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 — ONDŘEJ PLUHAŘ
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. MILOŠ KOCH, CSc.
SUPERVISOR

BRNO 2010

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2009/10
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Ondřej Pluhař

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
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza problému
Vlastní návrhy 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 2009/10.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta podnikatelská

L.S.

Ing. Jiří Kříž, Ph.D.
Ředitel ústavu

doc. RNDr. Anna Putnová, Ph.D., MBA
Děkanka

V Brně, dne 7. 2. 2010

Abstrakt

Bakalářská práce se zabývá problematikou bezdrátových komunikací, konkrétně bezdrátových sítí. Pojednává o standardu IEEE 802.11 a jeho modulacích. Dále se věnuje historii a vývoji bezdrátového připojení k síti, druhům a vlastnostem používaného hardwaru, a možnostem zabezpečení tohoto druhu připojení.

V další části přibližuje současný stav v konkrétní společnosti, pokouší se o jeho zhodnocení a navrhuje inovace, které mohou přispět k pohodlnému přístupu na internet s patřičnou úrovní zabezpečení sítě.

Abstract (EN)

The bachelor's thesis is about wireless communication, concretely wireless fidelity networks. It deals about IEEE 802.11 standard and also about its modulations. History, development, kinds and properties of wireless network and security is also mentioned.

Current situation of one particular company is viewed in further part of the thesis. Some innovations in internet access and security of wireless communication in company network is suggested.

Klíčová slova

Bezdrátová síť, Wi-Fi, IEEE 802.11, bezpečnost sítí, autentifikace, VPN, WLC

Key words

Wireless network, Wi-Fi, IEEE 802.11, wireless fidelity, network security, authentization, VPN, WLC

Bibliografická citace:

PLUHAŘ, O. *Problematika bezdrátových sítí.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2010. 51 s. 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 v práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským, ve znění pozdějších předpisů).

V Brně dne 31. května 2010

Podpis: ……..…….....

Poděkování:

Tímto bych chtěl poděkovat doc. Ing. Miloši Kochovi, CSc. a Ing. Janu Skořepovi za jejich odbornou pomoc při sepsání této práce.

Obsah

Úvod ... 8

1 Cíl práce ... 9

2 Teoretická část ... 10

2.1 Počítačová síť ... 10

2.1.1 Model ISO/OSI ... 10

2.1.2 OSI vs. TCP/IP ... 14

2.1.3 Velikosti sítí ... 14

2.1.4 Topologie ... 16

2.2 Virtuální LAN ... 18

2.2.1 Komunikace ve VLAN ... 18

2.3 Bezdrátová LAN ... 19

2.3.1 Ad-hoc ... 19

2.3.2 Sítě s infrastrukturou ... 20

2.4 802.11 ... 20

2.4.1 Technologie a kódování ... 21

2.5 Bezpečnost ... 22

2.5.1 SSID ... 22

2.5.2 WEP ... 23

2.5.3 WPA ... 24

2.5.4 WPA2 ... 26

2.6 Centrální řízení WiFi sítě ... 29

2.7 Power Over Ethernet ... 30

2.8 Antény ... 31

2.8.1 Všesměrové antény ... 32

2.8.2 Směrové antény ... 32

2.8.3 Sektorové antény ... 32

3 Analýza současného stavu bezdrátové sítě ve firmě ... 33

3.1 Informační systém společnosti ... 33

3.2 Zabezpečení sítě ... 33

3.3 Nástin problému 34
4 Vlastní návrhy 36
4.1 Navrhovaný systém 36
4.2 Návrh zabezpečení 37
4.3 Návrh rozložení sítě 38
4.4 Výběr hardwaru 40
4.5 Cenová kalkulace 43
Závěr 44
Seznamy 45
Seznam literatury 45
Seznam obrázků 49
Seznam tabulek 50
Seznam použitých zkratek 50

Úvod

Bezdrátovou sítí se označuje spojení dvou nebo více počítačů bez potřeby použití kabeláže (ať už metalické nebo optické). Díky využití bezlicenčního pásma 2,4 GHz se bezdrátové sítě rozšiřovaly po celém světě obrovskou rychlostí.

Bezdrátové sítě se staly hojně využívanými v domácnostech, ale i v různě velkých podnicích. Domácímu použití nahrává odpadnutí nutnosti připojení počítače na jednom místě pomocí kabelů. V dnešní době se namísto desktopů pořizují notebooky s vestavěným bezdrátovým síťovým adaptérem, a tak není žádný problém vzít si počítač s sebou například na zahrádku a pracovat na čerstvém vzduchu.

V rámci firem se, vedle přístupu zaměstnanců do bezdrátové sítě, využívá především volného přístupu pro zákazníky.

1 Cíl práce

Cílem bakalářské práce je seznámení čtenáře se základními termíny, které souvisejí s problematikou bezdrátových sítí. Postupně jsou probrány jednotlivé topologie, s nimiž se můžeme běžně setkat, často používané virtuální rozdělení sítí a samotné bezdrátové sítě. V rámci bezdrátových sítí je zacíleno na důležité pojmy týkající se zabezpečení, možnosti řízení a moderního druhu napájení jednotlivých síťových zařízení. Dále jsou naznačeny základní pojmy vztahující se k anténám, které se používají při realizaci bezdrátových sítí.

V části zabývající se analýzou současného stavu je zhodnocen stávající informační systém firmy. Následuje nástin zadaného problému, týkající se bezdrátové sítě.

Při samotném návrhu bezdrátové sítě je zohledněna současná infrastruktura podnikové sítě. Je vyvinuta snaha na vzájemné provázání těchto sítí. Pro navrhovaný systém bude samozřejmě předem stanoven i rozpočet, který by neměl být při realizaci překročen. Návrh musí splňovat požadavky na vysokou bezpečnost, efektivitu a snadnou údržbu.

2 Teoretická část

Teoretická část bakalářské práce vysvětluje základní pojmy, které se vyskytují v oblasti sítí. Nejprve je pozornost věnována počítačovým sítím všeobecně. Následují jejich vlastnosti, rozdělení a topologie. V další části jsou přiblíženy virtuální lokální sítě, které jsou v současnosti nedílnou součástí podnikových sítí (i bezdrátových). Poslední kapitoly, v rámci teoretické časti práce, jsou věnovány bezdrátovým sítím. Zde se jedná o autentifikaci, kódování, bezpečnost bezdrátových sítí apod.

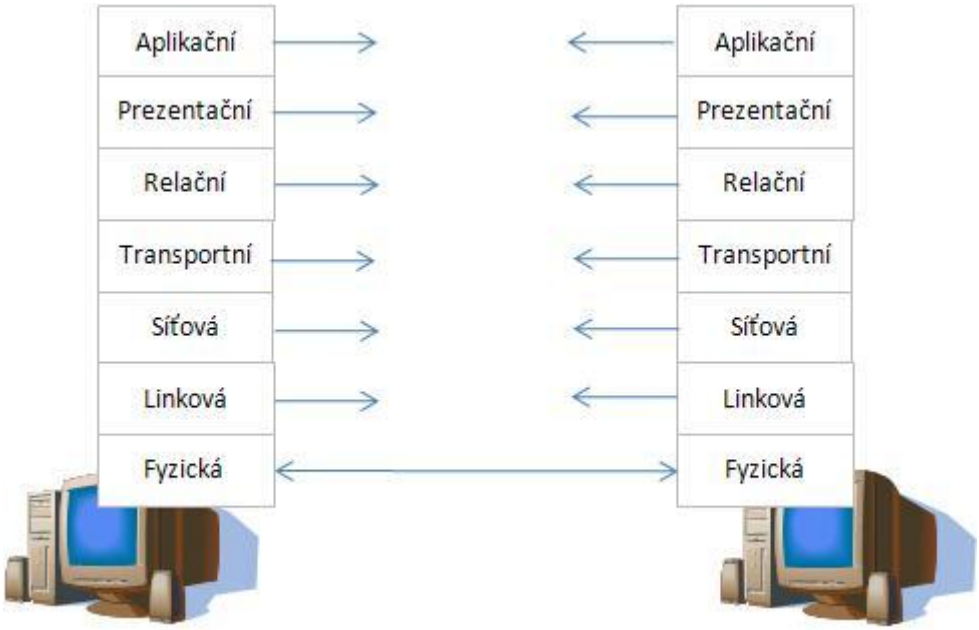
2.1 Počítačová síť

Obecně se za počítačovou síť označuje spojení dvou a více pracovních stanic telekomunikačním kanálem. Dnes se nejčastěji setkáváme se sítěmi založenými na technologii ethernet.

2.1.1 Model ISO/OSI

Referenční komunikační model ISO/OSI rozděluje komunikací mezi pracovními stanicemi uvnitř sítě do sedmi vrstev. Podle modelu OSI je vždy možné komunikovat pouze se sousední vrstvou (nad nebo pod). Všechny vrstvy musí být v komunikaci zahrnuty. To má za důsledek rovnoměrnou zátěž na všech vrstvách. V praxi je tento fakt spíše na obtíž (časově i datově náročnější).

I když v reálném prostředí nelze referenční model ISO/OSI použít pro svou těžkopádnost, je často využíván pro teoretický popis sítí. [10]



Obrázek 1 - Průběh komunikace v rámci modelu ISO/OSI [10]

2.1.1.1 Fyzická vrstva

Fyzická vrstva zahrnuje parametry bitového přenosu. Po něm probíhá komunikace mezi pracovními stanicemi pomocí fyzického média, které však již není součástí vrstvy.

Hlavním úkolem fyzické vrstvy je synchronizace komunikace a multiplexování (více logických spojení je realizováno pomocí jediného fyzického přenosového média).

Přicházející bity, odesílá vrstva dál v nezměněném tvaru. Prvky, pracující na úrovni fyzické vrstvy, se nazývají opakovače (repeater) a rozbočovače (hub). [25]

2.1.1.2 Linková vrstva

Linková vrstva je schopna zajistit přístup ke sdílenému médiu a adresaci na úrovni fyzického spojení.

