu jiných chyb. Nespolehlivý přenos se chová tak, že při zjištěné chybě není ani jedna strana povinna starat se o nápravu a poškozená data se mohou bez náhrady zahodit. Spolehlivý přenos se chová tak, že strana, která chybu zjistí, je povinna postarat se o nápravu. Výhodou nespolehlivého přenosu je jeho nenáročnost na režii. To znamená, že data mohou být přenášena rychleji a s větší pravidelností. O případnou nápravu se pak může postarat některá z vyšších vrstev, pokud je to žádoucí. [10] [11]

Relační vrstva

Již z názvu relační vrstvy je patrné, že se stará o relace, konkrétně o navazování a ukončování spojů pro přenos dat. Z tohoto důvodu bývá také označována jako spojová vrstva. Dále pak zajišťuje možnost navázat na již přenesená data po přerušení spojení, takže není nutné opakovat celý přenos a posílat všechna data znova. Stará se také o bezpečnost přenosů a překlad aliasů na adresy. [10] [11]

Prezentační vrstva

Prezentační vrstva umožňuje naplnit základní předpoklad každé komunikace, tedy to, že obě strany chápou komunikovanou informaci stejně. Tato vrstva zajišťuje konverzi přenášených dat. Musí zajistit, aby data měla stejný význam pro odesilatele i příjemce. Týká se to jak kódování textů, tak i znázornění celých čísel a čísel reálných a různých datových struktur. Prezentační vrstva může zajišťovat i šifrování dat, pokud se tak neděje, zvládá toto i fyzická či transportní vrstva. [11]

Aplikační vrstva

Aplikační vrstva je mezičlánek uživatelských aplikací a síťové komunikace. Jako jediná nemá nadřazenou vrstvu. Obsahuje části aplikací, které musejí být standardizovány. Bylo nutno upustit od původního záměru, aby byly veškeré síťové aplikace umístěny v aplikační vrstvě, protože praxe ukázala, že v některých částech většiny aplikací to není nutné a je to dokonce naopak nežádoucí. Takovým příkladem může být třeba uživatelské rozhraní aplikací. Je výhodnější, aby nespadalo pod aplikační vrstvu, protože potom nepodléhá nutné standardizaci a autoři aplikací mají více možností přizpůsobit uživatelské rozhraní aplikace uživatelově komfortu. Dobrým příkladem tohoto řešení je elektronická pošta. Poštovní servery je nutno velmi striktně standardizovat, aby si mohly snadno předávat zprávy a dodržely přitom formát, který je pro všechny srozumitelný. Na druhou stranu klientské programy elektronické pošty byly vysunuty zcela mimo ISO / OSI model a tento fakt umožnil vznik různých programů s různým prostředím a uživatelům tak dal možnost volby. [10] [11]

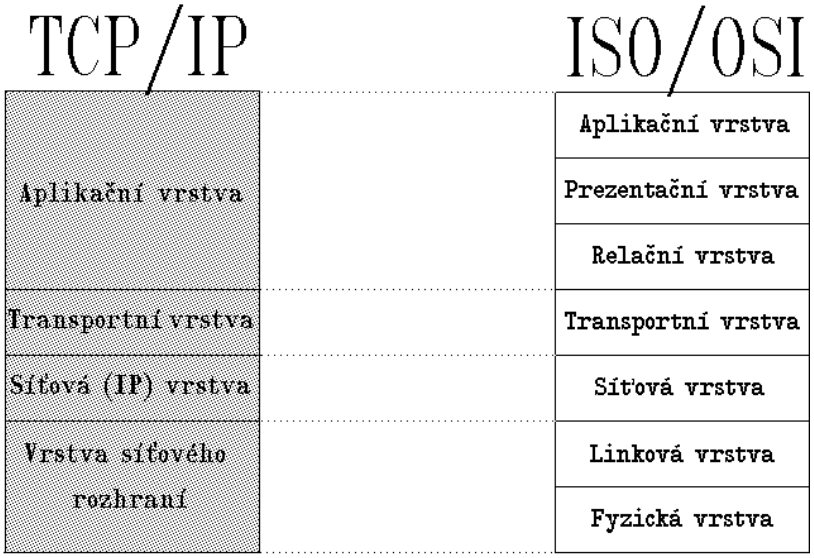
Obrázek 1: Referenční model ISO / OSI [11]

3.1.2. Model TCP / IP

V praxi se lépe uchytil model TCP / IP (*Transmission Control Protocol* / *Internet Protocol*), který z modelu OSI vychází. Mnohem více se blíží skutečnému stavu. Bývá také nazýván *Internet Reference Model*. Původně byl navrhován hlavně pro UNIX, dnes je však součástí prakticky všech operačních systémů. Využívá se i v komunikaci po síti Internet, což je důvodem jeho narůstajícího významu a staví jej do pozice celosvětového standardu.

Je tvořen čtyřmi vrstvami. Řazeny vzestupně to jsou:

- Vrstva síťového rozhraní
- Síťová vrstva
- Transportní vrstva
- Aplikační vrstva [12]



Obrázek 2: Srovnání TCP / IP vs. ISO / OSI [12]

3.2. Dělení sítí

Sítě lze z pohledu způsobu přenosu dat rozdělit jednoduše na drátové a bezdrátové. K realizaci sítě pomocí drátové technologie je zapotřebí kabelový vodič signálu. Ať už se jedná o vodiče metalické, kde patří různé typy kabelů (od koaxiálního po splétané kabely různých specifikací), nebo vodiče optické, kde je k vedení signálu použito optické vlákno.

Drátové sítě mají oproti bezdrátovým četné výhody, ale i několik nevýhod. Mezi výhody jednoznačně patří nenáročný a prakticky bezúdržbový provoz, rychlost a bezproblémovost přenosu dat a v neposlední řadě také bezpečnostní kritéria, protože kabelovou síť je mnohem obtížnější odposlouchávat nebo napadnout. K nevýhodám pak určitě patří menší uživatelská vstřícnost, protože je nutné umisťovat síťová zařízení v blízkosti zásuvek, není zkrátka tak jednoduché připojit počítač k síti kdekoliv si uživatel přeje. Další nevýhodou je pak samotná realizace takové sítě. V dnešní době je určitě jednodušší pokrýt požadované lokality bezdrátově, než instalovat kabely, minimálně tedy zatím na domácí a méně rozsáhlé podnikové úrovni. Každý způsob má jistě své pro a proti.

Z pohledu mé práce jsou mnohem významnější sítě bezdrátové, budu se tedy nadále zabývat jimi. Jako médium pro šíření signálu je zde použit vzduch. Bezdrátové sítě lze z pohledu způsobu šíření signálu rozdělit na optické a rádiové.

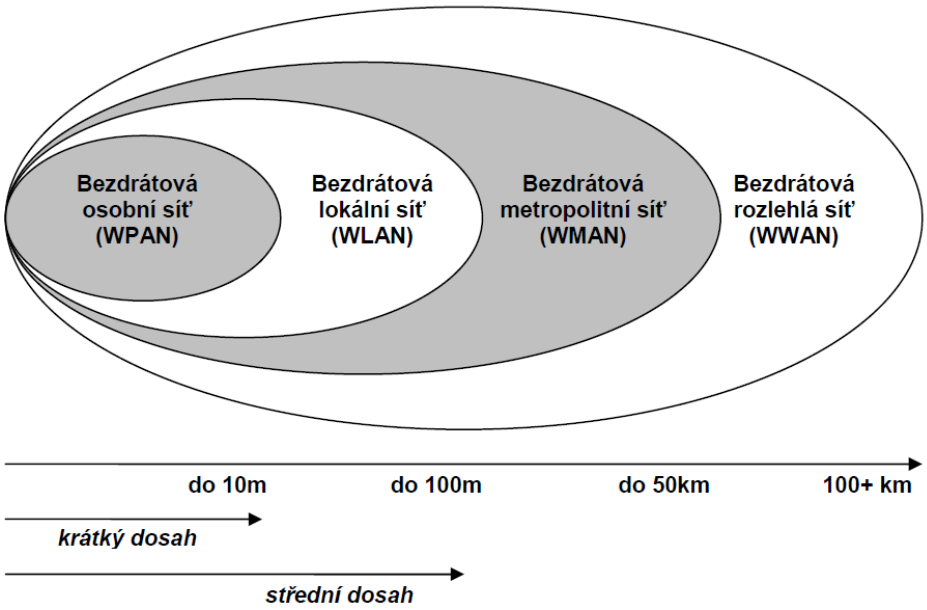
3.2.1. Klasifikace sítí

„Bezdrátové sítě lze klasifikovat podle mnoha odlišných druhů kritérií. Kromě dále podrobněji rozebraných kategorií podle dosahu a typu signálu je lze dělit podle topologie na point-to-point (především optické sítě) a point-to-multipoint (rádiové sítě), případně podle typu určení na vnitřní (infračervené, rádiové WLAN) a venkovní.“ [5, s. 36]

Dosah

Podle dosahu (viz obrázek) lze bezdrátové sítě rozdělit na:

- bezdrátové osobní sítě (WPAN – *Wireless Personal Area Network*)
- bezdrátové lokální sítě (WLAN – *Wireless Local Area Network*)
- bezdrátové metropolitní sítě (WMAN – *Wireless Metropolitan Area Network*)
- bezdrátové rozlehlé sítě (WWAN – *Wireless Wide Area Network*) [5]



Obrázek 3: Dosah bezdrátových sítí [5]

Typy signálu

Bezdrátové sítě lze podle typu signálu rozdělit do dvou základních kategorií:

