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

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE
AUTHOR

PAVEL HRŮZA

VEDOUCÍ PRÁCE
SUPERVISOR

doc. Ing. MILOŠ KOCH, CSc.

BRNO 2011

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2010/2011
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Hrůza Pavel

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

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,Lee. Wi-Fi: jak zabezpečit bezdrátovou síť. 1.vyd. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.
BRISBIN, Shelly. Wi-fi: postavte si svou vlastní wi-fi síť. 1.vyd. Praha: Neocortex, 2003. 248 s. ISBN 80-86330-13-3.
KöHRE,Thomas. Stavíme si bezdrátovou síť Wi-fi. 1.vyd. Brno: Computer Press, 2004. 296 s. ISBN 80-251-0391-9.
ZANDL,Patrick. Bezdrátové sítě WiFi : praktický průvodce. 1.vyd. Brno:Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

Vedoucí bakalářské práce: doc. Ing. Miloš Koch, CSc.

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 25.05.2011

Abstrakt

Bakalářská práce se zabývá návrhem bezdrátové sítě. V první části teoreticky popisuje technologie, které se používají pro stavbu bezdrátových sítí a následně je prakticky aplikuje při realizace bezdrátové sítě pro společnost WALMARK, a.s.

Abstract

This bachelor's thesis is focused on wireless network design. In the beginning it describes technologies, which are used for building of modern wireless networks. Practical part of thesis uses these technologies during creation of wireless network for company WALMARK.

Klíčová slova

Wi-Fi, bezdrátové sítě, MikroTik, IEEE, router, zabezpečení

Keywords

Wi-Fi, wireless networks, MikroTik, IEEE, router, security

HRŮZA, P. *Problematika bezdrátových sítí*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2011. 63s. Vedoucí bakalářské práce doc. Ing. Miloš Koch, CSc.

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 31. května 2011 ……

Poděkování

Tímto bych rád poděkoval panu doc. Ing. Miloši Kochovi, CSc., vedoucímu této bakalářské práce, za jeho přínosné rady, které jsem využil ke zdokonalení mé práce. A také bych chtěl poděkovat oddělení IT společnosti WALMARK, a.s., které mi poskytlo kompletní podklady pro zpracování praktické části této práce.

Obsah

Úvod

Bezdrátové sítě se staly v rámci informačních technologií revolucí. V dnešní době již nikomu nepřijde zvláštní, že je bezdrátovým signálem pokryta restaurace, obchodní dům, sportovní stadion a lidé považují za samozřejmé mít pokryt bezdrátovým signálem svůj dům nebo byt a aktivně této možnosti využívat.

Ve firemní sféře je ovšem problematika pokrytí bezdrátovou sítí daleko složitější než při běžném osobním využití. Zejména se jedná o zabezpečení sítě, které je důležité kvůli úniku dat a případné infiltraci do firemní sítě. Toto je také spojeno s výběrem aktivních prvků do sítě. Profesionálně provedená bezdrátová síť je kompletně řiditelná centrálně a je velmi dobře zabezpečena.

Tato bakalářská práce se zabývá realizací bezdrátové sítě v prostředí společnosti, která je velmi háklivá na ztrátu jakýchkoliv údajů a know-how. Proto bylo zapotřebí vybudovat pokrytí budovy ředitelství, které bude navazovat na stávající systém, který již fungoval v rámci skladů a dílčích míst ve společnosti. Takto vymezené požadavky dávají dopředu signál, že není možné využít klasických levných zařízení, která se běžně prodávají pro domácí a nenáročné použití, ale je třeba tuto bezdrátovou síť opravdu řešit profesionálním přístupem tak, aby i v rámci rozvoje IT holdingu zapadala do koncepce.

1 Vymezení problému a cíl práce

1.1 Vymezení problému

Bezdrátové sítě jsou dnes na trhu velmi důležitým artiklem i zejména z důvodu, že stále větší množství uživatelů si pořizuje přenosná zařízeni jako notebooky, netbooky, tablety, smartphony, různé čtečky, které využívají bezdrátových sítí naplno. Proto je důležité v rámci budování infrastruktury bezdrátové sítě dbát na její dostatečné dimenzování pro budoucí uživatele, kterých neustále přibývá, i proto, že se svých desktopových PC zbavují a láká je mobilita s bezdrátovými přenosy spojená. Proto musí být síť, která je realizována co nejefektivnější při co nejnižších vstupních nákladech, ale přesto musí být lehce spravovatelná a administrovatelná.

1.2 Cíl práce

Cílem mé práce je informovat o základních termínech spojujících se s problematikou bezdrátových sítí 802.11 typu Wi-Fi. Práce má dále za cíl sestavit přehled současných možností zabezpečení bezdrátové sítě, dále v teoretické části obecně rozebrat hardware používaný pro tvorbu bezdrátových sítí. Konečným cílem mé bakalářské práce je popsat výchozí stav a postupné fáze realizace bezdrátové sítě a jejího managementu v budově ředitelství společnosti WALMARK, a.s.

2 Teoretická východiska práce

2.1 Stručná historie bezdrátových sítí

Historie bezdrátových sítí sahá již do čtyřicátých let minulého století. Německá armáda tehdy prováděla experimenty s principy torpéda, které by bylo řízeno dálkově, pomocí rádiových vln. Bohužel měla tato technologie jednu podstatnou vadu, a sice, že se daly rádiové vlny velmi jednoduše odposlouchávat. Bylo tedy navrženo, aby byly rádiové vlny distribuovány náhodně v čase napříč sérií frekvencí. Přenos na každé frekvenci mohl být poté kratičký a celkový tok byl tedy mnohem méně náchylný k odposlouchávání. (1)

Dalším problémem byla nutná synchronizace mezi vysílajícím a přijímajícím zařízením. Tehdy byla použita perforovaná role papíru. (1)

Koncem padesátých let byla aplikována elektronická synchronizační metoda Americkou armádou do formy konceptu, který se později uchytil v dobách kubánské krize, když byl děrný synchronizační pás nahrazen elektronicky a systém sloužil americkým lodím k vzájemné zabezpečené komunikaci na otevřeném moři. (1)

Nadále byla technologie používána a s menšími úpravami je ostatně používána dodnes. Byla používána ve válce ve Vietnamu. V 80. letech ovšem nastal zlom, když padlo rozhodnutí, že tato technologie bude uvolněna pro civilní užití a dnes je tedy tato technologie používána v nejrůznějších oborech lidských činností od vojenství až po telekomunikace. (1)

Ovšem bezdrátové sítě z pohledu, jak jej známe dnes, spatřily světlo světa teprve před 15 lety, když byl v červenci roku 1994 organizací IEEE vydán první standard bezdrátových sítí 802.11. Tento standard používal principů modulace FHSS a také DSSS, tak také možnosti komunikovat pomocí infračervených signálů. Rychlost tehdy byla jeden či dokonce dva megabity za sekundu. (1)

Nedlouho poté bylo zapotřebí vymyslet něco lepšího, protože dosahované rychlosti byly příliš nízké a nemohly stačit. 5 let poté (v roce 1999) byl vydán standard 802.11b a byl zařazen do IEEE. Teoretická přenosová rychlostní maxima byla 5,5 až 11 megabitů za sekundu a použito bylo frekvenční pásmo 2,4 – 2,485 GHz. (1)

Souběžně s tímto standardem byl vydán standard 802.11a. Tento standard je od standardu 802.11b odlišný zejména tím, že pracuje na frekvenčním rozsahu 5,1 až 5,3

GHz a 5,725 až 5,825 GHz. Frekvence 2,4GHz byla totiž mezitím využita již mnoha zařízeními, která způsoboval v tomto pásmu velké rušení. Tento standard využívá modulace OFDM. (1)

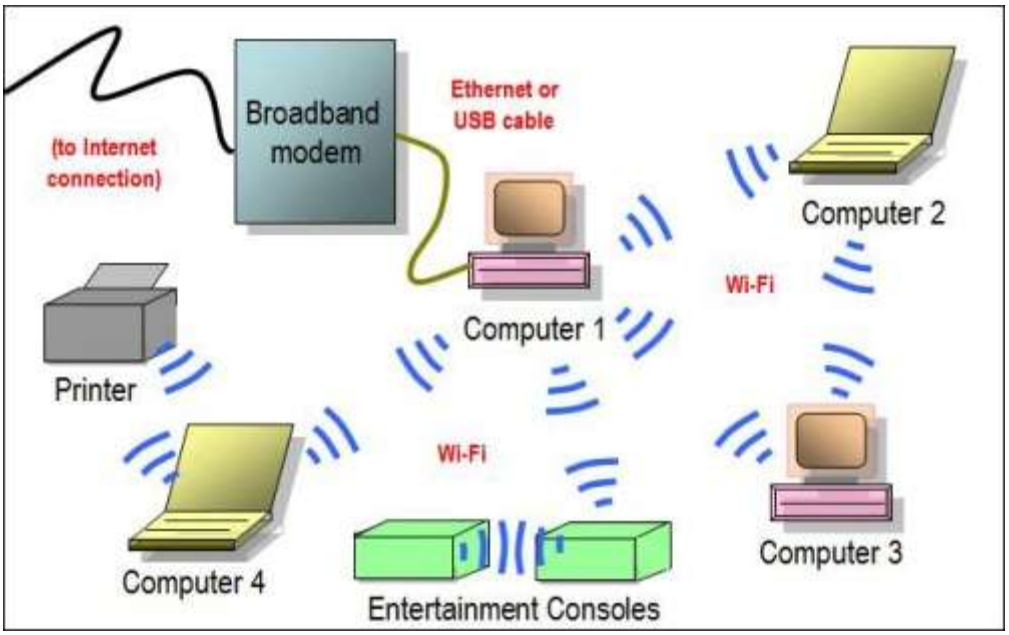
Pásmo 2,4 GHz, ale nepřestalo být využíváno a v roce 2003 byl vyvinut nový standard, který je označován jako 802.11g. Využívá modulaci OFDM a také DSSS z důvodu zpětné kompatibility se starším standardem 802.11b. (1)

V dnešní době se u nás využívá zejména standard IEEE 802.11n. Konečné schválení tohoto standardu bylo konsorciem výrobců velmi dlouho odkládáno, ačkoliv v nejrůznějších zařízeních již bylo používáno v několika konceptových normách. K definitivnímu schválení této normy došlo 7. září 2009. Toto schválení dává garanci, že veškerá vyráběná zařízení budou navzájem kompatibilní a to i se zařízeními budoucími. Tuto vlastnost nemohly garantovat výrobky, které používaly některý z konceptových standardů 802.11n. Standard 802.11n taktéž zlepšuje odolnost proti rušení díky použití technologie MIMO. (1)

2.2 Pojmy související s bezdrátovými sítěmi a jejich využití

Access Point, AP – Access Point neboli přístupový bod řídí komunikaci mezi wi-fi zařízeními, která jsou zapojena v infrastruktuře sítě. Přístupové body se používají pro poskytování různých služeb v lokálních sítích (tisk, FTP apod.) a také pro připojení k internetu. (2)

Ad-Hoc Mode – Ad-Hoc režim neboli nahodilý režim. Existují Wi-Fi sítě, které neobsahují žádný přístupový bod. Tyto sítě se nazývají ad-hoc wi-fi sítě. Aby zařízení mohla být v takové síti používána, musí být konfigurována pro použití v ad-hoc režimu. Někdy je Ad-Hoc síť uváděna jakožto síť s rovnocennými uzly (peer – to – peer), protože AP je nadřazeno a nebo jako nezávislá síť. (2)



Obr. 2.1: Schéma Ad - Hoc sítě (Zdroj: http://www.svethardware.cz/art_doc-E8854472EA5653EBC1257636003B03D0.html)

Basic Service Set – základní soubor služeb. **BSS** je Wi-fi síť, která obsahuje jeden přístupový bod a několik klientů. (2)

MIMO – technologie **MIMO** prodlužuje dosah a také zároveň propustnost síťových bezdrátových prvků, které pracují podle standardu 802.11b a 802.11g. Principem této technologie je kombinace vyšší citlivosti samotného chipsetu zařízení a několikanásobného vysílače s větším množstvím antén. Například tedy Access Point obsahuje celkem 4 antény a 4 nezávislé RF modulátory. 2 antény jsou integrovány přímo na základní desce samotného zařízení a další dvě jsou poté připojeny standardním způsobem pomocí RSMA konektorů. Zařízení pracuje v režimu **MIMO** i v případě, že připojená klientská zařízení tuto technologii nepodporují. Po zahájení komunikace s daným klientem jsou porovnávány údaje z jednotlivých přijímačů a dochází k výrazně lepší opravě chyb a také zároveň i vysílání je směřováno do těch antén, které jsou pro klientské zařízení optimální. Kombinací těchto vlastností je možné dosahovat několikanásobného (až osminásobného) zvýšení dosahu jednotlivých přístupových bodů. Tato technologie je zejména určena do budov, ve kterých bývají se signálem wi-fi potíže, nicméně také přístupové body, na které jsou připojeny sektorové antény budou vykazovat při použití této technologie daleko lepších parametrů než bez jejího využití.

Bridge – síťový most. Síťový most spojuje dva segmenty jedné sítě. Jakožto most se dá označit přístupový bod, který spojuje segmenty kabelové a bezdrátové sítě. Jiným druhem mostu může být bezdrátový most, který se používá naopak pro spojení segmentů bezdrátové sítě.

Channel – kanál. Frekvenční pásmo, ve kterém wi-fi síť pracuje je vždy rozděleno do určitého počtu kanálů. Pro specifikaci 802.11b platí, že komunikace mezi klientskými zařízeními a přístupovými body probíhá vždy po jednom konkrétním kanálu.

Client – klient. Klient nebo klientská zařízení jsou zařízení, které je částečně, či plně závislé na určitém druhu serveru. V bezdrátové wi-fi síti je klientem počítač, notebook, PDA, mobilní telefon, který komunikuje přes určitý přístupový bod. Klientské zařízení bývá označováno jako stanice.