Adresace je realizována na základě MAC adresy, která je pevně vázaná na síťový adaptér (lze ji změnit i softwarově, avšak v rámci jednoho síťového segmentu by měla být adresa MAC jedinečná. V případě, že je v síti více zařízení se stejnou MAC, všechna dostanou odpověď na žádost, kterou poslalo jedno z nich. Ta zařízení, která žádost neposlala, odpověď zahodí.

MAC adresa je tvořena 48 bity (např. 00-00-64-2a-cc-55). První tři oktety znamenají výrobce, další tři oktety zajišťují její jedinečnost.

Datové jednotky přenášené linkovou vrstvou jsou rámce (frame). [25]

2.1.1.3 Síťová vrstva

Síťová vrstva se stará o adresaci v rámci síťového prostředí. Adresy na úrovni síťové vrstvy jsou na rozdíl od MAC adresy logické, tzn., že uživatel si může změnit tuto adresu svépomocí.

Adresování slouží k přenosu dat z jednoho zařízení do konkrétního druhého jak v rámci LAN, tak i ve větších sítích. Adresy jsou navrženy tak, že první jejich část označuje síť, do které adresované zařízení patří a druhá část označuje přímo samotné koncové zařízení.

Na síťové vrstvě pracují aktivní prvky, nazývané směrovače (routery). Směrovače se starají o výběr nejvhodnější cesty od odesílatele k příjemci zprávy.

Datovým jednotkám přenášeným prostřednictvím síťové vrstvy se říká pakety (packets). [26]

2.1.1.4 Transportní vrstva

Transportní vrstva má za úkol zajišťovat spolehlivost a kvalitu přenosu v takové míře, jakou požadují vyšší vrstvy.

Spojované služby

V rámci spojově orientovaných služeb se navazuje virtuální spojení, vyměňují se informace o průběhu přenosu včetně ověřování doručení posílaných dat a ukončení spojení. Jestliže je některý rámec během přenosu ztracen nebo opožděn, spojová služba se postará o to, aby byl daný rámec vyslán znovu.

Nespojované služby

Nespojové služby pouze odesílají data bez toho, aby probíhala jakákoliv kontrola spolehlivosti odeslaných dat.

Datové jednotky přenášené přenosovou vrstvou jsou TPDU (Transport Layer Protocol Data Unit). [26]

2.1.1.5 Relační vrstva

Jak již název napovídá, relační (neboli spojová) vrstva se stará o navazování a ukončování přenosů dat mezi jednotlivými uzly v síti. Vedle toho se stará i o bezpečnost přenosu dat a překlad aliasů na adresy.

V rámci relační vrstvy se také vytvářejí značky v přenášených datech, pomocí kterých lze navázat při přerušení spojení na již přenesená data (přenos se nemusí opakovat jako celek od začátku).

Datové jednotky přenášené spojovou vrstvou jsou TPDU (Session Layer Protocol Data Unit). [26]

2.1.1.6 Prezentační vrstva

Základní předpoklad pro fungující komunikaci mezi dvěma počítači spočívá v tom, že obě zařízení dokážou stejnou informaci stejně i zpracovat. O splnění tohoto požadavku se stará prezentační vrstva. Vrstva nepotřebuje znát význam přenášených dat, jejím úkolem je pouze data správně interpretovat, aby jim rozuměla vyšší, aplikační, vrstva.

Na úrovni prezentační vrstvy se však nemusí odehrávat jenom konverze, ale i například zabezpečení přenášených dat pomocí šifrování. To ovšem zvládá i fyzická nebo transportní vrstva. Z důvodu minimalizování objemu přenášených dat, tak může být použita i jejich komprimace. [27]

Datové jednotky přenášené prezentační vrstvou jsou PPDU (Presentation Layer Protocol Data Unit). [29]

2.1.1.7 Aplikační vrstva

Aplikační vrstva je vrstvou, nejblíže uživateli. Jako jediná nezajišťuje služby pro vyšší vrstvy. Aplikační vrstva neobsahuje samotné aplikace, jak by se mohlo zdát. A to z jediného důvodu, aplikací je totiž tolik a liší se v tolika detailech, že by to nemohlo být možné. Aplikační vrstva tedy zajišťuje pouze služby, jež jsou pro aplikace běžné a stěžejní. Jde o jakési okno, přes které jsou schopné komunikovat aplikace běžící na různých uzlech sítě.

Datové jednotky, přenášené aplikační vrstvou, jsou APDU (Application Layer Protocol Data Unit). [30]

Tabulka 1 - Přehled vrstev modelu ISO/OSI [10]

Číslo vrstvy	Název EN	Název CZ	Jednotka	Příklad
7	Application	Aplikační	Data	Telnet, FTP
6	Presentation	Prezentační	Data	MIDI, MPEG
5	Session	Relační	Data	NetBIOS
4	Transport	Transportní	Segmenty	TCP, UDP
3	Network	Síťová	Pakety	IP, ICMP, ARP, RIP
2	Data Link	Linková	Rámce	Ethernet, FDDI, Token Ring, PPP
1	Physical	Fyzická	Bity	100BaseT, RS-232, 802.11g

2.1.2 OSI vs. TCP/IP

Skutečnosti se více než model OSI více blíží čtyřvrstvý TCP/IP model, Ten je někdy nazýván Internet Reference Model.

Tabulka 2 - Srovnání vrstev modelů TCP/IP a ISO/OSI [10]

TCP/IP	OSI
Aplikační	Aplikační
	Prezentační
	Relační
Transportní	Transportní
Síťová	Síťová
Vrstva síťového rozhraní	Linková
	Fyzická

2.1.3 Velikosti sítí

Počítačové sítě lze v základu rozdělit podle několika základních kritérií. V prvé řadě se sítě dělí podle jejich velikosti.

2.1.3.1 PAN (Personal Area Network)

Takzvaná osobní síť se používá především pro spojení mobilních telefonů, PDA, kapesních diářů, notebooků a osobních počítačů na velmi krátkou vzdálenost (max. jednotky metrů). Pomocí takto vytvořeného spojení se lze připojit k síti Internet, sdílet data, synchronizovat jednotlivá zařízení apod.

Síť PAN může být vytvořena spojením dvou zařízení pomocí kabelu (např. sériová linka, USB) nebo bezdrátově (BlueTooth, infračervený port).

2.1.3.2 LAN (Local Area Network)

Pro vzájemné propojení několika osobních počítačů a dalších síťových zařízení (např. tiskárny, scannery, IP telefony atp.) se používá lokální počítačová síť LAN. LAN lze použít v rámci domácností i firem. Může se však jednat maximálně o několik málo vzájemně blízkých budov.

Lokální počítačová síť poskytuje vedle sdílení dat mezi více počítači i připojení k WAN (viz. dále), a to přes bránu disponující modemem.

Jako přenosových médií se využívá buď metalického vedení (ethernet) nebo bezdrátového spojení (Wi-Fi). [11]

2.1.3.3 CAN (Campus Area Network)

CAN je tvořena vzájemně propojenými sítěmi LAN v rámci univerzitních kampusů nebo firem rozmístěných se ve větším počtu budov.

Campus Area Network je větší než LAN, ale zároveň je menší než metropolitní síť. [13]

2.1.3.4 MAN (Metropolitan Area Network)

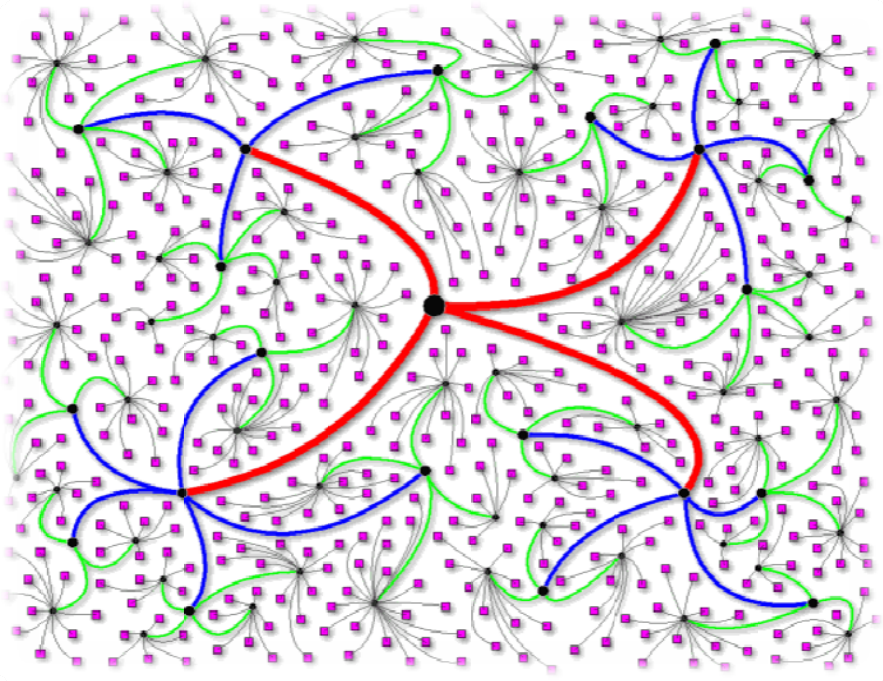
Označení MAN (metropolitní síť) se vztahuje k sítím, jež spojují mnoho LAN, ale nepřesahují hranice města.

Od této úrovně se již k propojení jednotlivých koncových bodů využívají optická vlákna. Mohou se však používat i bezdrátová spojení. [11]

2.1.3.5 WAN (Wide Area Network)

WAN jsou sítě, které uskutečňují přenos dat na velmi velké vzdálenosti. Může se jednat jak o mezinárodní, tak i o mezikontinentální spojení. Jednotlivé LAN připojené do WAN tvoří celosvětovou síť Internet, jejíž zásluhou je možné komunikovat s opačnou polovinou světa v reálném čase.