- optické a infračervené
- rádiové [5]

3.2.2. Optické a infračervené bezdrátové sítě

Optické a infračervené sítě jsou realizovány dvěma body, které musí mezi sebou mít přímou viditelnost. Z toho také plynou jejich nejpodstatnější výhody a nevýhody. Nutnost přímé viditelnosti je výhodou i nevýhodou zároveň. Na jednu stranu je taková komunikace velmi těžce odposlechnutelná, protože útočníkovi znemožňuje zachytávat provoz na síti, aniž by jej tím zároveň přerušil. Na stranu druhou klade vyšší nároky na výběr umístění vysílače a přijímače, protože je nutné zajistit, aby přenosu nebránila žádná překážka. Výhodou oproti rádiovým bezdrátovým sítím je pak minimalizace možnosti rušení a nevýhodou zase nemožnost vysílat na větší množství přijímačů současně. Pokud se jedná o sítě realizované infračerveným přenosem, jejich velkým omezením je velmi malý dosah, řádově jednotky metrů. Tento fakt zase na druhou stranu poskytuje velkou jistotu bezpečnosti, protože signál nemůže například opustit místnost. Vzhledem k malé rychlosti se infračervený přenos pro síťovou komunikaci dnes už prakticky nepoužívá. [1] [5]

3.2.3. Rádiové bezdrátové sítě

Rádiové bezdrátové sítě dnes tvoří většinu domácích a veřejných sítí. Jsou nejčastějším řešením připojení k internetu na veřejných prostranstvích a v podnicích, kde se předpokládá, že se zákazníci budou chtít připojit. Svou oblibu a masovou rozšířenost získaly především díky snadné instalaci, nízkým pořizovacím nákladům a uživatelské přívětivosti.

Jejich největší výhodou oproti optickým sítím je to, že rádiový signál se šíří i přes nejrůznější překážky, umí dokonce projít zdí. Odpadá tedy nutnost přímé viditelnosti. Dále pak je nespornou výhodou fakt, že lze do sítě přidávat více stanic, aniž by musela být dodržena podmínka párů, které spolu komunikují.

Nevýhodou rádiových bezdrátových sítí je poměrně časté rušení rádiových vln. Rádiové vlnění je náchylné na rušení jakýmkoliv zařízením pracujícím ve stejných kmitočtech. Další nevýhodou je pak velmi snadná odposlechnutelnost komunikace, což je nutné řešit různými zabezpečovacími mechanismy, jimiž se budu zabývat dále.

Rádiové bezdrátové sítě jsou stěžejním tématem této práce, proto se dále budu zabývat především tímto typem síťové komunikace.

3.2.4. Struktura bezdrátových sítí

Point-to-point

Jedná se o propojení dvou bodů nacházejících se ve dvou různých sítích LAN. Je to nejjednodušší možnost použití bezdrátového mostu. Dvě jednotky spolu komunikují skrze bezdrátovou síť. Tento model je vhodné použít všude tam, kde je potřeba spojit dvě oddělené LAN sítě. Typickým příkladem je případ, kdy je potřeba propojit dvě budovy, z nichž pouze jedna disponuje přípojkou k síti Internet. Aby mohly obě sítě vzájemně komunikovat a zároveň být připojeny na Internet, použije se propojení na bázi point-to-point (PTP). [7]

Point-to-multipoint

Jedná se o rozšířenou obdobu funkce point-to-point. Jak už z názvu vyplývá, lze díky této funkci připojit k jedné síti více dalších LAN sítí. I u této funkce platí, že slouží k propojení dvou sítí a nikoliv k přímému připojení klientů. Ty je nutno připojit vždy přes přístupový bod dedikovaný pro tuto činnost. V této topologii však postupným vývojem vznikla značná nejednotnost jednotlivých výrobců a proto je pravděpodobné, že při použití hardwaru více výrobců najednou nebude fungovat. Doporučuje se tedy použít hardware jednoho výrobce. [7]

3.3. Frekvenční pásma

Bezdrátové sítě využívající technologii rádiových vln je možné provozovat v několika frekvenčních pásmech. Nejvíce rozšířené jsou ty, které se provozují v pásmu 2,4 GHz. Důvod je prostý – síťové prvky, které pracují v tomto pásmu, jsou nejlevnější. Tato popularita má však samozřejmě také svá úskalí. Jedním z nich je poměrně častá přehlcenost tohoto pásma zvláště ve velkých městech. Je to dáno také tím, že v tomto pásmu je na výběr pouze ze 13 kanálů. Pokud komunikuje více klientů na stejném kanálu, mohou se vzájemně rušit. Dalším úskalím je dosah. Toto je však problém spíše při potřebě přenosu na větší vzdálenosti. Při potřebě pokrytí např. bytu a přilehlého okolí nebo menší kanceláře, je dosah dostačující. Pokud potřebujeme postavit síť s větším dosahem nebo chceme eliminovat riziko rušení, je možné využít pásmo 5 GHz. Zde je k dispozici mnohem více kanálů a dosah je postačující i pro větší haly. Hardware je však nákladnější.

Obě výše zmíněná pásma jsou pásma bezlicenční. Další možností je využití některého z licenčních pásem, například 11 GHz. Zde je však nutno zažádat o licenci, kterou uděluje radiokomunikační úřad. Ten přidělí žadateli vlastní kmitočet v závislosti na územním plánu.

3.4.Standardizace bezdrátových sítí

V počátcích vývoje rádiových bezdrátových sítí šel každý výrobce tak trochu svou cestou a výsledkem opět byla skutečnost, že spolu výrobky konkurenčních výrobců nekomunikovaly vůbec nebo komunikovaly s obtížemi. Jednotliví výrobci vyvíjeli vlastní normy a specifikace. V důsledku toho nedosahovaly rádiové sítě příliš velké popularity a nebyly moc rozšířené. Tento fakt bylo nutno vyřešit především v zájmu trhu a uživatelů. Standardizace se v roce 1990 ujala mezinárodní společnost IEEE (*Institute of Electrical and Electronics Engineers*), která vyvinula normu 802 LAN/MAN obsahující standardy pro bezdrátové sítě. Díky této normě bylo možné používat v bezdrátové síti prvky různých výrobců. [5]

Přehled vybraných standardů normy 802:

- IEEE 802.11 – bezdrátové lokální sítě (WLAN)
- IEEE 802.15 – bezdrátové osobní sítě (WPAN)
- IEEE 802.16 – bezdrátové metropolitní sítě (širokopásmový bezdrátový přístup, WMAN)
- IEEE 802.20 – širokopásmové mobilní bezdrátové sítě (MBWA)
- IEEE 802.21 – roaming mezi sítěmi (*Media Independent Handoff*)
- IEEE 802.22 – WRAN (*Wireless Regional Area Networks*) [5]

Z pohledu mé práce je nejpodstatnější standard pro bezdrátové lokální sítě 802.11, ze kterého vychází i specifikace WiFi, proto se dále budu zabývat především jím.

3.4.1. IEEE 802.11

První verze tohoto standardu byla vytvořena v roce 1997 a dnes se s ním můžeme setkat také pod názvem „802.11 legacy.“ Pro tento standard se počítalo s využitím bezlicenčního pásma 2,4 GHz. Protokol zahrnoval fyzickou a linkovou vrstvu a přenos mohl dosahovat rychlosti 1 Mbit/s nebo 2 Mbit/s. Pro přenos dat byly na fyzické vrstvě popsány tři metody. Jedna využívala infračervený přenos a zbylé dvě přenos rádiovým signálem – tyto metody nesou názvy FHSS a DSSS. [7]

FHSS – Zkratka slov *Frequency Hopping Spread Spektrum*. Stojí na principu neustálého přeskakování frekvencí, kdy se dané pásmo rozdělí na jednotlivé kanály o šířce 1 MHz a signál mezi nimi přepíná. Kanál je změněn nejpozději po 400 milisekundách. Výhodou tohoto řešení je možnost souběžného použití až dvaceti přístupových bodů ve stejném pásmu současně. Nevýhodou však je malá přenosová rychlost, která dosahuje 2 Mbit/s. [7]

DSSS – Zkratka slov *Direct Sequence Spread Spektrum*. Bezlicenční pásmo má šířku 83,5 MHz. DSSS využívá 13 kanálů v šířce pásma 22 MHz, což (vzhledem k faktu, že překrývající kanály se ruší) v praxi znamená, že je možné souběžně používat pouze tři přístupové body. [7]

Z pochopitelných důvodů byl tento standard poměrně brzy nedostatečný a tak začaly vznikat dodatky a úpravy normy 802.11

IEEE 802.11b

Jedná se o první úpravu. Vznikla v roce 1999 a původně nesla označení „High rate.“ Písmenem „b“ byla označena až dodatečně z důvodu přehlednosti. Tato úprava umožňovala zvýšení rychlosti až na 11 Mbit/s při zachování pásma 2,4 GHz. Pro přenos dat využívá pouze technologii DSSS a není zpětně kompatibilní s FHSS. Zajímavostí je možnost dočasného snížení přenosové rychlosti za nepříznivých podmínek. Pokud to situace vyžaduje, přenosová rychlost klesne na 5,5 Mbit/s a v extrémním případě dokonce až na 1 Mbit/s. Pokud dojde ke zlepšení podmínek, rychlost se opět vrátí na maximálních 11 Mbit/s. [2]