CSMA/CA – carrier sense multiple access with collision – avoidance. Metoda vícenásobného přístupu s detekcí nosné a zabráněním kolize. Metoda CSMA/CA je wi-fi zařízeními používána pro zprostředkování komunikace mezi zařízeními. V případě, že ethernet používá detekci kolizí pro zabránění kolizí v síti, wi-fi síť nedovolí dokončit přenosy, jestliže ke kolizi dojde. (2)

DHCP – dynamic host configuration protokol. Protokol dynamické konfigurace stanice. Umožňuje zařízení, které je síti získat IP adresu dynamicky hned po připojení k této síti. (2)

Driver – ovladač. Zařízení, která jsou připojena k počítači nebo jsou v počítači nainstalována, vyžadují pro svou identifikaci ovladač. Ovladače pro většinu standardních verzí systému Windows a případně MAC jsou většinou obsaženy na přiložených CD k zařízením. Uživatelé systémů Linux tyto ovladače většinou musí hledat jinou cestou. (2)

DSSS – direct sequence spread spektrum. Rozprostřené spektrum v přímé posloupnosti. **DSSS** je metoda frekvenční modulace, která byla stanovena v původní specifikaci 802.11 a používána v normě 802.11b. (2)

ESS – extended service set. Překrývající se soubor služeb. Rozšířený soubor služeb se skládá z několika sítí typu BSS, které jsou zapojeny dohromady tak, aby umožňovaly mezi sebou roaming. Zařízení, která mají k ESS přístup, mohou tak zůstat připojena k síti v případě, že zůstávají v dosahu alespoň jednoho z přístupových bodů **ESS.** (2)

FHSS – frequency hopping spread spektrum. Rozprostřené spektrum s přeskakováním mezi frekvencemi. Jedná se o další typ frekvenční modulace, který je uveden ve specifikaci 802.11. **FHSS** není v současné době využívána v žádné ze současných implementací 802.11, ale je využívána technologií Bluetooth. (2)

Firewall – chrání lokální počítačovou síť tím před potenciálními narušiteli tím, že omezuje vstup na klientskou stanici či do lokální počítačové sítě. Různé druhy firewallů poskytují různé typy a různé úrovně ochrany klientů a sítí včetně zablokování určitých portů, které používají internetové aplikace pro připojení se k jiným počítačům. Zabraňují přenosům na základě jejich původu a analýzy a odmítnutí pokusů o proniknutí na základě určitých modelů a chování podezřelých vstupů. Většina Access Pointů (přístupových bodů) obsahuje firewall. Většinu firewallů lze nakonfigurovat tak, aby byly schopny umožnit přístupy ke specifickým částem lokální sítě nebo naopak, aby byly schopny odepřít přístup z vnějšího prostředí. (2)

HiperLAN/2 – je norma pro bezdrátové sítě, které pracují ve vyšším frekvenčním pásmu 5 GHz. Tato norma má mnoho provozních charakteristik, které jsou obdobné specifikacím IEEE 802.11. Norma HiperLAN/2 je známější zejména v Evropě. Ve spojených státech známá příliš není. (2)

HomeRF – je specifikací pro bezdrátové sítě podporovanou zejména společností Intel, která pracuje v pásmu 2,4 GHz a byla primárně určena pro síťovou komunikaci

v domácích prostředcích. Specifikace IEEE 802.11b však tuto normu předběhla a firma Intel tedy přenesla svou podporu z **HomeRF** na 802.11. (2)

IEEE 802.11 – je institut inženýrů elektrotechniky a elektroniky (Institute of Electrical and Electrontechnics Engineers – IEEE). Je organizací, která se zaměřuje na vytváření počítačových norem. Normy IEEE jsou označovány čísly. IEEE 802.11 je skupina norem pro bezdrátové sítě, které jsou charakterizovány používáním rádiového spektra. Normy 802.11 sledují pravidla nastavená institutem IEEE, jimiž se řídí velká řada síťových norem. Tato větší skupina norem je pak označena číslem 802. (2)

Infrastructure Mode – infrastrukturní režim. Režim, při kterém zařízení komunikují s přístupovým bodem. Opakem je Ad-Hoc režim, ve kterém není žádný přístupový bod. (2)

IP – internet protocol neboli internetový protokol. Tento protokol je používán všemi internetovými aplikacemi. Taktéž je tento protokol využíván nejčastěji pro lokální a rozlehlé sítě. Veškerá zařízení wi-fi tento protokol podporují. (2)

IPSec – jeden z nejčastěji používaných protokolů pro vytváření virtuálních privátních sítí neboli VPN. Tento protokol využívá šifrování podle veřejného klíče pro zašifrování obsahu datových paketů a také záhlaví paketů tak, jak jsou vysílány. Poté dotváří bezpečnou cestu buď za použití protokolu tunelu nebo transportu. Mnoho access pointů má podporu průchodu za pomoci IPSec. Znamená to, že uživatel na wi-fi síti může použít VPN připojení na síť, která protokol IPSec používá také. (2)

LAN – local area network nebo lokální síť. Lokální síť je soustava všech zařízení, která jsou fyzicky připojena a to ať už drátově nebo bezdrátově v určité ohraničené oblasti. Segmenty lokální sítě je možné použít pro připojení částí sítě uvnitř jedné stejné lokální oblasti, ale všechna tato připojená zařízení jsou považována za součást jedné sítě LAN. (2)

NAT – network address translation neboli překlad síťových adres. NAT umožňuje síti počítačů, které používají své privátní IP adresy komunikovat s internetem, či jinými sítěmi pomocí jedné veřejné IP adresy. V bezdrátových sítích tuto funkci umožňuje přístupový bod, který poskytuje NAT. Sdílí připojení na internet se všemi stanicemi a pomocí DHCP jim přiděluje IP adresy. NAT také zejména maskuje síť počítačů tak, že se tváří jako jeden a umožňuje aplikovat takto centrálně Firewall. (2)

OFDM - orthogonal frequency division multiplexing neboli ortogonální frekvenční multiplex. OFDM je metoda frekvenční modulace rozprostřeného spektra, která je využívána normou 802.11a. (2)

OSI Model - open systems interconnect neboli propojení otevřených systémů. OSI model síťové hierarchie představuje strukturu síťových protokolů jakožto řadu vertikálních vrstev. Počínaje fyzickou (nejnižší vrstvou) až po aplikační (nejvyšší vrstvu). Bezdrátové wi-fi sítě pracují na nejnižší (fyzické) vrstvě a na vrstvě spojové OSI modelu. (2)

Packets - pakety. Pakety jsou informace, které jsou přenášeny po síti na druhou vrstvou (vrstva MAC - medium access control, řízení přístupu k médiu) a jsou organizovány do paketů. Uvnitř vrstev 1 a 2 jsou tyto jednotky nazývány rámce neboli frames. Některé pakety mohou obsahovat data, která jsou přenášena mezi zařízeními. Jiné pakety mohou obsahovat informace, které jsou potřebné pro kontrolu a management síťové transakce. (2)

Roaming - pokud se bezdrátová zařízení pohybují mezi různými přístupovými body, které jsou však nakonfigurovány jako jedna síť a tato zařízení neztratí připojení k hostitelské síti, tak je takovýto způsob komunikace známý jako roaming. (2)

Sniffer - sniffer je detekční nástroj. Je užíván jak správci sítí tak hackery jakožto detekční nástroj pro prohlížení, zkoumání a zachycování síťových paketů, které putují buď po kabelovém spojení nebo bezdrátovém spojení. Detekční nástroje mohou být z principu jako hardwarového tak i softwarového typu. Jejich možnosti nastavení jsou

široké, buď jsou nastaveny tak, že zachycují pouze některý síťový provoz nebo jej zachycují všechen. Případně jsou nastaveny tak, aby analyzovaly zabezpečení sítě. Toto může být buď z důvodu nalezení chyby v síti nebo proto, aby byla takto narušena bezpečnost sítě. (2)

Spread spectrum - neboli rozprostřené spektrum. Rozprostřené spektrum je určeno k rozptylu signálu přes určitý, přidělený počet frekvencí ve specifikovaném pásmu. Všechna wi-fi zařízení používají pro komunikaci jednu ze tří metod rozprostřeného spektra. (2)

SSID - service set identifier neboli identifikátor soubrou služeb. Identifikátor souboru služeb je řetězec, který označuje síť. SSID používají jak ad-hoc, tak i infrastrukturní sítě. Mnoho lidí považuje SSID za název této sítě. (2)

VPN - virtual private network neboli virtuální privátní síť. Virtuální privátní síť poskytuje bezpečný kanál pro zabezpečenou komunikaci mezi uživatelem a nějakou vzdálenou - většinou firemní - sítí. Při použití standardních internetových protokolů a zabezpečovacích protokolů, které zajistí proces autentizace, zabrání VPN tomu, aby jakýkoliv neoprávněný uživatel používal tuto privátní síť. Aby mohl zachycovat a případně dekódovat příslušná data. Dnešní moderní přístupové body podporují přístup do VPN předáním specifického VPN protokolu od uživatele na zabezpečenou síť.

Wardialing - bylo kdysi označováno jako činnost, kdy bylo náhodně vytáčeno telefonní číslo za účelem zjištění, zda není za určitým číslem modem. V dnešní době je tato činnost v přeneseném slova smyslu jako IP scanning, kdy se zjišťují aktivní stroje v adresním IP prostoru. (2)

WECA - wireless ethernet compatibility alliance neboli aliance pro kompatibilitu bezdrátového ethernetu. Tato aliance je sestavena z dodavatelů a dalších zainteresovaných subjektů na propagaci norem IEEE 802.11. Tato organizace poté odpovídá za certifikační program a proces wi-fi zařízení. (2)

Wi-Fi - aliance WECA přijala termín wireless fidelity (wi-fi - spolehlivá bezdrátová komunikace) pro odkaz na výrobky, které jsou certifikovány jakožto výrobky splňující nejen normu IEEE 802.11, ale také svůj vlastní testovací režim. (2)

2.3 Standardy IEEE

Obecné způsoby fyzického řešení bezdrátových lokálních sítí 802.11 – přenos rádiových vln o kmitočtech v pásmu od 2,4 GHz do 2,4835 GHz metodou přímo rozprostřeného spektra (DSSS) – DSSS vysílač přeměňuje tok dat na tok symbolů, kde každý symbol reprezentuje skupinu jednoho či více bitů. Při použití modulační techniky jako je QPSK (Quadrature Phase Shift Keying) vysílač moduluje nebo násobí každý symbol pseudonáhodnou šumovou frekvencí. Tato operace uměle zvětšuje použitou šířku pásma v závislosti na délce sekvence. (2)

DSSS dělí pásmo na 14 kanálu, které jsou rozčleněny po 22MHz, a které se částečně překrývají. Pouze tři z těchto kanálů se nepřekrývají vůbec. (2)

Sítě typu 802.11, které jsou založeny na DSSS nabízejí povinně rychlosti 1 nebo 2 Mbit/s. nižší rychlost je používána jako záloha pro případné rušení v prostředí.

Přenos rádiových vln o kmitočtech, které se nacházejí v pásmu od 2,4 do 2,4835 GHz metodou rozprostřeného spektra s přeskakováním kmitočtů (FHSS) – vysílá jeden nebo více datových paketů po jednom kmitočtu (pásmo je rozděleno na 75 podkanálů, kdy je děleno po jednom MHz), pak přeskočí na jiný kmitočet a pokračuje ve vysílání dál.

Způsob přeskakování mezi kmitočty se může jevit jako náhodný. Ve skutečnosti se však jedná o periodické pořadí, které je známé jak vysílači, tak přijímači. Různé konverzace se v bezdrátových sítích odehrávají podle různých klíčů. Tímto se minimalizuje možnost současného využití téhož podkanálu. FHSS nabízí povinně rychlost 1 Mbit/s a volitelně 2Mbit/s. (2)

Přenos infračerveným zářením (Diffused Infrared, DFIR) probíhá povinně rychlostí 1 Mbit/s a volitelně 2 Mbit/s. Infračervená varianta lokální datové komunikace je striktně omezena na jedinou kancelář či jiný souvislý prostor, protože komunikace infračervenými paprsky neprochází pevným materiálem, ale dochází k jeho odrazu. Řešení ba rzi infračerveného záření je podstatně dražší než řešení rádiovým přenosem, proto se takováto varianta používá jen velmi zřídka. (2)

Volné pásmo 2,4 GHz využívají zařízení jako bezdrátové telefony, mikrovlnné trouby i Bluetooth. Z toho vyplývá, že může – a dochází k vzájemnému rušení jednotlivých zařízení. (2)

IEEE 802.11a – jedná se o vysokorychlostní rádiovou normu, která pracuje ve frekvenčním pásmu 5 GHz. IEEE 802.11a využívá ortogonální frekvenční multiplex (Orthogonal Frequency Division Multiplexing – OFDM) jako frekvenční modulaci a dosahuje nejvyšší teoretické rychlosti 54 Mbit/s. (2)(8)

WLAN IEEE 802.11a na rozdíl od 802.11b pracuje již v licenčním pásmu 5 GHz a s výrazně vyšší teoretickou maximální rychlostí – 54 Mb/s (skutečná rychlost se pohybuje do 36 Mb/s v tzv. turbo režimu). (2)(8)

Pro dosažení této rychlosti se poprvé v paketových komunikacích používá ortogonální multiplex s kmitočtovým dělením (OFDM), který se do té doby uplatňoval pouze v systémech jako jsou DAB (Digital Audio Broadcasting) nebo DVB (Digital Video Broadcasting). (2)(8)

Výhodou 802.11a oproti 802.11b není, ale jen ve vyšších rychlostech, ale také v použitém kmitočtu. Pásmo 5 Ghz je méně vytíženo a dovoluje využití více kanálů bez vzájemného rušení. Rozdílně využívané kmitočty u obou specifikací znemožňují jejich vzájemnou spolupráci. Specifikace 802.11a nabízí až osm nezávislých a nepřekrývajících se kanálů. Kmitočet 5 GHz nutný pro IEEE 802.11a je v Evropě použit pro konkurenční WLAN – HiperLAN/2 a proto není jeho použití možné. Sice v Evropě existují dílčí povolení pro použití 802.11a, a obecně se usiluje o uvolnění rezervovaného spektra pro HiperLAN i pro další jiné rádiové LAN. (2)(8)

Produkty specifikace 802.11b jsou již ve velkém výběru značek k dispozici a jsou otestovány WECA (Wireless Ethernet Compatibility Alliance) na vzájemnou spolupráci a kompatibilitu, nelze to samé říct o specifikaci 802.11a. Testy se zatím připravují. Není ani pravděpodobný přechod ze sítí 802.11b na 802.11a. Ve většině případů už spíše došlo k přechodu na sítě 802.11g. (2)(8)

IEEE 802.11b – jedná se o normu, která je velmi hojně používána v bezdrátových sítích na bázi IEEE. Pracuje na kmitočtech 2,4 GHz a s maximální teoretickou rychlostí 11 Mbit/s.