Pro WAN se výhradně využívají optické kabely, které disponují vysokou rychlostí přenosů. [11]



Obrázek 2 - Rozdělení sítí podle velikosti [11]

Další kritérium, pro rozdělení sítě je topologie

2.1.4 Topologie

V počítačových sítích se můžeme setkat se čtyřmi základními topologickými druhy. Další druhy mohou vznikat různým kombinováním a rozšiřováním těchto čtyř:

2.1.4.1 Sběrnice

Sběrnice (bus) byla používána především v počátcích problematiky sítí. Ke sběrnici jsou připojeny všechny pracovní stanice pomocí koaxiálních kabelů.

Komunikace po sběrnici probíhá tak, že vyslaná data přijme pouze koncové zařízení, jemuž jsou určena. Toho se dosáhne zakódováním adresy počítače do několika prvních signálů vyslaných po sběrnici. Je tedy zřejmé, že tato topologie je pasivní tzn., koncová zařízení pouze čekají na data poslaná po sběrnici. Aby na koncích sběrnice nedocházelo k odrazům signálu a následnému rušení, je na ně zapotřebí nainstalovat terminátory (pasivní součástka pohlcující signál).

Mezi výhody lze řadit nízké pořizovací náklady, naproti kterým stojí nízká přenosová rychlost, vysoká pravděpodobnost kolize a velmi omezený počet připojených koncových zařízení.

V dnešní době se již toto propojení nepoužívá. [34]

2.1.4.2 Kruh

Topologie, kde jsou zařízení propojena za sebou bez použití ukončovacích prvků, se nazývá kruhová (ring). Každý počítač v kruhu zde plní funkci opakovače, který ještě před vysláním, signál zesiluje. To je možné pouze za předpokladu, že signály se v kruhu šíří v jednom směru (rozšířením se mohou šířit oběma směry). Každá pracovní stanice má dvě stanice sousední a je zřejmé, že při poruše na jediné z nich, selhává celá síť.

Data se sítí šíří pomocí tzv. tokenů. Z počítače vysílajícího data se token předává postupně z jedné pracovní stanice na druhou, dokud nenarazí na ten, který má data přijmout. Ten pošle token, změněn o svou adresu, zpět původně vysílajícímu počítači. Tento počítač následně uvolní další data. [34]

2.1.4.3 Hvězda

Nejrozšířenější topologií dnešní doby je hvězda (star). Tato topologie se vyznačuje tím, že vedle koncových zařízení obsahuje i řídící prvek, do něhož jsou přivedeny kabely všech zařízení v síti (ethernet).

Veškerý přenos dat po síti je řízen centrálním prvkem, kterým může být přepínač (switch), rozbočovač (hub), někdy i směrovač (router). V topologii hvězdy lze komunikaci na síti snadno centrálně spravovat, což je její nesporná výhoda.

V případě poruchy jednoho z koncových zařízení (nebo jeho kabelu) není nijak ovlivněna funkčnost zbytku sítě. Naproti tomu, při poruše samotného řídícího prvku je komunikace po síti nemožná. Z toho důvodu je zapotřebí mít řídící prvek záložní a také záložní zdroj v případě výpadku elektrické energie. [20]

2.1.4.4 Mřížka

Topologie mřížka (mesh) nedisponuje žádným řídícím prvkem, protože každá pracovní stanice v síti je fyzicky propojena se všemi ostatními stanicemi. To v důsledku znamená, že při poruše některého z kabelů, se data přesměrují a jsou posílána jinou cestou. Při větším počtu koncových uzlů se však jedná o poměrně složité a drahé zapojení, právě vinou velkého množství kabelů. [11]

Částečně se tato topologie využívá i u bezdrátových sítí Wi-Fi.

2.2 Virtuální LAN

Často se setkáváme s potřebou rozdělit např. jednu kompaktní firemní síť LAN na více „subsítí“ s různě nastavenými právy. To a mnohé další funkce dokáže poskytnout implementace virtuálních sítí VLAN (Virtual Local Area Network).

Jak již bylo řečeno, VLAN zjednodušují úlohy managementu sítí. Stejně tak je zjednodušena instalace nových komponent a pracovních stanic do sítě. Od klasické sítě LAN se VLAN liší především nezávislostí na fyzickém připojení. VLAN je jakýsi logický segment klasické LAN. Vše co VLAN řeší je převážně softwarovými záležitostmi podpořenými inteligentním hardwarem. [12]

2.2.1 Komunikace ve VLAN

Pracovní stanice se do jednotlivých VLAN přiřazuje typicky na switchi. Rozdělování na VLANy se může tvořit pomocí čtyř metod, z nichž v praxi se nejčastěji setkáváme s první metodou.

2.2.1.1 Zařazení podle portů

Tento druh rozdělení virtuálních sítí je svou podstatou nejjednodušší a nejsnáze konfigurovatelný.

Každý switch má množství portů. Do nich se připojují jednotlivé pracovní stanice nebo další switche. Přímo v nastavení switche lze zvolit, jaký port bude náležet do které virtuální sítě. Tudíž když se do takto přiřazeného portu připojí další switch, tak všechny další pracovní stanice patří do jedné VLANy. Stejně tak může být k portu switche připojen i router nebo centrální řídící jednotka bezdrátové sítě. [12]

2.2.1.2 Zařazení podle MAC adres

MAC je unikátní adresa, kterou disponuje každý síťový adaptér.

Na rozdíl od předchozí metody, tato nevyžaduje připojení zařízení do předem nastaveného portu switche. Uživatel tak může změnit číslo portu, prostřednictvím kterého je připojen na switch a přitom jeho členství ve virtuální síti zůstane beze změny. Toho je dosaženo pomocí manuálně vedených tabulek se seznamy všech adres zařízení. [12]

2.2.1.3 Zařazení podle protokolů

Poměrně málo rozšířenou metodou pro rozdělení pracovních stanic do různých VLAN je zařazení podle protokolů. Každý paket nese informaci o tom, jakým protokolem je možné jej přenášet. Toho tato metoda využívá. Na základě předem navolených IP adres je přístup do dané VLANy buď povolen, nebo zakázán.

Nevýhodou této metody je, že IP adresa se nachází ve třetí vrstvě modelu TCP/IP (ostatní metody využívají první nebo druhou vrstvu). Tento fakt způsobuje zpomalení celé metody. [12]

2.2.1.4 Zařazení podle autentizace

Zařazování koncových bodů do sítě podle autentizace má svůj základ v řízení přístupu do sítě (NAC – Network Access Control). Po rozšíření funkcí NAS je možné jej použít i pro rozčleňování do VLAN. [23]

Samotné zařazování zařízení do VLAN se děje na základě informací, které vyjdou z ověření pomocí protokolu IEEE 802.1x.

Tato metoda umožňuje automatické převedení uživatele do zvláštní „Host VLANy“ pokud se ho nepodaří autentizovat.

Zařízení značky Cisco mají dvě možnosti připojení hostů k portům. První z možností je single-host, který umožňuje připojení pouze jednoho autentizovaného zařízení. Druhou možností je multiple-host. V případě multiple-host je možné k portům připojit více zařízení. Zvláštností tohoto typu připojení je, že k autentifikaci všech zařízení stačí autentifikování pouze jednoho z nich. [12]

2.3 Bezdrátová LAN

Propojení několika počítačů jinak, než použitím kabeláže, se nazývá WLAN (Wireless LAN).

2.3.1 Ad-hoc

Tento druh sítí se vyznačuje přítomností pouze klientů, bez pomoci jakéhokoliv přístupového bodu nebo jiného aktivního síťového prvku. Toto uspořádání v rámci sítě se nazývá nezávislý základní soubor služeb (IBSS – Independent Basic Service Set). Jeho hlavní výhodou je jednoduchost, s jakou se síť dá vytvořit. Na rozdíl od přímého propojení

kabelem, v režimu Ad-hoc může komunikovat více zařízení. Šíře frekvenčního pásma se tak rozdělí rovnoměrně podle počtu klientů.

Ad-hoc je vhodný pro krátkodobé vytvoření sítě za účelem sdílení souborů, hraní her, ale i pro sdílení internetového připojení. Pro sdílení internetu musí být počítač přímo připojený k internetu nakonfigurován jako gateway (brána). [2]

2.3.2 Sítě s infrastrukturou

U sítí s infrastrukturou je nezbytné, aby obsahovaly minimálně jeden přístupový bod, který poskytuje jak sdílení souborů, tak i sdílení internetu. V případě, že základní stanice není integrovaná přímo v Access Pointu, jsou tyto dva prvky spojeny kabelem. Odsud je již síť tvořena jako běžná ethernetová LAN nebo bezdrátově.

2.3.2.1 Point-to-point

Existují-li dvě sítě, které spolu mají komunikovat stejně jako by se jednalo pouze o jednu síť, nabízí se možnost přemostění. Takové přemostění se může provádět jak pomocí kabelů, tak i bezdrátově.

K realizaci přemostění je zapotřebí mít v obou sítích aktivní prvek (AP), který slouží právě k přemostění (nelze ho už využít jako switch atp.). Přístupové body spolu musí komunikovat na stejném kanálu a mít přiřazen stejný název SSID.

Pro udržení vysoké úrovně zabezpečení je vhodné omezit množinu MAC adres a zároveň komunikaci mezi přístupovými body provozovat šifrovaně. [3]

2.3.2.2 Point-to-multipoint

V situaci, kdy mezi sebou má komunikovat více než dvě lokální sítě, nelze použít metodu point-to-point. Pro vyřešení tohoto problému se nabízí metoda point-to-multipoint. O konfiguraci mostů se starají samotné access pointy Ty by však měly být od stejného výrobce a se stejnou verzí firmwaru. Pokud, tomu tak není, může docházet ke kolizím. [3]

2.4 802.11

Standard IEEE 802.11 pochází z dílny organizace s názvem Institute for Electrical and Electronics Engineers (Institut pro elektrotechnické a elektronické inženýry). Tato nezisková organizace se zabývá inovováním a vývojem technologií v oblasti elektrotechniky, elektroniky a výpočetní techniky.