IEEE 802.11a

Tento standard vznikl taky v roce 1999, ale na rozdíl od předchozí verze pracuje v pásmu 5 GHz a umožňuje maximální přenosovou rychlost až 54 Mbit/s. Specifikem tohoto standardu byla technologie OFDM (*Orthogonal Frequency Division Multiplexing* – ortogonální multiplex s dělením kmitočtu). Tato technologie vysílá signál současně přes několik vzájemně nezávislých frekvencí, což kromě nárůstu rychlosti také výrazně eliminuje rušení. Tento standard nedosáhl zdaleka takové popularity jako předchozí zmíněný. Důvodem byla jednak vyšší pořizovací cena komponent a pak také fakt, že hardware podporující tyto specifikace se začal vyrábět až o několik let později. Původní výhody vyššího frekvenčního pásma s menším rušením a větší přenosové rychlosti tak byly potlačeny zájmem trhu. [2]

IEEE 802.11g

Tento standard vzniká v roce 2003 a vrací se zpět k využití pásma 2,4 GHz. Dochází však k navýšení rychlosti až na 54 Mbit/s, tedy stejně jako u 802.11a. Opět využívá technologii OFDM a z důvodu zpětné kompatibility je použita technologie DSSS. Uvedená maximální rychlost je pochopitelně dosažitelná pouze za předpokladu, že všechny články sítě budou splňovat normu 802.11g. V případě, že tomu tak není, rychlost celé sítě se podstatně sníží. Tento standard se stal jedním z nejrozšířenějších a dodnes tomu tak je. Důvodem byla zpětná kompatibilita s 802.11b, prakticky okamžitá podpora ze strany výrobců a cenová dostupnost hardwaru, který díky zachování 2,4 GHz pásma nebyl nákladný na výrobu a vývoj. [2] [7]

IEEE 802.11n

Zatím poslední standard této normy. Vývoj začal už v roce 2003 a dokončen byl na přelomu let 2009 a 2010. Při vývoji bylo kladeno za cíl vyrovnat (nebo ještě lépe překonat) tehdejší teoretickou rychlost ethernetu, tedy 100 Mbit/s. Bylo dosaženo teoretické rychlosti 300 Mbit/s a praktická rychlost se podle testů pohybuje okolo 130 Mbit/s, což samo o sobě je velmi dobré. Existují už ale návrhy pro zvýšení teoretické rychlosti až na 600 Mbit/s. Tento standard je zpětně kompatibilní s verzemi 802.11b/g, což usnadní jeho rozšíření. Využívá pro posílání dat dvě frekvence – 2,4 GHz a 5 GHz a to v závislosti na tom, jestli je potřeba komunikovat v režimu kompatibility nebo ne. Pokud i druhá strana podporuje standard 802.11n, pak komunikace probíhá v pásmu 5 GHz, pokud nikoliv, přepíná se na pásmo 2,4 GHz. Opět je zde použita technologie OFDM. Největším přínosem pro rychlost je však využití technologie MIMO (*Multiple-Input Multiple-Output*), někdy také nazývána technologie chytrých antén. Jedná se o princip současného vysílání více signálů na různých frekvencích. Základním předpokladem je přítomnost více antén na straně vysílače i přijímače. Samotný návrh matematického modelu MIMO pro zařízení používající více antén je znám již dlouho, zde však byl v praxi využit poprvé. Hardwarová zařízení, jako například routery, využívající tuto technologii jsou vizuálně velmi snadno identifikovatelná díky počtu antén. Nejčastěji mají antény tři, některé modely mívají dvě. [6] [7] [14]

Nutno ještě dodat, že všechny WiFi sítě pracují v režimu poloviční duplexu. Tedy že mohou v jednu chvíli buďto pouze vysílat nebo pouze přijímat. Tato skutečnost výrazně ovlivňuje rychlost a podílí se na tom, že v praxi nejsou teoretické maximální rychlosti ani zdaleka dosahovány.

Výše jsou popsány standardy nejvýznamnější a nejdůležitější pro problematiku WiFi sítí. Pro úplnost uvádím výčet všech standardů normy 802.11.

Tab 1: Všechny standardy normy IEEE 802.11 (zdroj [14], vlastní zpracování)

Dodatky standardu IEEE 802.11	
IEEE 802.11	Původní standard pro 1 a 2 Mbit/s rychlost s frekvencí 2.4 GHz (1999)
IEEE 802.11a	54 Mbit/s, 5 GHz standard (1999, produkty od 2001)
IEEE 802.11b	Vylepšení 802.11 s podporou 5.5 a 11 Mbit/s (1999)
IEEE 802.11c	Bezdrátové přemostění (*bridge*); (2001)
IEEE 802.11d	Mezinárodní roamingový dodatek (2001)
IEEE 802.11e	Vylepšení Quality of Service QoS, vč. dlouhých (*burst*) paketů (2005)
IEEE 802.11F[1]	Komunikace mezi bezdrátovými přístupovými body (2003) **Stažen v březnu 2006**
IEEE 802.11g	54 Mbit/s, 2.4 GHz standard (zpětně kompatibilní s 802.11b) (2003)
IEEE 802.11h	Správa spektra 802.11a (5 GHz) pro Evropu (2004)
IEEE 802.11i	Vylepšený autentifikační a šifrovací algoritmus (WPA2) (2004)
IEEE 802.11j	Dodatek pro Japonsko; nová frekvenční pásma pro multimedia (2004)
IEEE 802.11k	Vylepšení správy rádio zdrojů pro vysoké frekvence. (Navazuje na IEEE 802.11j)
IEEE 802.11l	(rezervováno a nebude použito)
IEEE 802.11m	Správa standardu: přenosové metody a drobné úpravy
IEEE 802.11n	Vylepšení pro vyšší datovou propustnost
IEEE 802.11o	(rezervováno a nebude použito)
IEEE 802.11p	Bezdrátový přístup pro pohyblivé prostředí (auta, vlaky, sanitky)
IEEE 802.11q	(rezervováno a nebude použito, aby se nepletlo s IEEE 802.1Q)
IEEE 802.11r	Rychlé přesuny mezi přístupovými body (roaming) (2008)
IEEE 802.11s	Samo organizující se bezdrátové sítě. (*ESS Mesh Networking*)
IEEE 802.11T[1]	Předpověď bezdrátového výkonu – testovací metody
IEEE 802.11u	Spolupráce se sítěmi mimo 802 standardy (například s mobilními sítěmi)
IEEE 802.11v	Správa bezdrátových sítí (konfigurace klientských zařízení během připojení)
IEEE 802.11w	Chráněné servisní rámce
IEEE 802.11x[2]	(rezervováno a nebude použito)
IEEE 802.11y	Pro běh ve frekvenčním pásmu 3650 – 3700 MHz (veř. pásmo v USA)

[1] 802.11F a 802.11T jsou samostatné dokumenty, a nejsou to tedy dodatky k IEEE 802.11 standardu. Proto obsahují velké písmeno.

[2] Pojem 802.11x je neformálně používán k označení libovolného 802.11 standardu. (Standard IEEE 802.1X pro řízení přístupu k síti založený na autentikaci a filtrování portů, je běžně nesprávně označován jako 802.11x.)

3.4.2. WiFi

Jedná se asi o nejznámější formu bezdrátové rádiové komunikace. Když se řekne WiFi, ví i laik o co se jedná. Tato zkratka se stala součástí běžné slovní zásoby. V češtině z této zkratky dokonce vznikla více či méně povedená slova. Tato zkratka vznikla ze slovního spojení *Wireless Fidelity* (bezdrátová spolehlivost) a ve standardizaci IEEE je popsána právě normou 802.11. Dnes již prakticky každé běžně dostupné zařízení s internetovým prohlížečem disponuje touto technologií. Laptopy počínaje a kapesními počítači a mobily konče. Většina z nich podporuje všechny běžně používané standardy, tedy 802.11a/b/g. Některé novější přístroje už podporují i standard 802.11n.

V každém větším městě České republiky je dnes možné najít tzv. „WiFi hotspoty." Velká většina kaváren a restauračních zařízení láká zákazníky označením „WiFi free zone." Tento na jednu stranu příjemný a komfortní fakt má však také svá úskalí. Kromě již několikrát zmíněné přehlcenosti bezlicenčního pásma ve městech je to často slabé nebo dokonce nulové zabezpečení těchto sítí. Je třeba k nim jako k takovým přistupovat a uvědomovat si rizika, která plynou z použití těchto veřejně dostupných sítí. Mnoho lidí si bohužel tento fakt neuvědomuje nebo o něm ani neví. Veřejné sítě mají jistě své velké využití, nejsou však vhodné pro odesílání citlivých dat jako jsou hesla a osobní údaje.

Obrázek 4: WiFi logo (zdroj: www.wi-fi.org)

Důvodem špatného zabezpečení veřejných sítí je často neodbornost osoby, která takový přístupový bod zřizovala. Routery bývají již továrně přednastavené a stačí je zapojit do sítě. Na druhou stranu, kvalitní zabezpečení zde zřejmě také není zcela na místě, protože heslo je pak stejně jakýmsi „veřejným tajemstvím“ a do značné míry pozbývá významu. Navíc je žádoucí, aby takové heslo nebylo příliš komplikované, protože už samotná jeho existence snižuje uživatelský komfort.

3.5. Zabezpečení

Zabezpečení bezdrátové sítě patří k nejdůležitějším parametrům, které je potřeba při návrhu a realizaci zohlednit. Důvody jsou zřejmé. Na rozdíl od klasické kabelové sítě je ta bezdrátová o mnoho náchylnější k různým útokům. Pro útočníka je o mnoho jednodušší odposlouchávat síť, kde se signál šíří volně vzduchem, než tu, kde signál putuje v uzavřeném systému kabelů. Proto je nanejvýš vhodné věnovat zabezpečení tím větší pozornost, čím citlivější data po síti budou putovat.