Největší problém původní WLAN normy (IEEE 802.11) byla nízká přenosová rychlost. High Rate (HR) neboli rychlé rozšíření základní normy IEEE 802.11b je přesná podskupina normy 802.11b, která je přezdívána Wi-Fi (Wireless Fidelity). WiFi poskytuje vyšší rychlosti v pásmu 2,4 GHz a to až teoreticky 11 Mbit/s. Pro dosažení těchto rychlostí se využívá nový způsob kódování – tzv. doplňkové kódové klíčování (Complementay Code Keying, CCK) v rámci DSSS na fyzické vrstvě. (2)

Tato norma také specifikuje, že podle momentální rušivosti prostředí se dynamicky mění rychlost na vyšší nebo naopak na nižší. 11 Mbit/s, 5,5 Mbit/s a 2 Mbit/s až 1 Mbit/s. Maximální teoretická rychlost je na fyzické vrstvě sice 11 Mbit/s, ale užitná rychlost je daleko nižší. Testovaná uživatelská rychlost je někde kolem 6 Mbit/s. Dosah sítě na specifikaci 802.11b je kolem 100 m. Výkonnější vysílač však může tuto vzdálenost přesáhnout. (2)

Produkty pro standard 802.11b jsou testovány WECA na vzájemnou spolupráci a kompatibilitu. (2)

Kromě problémů s nedostatečnou přenosovou rychlostí mohou nastat problémy s rušením s jinými zařízeními v otevřeném pásmu 2,4 GHz. V neposlední řadě standard 802.11b nezajišťuje kvalitu služeb (QoS) a dostatečnou bezpečnost komunikace. Z těchto důvodů se IEEE zabývá vývojem dalších norem 802.11. (2)

IEEE 802.11e – tato norma poskytuje kvalitu služeb pro sítě 802.11. Tato kvalita služeb (Quality of Services – QoS) poskytuje některým datovým paketům prioritu před jinými datovými pakety. QoS je považováno za kritický faktor pro vytvoření robustní normy na bázi 802.11, která bude vhodná jako médium pro hlasovou a datovou komunikaci, ale také pro multimediální aplikace. (2)(8)

IEEE 802.11g - je norma navazující na normu 802.11b. Pracuje ve stejném pásmu jako norma 802.11b – tedy 2,4 GHz. Obdobně jako norma 802.11a poskytuje maximální teoretickou přenosovou rychlost 54 Mbit/s (ovšem v pásmu 2,4 Ghz). Používá technologii OFDM rozprostřeného spektra. Vzhledem k použití pásma 2,4 GHz je síť 802.11g zpětně kompatibilní se sítí 802.11b. Systémy v normě IEEE 802.11g jsou slučitelné s 11 Mbit/s WLAN, včetně všech doplňků jako 802.11d, 802.11e a je tedy vlastně alternativou k síti 802.11b. Rychlejší alternativou. (2)(8)

Fyzická vrstva je zde založena na OFDM podobně jako u standardu 802.11a. Pro zpětnou kompatibilitu a slučitelnost s 802.11b podporuje také CCK a volitelně rovněž modulaci PBCC, která je zde jako ústupek vůči společnosti Texas Instruments. (2)
Tři modulační mechanismy jsou schopny pracovat simultánně, takže přístupové body podle normy 802.11g budou schopny podporovat jak stávající uživatele, tak nové klienty s vyššími rychlostmi. Práce 802.11b CCK, 802.11b PBCC a 802.11g OFDM vedle sebe při využití stejného kmitočtu může, ale vést k vzájemnému rušení. (2)

IEEE 802.11h – je doplňkem normy 802.11a. Je navržen s ohledem na evropské podmínky tak, aby bylo možné sítě využívat mimo budovy. Řeší také například problémy s rušením od ostatních zařízení pracujících na frekvenci 5 GHz. Na tomto pásmu pracují například radary nebo některé satelitní systémy. IEEE 802.11h vylepšuje řízení využití kmitočtového spektra - výběr kanálu a řízení vysílacího výkonu – a tím doplňuje normu 802.11a. (2)(8)

IEEE 802.11n – je nejnovější schválený standard pro bezdrátové sítě. Tento standard kombinuje zvýšení maximální teoretické přenosové rychlosti a zpětnou kompatibilitu v pásmech jak 2,4 GHz, tak 5 Ghz. Je tedy zpětně kompatibilní jak se standardy 802.11b tak s 802.11g. Pásmo na frekvenci 5 Ghz pak dosahuje vyšších reálných přenosových rychlostí. (2)
Maximální teoretické rychlosti se pohybují okolo 300 Mbit/s. Tato maximální teoretická přenosová rychlost je i hlavním důvodem masivního rozšiřování tohoto standardu. Příčinou zvýšení rychlosti je využití technologie MIMO. U tohoto standardu je použito na linkové vrstvě OFDM. (2)

Jednoduchý přehled standardů 802.11 a jejich dodatků

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); obsaženo v IEEE 802.1D standardu (2001)
IEEE 802.11d – Mezinárodní roamingový dodatek (2001)

IEEE 802.11e – Vylepšení QoS, včetně dlouhých (burst) paketů (2005)
IEEE 802.11F – 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 802.1Q)
IEEE 802.11r – Rychlé přesuny mezi přístupovými body (roaming)
IEEE 802.11s – Samoorganizující se bezdrátové sítě. (ESS Mesh Networking)
IEEE 802.11T – 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 – (rezervováno a nebude použito)
IEEE 802.11y – Pro běh ve frekvenčním pásmu 3650 – 3700 MHz (veřejné pásmo v USA)
(4)

2.4 Základy zabezpečení bezdrátových sítí

Bezpečnost bezdrátových sítí je diskutovaným tématem v každém období. Nezabezpečené nebo špatně zabezpečené sítě jsou pro potenciálního útočníka velkým lákadlem a velmi snadným cílem. Zabezpečení bezdrátových sítí proto vyžaduje

mimořádnou pozornost a v mnoha společnostech to stále velmi podceňovaný prvek, který se jim může v blízké budoucnosti velmi vymstít.

Základním zabezpečovacím mechanismem bezdrátových sítí a dodnes bohužel velmi hojně využívaným je zabezpečení WEP klíčem. Základní varianta zabezpečení WEP klíčem využívá k ochraně dat v bezdrátové sítí proudovou šifru RC4. Tato šifra kombinuje 40 bitový klíč WEP a 24 bitový náhodný inicializační vektor. Toto zabezpečení je vhodné pouze proti základnímu odposlechu. Potenciální útočník dokáže, v případě dostatečného provozu na síti, prolomit toto zabezpečení v řádech minut. Řešení zabezpečení pomocí standardu WEP vykazuje velké množství slabin. Jednou z hlavních slabin je možnost nalezení WEP klíče. Tento klíč se nemění dynamicky, ale pouze manuálně a inicializační vektor je dost krátký na to, aby se při častém provozu v síti opakoval. V případě odposlechu dostatečného množství paketů může tedy úročník ochranu prolomit. Další velkou slabinou je nemožnost ověření identity přístupového bodu. Když tedy útočník použije k útoku na síť svůj vlastní přístupový bod a tím jednoduše získat data, která uživatelé posílají. Zejména uživatelská jména a hesla. Obecně je slabinou systému WEP nemožnost dynamické změny klíčů. Ve velkých společnostech, které zabezpečení WEP používají je změna všech klíčů ve všech zařízeních natolik náročnou záležitostí, že se vůbec nekoná a tím se dává útočníkům čím dále větší prostor. V dnešní době se používají WEP klíče o délce 128 bit a některé i 256 bit, nicméně pořád pro ně platí stejná pravidla a to, že při odposlechu paketů není velkým problémem je prolomit, protože většina lidí klíče WEP nemění a má je pořád stejné - statické. (5)(7)

Další možností zabezpečení bezdrátové sítě je pomocí WPA. WPA je podmnožinou standardu IEEE 802.11i. Zavedení WPA znamená veliké vylepšení bezpečnosti, protože obsahuje tyto kontrolní mechanismy:

- vzájemné ověření účastníků v souladu s normou IEEE 802.1x (Extensible Authentication Protocol - EAP) nebo pomocí PSK (přednastavený sdílený klíč - Preshared Key)
- protokol TKIP (Temporary Key Integrity Protocol), tento protokol zajišťuje dynamickou změnu klíčů standardu WEP
- kontrola integrity zpráv

K ověřování identity účastníků a přístupových bodů se používá speciální ověřovací server. V rámci procesu ověření se vyskytují tito účastníci:

- klient, který žádá o ověření (klientské zařízení přistupující do sítě wi-fi)
- ověřovací server (server uvnitř zabezpečené sítě, který poskytne ověření)
- prostředník (zařízení, které je připojené mezi klientský zařízením a ověřovacím serverem, v případě sítí wi-fi je to access point)

Proces ověření je zahájen ve chvíli, kdy access point detekuje klientské zařízení, které žádá o spojení. Zařízení, které je neověřené má umožněno navázat spojení pouze s ověřovacím serverem, všechna ostatní spojení jsou zakázána. Až ve chvíli, kdy je zařízení ověřeno, může využit všech služeb bezdrátové sítě. Mechanismus také ověřuje access point, což je klíčovou podmínkou pro dobré zabezpečení bezdrátové sítě. V případě, že se neověří access point, není problém udělat útok podvrženou sítí. V případě domácností je ovšem neekonomické instalovat ověřovací server, proto se v těchto podmínkách využívá předem sdíleného klíče, případně má bezdrátové zařízení funkci ověření přímo integrovanou. (5)(7)

Ověření protokolem TKIP probíhá tak, že TKIP pravidelně mění 128 bitový dočasný klíč, který je sdílen klientem a přístupovým bodem. Dále paket TKIP zahrnuje MAC adresu klientského zařízení a 48 bitový inicializační vektor, který v paketu nahrazuje číslo sekvence. Vzhledem k dynamické změně dočasného klíče by případný útočník neměl mít tolik šancí na odchycení dostatečného množství paketů šifrovaných jedním klíčem. (5)(7)

Poslední částí je kontrola integrity. Můžeme ji označit jako formu digitálního podpisu v rámci TKIP paketu. Tato kontrola zaručuje, že paket nebyl útočníkem pozměněn, což se stává hlavně při útocích typu man-in-the-middle.

Současně nejlepším a nejsmysluplnějším systémem zabezpečení je WPA2. WPA bylo totiž navrženo tak, aby mohlo být implementováno na zařízeních původně jen pro WEP. WPA2 podporuje mechanismy WPA, avšak s některými změnami. TKIP používá algoritmus CCMP, který využívá blokové šifry AES a pro kontrolu integrity používá mechanismus CBC-MAC. Zabezpečení na úrovni WPA2 je už potom na velmi vysoké úrovni. (5)(7)

Veškeré tyto způsoby zabezpečení se snaží čelit různým typům útoků. Z těch nejznámějších druhů je to klasické prolomení WEP klíče, jak bylo výše popsáno. Dalším z běžných útoků je podvržená MAC adresa. Některá zařízení totiž kontrolují vstup do sítě pomocí této unikátní adresy, kterou má každé zařízení svou. Přístupový bod pak dovolí navázat komunikaci, protože si ověří, že zařízení je na seznamu povolených MAC adres a v případě, že už je rozluštěn WEP klíč, případně tam není vůbec, není problém sledovat provoz mezi autorizovanými zařízeními. Tento typ úroku může navazovat na útoky Man-in-the-middle při nichž útočník včleňuje své zařízení mezi účastníky a přístupový bod a může pak odposlouchávat veškerý datový provoz. Útočník ani access point přitom netuší, že nekomunikují přímo. Dalším z klasických útoků je prostý slovníkový útok, kdy se snaží pomocí tlaku kombinací čísel a písmen prolomit heslo do sítě. V tomto případě je vhodné volit tzv. "silná" hesla, která jsou pomocí takovéhoto útoku daleko hůře prolomitelná. Pro slovníkový útok je otázkou sekund kdy odhalí heslo typu "franta" či "1234", ale daleko složitější vzhledem k množství a různosti použitých znaků je odhalit heslo typu "hKE45!_gD9(" kteréžto se svou délkou a složitostí už dá považovat za heslo silné a slovníkovým útokem poměrně hůře prolomitelné. (5)

2.5 Hardware používaný při realizaci bezdrátových sítí

2.5.1 Antény

Antény jsou zařízení, která jsou využívána k příjmu nebo vysílání rádiových signálů - částí vysokofrekvenčního vedení upravených tak, aby účinně vyzařovala energii do prostoru. Elektromagnetické vlnění, které je na vysokých frekvencích se pak šíří podobným způsobem jako světlo. V tomto případě mluvíme o tzv. "přímé viditelnosti". V případě, že je mezi anténami překážka, může znemožnit příjem nebo přinejmenším méně či více výrazně omezit dosah rádiového signálu. Jako překážku můžeme chápat terénní nerovnost, ale také budovy, stromy a dokonce i počasí jako mlhu, déšť nebo sníh. Obecně je běžný dosah bezdrátových sítí v budovách asi 30 až 50 metrů. Ve venkovním prostředí za použití správné směrové antény může tento dosah narůst až na několik kilometrů. Ovšem platí, že s narůstající vzdáleností se rychlost přenosu snižuje. Antény mají několik technických parametrů:

Směrovost antény - je to schopnost antény vyzařovat resp. přijímat elektromagnetické vlny ve směru, který je požadován. Směrovost je posuzována dle tzv. vyzařovacích charakteristik. Tyto charakteristiky se dělí na vertikální a horizontální. (3)

Vyzařovací úhel antény - tento vyzařovací úhel antény je dán směrovým diagramem a je vypočítáván jako rozdíl úhlů bodů, kde je pokles signálu o 3 dB. (3)

Impedance antény - je vlastní impedance, která by měla být reálná. Impedance antény by se měla alespoň přibližně shodovat s impedancí přívodního kabelu, aby nedocházelo k odrazům a tím se nezvyšoval odražený výkon. Pro bezdrátové sítě se používají antény s impedancí 50 ohmů. (3)

Zisk antény - zisk antény nám udává, kolikrát větší výkon je potřeba dodat do půlvlnného dipólu tak, aby v místě příjmu byla stejná energie jako u směrové antény. Jednotkou je dB - decibel. Anténa, která tedy přijímá signál stejně jako dipól má zisk 0 dB. (3)

Základní typy antén, které se používají pro bezdrátové sítě můžeme dělit na:
Všesměrové - tyto antény vykrývají horizontálně 360°. Všesměrová anténa je ideální pro použití na centrálním access pointu v oblastech, kde není rušení. Do skupiny všesměrových antén spadají všechny antény od těch nejmenších 3 dB, které bývají standardní výbavou domácích access pointů a routerů až po velké antény, které používají zejména outdoorově, které mají zisk i přes 10 dB. (3)

Obr. 2.2: Všesměrové antény (Zdroj: http://www.barts.cz/index.php/pocitace/site/29-bezdratovesite.html)

Směrové antény - tyto antény vyzařují symetrický paprsek. Jejich pohybem (pootočením) lze změnit polarizaci vysílání. Směrové antény jsou ideální pro budování spojů typu bod-bod. Antény s vyšším vyzařovacím úhlem mohou nahradit sektorové antény. (3)

Tři příklady směrových antén jsou:

- YAGI antény - jedná se vývojově nejstarší typ antény. V současné bývají uzavřeny ve vodotěsném pouzdře.