Bezdrátové sítě, využívající standardu 802.11, jsou několika typů. Jejich počet s plynoucím časem roste. Každý z typů se vyznačuje jinou přenosovou rychlostí, jiným kódováním i jinými druhy modulací. Tím mohou být jednotlivé typy bezdrátových sítí různě vhodné pro využití v různých podmínkách. [4]

2.4.1 Technologie a kódování

FHSS

Metodu FHSS (Frequency-Hopping Spread Spectrum) žádná z aktuálních implementací založených na 802.11 nepoužívá, přestože původní norma 802.11 ji využívala vedle DSSS (viz. níže).

Při FHSS jsou pro přenos přes dostupné frekvenční pásmo data rozdělena na pomocné nosné vlny. [36]

DSSS

Při přímém rozprostření spektra (DSSS - Direct-sequence spread spectrum) je každý přenášený bit 11bitovou Barkerovou sekvencí. Každému informačnímu bitu je poté přiřazena určitá bitová sekvence.

Do přenášených dat se touto metodou zavádí mnohonásobná redundance, která na přijímací straně zlepšuje proces rekonstrukce dat.

S ohledem na šířku DSSS kanálu, je možné, aby v bezlicenčním pásmu 2400 – 2483 MHz pracovaly nezávisle 3 kanály DSSS vedle sebe.

Hlavní výhodou technologie rozprostřeného spektra je především eliminace rušení úzkopásmových zdrojů při klasickém přenosu. [36]

OFDM

Použitím kódování OFDM (Orthogonal frequency-division multiplexing) disponují standardy 802.11a a 802.11g.

Na rozdíl od FHSS, kde jsou data vysílána po shlucích, jsou zde rozdělena do paralelních kanálů, které jsou samostatně kódovány a modulovány do subkanálů. Každý z těchto subkanálů má výrazně nižší datové toky než kanál původní.

Výhodou používání OFDM je využití šířky kanálu. To znamená, že je možné přenášet větší objemy dat rychleji v daném frekvenčním pásmu i v přítomnosti vyšší hladiny šumu. [27]

MIMO

Technologie MIMO (Multiple-input multiple-output) je založena na větším počtu (2 - 4) antén, a to jak na vysílací, tak i na přijímací straně. Výhodou MIMO je to, že nespotřebovává frekvenční spektrum ve větším rozsahu, ale dokáže využít stávající frekvenční spektrum efektivněji. Využitím MIMO narůstá datová propustnost a dosah při využití jednoho kanálu a zachování celkového výdeje energie, která je vyzařována.

Výhodou jeho použití je nárůst datové propustnosti a dosahu při zachování šířky pásma a celkového výdeje vyzařovací energie. [28]

Tabulka 3 - Přehled standardů IEEE [37]

Standard	Frekvence [GHz]	Max. teoretická přenosová rychlost [Mb/s]	Průměrná skutečná přenosová rychlost [Mb/s]	Použité kódováni
802.11	2,4	2	0,9	FHSS/DSSS/IrDa
802.11a	5	54	23	OFDM
802.11b	2,4	11	4,3	DSSS
802.11g	2,4	54	19	OFDM/DSSS
802.11n	2,4 nebo 5	150	68	MIMO-OFDM

2.5 Bezpečnost

U klasických ethernetových sítí je jedinou možností napadení sítě fyzicky se připojit ke kabelu. Tudíž veškeré zabezpečení spočívá v udržení kabelů a přípojek mimo dosah neoprávněných osob. Bezdrátové sítě jsou specifické tím, že access pointy vysílají signál do svého okolí všemi směry a bez ohledu na to, kdo se v jejich dosahu vyskytuje.

Zabezpečení bezdrátových sítí je realizováno především prostřednictvím autentizace a šifrováním přenášených dat.

2.5.1 SSID

Základním bezpečnostním prvkem bezdrátové sítě je SSID (Service Set IDentifier). SSID je známé jako označení sítě, které musí klient znát, aby mu byl umožněn přístup do bezdrátové sítě. Délka tohoto identifikátoru může být v rozmezí 0 – 32 bajtů.

Implicitně vysílá access point v pravidelném intervalu několika sekund beacon, nesoucí informaci o aktuální podobě SSID. Díky tomu klient může bez námahy sledovat, k jakým bezdrátovým sítím v jeho okolí má teoreticky přístup, aniž by sám nějakou informaci o těchto

sítích musel znát. Jednoduchým nastavením přístupového bodu lze zamezit vysílání beacon s SSID do okolí a tím neprozrazovat běžným klientům přítomnost dostupného access pointu. V tomto případě musí klient (nebo i útočník), který se na AP se skrytým SSID chce připojit, zaslat prosbu (Probe Request) na kterou odpoví i „utajený“ access point pomocí tzv. Probe Response, který je velmi podobný beaconu.

Pro útočníka existuje několik možností, jak se k síti připojit i v případě, že není vysílán její SSID. Jednou z možností je sledování sítě a určení adresy některého skutečně připojeného klienta. Poté pošle na access point falešný požadavek na odpojení daného klienta. Ten se následně musí znovu připojit pomocí asociačních zpráv, ve kterých je SSID uvedeno. Další možností je pouhé sledování sítě a vyčkávání, dokud se některý klient nechce připojit nebo dokud nepřejde z AP se slabou intenzitou signálů na AP se signálem silnějším. V obou těchto případech spolu AP a klient komunikují prostřednictvím krátkých paketů, ve kterých může být informace o SSID uvedena.

Pro zvýšení zabezpečení bezdrátové sítě pomocí SSID se tedy obecně doporučuje nevysílat beacon obsahující informaci o SSID, změnit implicitní hodnotu SSID na hodnotu hůře odhadnutelnou a v neposlední řadě hodnotu SSID často měnit.

Naproti tomu v dnešní době příliš skrývání SSID postrádá smysl. Naopak např. v kombinaci MS Windows XP SP2 a WPA/WPA2 může skrývání SSID vést k potížím při automatickém připojení k síti. [4]

2.5.2 WEP

WEP (Wired Equivalent Privacy) je protokol, který slouží k řízení přístupu k síti a zabezpečení přenášených dat. Jak název napovídá, WEP byl vytvořen s cílem dosáhnout u bezdrátových sítí stejné bezpečnosti, jaká odpovídá zabezpečení ethernetové LAN.

WEP využívá šifru RC4 buď se 64 bitovým klíčem, kde 40 bitů odpovídá uživatelskému klíči a zbylých 24 bitů tvoří inicializační vektor, nebo lépe se 128 bitovým klíčem. U 128 bitového WEP má sdílený klíč délku 104 bitů a inicializační vektor zbylých 24 bitů. Inicializační vektor se mění s každým odeslaným paketem avšak v otevřené podobě, tím se WEP stává snadno narušitelný. [4]

Již od roku 2001 byl WEP považován za nedostatečný mechanismus, který má vážné bezpečnostní trhliny a slabiny.

2.5.2.1 Autentizace

Autentizace WEP je jednocestná, což znamená, že se ověřuje pouze klient u AP, nikoli však AP u klienta. WEP nabízí dvě možnosti autentifikace: otevřený systém (Open System) a autentifikace na základě sdíleného klíče (Shared Key).

Open system

Otevřený systém autentizace umožňuje jakémukoliv klientovi připojení k přístupovému bodu bez toho, že by záleželo na WEP klíči.

Klient vyšle svoje identifikační údaje na přístupový bod. Ten klienta na základě přijatých údajů přidruží do sítě. Doposud nevyužitý WEP klíč lze však následně použít pro šifrování přenášených dat. [9]

Shared key

Sdíleným klíčem se rozumí 40 bitový uživatelský klíč, který je stejný pro všechny uživatele dané sítě a je jejich tzv. sdíleným tajemstvím. Pro přidružení uživatele do sítě se neověřuje osoba uživatele, nýbrž pouze jeho síťová karta, což je největší slabinou tohoto druhu autorizace v rámci WEP. [4]

2.5.3 WPA

Jelikož, jak již bylo řečeno, byl WEP velmi nevyhovující pro účelné zabezpečení bezdrátové sítě, byla na konci roku 2002 představena jeho momentální náhrada WPA (Wi-Fi Protected Access). Nahrazení spočívalo ve využití těch bezpečnostních prvků z nové normy 802.11i, které by byly zpětně slučitelné se zařízeními pracujícími s WEP a zároveň by se zvýšila bezpečnost přenosu dat do doby, než by byl schválen bezpečnostní doplněk normy IEEE 802.11i. Jedná se tedy o dočasné řešení, které má odstranit nejvážnější nedostatky WEP. Toto dočasné řešení bylo vytvořeno tak, aby pro přechod mezi WEP a WPA nebylo zapotřebí nákupu nového zařízení, ale aby stačila pouze aktualizace jeho firmwaru. [4]

V případě, že se v jednu chvíli vyskytnou v jedné síti prvky, z nichž jeden podporuje WEP a druhý WPA, automaticky se všechny ostatní prvky musejí přizpůsobit slabšímu WEP.

2.5.3.1 Autentizace

V rámci WPA byly odstraněny největší nedostatky WEP, kde probíhala autentizace pouze v jednom směru. WPA tedy přešlo na vzájemnou (oboustrannou) autentizaci, při které se musí autentizovat jak host serveru, tak nově i server hostu. [4]

WPA je vytvořen tak, aby mohl poskytovat dva režimy autentizace podle toho, kde se síť nachází. První z těchto režimů je vytvořen pro účely domácího prostředí. V tomto režimu je na serveru přednastavený klíč (PSK), který je sdílen pouze s AP. Pro připojení musí uživatel zadat předem nastavené heslo. [4]

Druhý režim je navržen pro potřeby podnikového prostředí, ve kterém se předpokládá přítomnosti centralizovaného autentizačního serveru (RADIUS), jehož úkolem je distribuce klíčů.