V podnikovém prostředí se WLAN používá většinou jako jakési „prodloužení" klasické LAN, nejčastěji Ethernetu. Měla by tedy podle všech předpokladů plnit stejné funkce, a proto by měla splňovat i stejné bezpečnostní standardy jako celá síť. Na její budování, správu a zabezpečení musí být nahlíženo jako na součást komplexní podnikové sítě a nesmí být chápána odděleně. [5]

„Domácí sítě poskytují uživateli možnost efektivně propojit veškerá potřebná zařízení v domácnosti do jediné sítě, od výpočetní techniky přes spotřební elektroniku až k domácím spotřebičům a elektronickým systémům (pro automatizaci domácnosti). Domácí WLAN nemá běžně takové nároky na spolehlivost a výkonnost jako podniková WLAN. S rozvojem širokopásmových přípojek, které zařízení připojená na domácí síť sdílejí, se ovšem nároky na kapacitu zvyšují (pro přenos objemných souborů, od audia po komprimované video) a také domácí pracovníci mají vyšší požadavky na spolehlivost a také bezpečnost." [5, s. 55]

Ani ta nejobyčejnější domácí síť by však neměla být z hlediska zabezpečení podceňována. Kromě klasického brouzdání po internetu totiž dnes prakticky každý uživatel využívá mnoho stránek, kde je třeba se přihlašovat jako například email, sociální sítě apod. Hesla k takovým přístupům bývají často posílána v nešifrované formě a mnoho z těchto stránek nepoužívá ani zabezpečený protokol *https*. Pokud není síť nijak zabezpečena, je velmi snadné tato hesla získat a útočníkovi již nic nebrání v jejich přečtení a zneužití. Dále pak dnes již běžně většina domácností používá nástroje jako internetbanking. Tady je úroveň zabezpečení samotné komunikace se serverem podstatně vyšší, nicméně ani v tomto případě není na místě podceňovat zabezpečení

bezdrátové sítě. Nemluvě o možnosti zneužití dat z počítačů připojených do bezdrátové sítě.

Vzhledem k zaměření mé práce je klíčové zabezpečení WiFi sítí. Ostatní bezdrátové sítě tedy v této kapitole zmiňovat nebudu. Je více možností, jak WiFi síť zabezpečit. Počínaje skrytím sítě, přes filtr MAC adres a firewall až po různé druhy šifrování. Postupně si ty nejvýznamnější z nich probereme a popíšeme si jejich přednosti a slabiny. Na závěr se pokusím doporučit optimální nastavení zabezpečení pro veřejnou, domácí a firemní síť.

3.5.1. SSID

Tato zkratka znamená *Service Set IDentifier*. Je to tedy vlastně unikátní název sítě. Identifikátor je dlouhý až 32 oktetů a používá se pro označení všech prvků systému WLAN. Tento název implicitně vysílá AP[3] v pravidelných intervalech, typicky 100 ms, jako součást administrativní signalizace (tzv. *beacon*) do éteru, čímž ohlašuje svou přítomnost. Dává tak o sobě vědět, aby klienti, kteří vyhledávají AP, mohli síť snadno nalézt a připojit se k ní. Znalost názvu sítě zároveň brání klientovi, aby se omylem připojil k jinému přístupovému bodu. [1] [5]

Tato funkce usnadňuje připojení k síti a je užitečná zejména pro veřejné přístupové body, jakými jsou tzv. „free WiFi“ např. v kavárnách nebo jiných veřejných prostorách. Na základě těchto vysílání všech AP v dosahu se generuje seznam sítí při vyhledávání přes funkci zobrazení dostupných sítí.

Při pohledu z hlediska bezpečnosti však toto vysílání není zrovna vhodné. Útočník při takovémto nastavení nemá žádnou práci nalézt hledanou síť. Přístupový bod mu sám říká kdo je a nabízí, aby se připojil. Vysílání SSID je možné vypnout. Síť pak sama o sobě nedává vědět a klient, který se chce připojit, ji nenajde v seznamu dostupných sítí, pokud nezná její přesný název a cíleně ji nevyhledá. Takto nastavenou síť však nelze brát jako uzavřenou, protože pro útočníka není příliš těžké zjistit přítomnost sítě z komunikace připojených klientů. Pokud je útočník trošku znalejší, je schopen jednoho z připojených klientů odpojit tak, že vytvoří podvržený paket, který přikáže klientovi,

[3] AP = Access Point (přístupový bod)

aby se odpojil. Při opětovné snaze klienta o připojení pak stačí zachytit asociační paket a vyčíst z něj hodnotu SSID, která není nijak šifrována. [1] [5]

Smysl skrytí SSID tak spočívá hlavně v tom, aby byla síť skryta před náhodnými kolemjdoucími. Pokud útočník necílí konkrétně na tuto síť, je taky pravděpodobné, že jej složitější postup útoku odradí a najde si snadnější cíl.

3.5.2. Filtrování MAC adres

Bezdrátové karty mají, stejně jako klasické ethernetové karty, svou výrobcem vygenerovanou MAC (*Media Access Control*) adresu. Ta by měla být celosvětově unikátní. Její přidělování jsem již popsal výše. Zabezpečení pomocí filtrace MAC adres je založeno na tom, že se v AP udržuje aktuální seznam MAC adres, které jsou autorizovány pro přístup do sítě. Klient, který má MAC adresu, která není v seznamu, nedostane do sítě přístup.

Toto zabezpečení má však základní slabinu v tom, že MAC adresu je možné softwarově změnit. Mnoho bezdrátových karet je vybaveno ovladačem, který toto umožňuje, případně je to možné provést jiným dodatečně nainstalovaným softwarem. MAC adresy posílané po síti nejsou nijak šifrovány, proto je může útočník snadno odposlechnout a přiřadit své kartě MAC některého klienta s povoleným přístupem do sítě. Pak už stačí jen počkat, až se vybraný klient odpojí a vydávat se za něj. Případně si může nastavit MAC adresu přístupového bodu a vybranému klientovi poslat falešný paket s příkazem k odpojení. Potom už se může vydávat za odpojeného klienta a získat povolení pro vstup do sítě. [1]

Filtrování MAC adres je navíc nevhodné řešení pro podnikové využití. Čím větší firmu uvažujeme, tím je obtížnější toto zabezpečení používat. Je totiž nutné udržovat neustále aktuální seznamy MAC adres ve všech AP a to je vzhledem k tomu, že se v podnikovém prostředí tato zařízení často střídají nebo přibývají, velmi náročné. Taková administrace je v praxi neudržitelná. Naopak v malé kanceláři nebo domácím prostředí je to poměrně vhodný doplněk jiných druhů zabezpečení. Zde totiž bývá víceméně konstantní počet klientských zařízení.

Nejedná se opět o plnohodnotný druh zabezpečení. Jeho účelem je spíše odradit případného útočníka, který si většinou najde snadnější oběť. Jako doplněk jiných zabezpečení pro domácnost nebo malý podnik lze doporučit.

3.5.3. WEP

Zabezpečení WEP (*Wired Equivalent Privacy*) je dnes stále ještě hodně používanou formou ochrany. Vznikl jako volitelný doplněk ke standardu 802.11b za účelem zabezpečení přenášených dat. Zde už tedy (na rozdíl od předchozích případů) můžeme skutečně mluvit o zabezpečení jako takovém. Dalším účelem jeho vzniku bylo řízení přístupu k síti. Protokol 802.11 totiž nemá žádný mechanismus, kterým by se síť mohla identifikovat jako jednoznačně veřejná nebo naopak uzavřená. Jediný dostupný a známý údaj je SSID. Použití WEP tedy jasně dává tušit, že se jedná o uzavřenou soukromou síť. [1] [5]

Jak již z názvu vyplývá, myšlenkou WEP bylo zajistit zabezpečení bezdrátové sítě na stejné úrovni, jako má klasická LAN. Tento cíl bohužel ve výsledku nesplnil. Měl by sloužit především pro autentizaci a také pro ochranu přenášených dat a to pomocí šifrování se stejným sdíleným tajným klíčem. Norma však nespecifikuje způsob distribuce klíčů. Ta je problémem především ve větších organizacích. V prostředí malé sítě nepředstavuje nutnost změny hesla zase tak významnou překážku. Ale při představě, že je nutné heslo měnit pokaždé, když společnost opustí zaměstnanec, který jej znal, nebo když dojde k odcizení např. notebooku, by asi nikdo nechtěl být v kůži administrátora velké firmy s několika stovkami počítačů. [1]

Wi-Fi Alliance pro certifikaci WiFi produktů požaduje WEP povinně. To je možná taky jeden z důvodů jeho stálé oblíbenosti a častého použití, přestože (jak si dále vysvětlíme) je dnes již překonán a není z dnešního pohledu zrovna bezpečný. Kdyby nebyla jeho přítomností v hardwaru pro bezdrátové sítě podmíněna certifikace, možná by jej dnes už téměř nikdo neznal a sloužil by jen pro pochopení šifrovacích principů při výuce kryptografie. [5]

Nebudu se vzhledem k obecnějšímu zaměření mé práce a snaze o celkový pohled na problematiku bezdrátových sítí snažit rozebrat fungování a postupy při šifrování metodou WEP dopodrobna. Spíše se pokusím naznačit principy fungování, popsat její

nedostatky a naznačit možnosti útoku. Pokusím se shrnout vhodnost či nevhodnost užití WEP v různých prostředích, kde se lze s bezdrátovými sítěmi setkat.