Obr. 2.3: Směrová anténa Yagi (Zdroj: http://www.barts.cz/index.php/pocitace/site/29-bezdratovesite.html)

- Síta neboli Grid antény - díky svému provedení jsou méně náchylné na poškození větrem.

Obr. 2.4: Směrová anténa síto (Zdroj: http://www.barts.cz/index.php/pocitace/site/29-bezdratovesite.html)

- Paraboly - jsou směrové antény s nejlepšími parametry. Vzhledem ke svému tvaru jsou bohužel často náchylné na vychýlení větrem.

Obr. 2.5: Směrová anténa parabola (Zdroj: http://www.barts.cz/index.php/pocitace/site/29-bezdratovesite.html)

Panelové antény - tyto antény ve tvaru panelu bývají podle vyzařovací charakteristiky buďto sektorové

Obr. 2.6: Panelová anténa sektorová (Zdroj: http://www.barts.cz/index.php/pocitace/site/29-bezdratovesite.html)

nebo směrové

Obr. 2.7: Panelová anténa směrová (Zdroj: http://www.barts.cz/index.php/pocitace/site/29-bezdratovesite.html)

V oblastech, které jsou hustě osídleny, tedy zejména v aglomeracích, je víceméně všude množství signálů, které způsobují rušení. Některé dokonce i na stejném kanále, jako

požadovaný signál. Signál, který pak chceme přijímat nemusí být nejsilnější ze signálů, které na daném místě jsou. Tyto nežádoucí rušivé signály pak mohou spojení úplně znemožnit. Takovéto situace se pak řeší zejména přeladěním na jiný kanál a přesměrováním antény. Často se pak anténa natáčí nikoliv na maximum signálu, který chceme, ale tak, aby se potlačilo maximum rušivých signálů. Ke směrování antény se pak přistupuje vždy až po nalezení kanálu, který má minimální rušení. (3)

Problémy nastávají spíše u přístupových bodů, které jsou vždy stavěny tak, aby obsloužily více klientů. V případě, že je přístupový bod situován tak, že jsou klienti rozmístěni v různých směrech, je zapotřebí použít všesměrovou anténu, ovšem všesměrový anténa také přijímá rušení všech směrů. (3)

2.5.2 Kabely a konektory

Většina antén, se kterými se běžně setkáváme, je navržena pro napájení koaxiálním kabele o impedanci 50 ohmů. Rozhodujícím faktorem pro použití určitého druhu kabelu je jeho útlum. Útlum je vždy vztažen k pracovnímu kmitočtu a jednotkové délce. Uvádí se tedy např. v dB/100m při daném kmitočtu. Obecně platí, že kabely s větším průměrem mívají útlum nižší. Konstrukčně je pak kabel uspořádán tak, že je utvořen středním vodičem, dielektrikem, vnějším stíněním a ochranným pláštěm. Střední vodič bývá obvykle plný nebo typu lanko. (3)

Dielektrikum bývá polyetylenové nebo pěnové nebo teflonové. Někdy může být i vzdušné a nebo kombinované. U kabelů, kde je použito vzdušné dielektrikum bývá použitý střední vodič zafixován ve správné poloze např. pomocí korálků nebo polyetylenové hvězdičky. Vnější stínění kabelu bývá poté většinou provedeno jako měděné opletení, které může být i dvojité. Stínění se taktéž vyskytuje postříbřené či stříbrné, někdy ho může tvořit měděná trubka, která také může být zvlněná. Samozřejmě se také mohou vyskytovat kombinace opletení a fólie a jiné. Konstrukční uspořádání v kabelu má obrovský vliv na jeho útlum. Obyčejné levné kabely mají pouze jednoduché stínění, které je tvořeno jednovrstvým opletením. Dražší kabely mají opletení dvojité, či výše zmíněné kombinace stínění. (3)

V případě konektorů se v praxi setkáváme s dvěma typy:

Prvním typem je konektor typu N. Bývá použit na anténách a důvodem jeho užití bývá možnost montáže jak na kabel o větším průměru (10 - 11 mm) tak i na tenčí kabely

(průměr 4 - 6 mm). Tento konektor lze umístit i ve venkovním prostředí, kde jej stačí ošetřit proti pronikání vlhkosti. (3)

Druhým typem konektoru je konektor RSMA. Někdy je také nazýván jako reverzní SMA. Běžně se vyskytuje na wi-fi kartách. Běžně dostupné RSMA konektory nejsou vhodné pro venkovní použití. Jsou většinou zlacené a vhodné pro montáže kabelů pouze o tenčím průměru. (3)

Pro případné propojení různých druhů kabelů můžeme použit tzv. "Pigtail". Jedná se o propojovací kabel, který může být na stranách opatřen různými konektory. (3)

3 Analýza současného stavu

3.1 Základní údaje o společnosti

Obchodní jméno: WALMARK, a.s.

Sídlo holdingu: Oldřichovice 44
739 61, Třinec
Česká Republika

IČO: 00536016

DIČ: CZ00536016

Právní forma: a.s.

Den zápisu: 30.07.1990

Predmět podnikání (činnosti):

1. Poradenské a konzultační činnosti
2. Koupě zboží za účelem jeho dalšího prodeje a prodej
3. Zprostředkovatelská činnosti v oblasti obchodu a služeb
4. Výroba jiných nealkoholických nápojů /bez ovocných šťáv/
5. Zpracování zemědělských produktů (vyjma živností řemeslných, vázaných a koncesovaných)
6. Výroba nápojů a potravinových doplňků (vyjma živností řemeslných, vázaných a koncesovaných)
7. Výroba kosmetických přípravků
8. Výroba potravin (vyjma živností řemeslných, vázaných a koncesovaných)
9. Marketingové služby

3.2 Výrobní sortiment

Společnost Walmark, a.s. se primárně zaměřuje na výrobu a distribuci potravinových doplňků a volně prodejných léčiv. Ze začátku existence bylo její jméno spojováno hlavně s džusy a limonádami, později se společnost přeorientovala na výše zmíněný sortiment.

V dnešní době společnost Walmark, a.s. má ve svém portfoliu několik desítek různých těchto doplňků a volně prodejných léčiv včetně velmi známých značek jako jsou Proenzi, Prostenal, GinkoPrim a mnohé jiné.

3.3 Organizační struktura společnosti

Společnost Walmark, a.s. je akciovou společností, která má akcie na jméno. Základní jmění (105 000 000 Kč), které do ní bylo vloženo, je vloženo některými členy představenstva (Mgr. Adam Walach, Ing. Mariusz Walach, RNDr. Valdemar Walach). Společnost je dále většinovým či 100% vlastníkem společností jako je Aminostar apod.

3.4 Představenstvo společnosti

Představenstvo společnosti je tvořeno jejími zakladateli a členy výkonných orgánu společnosti:
Mgr. Adam Walach - předseda představenstva
RNDr. Valdemar Walach - 1. místopředseda představenstva
Ing. Petr Turoň - 2. místopředseda představenstva, výkonný ředitel
Ing. Mariusz Walach - člen představenstva
Ing. Roman Kantor - člen představenstva, ředitel pro strategické projekty a marketing

3.5 Dozorčí rada společnosti

Dozorčí rada společnosti je tvořena ze dvou třetin výkonnými orgány společnosti:
Ing. Věslava Štéblová - předseda dozorčí rady, hlavní ekonom
Ing. Miroslav Haratek - člen dozorčí rady, provozní ředitel
Zuzana Turoňová - člen dozorčí rady

3.6 Vedení společnosti (holdingu)

Ing. Petr Turoň - výkonný ředitel
Ing. Roman Kantor - ředitel pro strategické projekty a marketing
RNDr. Vladimír Voda, Ph.D. - ředitel mezinárodního obchodu
Ilona Urbanová - personální ředitelka

Ing. Miroslav Haratek - provozní ředitel

Dr.Ing. Karel Kučera - ředitel mezinárodního marketingu

Ing. Anestis Dimitris - ředitel exportu

Ing. Zdeněk Podlipný, MBA - finanční ředitel

3.7 Informační technologie ve společnosti

Společnost Walmark, a.s. jakožto výrobce a distributor potravinových doplňků resp. léčiv musí mít infrastrukturu dotaženou víceméně k dokonalosti, protože výroba, sklady a ředitelství nejsou centralizovány a v tom případě je nutné precizní propojení v rámci IT infrastruktury.

Pro potřeby společnosti jsou v rámci serverů i koncových stanic použity produkty z portfolia společnosti Microsoft. U starších koncových stanic jsou jako operační systém použity Windows XP Professional, u ostatních Windows Vista Business. Tyto verze jsou použity kvůli tomu, aby mohly být připojeny v doméně. Plánem do budoucna je migrace na systém Windows 7, ale tato záležitost je v holdingu s více než tisícovkou zaměstnanců finančně a technologicky velmi náročná už jen kvůli tomu, že veškeré systémy musí po migraci bezchybně fungovat. Servery běží na operačním systému Windows Server 2008 R2 a je zde využíván virtualizační SW VMWare. Z dalších základních potřeb je zde pošta, která je také vyřešena na platformě Microsoftu systémem Exchange 2010. Pro potřeby managementu a výkonných složek společnosti se ve společnosti momentálně zavádí jednotný systém manažerských komunikátorů. Jako přístroje byly vybrány komunikátory společnosti BlackBerry pro jejich výbornou možnost integrace s platformou Microsoft.

Samozřejmě v takto velké společnosti je používán databázový systém SAP jakožto centrální ekonomický systém společnosti. Jakožto intranetový portál je opět využita platforma Microsoftu, konkrétně produkt SharePoint. Jako DMS (document management system) je ve společnosti použit LiveLink.

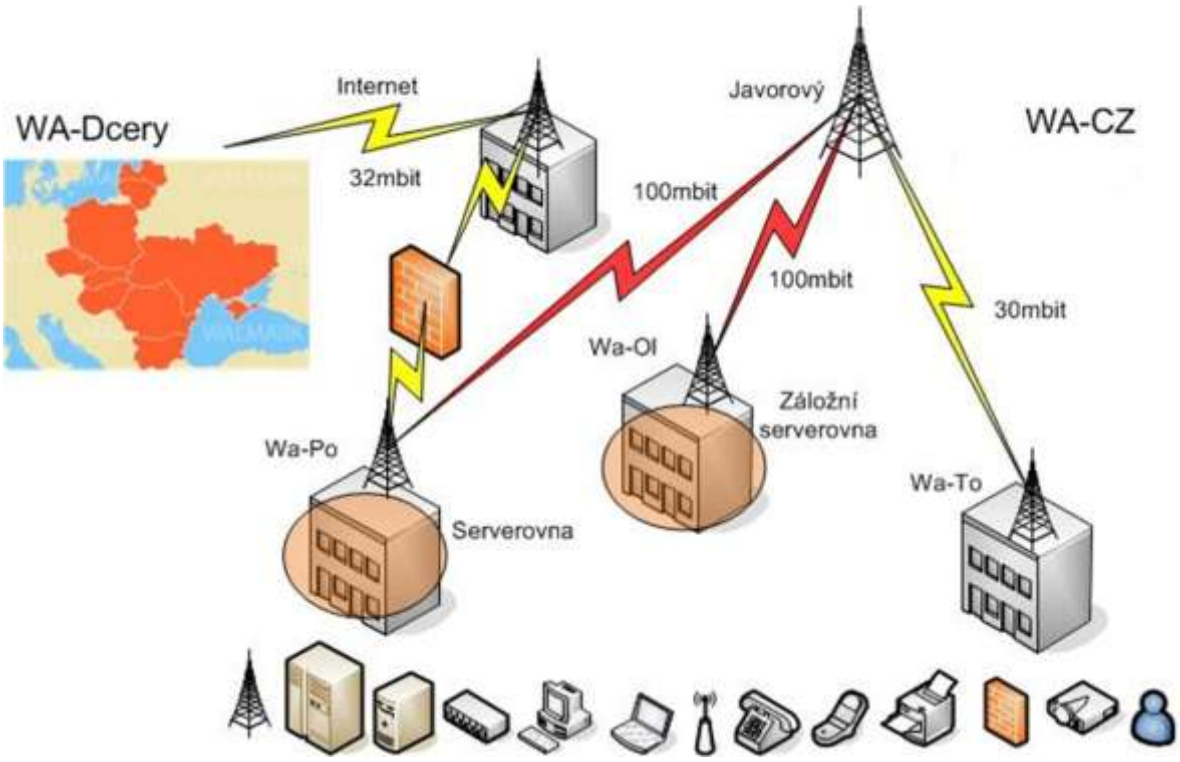
Realizace nákupu HW probíhá přes standardní business dodavatele. V našem případě se pro koncové pevné stanice využívá služeb společnosti Autocont. Pro notebooky se využívá služeb společnosti DELL, které k nim nabízí záruku formou servisu Next Business Day. Serverovna je vybavena produkty společnosti IBM. Servery, diskové pole, pásková mechanika na zálohy. Stejným HW je vybavena i redundantní

serverovna, která byla loni realizována. Samozřejmě serverovny jsou opatřeny klimatizací, dvojitou autentizací při vstupu + mechanické zabezpečení a výpadky elektrického proudu jsou pojištěny dieselovým agregátem.