2.5.3.2 TKIP

Protokol TKIP (Temporal Key Integrity Protocol) řeší hlavní nedostatky WEP a je možné ho použít na hardwaru, který ještě nepodporuje CCMP.

Při využití stávajícího hardwaru, byly odstraněny některé slabiny WEP. Tyto inovace zvýšení zabezpečení se týkají náhodného generování klíčů pro každý odesílaný paket (u WEP byl pro všechny přenosy statický klíč). Dále bylo implementováno číslování jednotlivých paketů. To slouží jako prevence před útokem typu replay. Posledním zmíněným zlepšením je zachování integrity dat (MIC). [4, 7]

V listopadu 2009 vyšel článek, podle kterého je možné WPA-TKIP prolomit za pouhou jednu minutu. Z toho jasně vyplývá, že toto zabezpečení bezdrátové sítě by mělo být používáno nejvýše pro domácí AP, u kterých majitel nepožaduje vysokou ochranu. Naproti tomu WPA-AES při využití 128bitového klíče je stále bezpečný, tudíž je mnohem lepší volbou pro zabezpečení AP v domácím prostředí. [22]

2.5.3.3 MIC

Kód MIC (Message Integrity Code) zajišťuje integritu dat přenášených prostřednictvím bezdrátových sítí. Jeho funkce spočívá v přikládání digitálního podpisu každému vysílanému rámci.

Digitální podpis je vypočítán na vysílací straně přenosu dat z MAC adresy odesílatele a příjemce, pořadového čísla paketu, náhodného čísla a ze samotné datové části přenášeného rámce. Takto vytvořený podpis se vloží do datové části rámce, který se následně zašifruje a odešle příjemci.

Přijímací strana nejprve ověří inicializační vektory a teprve potom zkontroluje MIC. V případě, že se ukáže poškození nebo jakákoliv nesrovnalost v MIC, je zřejmý pokus o aktivní útok na komunikaci (integritu přenášené zprávy). V tom případě se okamžitě

přestanou používat doposud platné klíče a po určitém krátkém časovém intervalu (desítky sekund) dojde ke změně klíče.

MIC slouží k zachování integrity dat při přenosu před aktivním útokem man-in-the-middle.

Jelikož byl MIC vytvořen pro účely WPA, který vychází z hardwaru použitého původně pro WEP, je navržen tak, aby nezpůsoboval problémy s ohledem na nízkou výpočetní složitost, kterou disponovaly adaptéry pro WEP. [4]

2.5.4 WPA2

V roce 2004 vydal institut IEEE oficiální verzi nového bezpečnostního systému 802.11i. Tento systém má všechny vlastnosti předchozího WPA a navíc je obohacen o šifrování dat algoritmem CCMP (Counter Mode with Cipher Block) využívající blokovou šifru AES (Advanced Encryption Standard). AES poskytuje dostatečnou bezpečnost pro využití ve standardu FIPS (Federal Information Processing Standard), který se používá v rámci vládních a bankovních organizací. Pro možnost využití AES v rámci WPA2 je nutností použít nový a výkonnější hardware, protože AES je pro výpočet mnohem složitější než tomu tak bylo u TKIP. [21]

Kontrola integrity dat pomocí MIC u WPA byla pro WPA2 nahrazena algoritmem CBC-MAC (Cipher Block Chaining Message Authentication Code). Tento algoritmus spočívá v zašifrování každého bloku otevřeného textu pomocí AES. Každý tento šifrovaný blok se XOR-uje s blokem následujícím. Výsledek XOR-ovaného bloku se potom XOR-uje s dalším zašifrovaným blokem. Výsledkem toho je, že při dekrypci jsou mezi sebou jednotlivé bloky svázané a není možné dešifrovat všechna data, pokud se některý paket ztratí. [7, 21]

2.5.4.1 AES

AES (Advanced Encryption Standard) je bloková šifra, která byla vydána v roce 2001. Šifrování se provádí po 128 bitových blocích, s použitím 128, 192 nebo 256 bitového symetrického klíče.

Bloky obsahující 128 bitů dat jsou rozloženy v poli 4x4 bajtů. Tato pole jsou na základě délky klíče rozdělena na několik „subpolí“, ve kterých se prohazují řádky, sloupce, obsah polí se s klíčem XOR-uje. Poté co všechny procedury proběhnou, vychází šifrovaný text. [7]

AES již přes 13 let odolává prolomení a vyznačuje se velmi vysokou rychlostí šifrování.

2.5.4.2 CCMP

CCMP (Counter CBC-MAC Protocol) je šifrovací protokol v rámci standardu 802.11i. Používá 128 bitové klíče a jejich dynamické regenerování. Současně zajišťuje autenticitu, utajení, kontrolu integrity zpráv a číslování jednotlivých paketů, posílaných po síti.

Pro šifrování přenášených dat je používána šifra AES. Vzhledem k síle AES není zapotřebí generovat klíče pro každý paket. Proto CCMP používá relační klíč pro šifrování dat a generování kontrolního součtu. [4]

2.5.4.3 RADIUS

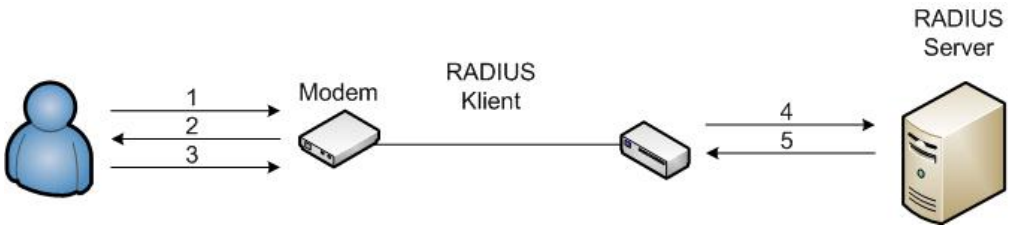
RADIUS (někdy také 802.1x) je zabezpečovací služba pro autentifikaci a autorizaci připojovaných uživatelů. Typická podniková síť má přístupový server připojený přímo k modemu společně s RADIUS serverem, který tam poskytuje autentizaci. Uživatel se připojuje k přístupovému serveru a ten posílá požadavek na autentifikaci serveru RADIUS. RADIUS server autentizuje uživatele a autorizuje ho k přístupu do vnitřní sítě. Samotní uživatelé jsou vzhledem k přístupovému serveru bráni jako klienti. Stejně tak je jako klient brán přístupový server vzhledem k RADIUS serveru.

Vzhledem k faktu, že RADIUS je otevřený protokol, je distribuován jako zdrojový kód. Ze stejného důvodu se může používat i v prostředí, kde se využívají bezpečnostní systémy třetích stran. Jakýkoliv přístupový server, jež podporuje protokol RADIUS-klient, může komunikovat s RADIUS serverem.

RADIUS bývá často označován jako RADIUS AAA proto, že nabízí autentifikační, autorizační a účtové (accounting) funkce. Accounting se říká vlastnosti RADIUSu, která shromažďuje informace o uživatelích. Tyto informace mohou být potom využívány např. pro analýzu zatížení sítě.

Ve skutečnosti je RADIUS kvůli vyšší míře zabezpečení rozdělen na více částí i fyzicky. Komunikační (přístupový) server je oddělen od autentifikačního serveru. Údaje o uživatelských účtech jsou uloženy na centrálním RADIUS serveru, který může být přístupný z libovolného množství přístupových serverů. Takovéto rozdělení je základem pro rozsáhlé sítě (stovky až tisíce uživatelských účtů).

Autentifikační mechanismus funguje podle následujícího obrázku:



Obrázek 3 - Autentifikační mechanismus zabezpečovacího systému RADIUS [19]

1 – Uživatel iniciuje autentifikaci směrem k přístupovému serveru.

2 – Přístupový server si žádá přihlašovací údaje.

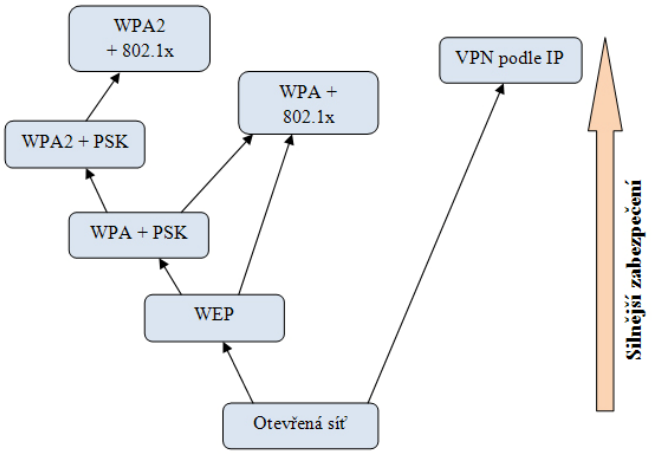
3 – Uživatel posílá přihlašovací údaje.

4 – RADIUS klient posílá přihlašovací údaje na RADIUS server (heslo je zašifrované).

5 – RADIUS server odpovídá: schváleno nebo odmítnuto.

Pokud je uživatel ověřený a má schválen přístup do sítě, mohou být poslány dodatečné informace (např. požadavky na spojení, informace o politice sítě – povolené úrovně služeb pro daného uživatele). [19, 36]

Zabezpečení podle IEEE 802.11i je na velmi vysoké úrovni a záleží pouze na uživateli, zda tyto zabezpečovací mechanismy aktivuje a využije pro svou ochranu.