Autentizace

U metody WEP je použit symetrický postup. To znamená, že pro šifrování a dešifrování se používá stejný algoritmus i stejný klíč. Autentizace se může provádět dvěma způsoby:

- otevřeně (*open system*)
- na základě sdíleného klíče (*shared key*). [5]

„Otevřená autentizace (implicitní) není založena na žádném prověření 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.“ [5, s. 68]

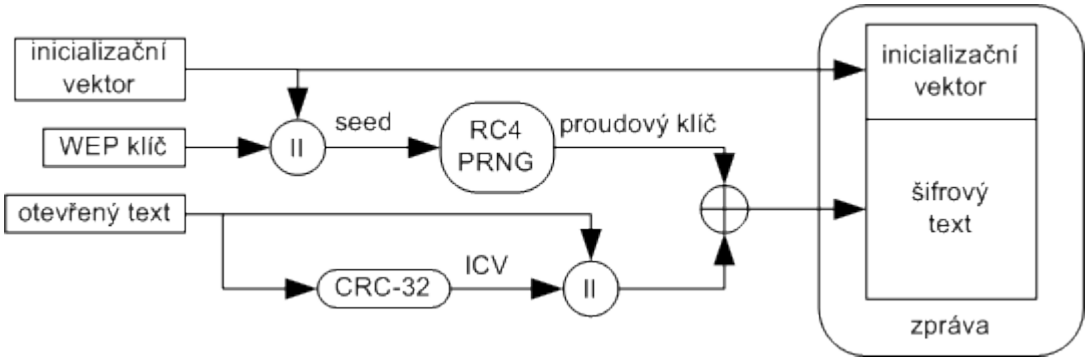
“Při **autentizaci sdíleným klíčem** se použije 40bitový uživatelský klíč, který je statický a stejný pro všechny uživatele dané sítě (sdílený klíč, *shared secret*). Ve skutečnosti se ověřuje totožnost síťové karty, nikoli samotné osoby uživatele, což je jedna z hlavních slabin autentizace v rámci WEP.“ [5, s. 69]

Otevřená autentizace je ve WLAN implicitní volbou. Probíhá tak, že klient pošle autentizační rámec, který obsahuje jeho identifikační údaje a příjemce, což může být AP nebo jiný klient, zkontroluje identitu stanice a zpátky pošle rámec *authentification verification* (ověření autentizace). [5]

Autentizace na základě sdíleného klíče probíhá tak, že klient vyšle rámec, jenž obsahuje jeho identifikační údaje a požadavek na autentizaci, příjemce zpět pošle výzvu (*challenge*). Klient odpoví autentizátorovi tak, že pošle výzvu zašifrovanou pomocí WEP a klíče, který je odvozen ze sdíleného autentizačního klíče. Autentizátor tuto zprávu dešifruje a porovná výsledek s původní výzvou. Poté o výsledku informuje klienta. A to je právě jedna ze slabin WEP, protože se přenáší otevřený text, který je ihned následován textem šifrovaným, což útočníkovi dává možnost odhalit klíč. [5]

Šifrování

„Proces šifrování vždy začíná nešifrovaným textem, který chceme chránit. Nejprve WEP z tohoto textu vypočítá 32bitový cyklický redundantní součet (CRC), tedy kontrolní součet pro ověření integrity dat. Tento kontrolní součet se následně připojí za přenášenou zprávu. Dále vezmeme tajný klíč a připojíme jej k inicializačnímu vektoru (IV). Kombinaci IV a tajného klíče předáme do generátoru pseudonáhodných čísel RC4 (PRNG) a výstupem bude šifrovací klíč. Šifrovací klíč je sekvence nul a jedniček stejně dlouhá jako původní zpráva plus kontrolní součet. Následně mezi textem spojeným s kontrolním součtem a šifrovacím klíčem provedeme logický výhradní součet (XOR). Výsledkem je šifrovaný text. Před něj připojíme hodnotu inicializačního vektoru a tento výsledek pak přenášíme.“ [1, s. 45]



Obrázek 5: Princip šifrování WEP [13]

Slabiny

Ačkoliv je WEP šifrování povinně na každém zařízení splňujícím normu 802.11, nebývá implicitně zapnuté. Je na uživateli, aby jej aktivoval. Může si zvolit ze dvou typů šifrování – 64bitové a 128bitové. V obou případech zabírá prvních 24 bitů inicializační vektor. Velkou slabinou protokolu WEP je pravidlo, které zakazuje opakované použití inicializačního vektoru. Předpokladem správné funkce je totiž to, že se každý paket bude šifrovat generátorem RC4 při použití jiné inicializační hodnoty. Jakmile ale dojde prostor inicializačních vektorů, musí se začít opakovat. Vzhledem k délce IV 24 bitů může k tomuto dojít během několika hodin. Útočníkovi tedy stačí poměrně krátkou dobu odposlouchávat provoz na síti a nasbírat dostatek paketů. Jakmile dojde k opakování IV, je již možné data dešifrovat. Příliš velkou roli v tomto případě nehraje ani délka samotného klíče. [1] [5]

Další slabinou protokolu WEP je jednoduchý mechanický útok. Bezpečnost sítě lze narušit krádeží jednoho z koncových zařízení. Jak jsem již zmínil výše, heslo je zde sdíleným tajemstvím a je pro všechny účastníky totožné. Jakmile dojde k takovémuto narušení bezpečnosti, musí se provést kompletní změna všech klíčů v celé síti, tedy ve všech zařízeních. [5]

„Další možnost, jak zjistit WEPový klíč, je útok hrubou silou. Sdílená tajná část WEPového klíče má délku 40 nebo 104 bitů podle toho, jak silný klíč používáme. Bezpečnostní specialista Tim Newsham zjistil, že u některých výrobců špatně funguje generátor klíče. Útok hrubou silou na 40bitový klíč vytvořený slabým generátorem může trvat zhruba minutu.“ [1, s. 51]

Shrnutí

Navzdory prakticky neustálému rozvoji zabezpečovacích mechanismů a specifikací pro WLAN lze předpokládat, že se bude protokol WEP používat ještě dlouho. A to zejména z těchto důvodů:

- jednoduchost nastavení
- podpora ze strany všech produktů s 802.11
- prvky stávajících sítí nemusí podporovat novější a vylepšené mechanismy zabezpečení
- nový hardware ve spojení se staršími zařízeními neřeší bezpečnostní slabinu sítě, tedy WEP
- komplikace s upgradem firmwaru a ovladačů na podporu vyššího zabezpečení
- implementace 802.11i / WPA2 vyžaduje většinou i upgrade hardwaru [5]

Názory na použití protokolu WEP se v odborné lieratuře i komentářích IT odborníků značně liší. Podle mého názoru je z pohledu domácí sítě na místě tvrzení, že je lepší toto zabezpečení, než žádné. WEP zde plní jednak funkci jakési značky, že se opravdu jedná o soukromou síť a pak také do značné míry zajišťuje, že útočník půjde tzv. „o dům dál.“ Ve většině případů nejsou pro něj data v konkrétní síti natolik cenná, aby ztrácel čas s prolomením tohoto zabezpečení. Daleko jednodušší je napadnout jinou síť. Přítomnost

WEP zabezpečení navíc může mít zásadní vliv při případném právním sporu, protože takto „zamknutá“ síť je jednoznačně brána jako soukromá.

Z pohledu veřejné sítě mohu WEP jen doporučit. V prostředí kavárny nebo podobného veřejného místa s přístupovým bodem se předpokládá snadná konektivita a naopak se neočekává silné zabezpečení pro práci s velmi citlivými daty. Na druhou stranu je často žádoucí, aby k síti měli přístup např. jen zákazníci konkrétního podniku nebo jinak specifikovaná skupina lidí.

Naopak z pohledu podnikové sítě podle mého názoru protokol WEP doporučit nelze. V tomto prostředí se často pracuje s mnohem citlivějšími daty a navíc celá režie kolem případné změny klíčů je dosti náročná. O odrazení útočníka na úkor snadnějšího cíle zde asi taky nemůžeme uvažovat. Pro podnikové řešení je jednoznačně vhodnější nějaký sofistikovanější systém zabezpečení.

3.5.4. TKIP

Protokol TKIP (*Temporary Key Integrity Protocol*) byl vyvíjen s cílem odstranit hlavní známé nedostatky WEP. Proto bývá také často označován jako „WEP-fix.“ Jak již samotný název napovídá, hlavní inovací je zde použití dočasných klíčů. Protokol TKIP obsahuje tyto funkce:

- mixování klíče pro každý paket
- vylepšená funkce kontroly integrity – *Message Integrity Check* (MIC), pojmenovaná Michael[4]
- vylepšená pravidla pro generování inicializačního vektoru včetně sekvenčních pravidel [1]

V podstatě se jedná o dočasnou opravu protokolu WEP, která byla vyvíjena tak, aby bylo bez problému možné implementovat ji jednoduchým upgradem softwaru. Z požadavku zpětné kompatibility plynou velké kompromisy oproti původnímu řešení, přesto však je TKIP účinným bezpečnostním mechanismem.