V budovách - ať už administrativních či výrobních - je síť LAN rozvedena pomocí klasické strukturované kabeláže. Dále je samozřejmě v těchto použita i bezdrátová síť. Např. pro sklady léčiv a doplňků stravy jsou použity speciální bezdrátové čtečky, které jsou napojeny na vnitřní WLAN síť realizovanou na platformě Mikrotik a napojeny přímo do systému SAP.

3.8 Schéma propojení jednotlivých lokalit v rámci Walmark Česká republika

Společnost Walmark má v rámci Třinecka (patří zde i lokalita Český Těšín) několik budov, které bylo zapotřebí vzájemně propojit. Na následujícím schématu je naznačeno, jakým způsobem jsou lokality propojeny.



Obr. 3.1: Schéma propojení lokalit v rámci Walmark Česká republika (Zdroj: vlastní)

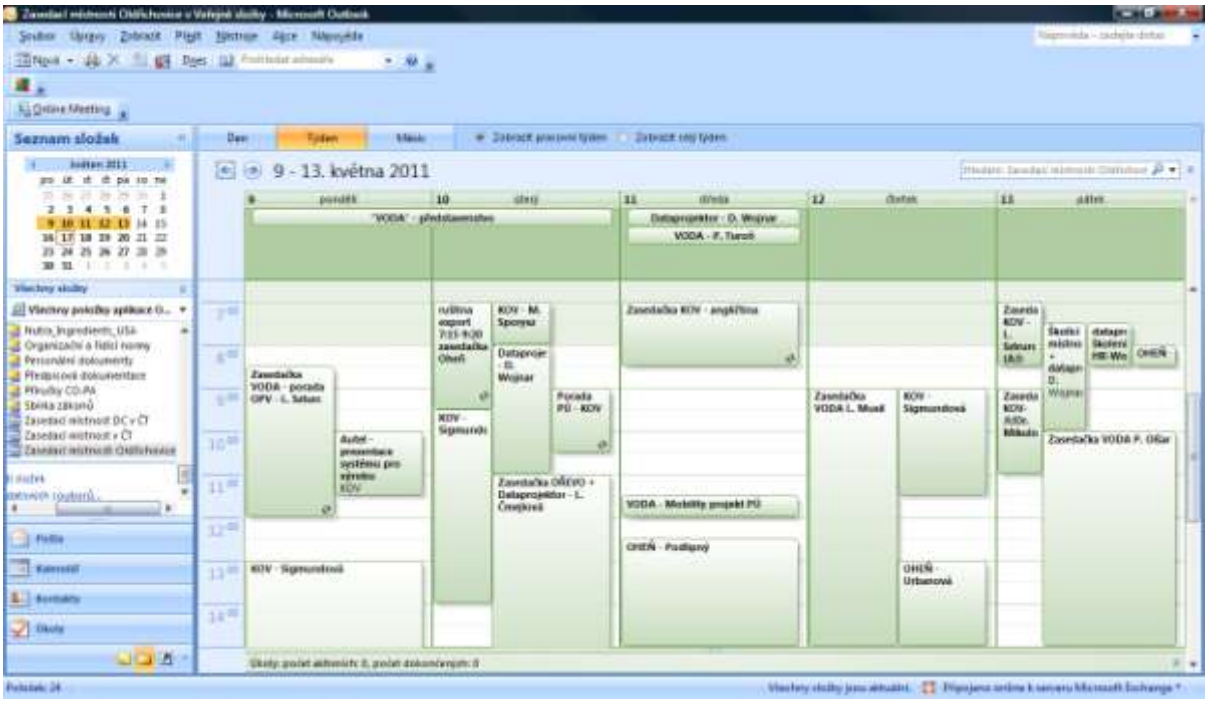
Tři hlavní budovy jsou Walmark - Polní (Wa-Po, výrobní závod na ulici Polní v Třinci), Walmark Oldřichovice (Wa-Ol, budova ředitelství v městské části Oldřichovice v

Třinci) a Walmark Tovární (Wa-To, sklady a závod na ulici Tovární v Českém Těšíně). Tyto budovy bylo zapotřebí propojit vhodným způsobem do jednoho celku. Jako optimální se ukázalo propojení přes jeden styčný bod, který je umístěn na vrcholu kopce Javorový vrch, na který je přímá viditelnost ze všech tří lokalit. Tyto lokality jsou pak vzájemně propojeny a jsou v jedné síti. Zároveň takto mohou fungovat obě serverovny - hlavní, která je umístěna v budově na Polní a nová záložní, která byla vybudována v budově ředitelství v Oldřichovicích. Do budovy na Polní je přivedena hlavní internetová konektivita od společnosti GTS a je zde také umístěn hlavní firewall. Vzhledem k tomu, že jsou budovy takto propojeny do jedné sítě, v případě výpadku bezdrátového spoje není možné ani síťově tisknout tak, že tiskárna na kterou je dokument zaslán je ve stejné budově jako klient, který chce tisknout. Pro zamezení těchto problémů, které mohou nastat zejména v zimě, protože vrch Javorový se nachází ve výšce cca. 1000 m.n.m. byly vybudovány další záložní spoje. V levé části schématu je poté na mapce nastíněno, kde má společnost Walmark své dceřinné společnosti, které jsou centrálně spravovány ze sídla holdingu v Třinci.

3.9 Analýza výchozího stavu ve společnosti

Výchozím stavem projektu realizace bezdrátové sítě v budově ředitelství společnosti WALMARK, a.s. byl požadavek vedení společnosti, aby byla nově zrekonstruovaná budova pokryta signálem bezdrátové sítě a případné návštěvy mohly využívat připojení k internetu ať už v rámci business prezentací nebo klasických obchodních jednání. Využití kabelu RJ-45, který se zapojit do ethernetové zásuvky se pro tyto případy již jevilo jako zastaralé a nepoužitelné.

V budově ředitelství se nachází 5 jednacích místností (Oheň, Voda, Kov, Dřevo, Školící místnost), které jsou využívány jak pro interní, tak také pro externí jednání v rámci obchodu společnosti. Tyto jednací místnosti jsou rezervovány přes systém SharePoint, který je propojen s kalendářem v Exchange.



Obr. 3.2: Systém rezervací jednacích místností přes Outlook (Zdroj: vlastní)

V rámci těchto místností se také rezervují veškeré zdroje, které jsou v jednacích místnostech používány jako - flip-chart, dataprojektor (pokud není v jednací místnosti umístěn tzv. "napevno"). Vzhledem k absolutnímu vytížení těchto místností a pouhému kabelovému připojení, které bylo shledáno jako naprosto nedostatečné, bylo rozhodnuto o pokrytí - v této fázi zatím jen - jednacích místností.

Tento krok byl proveden zapojením klasického routeru značky D-Link, který používal pro zabezpečení standardní šifrování s WEP klíčem.

Obr. 3.3: Router D-Link (Zdroj: http://patrikvogl.cz/clanek/391-levny-a-kvalitni-wifi-router-d-link-di-524.html)

Tento router byl přístupový bod kombinovaný s routerem. Podporuje standardy IEEE 802.11b a IEEE 802.11g. Pro bezpečnost podporuje funkce jako jsou NAT, DDNS a jiné. Vestavěný DHCP server zabezpečuje automatické přidělování IP adres. Z hleediska zabezpečení podporuje 64/128-bitové šifrování dat WEP a WPA. Samozřejmě je plně konfigurovatelný přes webové prostředí. K tomuto zařízení je možnost připojení externí antény standardním konektorem. (6)

Zabudovaný Firewall u tohoto routeru disponuje možností filtrovat MAC adresy, IP adresy a URL adresy. Dále disponuje možností blokování domén.

Komunikační rozhraní jsou 1x RJ-45 WAN Ethernet 10/100 Mbps, 4x RJ-45 LAN Ethernet 10/100 Mbps a konektor pro externí anténu. (6)

Takovéto zařízení ovšem bylo shledáno jako nedostatečné vzhledem k narůstajícím potřebám využití bezdrátové sítě. Dále také takovéto zařízení není schopno správně spolupracovat s doménovou politikou, která se dá velmi účinně využít pro autentizaci uživatele. WEP klíč je také již zastaralý jakožto jediný způsob zabezpečení, zvláště v případě, že si uvědomíme, že budova stojí v zástavbě, kde může teoreticky existovat možnost, že se někdo bude pokoušet o odposlech komunikace a v případě, že by se zrovna prezentovala citlivá firemní data, bude schopen společnost svým zásahem nenávratně poškodit, třeba už jen tím, že zcizí know-how k farmaceutickým přípravkům, či například jen hesla k přístupu na některá PC.

Toto se může stát zejména v případě, že budou probíhat firemní a produktová školení, či prezentace hospodářských výsledků a podobně, protože zasedací místnosti jsou užívány i k těmto účelům. Z této výchozí situace vnikl plán na vytvoření sofistikovanějšího systému pokrytí jednacích místností signálem bezdrátové sítě wi-fi.

4 Vlastní návrh řešení

4.1 1. fáze řešení realizace bezdrátového pokrytí jednacích místností

4.1.1 Parametry výběru řešení

Základními parametry pro výběr řešení pokrytí jednacích místností bylo zejména vybrání ucelené platformy, která bude jakožto řešení dlouhodobě stabilní a prověřená. Bylo třeba od začátku zabránit nakoupení hardwaru, který bude mít obyčejné ("krabičkové") řešení a v případě vydání příštího modelu už se na tomto systému může mnoho věcí změnit tak, že nebudou zpětně kompatibilní v plné míře a tím pádem nebudou schopny pohromadě v pořádku fungovat.

Dalším požadavkem byla velká možná míra konfigurovatelnosti těchto zařízení. Vzhledem k tomu, že se již systém bezdrátových sítí používal v produktových skladech, kde byl přes bezdrátové čtečky propojen přímo se systémem zásob SAP, bylo třeba, aby platforma byla schopna s tímto systémem spolupracovat v plné míře a případně se s ním na úrovni VLAN protnout.

Požadavkem ze strany vedení bylo, že v zasedacích místnostech se často vedou porady vedení a představenstva. Každý manager samozřejmě disponuje svým osobním přenosným počítačem, který pro pracovní účely využívá. Nicméně, aby mohly být porady funkční, bylo potřeba, aby některé počítače mohly být autentifikovány tak, že jsou připojeny k místní síti a mají plný přístup jak síťovým disků, tak k síťovým tiskárnám apod. Vzhledem k velmi složité struktuře sítě (bezdrátové páteřní spoje mezi serverovnami, síťové tiskárny na různých částech společnosti včetně výrobních závodů atd.) bylo zapotřebí tedy vybrat platformu, která je stále schopna veškeré tyto nápory zvládat za plného provozu sítě. Ve zkratce - uživatel nesmí mít možnost poznat, že nesedí ve své kanceláři u pevného PC nebo nemá přenosný počítač zapojen v dokovací stanici.

Dalším požadavkem, který vzešel z brainstormingu bylo vytvoření dvou pásem rychlostí pro hosty. Někdy je totiž zapotřebí pro produktové prezentace, či pro prezentace řešení externích společností rychlejšího připojení k internetu. Bylo proto

dohodnuto, že budou vytvořena 2 rychlostní pásma, která budou k využití pro externisty.

1. pásmo - rychlost 512 kbps, které je neautentifikované, bez hesla a je zcela mimo interní síť společnosti. Zde sice stále existuje riziko, že jej může zachytit několik okolních domů, ale toto riziko je již na únosné míře.

2. pásmo - rychlost 5 Mbps, pro jehož využití již host musí znát přihlašovací jméno a heslo, aby jej mohl využít.

Posledním faktorem byla samozřejmě finanční otázka celého řešení. Tato realizace probíhala v době ekonomické recese, proto se hledělo i na rozpočet, nicméně bylo třeba zvolit přiměřeně kvalitní platformu, která bude zejména moct být spravována interními zaměstnanci IT oddělení a nebudou vynaloženy další náklady navíc na případné odborníky v oblastí, kteří by museli provádět servis.