Obrázek 4 - Úrovně bezpečnosti standardů IEEE [4]

2.6 Centrální řízení WiFi sítě

Protože se v posledních několika letech využívá bezdrátových sítí i ve firmách a různých institucích (školy, kavárny, hotely, restaurace atd.), je zapotřebí často řešit jejich správu. V případě, že je celá bezdrátová síť realizována pouze s jedním AP, konfigurace je snadná a časově nenáročná. Pokud je však v síti použit větší počet AP, nabízí se řešení pomocí centrální správy všech AP v síti. V tom případě je veškerá konfigurace a monitoring sítě prováděn na jednom místě. [8]

Společnost Cisco přišla se systémem postaveným na CUWN (Cisco Unified Wireless Network), jenž usnadňuje správu většího počtu zařízení v síti. Hlavní roli v tomto systému sehrává WLC (Wireless LAN Controller). WLC je zařízení, přebírající na sebe funkce, jež běžně provádějí AP (přidružení nebo autentizace bezdrátových klientů). Access Pointy, které se používají ve spojení s WLC, se nazývají LAP (Lightweight Access Point). Cisco nabízí AP, individuálně nastavitelné pro chod jako plnohodnotný AP nebo jako součást centrálně řízené sítě. Pro použití v centrálně řízené síti musí být všechny AP v režimu LAPP (Lightweight Access Point Protocol).

Komunikace mezi WLC a jednotlivými AP zahrnuje veškerý management a přenos datových paketů a probíhá přes šifrovaný komunikační tunel. [39]

Na WLC existuje několik fyzických portů, mapující se na různý počet virtuálních rozhranní (podle konkrétního typu). Základními rozhraními, přítomnými u každého WLC jsou AP-manager, management a virtual.

Rozhraní AP-manager zajišťuje šifrovanou komunikaci mezi jednotlivými AP a samotným WLC. Často se pro tuto komunikaci doporučuje využít vlastní samostatné VLAN.

Managementové rozhraní slouží pro správu a přístup k administraci sítě.

Poslední, virtuální rozhraní není nikam fyzicky připojeno a řeší speciální funkce.

Jednotlivá rozhraní se dají přiřadit do různých VLAN, kde mají nastavené IP adresy, masku podsítě a výchozí brány. Další možností je nastavení DHCP serveru a omezení přístupu pomocí Access Listu. Nutným nastavením je přiřazení rozhraní k určitému fyzickému portu na WLC. Tím lze různé bezdrátové sítě oddělit nejen pomocí VLAN, ale také fyzicky. [8]

2.7 Power Over Ethernet

Power Over Ethernet (PoE) je schopnost infrastruktury LAN poskytovat elektrický výkon napájenému zařízení přes ethernetovou kabeláž. Společnost Cisco v roce 2000 představila tento druh napájení zařízení především proto, aby podpořila rozvoj IP telefonie. Další vývoj byl zaznamenán s větším rozšířením bezdrátových sítí, kde byly napájeny jednotlivé Access Pointy, switche nebo jiné síťové prvky, ke kterým nebylo možné přivést klasické napájecí kabely.

Novější standard 802.3af dovoluje tuto technologii použít u širšího okruhu koncových zařízení. Mohou tak být napájeny i kamery, čtečky přístupových karet, platební terminály atp. [33]

Napájení zařízení přes běžný síťový kabel s konektory RJ-45 je realizováno využitím buď již signálem využitým, nebo nevyužitým párem v datovém kabelu. Zpravidla se používá napětí 48 V a maximální proudový odběr činí 400 mA. Maximální udávaná hodnota výkonu, který je možné dodat pomocí 802.3af je 15,4 W. [32]

Pro možnost využití technologie PoE u zařízení s větším příkonem, než je 15,4 W byl vyvinut nový standard 802.3at (PoE+). Tento standard je schopný poskytovat výkon až 24,6 W na jeden síťový port. Připojené zařízení může mít proudový odběr až 600 mA.

802.3at je tak vhodné použít například u Access Pointů, které podporují standard 802.11n.

Z jiných oblastí, než je IT může být napájeno přes PoE+ nejen nouzové osvětlení v budovách, různé senzory bezpečnostních systémů, biometrické senzory, ale dokonce i lékařské monitorování pacientů v nemocnicích. [6, 17]

Výhodou tohoto druhu napájení je bezesporu zjednodušení zprovoznění zařízení (místo datového a napájecího kabelu stačí pouze datový), možnost restartování daného zařízení na dálku. Další výhodou je to, že napájení přes ethernetovou kabeláž bývá centrálně zálohovaná, tzn., že i při přerušené dodávce elektrické energie můžeme telefonovat (IP telefony).

2.8 Antény

Antény jsou zařízení, která slouží k přeměně elektrické energie na energii elektromagnetických prostorových vln. Jelikož antény dokážou pracovat recipročně, dá se pomocí stejné antény přeměnit elektromagnetické vlnění na elektrickou energii vysokofrekvenčního proudu.

Antény mají několik základních technických parametrů, kterými jsou zisk, směrovost, šířka vyzařujícího úhlu, součinitel směrovosti, účinnost, vstupní impedance antény atd.

Směrovost

Směrovostí se rozumí schopnost antény vyzařovat elektromagnetické vlny v žádaném směru.

Šířka vyzařovacího úhlu 2Θ

Vyzařovací úhel je úhel, v němž je výkon vyzářený anténou snížen na polovinu oproti směru vyzářeného výkonu. Vzhledem k tomu, že je vyzářený výkon úměrný druhé mocnině intenzity pole, jsou meze vyzařovacího úhlu dány poměrem $\frac{E}{E_{\max}} = \frac{1}{\sqrt{2}} \approx 0{,}707$

Účinnost antény η

Účinnost je poměr výkonu vyzářeného k výkonu do antény přivedenému.

Součinitel směrovosti D

Součinitel směrovosti udává, kolikrát je potřeba zvýšit výkon vysílače, aby intenzita signálu v místě příjmu zůstala na stejné úrovni při přechodu ze směrové antény na všesměrovou (viz. dále).

Zisk G

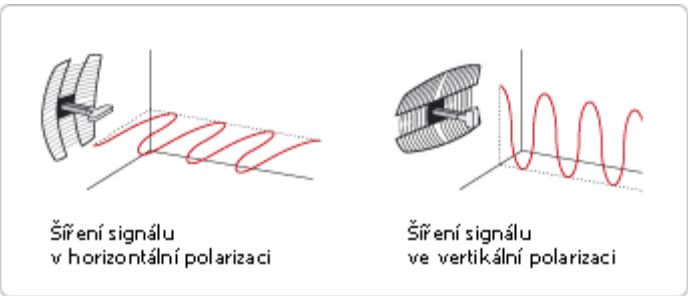
Zisk antény je dán součinem součinitele směrovosti a účinnosti antény. Jednotkou zisku je dB (decibel).

Vstupní impedance

Anténa musí být přizpůsobena impedanci vysokofrekvenčního vedení.

Polarizace

U Wi-Fi je signál anténami vysílán buď ve vertikální, nebo v horizontální polarizaci



Obrázek 5 - Polarizace antény [40]

2.8.1 Všesměrové antény

Všesměrové antény se vyznačují výkonem vyzařujícím buď vertikálně, nebo horizontálně do všech stran. Proto vyzařovací diagram těchto antén má zpravidla tvar kružnice.

2.8.2 Směrové antény

U směrových antén je většinou možné změnit polarizaci jednoduchým otočením antény o 90°.

2.8.3 Sektorové antény

Všesměrové a sektorové antény jsou konstruované pro jednotlivé polarizace už při výrobě. [40]

3 Analýza současného stavu bezdrátové sítě ve firmě

V kapitole analýzy současného stavu bezdrátové sítě je popsán informační systém společnosti Pojišťovna České spořitelny, a. s., Vienna Insurance Group (dále jen „PČS“) jako celek. Jsou zde vyjmenovány druhy a typy některých zařízení, které společnost využívá, a tudíž se kterými se musí počítat při navrhování bezdrátové podnikové sítě. Dále je představeno zabezpečení sítě a nastíněn problém týkající se bezdrátové sítě ve společnosti.

3.1 Informační systém společnosti

V celé společnosti je výpočetní technika založena na platformě PC. Na všech počítačích je z důvodu stability a spolehlivosti nainstalován operační systém Microsoft Windows XP Professional SP3, nicméně se v brzké době dá očekávat přechod na novější verzi MS Windows 7. Základem pro všechny pracovní stanice je kancelářský balík MS Office 2007.

Jednotlivým pracovním pozicím je k dispozici odpovídající specializovaný software.

Pochopitelně je vedle desktopů využíváno i mnoho notebooků a mobilních telefonů, které mají možnost připojení k internetu pomocí Wi-Fi.

Co se týká infrastruktury počítačové sítě, všechny pracovní stanice jsou propojeny s firemním serverem pomocí ethernetové kabeláže.

3.2 Zabezpečení sítě

Společnost dbá na kvalitní a účelné zabezpečení sítě. Proto trvalo tolik let, než se rozhodla využívat bezdrátovou síť.

Veškerá bezpečnostní opatření v oblasti IT jsou předepsána ve vnitřních směrnicích. Jelikož se dlouhou dobu čekalo na možnost využití bezdrátové sítě, ve směrnicích zmínky o Wi-Fi uvedeny nebyly.

Společnost disponuje nebytovými prostory, které využívá čistě pro hardware. Patří sem místnost serverů, která je vybavena klimatizačním zařízením, protipožárním zabezpečením, kamerovým systémem a zařízením elektronické kontroly vstupu. Přístupová práva do místnosti serverů jsou přidělena pouze určeným zaměstnancům. V místnosti jsou umístěny jak webové servery, tak servery intranetu, centrální záloha dat, ale hlavně centrální řízení bezdrátové sítě WLC.

Někteří zaměstnanci jsou vybaveni jednotným typem firemních notebooků. Na nich je nainstalován operační systém Microsoft Windows XP Professional SP3. Na něj má společnost zakoupený určitý počet licencí.