[4] Jedná se o jednocestnou hashovací funkci, která není lineární. Pro útočníka je tak obtížné modifikovat paket při přenosu. Výstup algoritmu je dlouhý 8 bajtů a je součástí přenášených dat. [1]

Silnějšího zabezpečení je zde dosaženo dynamicky se měnícím klíčem pro každý paket a také delším inicializačním vektorem, který má nyní 48 bitů. Dále se zde používá již zmíněná kontrola integrity zpráv MIC. Novinkou je zde sekvenční počítadlo, díky kterému se zvyšuje hodnota IV postupně a všechny pakety s IV mimo očekávanou posloupnost se zahazují. Ztracené pakety jsou zde řešeny tak, že software si pamatuje posledních 16 hodnot IV a kontroluje, zda opětovně vyslaný rámec do něj zapadá. Pokud ano a nebyl dosud obdržen, je přijat. [5] [6]

Šifrovací klíč, který je zde označován jako *Temporary Key* (TK), má délku 128 bitů a mění se každých 10 000 paketů. Klíč pro zajištění integrity (MIC) je 64bitový a nahradil zde prostý kontrolní součet používaný u WEP. Délka inicializačního vektoru se zdvojnásobila na již zmíněných 48 bitů. [1] [6] [7]

Nebudu zde dopodrobna popisovat funkci protokolu TKIP. K povědomí o zlepšené bezpečnosti je dostatečná znalost funkce WEP a přínosy TKIP, které jsem nastínil výše. TKIP řeší především tyto slabiny:

- útok opakováním – lze opakovaně použít hodnotu IV
- podvržení
- útoky založené na kolizi – kolize IV
- útoky na slabé klíče [1]

Protokol TKIP řeší mnohé slabiny WEP a i když je to řešení na půli cesty k bezpečnému šifrování i autentizaci, lze jeho použití jednoznačně doporučit.

3.5.5. AES

Tato zkratka znamená *Advanced Encryption Standard*. Jedná se o blokový šifrovací algoritmus, který je založen na DES[5]. Je to jeho přímý nástupce, založený na Rijndaelovu algoritmu. Ten specifikuje použití klíčů o délkách 128, 192 nebo 256 bitů na šifrování bloků, které mají délky rovněž 128, 192 nebo 256 bitů, přičemž je možná libovolná kombinace délky klíče a bloku. Šifra AES odpovídá americkému federálnímu standardu FIPS (*Federal Information Procesing Standard*) a byla navržena z důvodu

[5] „DES (*Data Encryption Standard*) je příkladem soukromého klíče. K efektivnímu využití postačí délka klíče typicky 40 nebo standardně 56 bitů. DES již není nerozluštitelný, proto se doporučuje používat silnější šifrování trojitým použitím klíče DES (3DES, ANSI, X9.52).“ [6, s. 376]

nutnosti nahrazení RC4. Před přijetím byla šifra podrobena rozsáhlá analýze a revizi ze strany americké vlády. I z těchto důvodů lze AES považovat za velmi vyspělý a sofistikovaný bezpečnostní mechanismus. [1] [6]

Šifra AES byla vyvinuta v roce 1997 týmem belgických kryptografů a je součástí specifikace 802.11i vydané a schválené v roce 2004, stejně jako WPA2 (viz níže). Jak jsem již zmínil, jedná se o blokový šifrovací mechanismus, protože pracuje s bloky textu o velikosti 128bitů. Stejně jako RC4 pracuje i AES se symetrickým klíčem, což znamená, že text se šifruje i dešifruje stejným tajným klíčem, který obě strany sdílí. [1]

Výsledkem AES je podstatně silnější šifra, než při použití WEP/TKIP a RC4. Nevýhodou však jsou zvýšené šifrovací nároky, které vyžadují nový hardware. V době, kdy byla šifra schválena, nebyly tehdejší zařízení výkonově dostatečné. Z toho vyplývá nekompatibilita s předchozí generací bezdrátových zařízení. Tento fakt způsobil pomalejší rozšíření standardu 802.11i, jehož je AES součástí. [1]

Dnes je možné šifrování i autentizaci pomocí AES jedině doporučit. Nároky na hardware už nejsou překážkou a kompatibilita se všemi zařízeními je dnes zaručena. Výrobci se navíc většinou snaží splňovat rovnou standard 802.11n, pro který je šifrování AES podmínkou. V prostředí veřejných sítí je použití AES podle mého názory přehnané, ale pro dobře zabezpečenou domácí síť je rozhodně přínosné a pro podnikovou síť je pak nutností.

3.5.6. WPA

Protokol WPA byl vydán v roce 2002. Jedná se o dočasné řešení, které si vynutily okolnosti kolem zjištění a zveřejnění všech slabin WEP. V té době byl vyvíjen standart 802.11i, který ale ještě nebyl hotov. *Wi-Fi Alliance* však rozhodla, že je nutné vydat alespoň toto polovičaté řešení, protože důvěra ve WEP významně klesla. Původně byl projekt vyvíjen pod názvem WEP2, ale bylo rozhodnuto, že ztracená důvěra si žádá jiný název. Protokol byl tedy pojmenován zkratkou WPA, která znamená *WiFi Protected Access*. [4] [7]

WPA si lze představit jako podmnožinu prvků 802.11i. Byly zvoleny takové prvky, aby byl možný přechod z WEP na WPA pouze aktualizací softwaru. Protože bylo WEP

od začátku bráno jako dočasné řešení, bylo logické, že by nemělo vyžadovat výměnu hardwaru. Naprostá většina zařízení tedy mohla být upravena pouhým provedením softwarových/firmwarových změn. Z tohoto důvodu také WPA používá stejný šifrovací mechanismus jako WEP, tedy RC4. Je zde však použit protokol TKIP, který je podrobněji popsán výše. Protože protokol TKIP používá složitější algoritmus, má implementace WPA jistý vliv na výkonnost zařízení. Uvádí se něco mezi 5-15 %. Výhodou WPA je použití dynamických klíčů, je zde však ponechán prostor i pro klíče statické, které je vhodné použít např. v prostředí domácí sítě. [5]

Jak jsem již uvedl, jedná se o podmnožinu 802.11i, takže stejně jako je WPA zpětně kompatibilní s WEP, je i dopředně slučitelné s 802.11i. Ještě však neobsahuje některé jeho prvky, jako například AES. Jistým úskalím kompatibility je však skutečnost, že pokud se v síti nachází byť jen jeden prvek, který WPA nepodporuje, klesá zabezpečení celé sítě na úroveň WEP. Není totiž možné používat v jedné síti oba mechanismy současně. [4] [5]

Tři hlavní složky WPA:

- *Tepmorary Key Integrity Protocol* (TKIP)
- *Message Integrity Check* (MIC) – ochrana proti falešným přístupovým bodům zajištěním integrity dat
- *Extensible Authentication Protocol* (EAP) – vzájemná autentizace uživatele i sítě a distribuce klíčů [5] [7]

„WPA nabízí různé režimy autentizace pro různá prostředí: v podnikovém prostředí předpokládá využití centralizovaného autentizačního serveru zodpovědného za distribuci klíčů (typicky RADIUS), zatímco v prostředí domácích sítí se používá jednodušší režim přednastaveného klíče (PSK, *Pre-Shared Key*), kdy stanice tento klíč sdílí s AP a žádné ověřování identity se dál neprovádí. Domácím uživatelům postačí manuálně nakonfigurovat heslo (*master key*) na přístupový bod a na všechna připojovaná zařízení.“ [5, s. 94]

RADIUS

Jedná se o službu (poskytovanou serverem) pro autentizaci vzdálených uživatelů. Název vznikl jako zkratka slov *Remote Authentification Dial-In User Service*. Tato

služba především zodpovídá za ověření uživatelů před udělením přístupu do sítě. Pracuje na principu klient/server a má tři složky – protokol, server pro autentizaci (RADIUS server) a klient. Transakce mezi serverem a klienty se provádí za použití sdíleného tajemství (hesla). Toto heslo se nikdy nepřenáší v síti. Uživatelská hesla se navíc posílají na trase mezi klienty vždy zašifrovaná. RADIUS se využívá pro přístup do podnikových sítí včetně WLAN. [3]

3.5.7. WPA2

V roce 2004 byl vydán standard 802.11i, jehož součástí je WPA2. Vychází částečně ze svého předchůdce, avšak nepoužívá již šifrovací mechanismus RC4. Místo něj je zde použit AES. Přítomnost WPA2 je povinná pro prvky specifikace WiFi podle 802.11n. WPA2 je zpětně slučitelné s WPA a míchání obou je v sítích běžné. Režim WPA2/WEP však není podporován. Certifikace pro WPA2 je stejně jako u předchůdce rozdělena do dvou kategorií, tedy pro podnikové a osobní využití. [4] [5]

3.5.8. Shrnutí

V následující tabulce je uvedeno přehledné srovnání výše popsaných typů zabezpečení. Jak je patrné, nejvyšší stupeň zabezpečení nemusí být vždy nejvhodnějším. Není tím samozřejmě myšleno to, že by pro domácí sítě nebyl tak bezpečný, jako pro sítě podnikové. Spíše je zde zohledněna složitost implementace a fakt, že v domácím prostředí je tato volba zbytečně nadhodnocena a ubírá uživatelský komfort.

Tab. 2: Doporučení pro nasazení bezpečnostního řešení v sítích [5]

	autentizace	šifrování	použitelnost pro podnikové sítě	použitelnost pro domácí sítě
WEP	Nulová	WEP	nedostatečná	dobrá
WPA (PSK)	PSK	TKIP	nedostatečná	nejlepší
WPA2 (PSK)	PSK	AES	nedostatečná	nejlepší
WPA (plná)	802.1x	TKIP	lepší	dobrá
WPA2 (plná)	802.1x	AES	nejlepší	dobrá

4. Analýza problému a současného stavu

Při řešení praktické části své bakalářské práce jsem spolupracoval s mezinárodní spediční firmou sídlící na Opavsku. Firma se zabývá mezinárodním i vnitrostátním zasílatelstvím, přepravou v rámci celé EU, včetně bývalých států SNS, tranzitní přepravou, skladováním a přepravou v režimu Just In Time. Dále pak spíše okrajově provozuje expresní balíkovou službu a kusovou přepravu. A právě v této oblasti plánuje firma do budoucna rozšířit své pole působnosti a objem přepravovaných zásilek. V souvislosti s tímto rozhodnutím bude třeba rozšířit a modernizovat skladovací prostory. V současné době je ve výstavbě nový sklad, který by si firma přála obsluhovat pomocí moderních zařízení propojených bezdrátovou technologií. Budu se tedy ve své práci zabývat pouze tímto odvětvím firemních aktivit a budu brát v úvahu pouze prostory související se sekcí expresní balíkové služby a kusové přepravy.