4.1.2 Vhodnost výběru platformy MikroTik

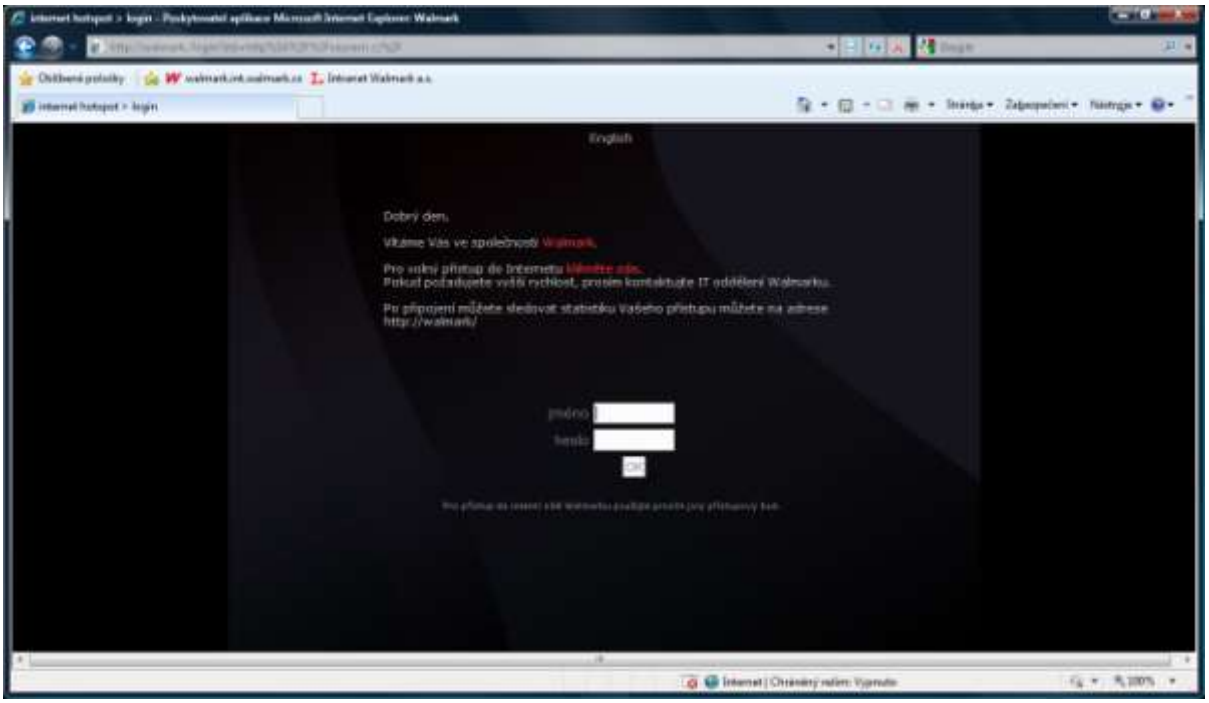
Ze všech uvedených vstupních parametrů vyšla jako vítěz platforma MikroTik. Zejména také proto, že již byla nasazena v systému řízených skladů společnosti a pro ujednocení správy byla jasnou volbou. Zadání sice bylo specifikováno poměrně přesně, nicméně z analýz vyplynulo, že obdobný systém, který by dodávala společnost CISCO by byl mnohonásobně finančně náročnější, nehledě na to, že správa CISCO zařízení má svá specifika a školení na tuto platformu jsou finančně velmi nákladná.

Aby mohlo být zabezpečeno pásmo jak pro interní systém, který by používali zaměstnanci společnosti, ale také pásmo pro návštěvníky v obou rychlostech, bylo nakonec rozhodnuto tak, že pro pásmo hostů (jak volné tak i pásmo s autentifikací) bude použito separátní zařízení a pro pásmo přístupu do interní sítě bude použito také separátní zařízení. Toto řešení nebylo nutné z hlediska konfigurace routerboardů, které jsou schopny pojmout klidně i tři rádiové karty, které jsou schopny samostatně managovat, nicméně v rámci realizace projektu se tato možnost prokázala jakožto nejoptimálnější řešení. Každé zařízení se totiž potom dá v rámci dohledového centra spravovat hromadně.

Problém dvou pásem pro hosty byl využit vlastní platformy MikroTik, která se nazývá HotSpot. V přihlašovací obrazovce si uživatel buď zvolí možnost, kdy se přihlásí jako host a je přihlášen jako uživatel, který využívá první pásmo s rychlostí 512 kbps nebo

zadá uživatelské jméno a heslo a je mu umožněno využívat vyšších rychlostí. Toto řešení se projevilo jako maximálně efektivní a účinné.

Z ekonomického hlediska byl výběr platformy MikroTik ideální, protože jakožto modulární stavebnici si může zákazník sestavit své zařízení dle svých požadavků bez zbytečných komponent a funkcionalit, za které by musel připlácet.



Obr. 4.1: Login obrazovka funkce Hot-Spot (Zdroj: vlastní)

4.1.3 Princip autentifikace interních uživatelů do sítě wi-fi

V rámci funkcionality systému Windows Server 2008 můžeme použít služeb standardů IEEE 802.1x ověření klientů bezdrátových služeb pro standard IEEE 802.11. V kombinaci standardu 802.1x a přístupového bodu jej podporujícího a dalších služeb sytému Windows Server 2008, které jsou nasazeny na síti, jsou tyto služby použitelné pro kontrolu zařízení, které k této síti přistupují.

Samozřejmě je také možné použít funkcí systému Windows Server 2008 pro definování konektivity a nastavení zásad zabezpečení, které poté bezdrátový adaptér užívá pro pokusy o připojení do této sítě. NPS neboli Network Policy Server umožňuje vytvářet a posilovat pravidla přístupu do sítě pro autentizaci, autorizaci a "zdraví" klientů. Politiky bezdrátových sítí v systému Windows Server 2008 umožňují konfiguraci klientských

počítačů v síti s bezpečnostními nastaveními připojení, které musí použít pro připojení do této sítě.

Pro nasazení systému ověřování bezdrátových sítí v prostředí Windows Server 2008 je zapotřebí, aby měla síťová infrastruktura následující prvky:

- Služby Active Directory Domain (AD DS)
- Vzdálenou autentizaci dial-in uživatele služby (RADIUS)
- Osvědčení infrastruktury - známé jako Public Key Infrastructure (PKI)
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)

Tyto služby společně poskytují bezpečnost, dostupnost a škálovatelnost potřebnou pro bezdrátové lokální sítě.

NPS musí být nainstalován na jeden nebo více serverů v síti. NPS servery musí být logicky připojeny k síti tak, aby mohly přijímat příchozí žádosti o přístup přímo z bezdrátového přístupového bodu.

V rámci Active Directory je poté vymezena skupina uživatelů, kteří jsou skupině WIFI a jsou pak systémem autentifikováni + ve skupině počítačů je také vytvořena skupina, kde je použit ještě dále systém kontroly MAC adresy, tak aby se maximálně minimalizovalo riziko neoprávněného přístupu. Samozřejmě je potřeba ještě zadat klasické heslo pro přístup do PC resp. domény spravované systémem Active Directory.

4.1.4 Platforma MikroTik a použitý hardware při 1. fázi realizace

MikroTik Router OS je operační systém pro routery, který je založen na bázi systému Linux OS. Tento systém je vhodný zejména pro bezdrátové sítě a nebo třeba jako bezpečný hardwarový firewall. Taktéž může sloužit jako router s velmi dobrou možností konfigurace přes grafické rozhraní. Komunikace s operačním systémem se provádí zejména přes grafické rozhraní Winbox, SSH, telnet, sériovou konzolu. V dnešní době je tento systém uplatňován zejména u spojů 802.11a/b/g/n, které vysoce dbají na kvalitu.

Vývoj MikroTik Router OS sahá do roku 1995, kdy společnost MikroTik nastartovala svou činnost vývojem a prodejem bezdrátových komunikačních systémů pro ISP. MikroTik Router OS byl původně vyvíjen v Lotyšsku. Postupné zkušenosti přivedly vývojáře k vytvoření routovacího software MikroTik v2 PC. Tento software přinesl

výraznou stabilitu, ovladatelnost, flexibilitu a celkově vše potřebné pro všechny typy komunikačních zařízení.

Role, které MikroTik běžně zastává se dají rozdělit takto:

- Bezpečnostní Firewall
- Omezující Firewall (QoS)
- VPN Server / Klient, podpora protokolů PPP, PPTP, L2TP, OVPN, EoIP, IPsec
- Wifi zařízení v režimech AP, Klient, WDS
- Hotspotové řešení (využito i v našem případě)
- Proxy server
- Bridge
- Router s podporou dynamických protokolů (RIP, OSPF, BGP, MME)
- Syslog
- Traffic Monitor Server

Pro první fázi realizace projektu pokrytí - v tomto případě zasedacích místností byl použit následující hardware:

Zařízení, které je použito pro přístup zaměstnanců do vnitřní sítě společnosti využívá jako základ **MikroTik Routerboard RB433AH**.

Obr. 4.2: Routerboard RB433AH (Zdroj: http://wifi-shop.cz/mikrotik-routerboard-rb433ah-128mb-ddr-sdram-680-mhz-3x-minipci-l5_d1999.html)

Základní technické specifikace:

Procesor - Atheros A7130, 680 MHz

RAM - 128 MB DDR SDRAM

Napájení - Jack + POE (Power Over Ethernet)

Porty - 3x RJ-45 10/100 Mbps MDI/MDI-X

Sloty - 3x miniPCI

Rozšiřující sloty - slot pro MicroSD karty

Plná podpora IPv6

Pro bezdrátovou komunikaci je do RouterBoardu vsazena karta **miniPCI 802.11n R52Hn**

Obr. 4.3: miniPCI karta 802.11n R52Hn (Zdroj: http://www.mikrotik.cz/r52hn-minipci-karta-802-11n-atheros-ar9220-2-4-5-ghz-25-dbm-_d1746.html)

Základní technické specifikace:

Chipset - Atheros AR922D

Přenosová rychlost - až 300 Mbps

Rozhraní - miniPCI IIIA+

Šifrování - WEP 64/128, WPA, WPA2, 802.1x

Maximální výstupní výkon: 25 dBm

Frekvence - 2,4 GHz, 5 GHz

Použitá anténa, napájení, case a pigtail pro propojení externí antény s miniPCI kartou:

Case:

Obr. 4.4: Case pro RouterBoard RB433 (Zdroj: http://www.mikrotik.cz/kovovy-indoor-case-pro-rb433_d1035.html)

Standardní case pro RouterBoard RB433 pro použití v budovách.

Zdroj:

Obr. 4.5: Napájecí zdroj (Zdroj: http://www.mikrotik.cz/napajeci-zdroj-24-v-0-8-a-pro-rb-19w-spinany-_d1027.html)

Standardní napájecí zdroj 24V, 0,8A pro RouterBoardy. Výstupní výkon je 19W. Tento zdroj je dodáván jako značkové příslušenství výrobcem MikroTik.

Pigtail:

Obr. 4.6: Pigtail pro propojení RouterBoardu a miniPCI karty (Zdroj: http://www.mikrotik.cz/pigtail-mmcx-male-rsma-pro-minipci-90-uhlovy_d980.html)

Pigtail, který má na jedné straně konektor MMCX pro připojení na miniPCI kartu a na straně druhé konektor RSMA pro připojení externí antény.

Anténa:

Obr. 4.7: Všesměrová anténa 5dBi (Zdroj: http://wifi-shop.cz/vsesmerova-antena-5-dbi-rsma-konektor_d675.html)

Standardní všesměrová anténa s 5 dBi a RSMA konektorem. Tím je napojena přes pigtail na miniPCI kartu.

HW použitý pro pásmo hostů se liší pouze v použitém RouterBoardu (nižší provedení) a bezdrátové karty (taktéž nižší provedení). RouterBoard je vzhledově stejný jako výše uvedený, ale disponuje následujícími parametry:

MikroTik RouterBoard RB 433

Procesor - MIPS, 300MHz

RAM - 64 MB DDR SDRAM

Napájení - Jack + POE (Power Over Ethernet)

Porty - 3x RJ-45 10/100 Mbps MDI/MDI-X

Sloty - 3x miniPCI

Rozšiřující sloty - nejsou

Plná podpora IPv6

Bezdrátová karta - **WLM200NX miniPCI karta 802.11n**

Obr. 4.8: miniPCI karta WLM200NX miniPCI 802.11n (Zdroj: http://www.mikrotik.cz/wlm200nx-minipci-karta-802-11n-atheros-ar9220-2-4-5-ghz-_d2209.html)

Základní technické specifikace:

Chipset - Atheros AR9220

Přenosová rychlost - až 300 Mbps

Rozhraní - miniPCI

Šifrování - WEP 64/128, WPA, WPA2, 802.1x

Maximální výstupní výkon: 23 dBm

Frekvence - 2,4 GHz, 5 GHz

4.1.5 Náklady na 1. fázi realizace pokrytí budovy bezdrátovým signálem

Náklady v rámci 1. fáze pokrytí budovy bezdrátovým signálem jsou rozděleny následujícím velmi jednoduchý způsobem:

Tabulka 4.1: Náklady na zařízení pro vstup do interní sítě společnosti (Zdroj: vlastní)

RouterBoard	2147 Kč (2578 Kč vč. DPH)
Bezdrátová karta	699 Kč (841 Kč vč. DPH)
Case	300 Kč (360 Kč vč. DPH)
Zdroj	143 Kč (173 Kč vč. DPH)
Pigtail	72 Kč (86 Kč vč. DPH)
Anténa	75 Kč (90 Kč vč. DPH)
CELKEM	3436 Kč (4128 Kč s DPH)

Tabulka 4.2: Náklady na zařízení pro 2 pásma hostů (Zdroj: vlastní)

RouterBoard	1433 Kč (1721 Kč vč. DPH)
Bezdrátová karta	347 Kč (418 Kč vč. DPH)
Case	300 Kč (360 Kč vč. DPH)
Zdroj	143 Kč (173 Kč vč. DPH)
Pigtail	72 Kč (86 Kč vč. DPH)
Anténa	75 Kč (90 Kč vč. DPH)
CELKEM	2370 Kč (2848 Kč vč. DPH)

V rámci 1. fáze realizace pokrytí zasedacích školících místností společnosti byly náklady na použitý hardware celkově 5806 Kč resp. 6976 Kč vč. DPH. Montáž + instalace není započtena z důvodu, že ji prováděli sami zaměstnanci IT oddělení v rámci náplně své práce.

4.2 2. fáze realizace řešení - pokrytí signálem budovy celého ředitelství v Třinci - Oldřichovicích

V návaznosti na 1. fázi projektu, kdy byly bezdrátovým signálem v budově pokryty zasedací a školící místnosti, se toto řešení ukázalo jako velice funkční a využívané pro, ať už obchodní či interní, schůze a zasedání, nastal požadavek pro pokrytí celé budovy ředitelství společnosti Walmark v Třinci - Oldřichovicích bezdrátovým signálem za stejné funkcionality, která zatím fungovala v zasedacích a školících místnostech.