3.3 Nástin problému

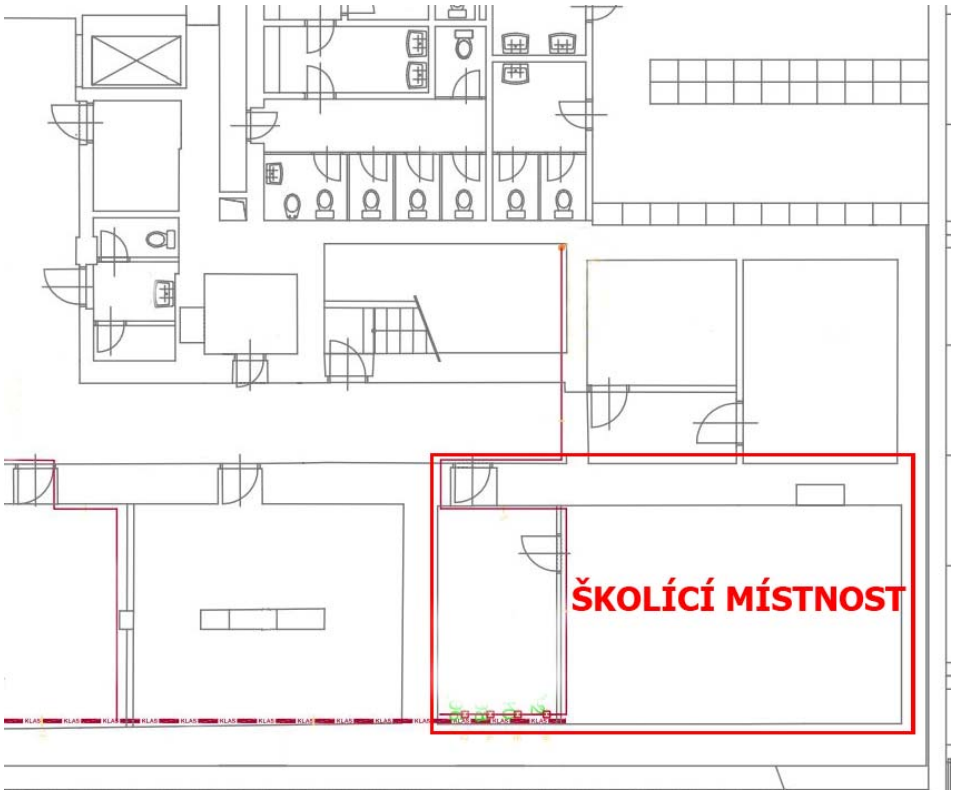
V nedávné době byla část nebytovch prostor PČS přenechána společnosti Kooperativa pojišťovna, a.s., která je též členem pojišťovací skupiny Vienna Insurance Group. V rámci této přeměny se někteří zaměstnanci PČS i se svým vybavením přestěhovali do nově upravených velkoplošných kanceláří, případně do dalších kanceláří budovy centrály.

Tato přemístění pracovišť si vyžádala rozsáhlé přeměny funkčnosti některých prostor. V přízemí tak z původního skladu IT techniky vznikla malá školící místnost (pro cca 16 lidí), která sousedí s další místností, jež by měla být využita pro PC podporu školící místnosti.

Zároveň s reorganizací pracovišť bylo rozhodnuto, že některé prostory budou pokryty bezdrátovou sítí.

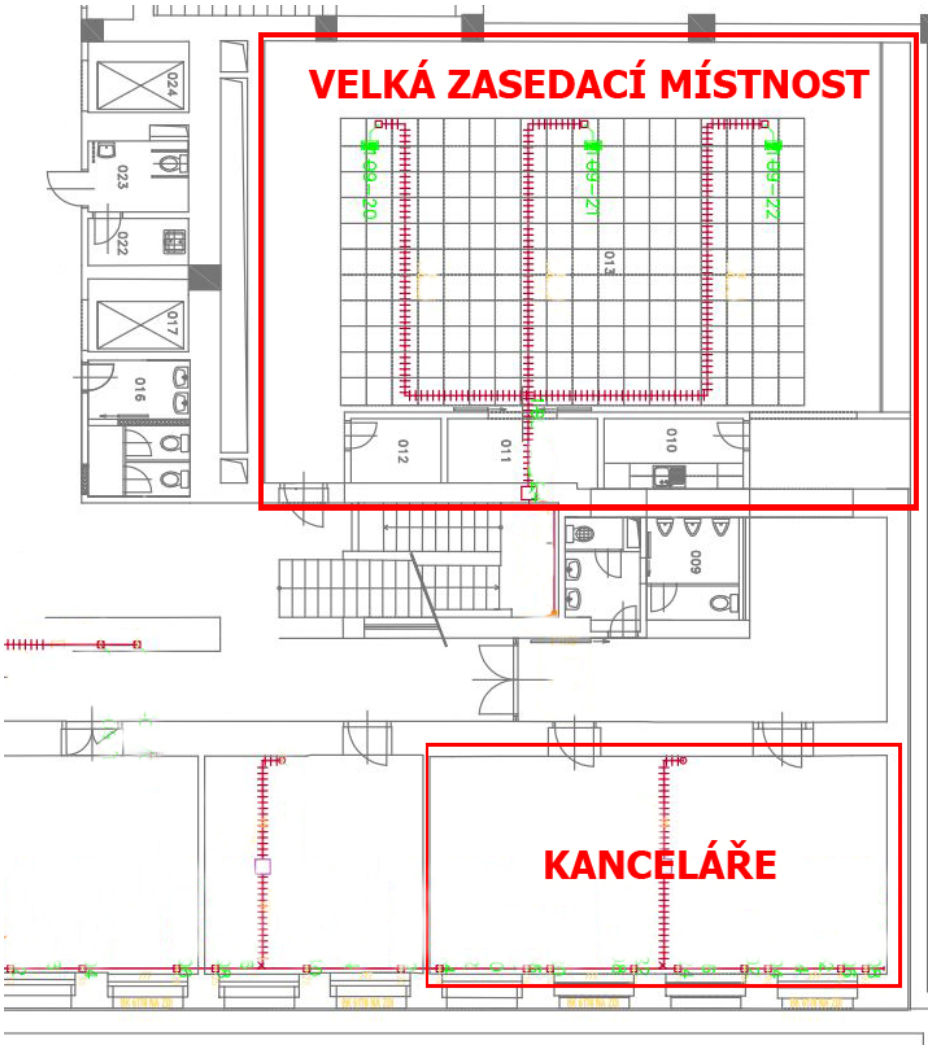
Tento stav je znázorněn na následujících půdorysech přízemí a prvního patra (v červeném rámečku je vždy znázorněna požadovaná oblast pokrytí Wi-Fi signálem).

1. patro:



Obrázek 6 - Půdorys prvního patra centrály PČS

Přízemí:



Obrázek 7 - Půdorys přízemí centrály PČS

4 Vlastní návrhy

Praktický návrh realizace je tvořen pro centrálu společnosti Pojišťovna České spořitelny, a. s., Vienna Insurance Group se sídlem v Pardubicích. Společnost působí na českém trhu od roku 1993 a patří mezi přední poskytovatele životního pojištění v České Republice.

Úkolem bude návrh řešení pokrytí kancelářských a učebních prostor ve dvou patrech budovy bezdrátovým signálem Wi-Fi. Společnost požaduje minimální úroveň přenosové rychlosti 11 Mb/s a vysokým stupněm zabezpečení pro síť určenou interním zaměstnancům. Stavební konstrukce prostor, ve kterých je požadováno pokrytí Wi-Fi signálem, je tvořen železobetonovým skeletem s vnitřními příčkami z různých typů materiálů (železobeton, cihly, sádrokarton).

Mezi prostory, které mají být pokryty bezdrátovou sítí, patří konkrétně velká zasedací místnost a dvě kanceláře v přízemí a malá školící místnost v prvním patře.

4.1 Navrhovaný systém

Vzhledem k jednoduchosti, spolehlivosti a především k bezpečnosti bude pro návrh využito standardu 802.11g, který využívá frekvenčního pásma na 2,4 GHz a jeho průměrná přenosová rychlost se pohybuje okolo 19 Mb/s. Starší standard 802.11b nesplňuje podmínku minimální úrovně přenosové rychlosti 11 Mb/s (tuto hodnotu má standard 802.11b udanou jako maximální teoretickou). Naproti tomu novější standard 802.11n by požadovanou minimální rychlost měl zvládnout bez sebemenších potíží, avšak ceny, za které se dají nakoupit jednotlivé prvky, jsou neadekvátní předpokládané míře využití navrhované sítě (např. v učebně není zapotřebí tak rychlého připojení).

Protože se jedná o společnost zabývající se životním pojištěním, a tudíž se v rámci firmy pohybuje velké množství důvěrných dat o zákaznících, je zapotřebí, aby byla zaručena velmi silná úroveň zabezpečení bezdrátové sítě. Proto se vedle přenosových rychlostí musí brát v úvahu i možnosti zabezpečení jednotlivých standardů IEEE. I v tomto ohledu je nejlepší možností použít 802.11g. I přesto, že všeobecně nejlepší vlastnosti má standard 802.11n, nebyla by jeho implementace do daného prostředí nejjistějším krokem. Bankovní instituce obecně čekají, až budou mít jistotu, že implementovaný systém je dostatečně bezpečný a prověřený časem. To se v případě 802.11n, jehož konečná verze byla vydána v roce 2009, prozatím říct nedá.

4.2 Návrh zabezpečení

Fyzické zabezpečení bezdrátové sítě a jejího centrálního řízení tkví v omezeném přístupu zaměstnanců do serverové místnosti, kde se nachází veškeré prvky týkající se sítí (samozřejmě mimo samotných koncových PC). Všechny navrhované access pointy jsou také v uzamčených místnostech, do kterých má možnost vstoupit pouze pověřená osoba. Celá část budovy, ve které se nachází PČS, je monitorována kamerovým systémem, který by okamžitě odhalil pohyb neoprávněné osoby po budově.