4.1.Současné podmínky

Současný sklad je řešen na dnešní poměry již nevyhovujícím a zastaralým způsobem. Z tohoto důvodu bylo rozhodnuto o výstavbě nové budovy a je požadováno co nejsnadnější řešení naskladňování a vyskladňování zboží z pohledu manipulace s balíky. Ve starém skladě je nutno buď manuálně do systému zadávat EAN kódy jednotlivých balíků nebo skenovat balíky laserovým snímačem čárových kódů v blízkosti počítače.

Současný sklad obsluhuje jeden skladník, který pracuje se stolním počítačem HP Compaq Pro6000 MT, ke kterému je přes USB port připojena multifunkční laserová tiskárna Samsung SCX-3200. Tiskárna umožňuje jak skenování či kopírování dokumentů, tak i tisk čárových kódů na samolepící papír, což se využívá při označování veškerých zásilek. Pro zjednodušení naskladňování zásilek je k počítači připojena laserová čtečka čárových kódů Honeywell MS9540 VoyagerCG, rovněž přes USB port. Počítač z důvodu stability a nenáročnosti běží, stejně jako všechny ostatní počítače ve firmě, pod operačním systémem MS Windows XP Professional SP3. Do budoucna se však předpokládá přechod na MS Windows 7.

4.1.1. Konfigurace počítače:

HP Compaq Pro6000 MT

Procesor Intel Core 2 Duo E5700 (3.0 GHz, 3 MB L2 cache, 1066 MHz FSB)

Harddisk 320 GB Serial ATA 3.0-Gb/s NCQ, Smart IV (7200 rpm)

Paměti 2 GB DDR3 DRAM 1066 MHz

OS: MS Windows XP Professional SP3

4.1.2. Příslušenství:

Klávesnice, myš

Tiskárna Samsung SCX-3200 1200x1200 16ppm USB

Laserová čtečka čárových kódů Honeywell MS9540 VoyagerCG, USB (KBD)

Obrázek 6: Tiskárna Samsung SCX-3200 (zdroj: www.atcomp.cz)

Obrázek 7: Čtečka čárových kódů Honeywell MS9540 VoyagerCG (zdroj: www.atcomp.cz)

4.2. Nástin problému

Současný systém skladu je nevyhovující především z důvodu nutnosti přílišné manipulace s balíky, která je časově náročná a tudíž neefektivní. Zboží je nutné buď vždy přinést na pracoviště skladníka a sejmou jeho kód nebo procházet sklad či auto se zbožím a následně zadávat poznamenané kódy do počítače ručně. Tato možnost je navíc u větších balíků jediná možná. Takovéto dočasné řešení neumožňuje plánovanou expanzi na trhu expresních balíkových přeprav.

Firma proto chce v budově nového skladu řešit tento problém bezdrátovou technologií. Pomocí bezdrátových snímačů čárových kódů apod. Pro tyto účely by měla být dostačující WiFi síť pracující v pásmu 2,4 GHz. Vzhledem k umístění areálu firmy na okraji města v lokalitě s ne příliš hustou zástavbou a v kombinaci s použitím 13. kanálu tohoto kmitočtu by rušení neměl být problém.

Budova nového skladu bude postavena přímo v areálu firmy v těsné blízkosti jedné z hlavních budov, kde je umístěna serverovna. Mezi těmito budovami bude postaven spojovací průchod, takže ani napojení nového objektu na stávající firemní síť nebude problém a v projektu se s ním počítá.

5. Vlastní návrh řešení

Pří návrhu řešení jsem vycházel z požadavků firmy na vysokou kvalitu a spolehlivost použitého systému při zachování minimálních servisních nákladů a předem daného rozpočtu na realizaci, který byl maximálně 30 000 korun. Jedním z požadavků bylo zachování stávajícího systému a celkového řešení tak, aby pouze přibyla výhoda bezdrátové technologie a nebyly nutné žádné organizační či systémové změny ve způsobu práce a také aby nebylo nutné příliš rozsáhlé přeškolování personálu. Dále jsem návrh přizpůsobil plánovanému budoucímu přechodu firmy na systém MS Windows 7 tak, aby nebyly nutné žádné další investice.

Stávající hardwarové vybavení skladu bylo před nedávnou dobou inovováno a je technicky na dobré úrovni. Není proto nutné pořizovat nový počítač. Rovněž současně používaná tiskárna je dostatečná a není ji proto nutné měnit. Laserová čtečka čárových kódů Honeywell zůstane činnosti pro případ poruchy nebo náhlého výpadku bezdrátové sítě.

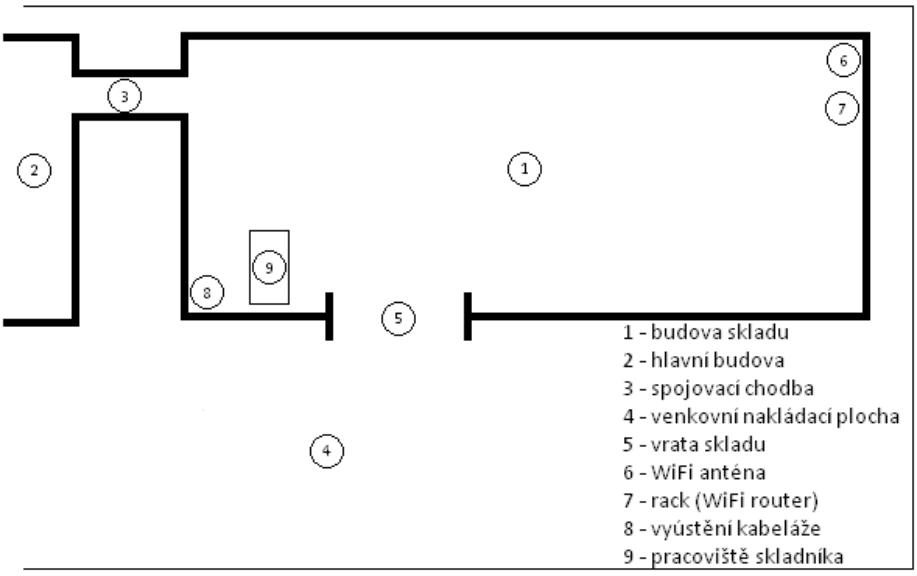
Projekt budovy skladu předpokládá při stavbě založení metalických síťových kabelů s napojením na vedlejší budovu, kde se nachází serverovna. Je tedy nutné navrhnout pouze samotné koncové řešení.

5.1. Realizace

Z důvodu jednoduchosti řešení jsem zvolil variantu jednoho WiFi routeru v kombinaci s externí anténou zesilující jeho dosah. Areál skladu a venkovní nakládací plochy je příliš velký na spolehlivé pokrytí jedním routerem se standardní všesměrovou anténou. Zařízení není možné umístit do ideální pozice uprostřed areálu a řešení se dvěma routery, které by spolehlivě pokryly celý prostor je podle mého názoru zbytečně složité a neefektivní. Variantě se směrovou externí anténou nahrává i poloha skladu v rohu parcely. Není žádoucí, aby vysílání pokrývalo zbytečně i sousední pozemky a to jak z důvodu nízké efektivity takového řešení, tak i z důvodů bezpečnostních.

5.1.1. Návrh projektu sítě

Budova skladu bude napojena na podnikovou gigabitovou síť, která běží pod MS Windows Server 2008. V centrální budově, kde se nachází i serverovna, bude instalován gigabitový switch, přes který bude objekt skladu připojen. V samotném skladu budou ve dvou protilehlých rozích vyústění kabeláže standardními konektory RJ-45. V jednom z těchto rohů bude umístěn 10 palcový uzamykatelný rozvaděč (rack) s prosklenými dvířky, ve kterém bude instalován WiFi router. V protilehlém rohu se bude nacházet pracoviště skladníka s počítačem připojeným do sítě přes UTP kabel. Rozmístění jednotlivých prvků je patrné z nákresu.



Obrázek 8: Nákres objektu

5.1.2. Použitý hardware

Jako centrální bod bezdrátové sítě jsem vybral WiFi router značky Asus, model WL-500gP V2. Jde o multifunkční zařízení spojující možnosti internetové brány, routeru i Access Pointu s integrovaným čtyřportovým switchem a řadou nadstandardních funkcí, pracující v pásmu 2.4 GHz. Podporuje standardy 802.11b/g a je „802.11i – Ready," což znamená možnost použití šifrování i autentizace protokolem WPA2. Jedním z kritérií pro jeho výběr byla i technologie Afterburner, díky které dosahuje zařízení až o 35% lepší propustnosti bezdrátového spojení, oproti standardním 802.11g zařízením a to za současné eliminace rušení. Dále disponuje technologií BroadRange, která zajišťuje větší rozsah pokrytí plochy až několikanásobně, oproti jiným 802.11g produktům. Jádrem tohoto routeru je rychlý RISCový procesor Broadcom a velká paměť DDR SDRAM, která umožňuje nasazení i v náročnějších podmínkách a zajišťuje dostatečný výkon a spolehlivost. Tento router disponuje anténním systémem se dvěma nezávislými anténami, přičemž jednu lze odpojit a nahradit dokoupenou externí anténou přes reverzní SMA konektor. Cena zařízení je 1684 korun, což je vzhledem k vlastnostem, kterými disponuje, přijatelné.