4.2.1 Výchozí požadavky a důvody k rozšíření pokrytí budovy

V rámci 2. fáze realizace pokrytí bylo výchozím důvodem pro kompletní pokrytí celé budovy shledáno zejména to, že operativní porady zejména v rámci managementu probíhají čím dále, tím častěji v kancelářích jednotlivých managerů. V rámci těchto porad je často potřeba najednou využít některých zdrojových dat, která má zaměstnanec ve svém přenosném počítači, ale v rámci kanceláře se není na síť jak napojit, protože kabel RJ-45 není k dispozici a takovýto systém je neefektivní a zdržuje. V rámci tohoto bylo třeba najít řešení, které bude rozumné a maximálně účinné. Ze strany vedení společnosti bylo tedy oddělení IT uložen úkol, aby rozšířili bezdrátové připojení z jednacích místností do celé budovy ředitelství v Třinci - Oldřichovicích. Funkcionalita přitom má zůstat na stejné úrovni - tedy 2 pásma (autentifikované a neautentifikované) pro volný přístup a interní pásmo pro využití zaměstnanců společnosti.

4.2.2 Realizace 2. fáze pokrytí bezdrátovým signálem

Vzhledem k předchozí kladné zkušenosti s vybraným hardwarem a jeho následnou funkčností nebylo třeba o hardwaru přemýšlet. Pro pokrytí zbytku budovy byly použity stejné sestavy jako v případě zasedacích místností. Pro pásmo, které používají interními zaměstnanci to tedy byla sestava:

MikroTik RouterBoard RB433
miniPCI 802.11n R52Hn
Standardní case pro RouterBoard 433 pro indoor použití
Standardní napájecí zdroj 24V, 0,8A, který je dodáván jako originální příslušenství MikroTik
Pigtail s konektory MMCX a RSMA
Standardní všesměrová anténa 5 dBi s konektorem RSMA

Pro pásma hostů (autentifikované a neautentifikované) byla použita sestava:

MikroTik RouterBoard RB433AH
WLM200NX miniPCI karta 802.11n

Standardní case pro RouterBoard 433 pro indoor použití
Standardní napájecí zdroj 24V, 0,8A, který je dodáván jako originální příslušenství MikroTik
Pigtail s konektory MMCX a RSMA
Standardní všesměrová anténa 5 dBi s konektorem RSMA

V rámci této fáze realizace bylo nejnutnější rozměřit dobře signál po budově tak, aby bylo možno použít co nejmenšího množství komponent a minimalizovat tím náklady na pokrytí budovy, protože tento plán vznikl postupně bez toho, aby se s velkou akcí počítalo ve finančním plánu IT oddělení.
K měření byly použity klasické měřiče bezdrátového signálu + notebooky, kdy se přímo testovala funkčnost ve všech kancelářích v budově tak, aby provoz byl bezproblémový. Po sérii těchto měření a testů bylo nakonec rozhodnuto o umístění dalších dvou resp. čtyř přístupových bodů (2 pro interní přístup a 2 pro hosty) v rámci pokrytí budovy. Celkově tedy je v rámci pokrytí budovy ředitelství společnosti v budově umístěno 6 přístupových bodů s tím, že jsou vždy umístěny po dvou, aby z tohoto místa vycházelo pokrytí jak pro interní pásmo, tak pro dvě pásma pro hosty.
Všechna zařízení stejného druhu mají nastaveno stejné SSID tak, aby si klientské zařízení vyhodnotilo, na kterém z nich bude mít nejsilnější signál a automaticky se na něj přeladilo - viz. funkce Roaming. V rámci této funkce je pak přeladění pro klienta v podstatě prakticky neznatelné. Přeladění se může prakticky projevit snad jen v případě, že by se zrovna z počítače konal telefonický rozhovor. Tehdy by zřejmě k přeskočení signálu došlo, nicméně implicitně nebyla síť stavěna pro využití klientských zařízení jako telefonů, ale opravdu pouze v rámci využití resp. odstranění nutnosti využití klasického kabelového připojení.

4.2.3 Náklady na 2. fázi pokrytí budovy bezdrátovým signálem

Vzhledem k nákladům na 1. fázi pokrytí budovy a nezměněným cenovým podmínkám, protože realizace 2. fáze proběhla velmi rychle po té první, jsou náklady opět rozčleněny logicky takto:

Tabulka 4.3: Náklady na zařízení pro vstup do interní sítě společnosti (Zdroj: vlastní)

2x RouterBoard	2147 Kč (2578 Kč vč. DPH)
2x Bezdrátová karta	699 Kč (841 Kč vč. DPH)
2x Case	300 Kč (360 Kč vč. DPH)
2x Zdroj	143 Kč (173 Kč vč. DPH)
2x Pigtail	72 Kč (86 Kč vč. DPH)
2x Anténa	75 Kč (90 Kč vč. DPH)
CELKEM	6872 Kč (8256 Kč s DPH)

Tabulka 4.4: Náklady na zařízení pro 2 pásma hostů (Zdroj: vlastní)

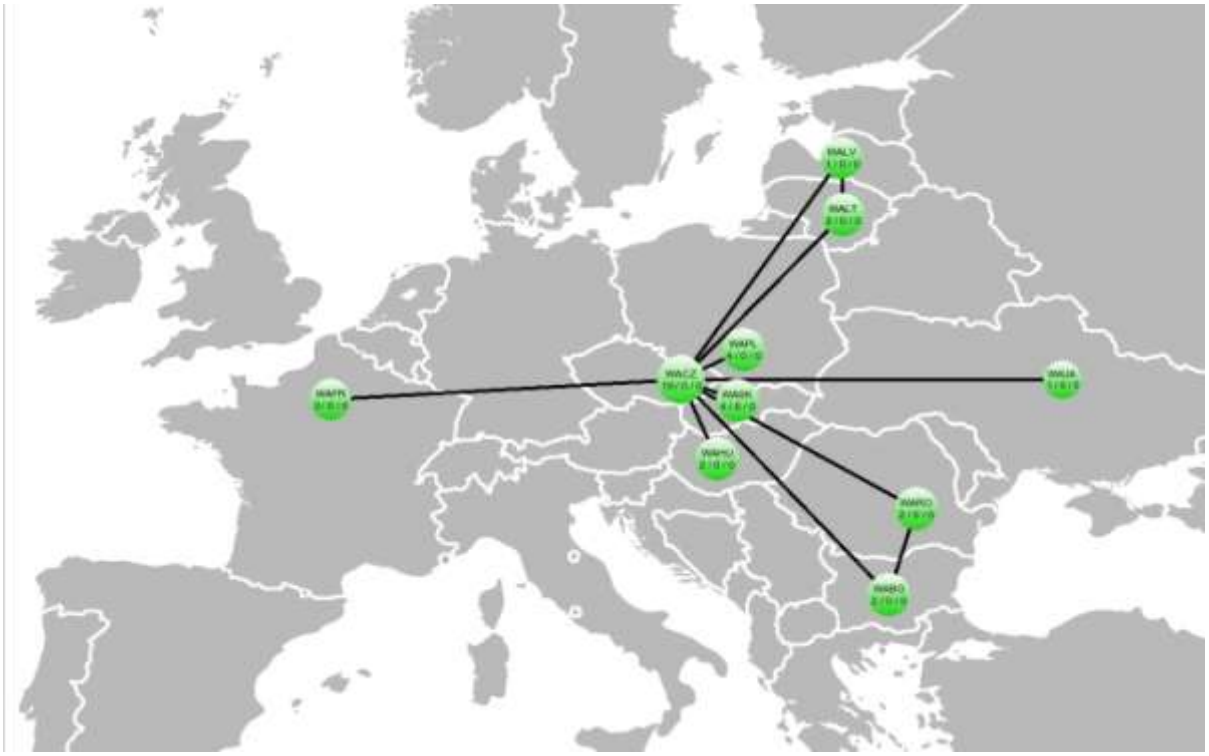
2x RouterBoard	1433 Kč (1721 Kč vč. DPH)
2x Bezdrátová karta	347 Kč (418 Kč vč. DPH)
2x Case	300 Kč (360 Kč vč. DPH)
2x Zdroj	143 Kč (173 Kč vč. DPH)
2x Pigtail	72 Kč (86 Kč vč. DPH)
2x Anténa	75 Kč (90 Kč vč. DPH)
CELKEM	4740 Kč (5696 Kč vč. DPH)

V rámci 2. fáze realizace pokrytí budovy bezdrátovým signálem byly kompletní náklady vyčísleny na 11612 Kč resp. 13952 Kč vč. DPH. Opět není třeba zahrnovat instalaci zařízení, jejich konfiguraci a ostatní činnosti s tímto spojené, protože byly opět provedeny v rámci náplně práce zaměstnanců oddělení IT.

4.3 3. fáze řešení - propojení jednotlivých lokalit a centrální správa pomocí management centra

V rámci třetí fáze realizace pokrytí, která již není přímo spojena s pokrytím budovy ředitelství společnosti bezdrátovým signálem, ale spíše se v ní jedná o komplexní správu bezdrátových sítí ve společnosti, propojení jejich správy na všech pobočkách a dceřiných firmách.

V této fázi hraje hlavní roli použitý nástroj od společnosti MikroTik - Dude network monitor. Tento nástroj výrazně zlepšuje možnosti řízení síťového prostředí ve společnosti. Automaticky prohledá veškeré stanovené sítě a podsítě, vyhledá v nich všechny přístroje a nakreslí mapu sítě a její propojení. Tento systém je v podstatě takovým dohledovým centrem nad sítí, která se sestává z mnoha aktivních prvků, protože díky své rozsáhlé funkcionalitě se umí dostat ke všem možnostem těchto zařízení, ale i komplexně monitoruje, jestli nějaké zařízení nemá problémy apod.
Na následujícím schématu z Dude network monitor můžeme vidět propojení jednotlivých dceřiných společností holdingu Walmark v rámci Evropy. Každá sekce má své logické pojmenování podle země a uveden počet zařízení, se kterými lze v rámci dohledového centra operovat.



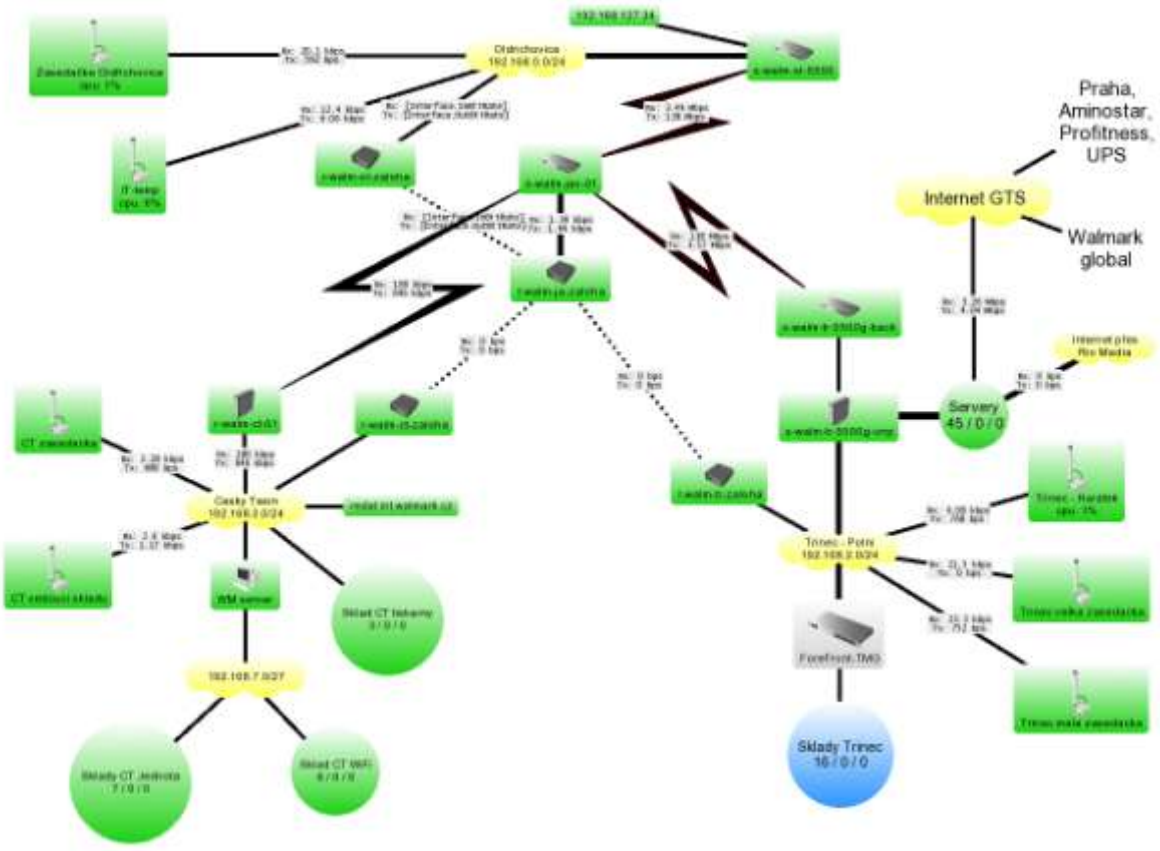
Obr. 4.9: Schéma propojení dceřiných společností (Zdroj: vlastní)

V rámci třetí fáze máme zejména na zřeteli použití této bezdrátové technologie na všech dceřiných společnostech v rámci Evropy. V rámci České republiky byl později systém také nasazen na pobočce v Praze se stejnou funkcionalitou jako na ředitelství v Třinci - Oldřichovicích, aby kdokoliv z manažerů společnosti neměl žádný problém s

komunikací v rámci společnosti a nemusel řešit po příjezdu na pražskou pobočku připojování se pomocí kabelů.

Management centrum umí také shromažďovat velké množství údajů, které lze poté zpětně v rámci síťového provozu analyzovat, což může být velmi užitečné v rámci vylepšování síťové infrastruktury a poté zpětného hodnocení investice jakožto správné. V rámci analýzy se ve společnosti zejména využívají grafy pro příkaz Ping, kterým zjišťujeme síťovou odezvu. Další analytické nástroje sledují zejména důležité faktory, které se týkají serveroven jako teplotu v těchto místnostech, vlhkost a další důležité parametry. Mapa sítí se pak dá rozdělit do různých podsítí, které v naší společnosti bývají rozděleny logicky podle zemí, ve kterých se zařízení nacházejí a poté níže na různé další jednotky jako jsou sklady, výrobní závody, zasedací místnosti apod.

Následující schéma ukazuje síťovou infrastrukturu tak, jak ji rozkresluje Dude network monitor.



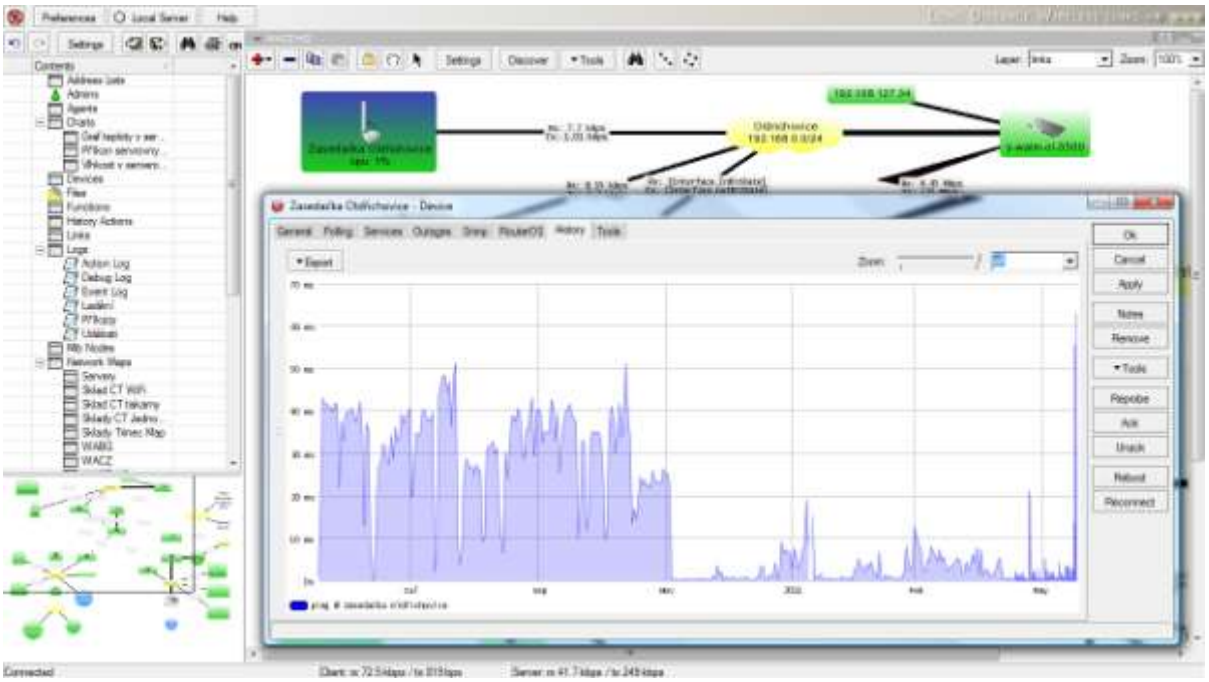
Obr. 4.10: Schéma infrastruktury Walmark Česká republika (Zdroj: vlastní)

Toto schéma naznačuje rozdělení aktivních prvků v rámci Walmarku v České republice, ovšem pouze v jeho části, protože jak je vidět, vůbec nejsou rozbaleny lokality jako Praha, Aminostar a Profitness, což jsou společnosti, jejichž je Walmark stoprocentním vlastníkem. Další "lokalitou" je poté Walmark global, jejíž schéma je již vyobrazeno na předchozí stránce.

Na schématu je dále vidět napojení dalších lokalit, jako je výrobní závod v Českém Těšíně, který je také dále rozdělen.

Modrá část ve schématu jsou právě řízené sklady, které jsou napojeny přímo do systému SAP a díky tomuto bezdrátovému systému a systému bezdrátových čteček se řídí celé skladové zásobování.

V rámci dohledového centra je možné takto sledovat také aktuální datové přenosy a vytížení veškerých aktivních prvků v síti. A to jak na hlavních spojích, tak i na dílčích spojích ke koncovým zařízením. Lze takto i jednoduše zjišťovat co se kde na síti děje a jestli někam nesměřuje nadbytečný tok dat, než by směřovat měl.



Obr. 4.11: Analýza časů Ping v systému Dude (Zdroj: vlastní)

Na tomto konkrétním screenshotu můžeme vidět funkci, která v čase analyzuje průměrný čas příkazu Ping na zařízení, které umístěno u zasedacích místností. Dále zde můžeme vidět v levé části obsahu okna rozčlenění jednotlivých síťových map podle

jejich lokalit a využití. Takto zavedený systém je již komplexně funkční po všech stránkách a nad celým systémem bezdrátových sítí ve společnosti je komplexní přehled přesně podle potřeb správců z oddělení IT.

4.4 Ekonomické zhodnocení realizovaného projektu

V rámci ekonomického hodnocení je nutné dodat, že do tohoto hodnocení zahrnuji pouze pokrytí budovy ředitelství společnosti V Třinci - Oldřichovicích. Náklady na pokrytí celého holdingu by bylo daleko složitější spočítat i proto, že se nakupovalo od různých dodavatelů a v různých časech. Popis jejich realizace není také bohužel k dispozici v ucelené formě tak, aby byl prezentovatelný.

4.4.1 Náklady na realizaci projektu, výnosy

Náklady na projekt jsou velmi lehce vyčíslitelné, protože můžeme zanedbat náklady na lidský faktor. Zaměstnanci oddělení IT mají již z předchozích projektů zkušenosti s nastaveními zařízení na platformě MikroTik a proto tuto instalaci dělali v rámci své pracovní doby. Kompletní náklady na pokrytí budovy ředitelství společnosti jsou tedy následující:

Tabulka 4.5: Náklady na zařízení pro vstup do interní sítě společnosti (Zdroj: vlastní)

3x RouterBoard	2147 Kč (2578 Kč vč. DPH)
3x Bezdrátová karta	699 Kč (841 Kč vč. DPH)
3x Case	300 Kč (360 Kč vč. DPH)
3x Zdroj	143 Kč (173 Kč vč. DPH)
3x Pigtail	72 Kč (86 Kč vč. DPH)
3x Anténa	75 Kč (90 Kč vč. DPH)
CELKEM	10308 Kč (12384 Kč vč. DPH)

Tabulka 4.6: Náklady na zařízení pro 2 pásma hostů (Zdroj: vlastní)

3x RouterBoard	1433 Kč (1721 Kč vč. DPH)
3x Bezdrátová karta	347 Kč (418 Kč vč. DPH)

3x Case	300 Kč (360 Kč vč. DPH)
3x Zdroj	143 Kč (173 Kč vč. DPH)
3x Pigtail	72 Kč (86 Kč vč. DPH)
3x Anténa	75 Kč (90 Kč vč. DPH)
CELKEM	7110 Kč (8544 Kč vč. DPH)

Tabulka 4.7: Celkové náklady (Zdroj: vlastní)

Náklady na zařízení pro interní sít	10308 Kč (12384 Kč vč. DPH)
Náklady na zařízení pro 2 pásma hostů	7110 Kč (8544 Kč vč. DPH)
CELKEM	17418 Kč (20928 Kč vč. DPH)

Celkové náklady na pokrytí budovy systémem pro bezdrátovou komunikaci činí vč. DPH 20928 Kč. Za systém, který je plně managovatelný a hlavně modulární a použitelný i pro jiné příležitosti je takováto cena velice přijatelná. Systém autentifikace je bezpečný a funkční a zadavatelé projektu (vedení společnosti) jsou s funkčností systému spokojeni.

Projekt nemá žádné finanční výnosy, protože je to interní projekt společnosti, který byl vymyšlen pro zejména pro komfort uživatelů v rámci společnosti. Momentálně není v plánu žádné další rozšíření tohoto projektu v rámci budovy ředitelství, protože funguje spolehlivě. Proto lze říci, že celková cena asi 21 tisíc korun včetně DPH za pokrytí budovy takovýmto systémem, který má velmi rozsáhlou funkcionalitu a platforma, na které je postaven zajišťuje ještě další mnohonásobně větší rozšíření funkcí je jistě více než výhodná.

Výhodou je taktéž modularita systému. Budeme-li jako konkurenci uvažovat zařízeni na platformě CISCO, tak routery obdobných parametrů, které navíc nejsou modulární tak jako platforma MikroTik, tak se pohybujeme na cenách jednoho routeru okolo 13 tisíc korun včetně DPH. V tomto případě se pohybuje na výsledné ceně blížící se 40 tisícům korunám za pokrytí celé budovy, což je skoro dvojnásobek našeho rozpočtu. Dále by nebylo možné routery od CISCO spravovat v dohledovém centru, kde jsou již zapojeny všechny ostatní aktivní prvky. Z tohoto pohledu je tedy nákup zařízení CISCO velmi neekonomický a také nepraktický.

Z hlediska měsíčních nákladů na provoz těchto zařízení můžeme mluvit o zanedbatelných položkách. Napájení má naprosto minimální spotřebu v rámci budovy. Na nejdůležitější součástky - tedy routerboardy je od výrobce záruka 5 let, takže i z tohoto hlediska je nákup těchto zařízení velmi dobrým tahem. Jinak jsou tato zařízení po stránce technické údržby naprosto bezúdržbová díky tomu, že i chlazení routerboardů je v těchto sériích pasivní a proto není třeba kontrolovat funkčnost chlazení. V rámci dohledového centra se navíc zobrazuje teplota jádra na routerboardu, čili lze mít velmi dobrý přehled o stavu zařízení. Údržba tedy spočívá víceméně pouze v nastavení parametrů spojení. Pokud se tyto nemění, jsou zařízení naprosto bezúdržbová.

4.4.2 Přínosy projektu

Hlavním přínosem tohoto systému je výborná míra komfortu pro uživatele. Tento přínos je i tím hlavním, o který šlo a i proto lze říct, že zadání projektu bylo úplně splněno. Funkčnost systému je výborná a v případě, že se vyskytují potíže, jsou zejména na straně uživatelských stanic a ne na straně zařízení.

Dalším přínosem je zvýšená bezpečnost přístupu do sítě, která byla nutností při realizaci této sítě, protože starý systém s obyčejným routerem D-Link byl potenciálně nebezpečím, které bylo zapotřebí eliminovat.

Závěr

V rámci této práce jsem popsal postup realizace pokrytí budovy ředitelství společnosti Walmark v několika fázích, jak bylo realizováno pracovníky oddělení IT. Zejména fáze výběru platformy se ukázala jako klíčová nejen v rámci napojení do sítě, která již byla v provozu, ale také z ekonomického hlediska, protože požadavek na vybudování pokrytí jednacích místností, resp. celé budovy ředitelství se může zdát finančně jako velmi náročný, nicméně opak se ukázal jako pravdivý s tím, že platforma MikroTik je opravdu velmi zajímavou alternativou k finančně velmi náročným produktům společnosti CISCO. Také dohledové centrum Dude network monitor, které je dispozici zdarma a svou velkou funkcionalitou překvapuje, dodává takto vybudované síti velmi zajímavý náboj, protože je velmi lehce administrovatelná a sledovatelná a správci IT nemusí vynakládat nijak veliké úsilí, aby síť fungovala v naprostém pořádku.

Vzhledem k tomu, že tento projekt byl úspěšně realizován a dnes můžeme sledovat bezproblémový chod sítě postavené na této platformě, není překvapením, že se zařízení na platformě MikroTik používají i v dalších dceřiných společnostech holdingu Walmark a jejich další rozšíření je v plánech do budoucích let.

Z hlediska zadání projektu je tedy možné konstatovat, že se podařilo realizovat velmi zajímavý výsledek, který je z hlediska finanční náročnosti velmi příznivý, tak i z hlediska údržby velmi přátelský. Funkcionalita sítě je vysoká a je třeba zmínit, že není zdaleka využit potenciál platformy a funkce, které zařízení dovolují. Můžeme tedy na závěr říci, že do budoucna bude tato problematika stále více zajímavější a zabývat se jí do budoucna v profesním životě má velikou budoucnost.

Seznam použité literatury

Elektronické zdroje

[1] Svět Hardware [online]. 2.10.2009 [cit. 2011-05-25]. Historie Wi-Fi: od FHSS k bezdrátu. Dostupné z WWW: <http://www.svethardware.cz/art_doc-E8854472EA5653EBC1257636003B03D0.html>.

[2] 802.11b.cz [online]. 15.8.2008 [cit. 2011-05-25]. Slovníček pojmů. Dostupné z WWW: <http://802.11b.cz/pojmy.asp>.

[3] Stránky o elektronice a počítačích [online]. 2009 [cit. 2011-05-25]. Bezdrátové sítě. Dostupné z WWW: <http://www.barts.cz/index.php/pocitace/site/29-bezdratovesite.html>.

[4] IT-Koko [online]. 2009 [cit. 2011-05-25]. Základy wifi sítí – II. Přehled standardů IEEE 802.11. Dostupné z WWW: <http://koko.over.cz/wi-fi/zaklady-wifi-siti-ii-prehled-standardu-ieee-802-11/>.

[5] Automa [online]. 2010 [cit. 2011-05-25]. Zabezpečení bezdrátových sítí Wi-Fi. Dostupné z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=32563>.

[6] Alza.cz [online]. 2010 [cit. 2011-05-25]. D-Link DI-524. Dostupné z WWW: <http://www.alza.cz/bezdratovy-wifi-router-d-link-di-524-d71983.htm>.

Knižní zdroje

[7] JANEČEK, V. *Zapomeňte na drát*. *Computer*. 2010, roč. XVII, č. 8, s. 83 - 95. ISSN 1212-8554.

[8] ZANDL, P. *Bezdrátové sítí Wi-Fi : Praktický průvodce*. Brno : Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

Seznam obrázků

Seznam tabulek