Obrázek 9: WiFi router ASUS WL-500gP V2 (zdroj: www.asus.com)

Router bude doplněn externí směrovou anténou o výkonu 13 dBi, což by mělo být dostatečné vzhledem k velikosti plochy, kterou je potřeba signálem pokrýt. Typové označení antény je BP-24PL-13 a jedná se o panelovou anténu pracující v obou rovinách záření, tedy horizontálním i vertikálním, což by mělo při správném natočení zajistit kvalitní pokrytí jak bezprostředně pod anténou, tak i v opačném rohu skladiště. Úhel vyzařování je vertikálně 38° a horizontálně 37°. Kromě skladiště samotného je žádoucí pokrýt signálem i přilehlou nakládací plochu a to nebude, vzhledem k výkonu antény, žádný problém. Anténa plně odpovídá specifikaci 802.11x a je uzavřena v hermeticky utěsněném pouzdru, což zaručuje její vysokou spolehlivost a stálost. Toto řešení umožňuje i venkovní instalaci, kterou zde sice nevyužijeme, ale je to dokladem kvality zařízení. Anténa má pevně připojený kabel Belden H-155 o délce 3 metry. Kabel je ukončen konektorem RSMA, což umožňuje přímé napojení na router bez nutnosti instalace redukcí apod.

Obrázek 10: Externí směrová anténa BP-24PL-13 (zdroj: www.atcomp.cz)

Router bude umístěn v 10 palcovém síťovém rozvaděči s prosklenými dvířky ve výšce cca 2m. Délka kabelu je dostačující, aby anténa byla umístěna na zdi na anténním držáku v optimální výšce okolo 5m nad úrovní podlahy a to jednoduše pomocí dodávaného držáku.

Obrázek 11: Rack TRITON 4U / 260 (zdroj: www.atcomp.cz)

Hlavním pracovním nástrojem bude moderní terminál MC3100 značky Motorola. Tento terminál disponuje 1D laserovým a 2D všesměrovým snímačem čárových kódů s vysokým rozlišením a barevným dotykovým displejem s rozlišením 320 x 320 obrazových bodů, který je dobře čitelný za všech světelných podmínek, tedy jak v přítmí skladiště, tak i na ostrém slunci venku na nakládací ploše. Na výběr jsou zde dva operační systémy: MS Windows Mobile 6.X nebo MS Windows CE 6.0. Zařízení podporuje bezdrátovou komunikaci ve standardech 802.11a/b/g a taky Bluetooth 2.1. Dále má komunikační rozhraní USB a RS232. Mezi jeho přednosti patří nízká hmotnost a dlouhá výdrž baterie. Z uživatelského pohledu pak také integrovaná senzorová technologie, která zvládá detekci pohybu a je tak schopna měnit orientaci displeje v závislosti na natočení přístroje nebo například uspat přístroj při položení displejem dolů atd. Další uživatelskou předností je odolnost proti opakovanému pádu a rozsah provozních teplot v rozmezí -20 až 50 °C.

Obrázek 12: Bezdrátový terminál Motorola MC3100 (zdroj: www.motorola.com)

5.1.3. Zabezpečení

První předpoklad zabezpečení je již samotné umístění antény prakticky v rohu pozemku s vyzařováním směrem do areálu firmy. Nedochází tak ke zbytečně velkému přesahu signálu do prostor, kde to není žádoucí. Přesto bych doporučil použít funkci skrytí SSID v kombinaci s filtrem MAC adres do kterého se nastaví MAC adresa síťové karty bezdrátového terminálu MC3100. Toto jsou však spíše doplňková nastavení. Hlavním bezpečnostním mechanismem by měl být protokol WPA2 v kombinaci se šifrováním AES, při použití dostatečně dlouhého a silného hesla navrženého v souladu s dodržením zásad pro tvorbu hesel. Takto zabezpečenou bezdrátovou síť s napojením na podnikovou LAN chráněnou navíc silným firewallem považuji za odpovídající bezpečnostní politice firmy.

5.1.4. Cenová kalkulace

Tab. 3: Cenová kalkulace

Mobilní terminál Motorola MC3100	23 836 ,-
Router ASUS WL-500gP V2	1 347 ,-
Externí panelová anténa BP-24PL-13	346 ,-
Rack TRITON 4U / 260	1 393 ,-
SUMA	**26 922 ,-**

Poznámka: Cenová kalkulace vychází z katalogu dodavatele AT Computers a je aktuální k 20.5.2011. Katalog je dostupný online na stránkách www.atcomp.cz. Všechny ceny jsou uvedeny bez DPH.

5.1.5. Shrnutí

Bezdrátové řešení skladu nepochybně usnadní manipulaci s balíky a ušetří mnoho času, což firmě umožní urychlení a rozšíření této sekce její činnosti a celkovou expanzi na poli expresní balíkové přepravy. Při návrhu řešení jsem vycházel ze současného stavu a požadavků firmy na zachování celkové koncepce řešení manipulace se zásilkami při zvýšení komfortu a rychlosti naskladňování a vyskladňování zásilek. Díky použití stávajícího softwaru a hardwaru je možné během okamžiku přejít zpět na původní řešení, pro případ výpadku bezdrátové sítě nebo například při potřebě chvilkového urychlení práce současným použitím bezdrátového i kabelového skeneru. Rovněž je samozřejmě možné při větším vytížení jednoduše zvýšit kapacitu dokoupením dalšího bezdrátového terminálu.

6. Závěr

Tato práce je zpracována jako celkový pohled na problematiku bezdrátových sítí. Vysvětluje základní pojmy a podrobněji přibližuje principy fungování rádiových bezdrátových sítí. Dále pak podrobně rozebírá mezinárodní standardy pro WiFi sítě. Zvláštní pozornost byla věnována zabezpečení bezdrátových sítí, kde jsem popsal různé možnosti ochrany před útočníkem a na závěr jsem se snažil doporučit optimální nastavení pro jednotlivé skupiny bezdrátových sítí.

V praktické části své práce jsem navrhl bezdrátové řešení do nové budovy skladu spediční firmy. Při návrhu řešení jsem se maximálně soustředil na uživatelský komfort, jaký takové řešení může přinést, ale současně jsem nepodcenil důležitou bezpečnostní stránku věci. Věřím, že mé řešení přinese požadované urychlení a usnadnění práce a bude fungovat k plné spokojenosti uživatelů i majitelů firmy.

7. Seznam použité literatury

1. BARKEN, L. *Wi-Fi: Jak zabezpečit bezdrátovou síť*. 1. vyd. Brno: Computer Press, 2004.174 s. ISBN80-251-0346-3
2. BRISBIN, S. *Wi-Fi: Postavte si svou vlastní wi-fi síť*. Praha: Neocortex, 2003. 248 s. ISBN 80-86330-13-3
3. HASSELL, J. *RADIUS*. Sebastopol: O'Reilly, 2002. 206 s. ISBN 0-596-00322-6
4. KÖHRE, T. *Stavíme si bezdrátovou síť Wi-Fi*. 1. vyd. Brno: Computer Press, 2004. 297 s. ISBN 80-251-0391-9
5. PUŽMANOVÁ, R. *Bezpečnost bezdrátové komunikace: Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. 1. vyd. Brno: CP Books, 2005. 179 s. ISBN 80-251-0791-4
6. PUŽMANOVÁ, R. *Moderní komunikační sítě od A do Z: 2. aktualizované vydání*. Brno: Computer Press, 2006. 430 s. ISBN 80-251-1278-0
7. ZANDL, P. *Bezdrátové sítě Wi-Fi: Praktický průvodce*. 1. vyd. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2
8. ZEZULKA, F. – HYNČICA, O. Průmyslový Ethernet I: Historický úvod. *Automa*. 2007. roč. 13. č. 1. s. 41–43
9. BOUŠKA, P. *OSI model* [online]. 2008 [cit. 2011-05-11]. Dostupné z WWW: <http://www.samuraj-cz.com/clanek/osi-model/>
10. ODVÁRKA, P. *Síťová a vyšší vrstvy referenčního modelu ISO OSI* [online]. 2000 [cit. 2011-05-07]. Dostupné z WWW: <http://www.svetsiti.cz/view.asp ?rubrika=Tutorialy&temaID=1&clanekID=18>
11. PETERKA, J. *Referenční model ISO / OSI* [online]. 1999 [cit. 2011-04-28]. Dostupné z WWW: <http://www.earchiv.cz/anovinky/ai1552.php3>
12. PETERKA, J. *Síťový model TCP / IP* [online]. 1992 [cit. 2011-05-04]. Dostupné z WWW: <http://www.earchiv.cz/a92/a231c110.php3>
13. ROHLÍK, M. *Využití proudových šifer v současnosti* [online]. 2009 [cit. 2011-04-21]. Dostupné z WWW: <http://access.feld.cvut.cz/view.php?cisloclanku=2009080001>
14. Wi-Fi sítě Praha. *Wi-Fi standard IEEE 802.11* [online]. 2008 [cit. 2011-05-12]. Dostupné z WWW: <http://prahawifi.cz/wifi-standard-ieee-80211/>.