Co se týče přístupu k internetu pomocí bezdrátové sítě, firma používá jednotný typ notebooků. Na těchto noteboocích by měly být nainstalovány certifikáty, pomocí kterých je možné z notebooku přistoupit k firemní bezdrátové síti (jiným typem NTB, nebo bez nainstalovaného certifikátu nemá uživatel práva k přístupu). Vedle certifikátů nainstalovaných na noteboocích musí zaměstnanec vlastnit ještě token – USB klíč, na kterém je ve skrytém diskovém oddílu rovněž certifikát. K tomu by měl být použit WPA2 – Enterprice.

WPA2 – Enterprice šifruje data pomocí AES s autentizací proti RADIUS pomocí doménového účtu zaměstnance a vlastnictví certifikátu. Certifikát je vydáván doménou zvlášť pro jednotlivé notebooky a zvlášť pro doménové účty zaměstnanců. K šifrování AES by měl být použit alespoň 256 bitový klíč, který má v současnosti velký potenciál k odražení útoků.

Jelikož zaměstnanci používají firemní mobilní telefony s možností připojení k bezdrátové síti, bylo by přínosné, kdyby měli možnost připojit se přes ně k firemní síti. To na sebe však váže několik nepřekonatelných problémů. Firemní telefony jsou postaveny na platformě Windows Mobile 6.1, a to znamená, že dosud není možnost nainstalování vlastního doménového certifikátu, pomocí kterého by bylo možné se k síti přihlásit. Další problém, triviálnější, je ten, že dané mobilní telefony nemají podporu USB – host, tzn., při autentizaci není možné předložit token zaměstnance. Telefony se však mohou bez problému připojit k otevřené bezdrátové síti, ke které se přihlásí návštěvník pomocí dočasného hesla obdrženého na recepci.

Veškeré nastavení sítě, včetně zabezpečení však závisí na uvážení samotných IT odborníků ve firmě. Cisco WLC nabízí správu celé bezdrátové sítě pohodlně přes webové rozhraní, a tak není žádný problém s vyladěním všech detailů.

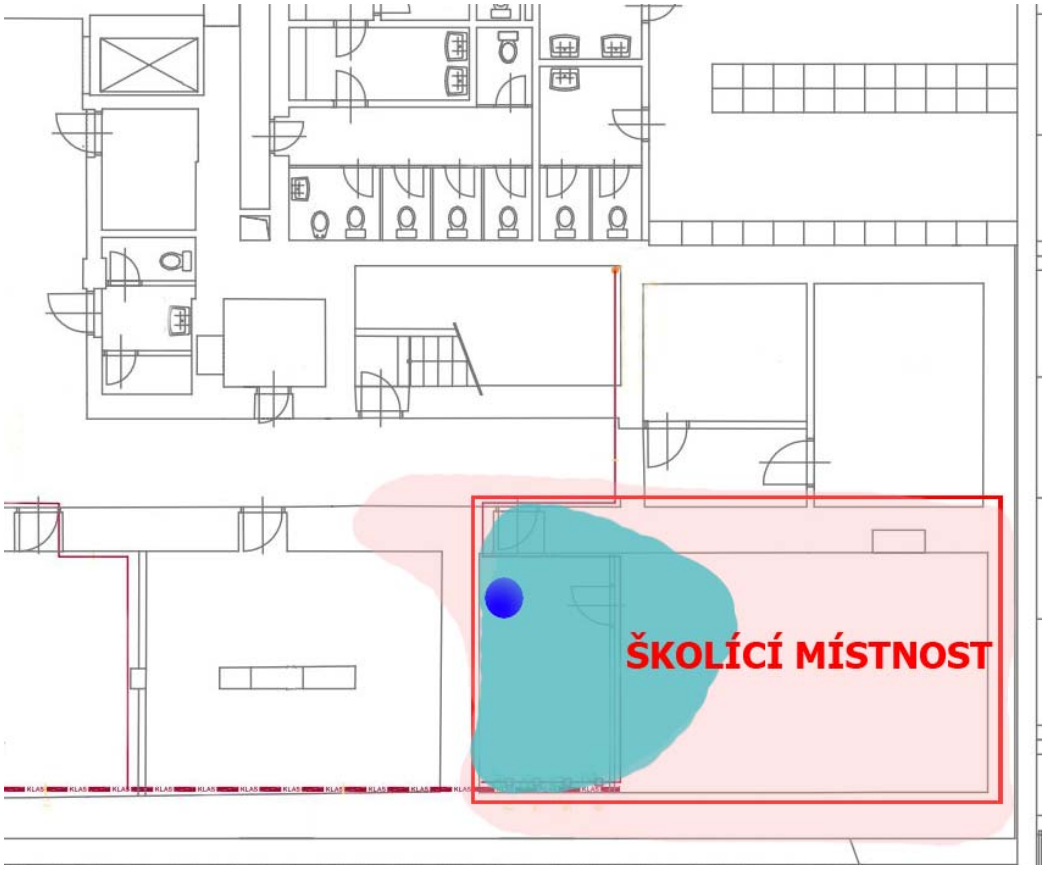
4.3 Návrh rozložení sítě

Bezdrátová síť, vytvořená v prvním patře budovy, by měla pokrývat školící místnost, kterou využívají interní zaměstnanci. Stejně tak se zde může provádět i školení pro externisty. Proto bude mít tato část bezdrátové sítě volný přístup k internetu, avšak na intranet bude mít zaměstnanec přístup až po zadání přístupových údajů. Rozdělení sítě na volně přístupnou a zaměstnaneckou bude provedeno pomocí nastavení politiky VPN na WLC.

Maximální hodnota útlumu v rámci školící místnosti se má pohybovat na úrovní 50 dB. Proto je nutné nastavení adekvátního vyzařovacího výkonu na anténě.

Access point by měl být umístěn na stěnu přilehlé chodbičky, hned vedle skříně s jističi. Tento access point by měl být nastaven na první Wi-Fi kanál.

Celá situace je znázorněna na následujícím obrázku.

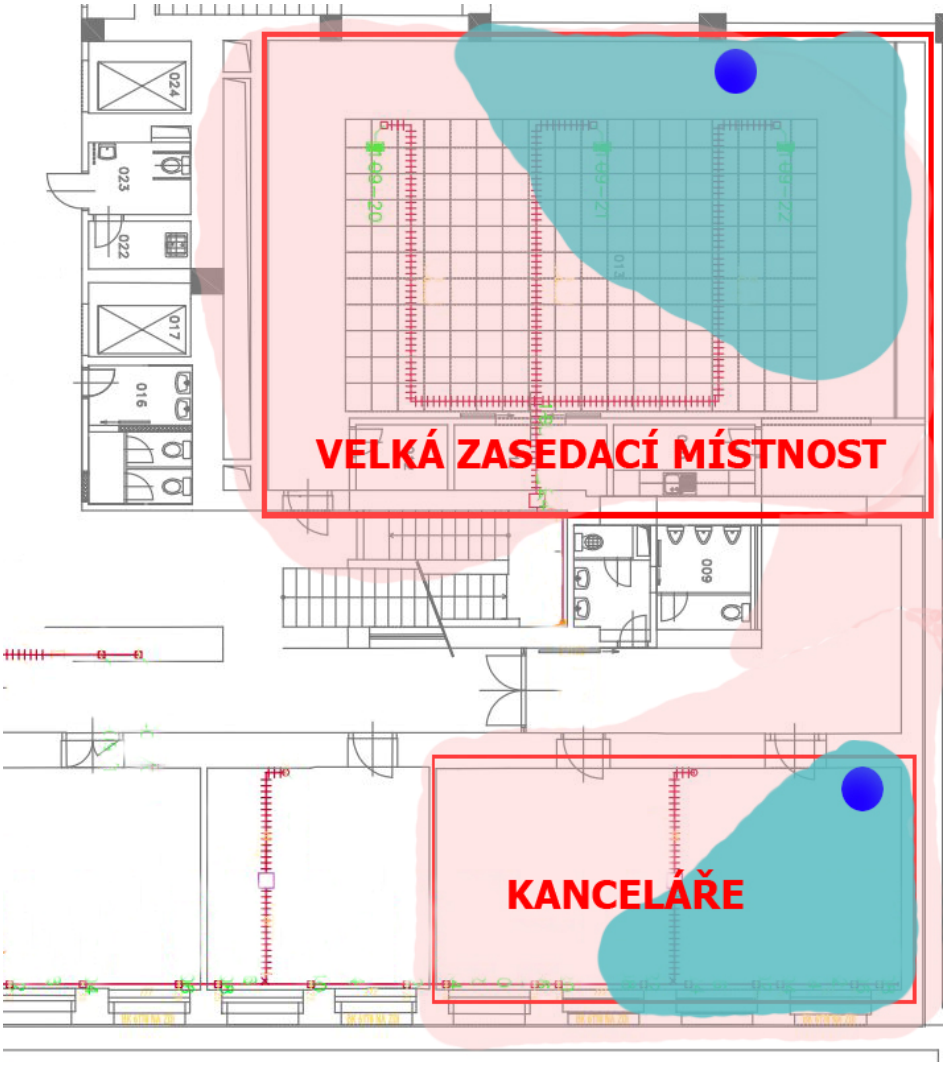


Obrázek 8 - Pokrytí prvního patra Wi-Fi signálem centrály PČS

Druhý access point je navržen pro umístění do velké zasedací místnosti v přízemí. Přívodní kabeláž povede podél již připraveného žlabu pro kabely klimatizace. Samotný access

point musí být umístěn na delší stěně místnosti, v protilehlém rohu, těsně u stropu. Přes sádrokartonovou příčku ve stropě je veden kabel k anténě. Anténa tak bude „viset“ ze stropu dolů.

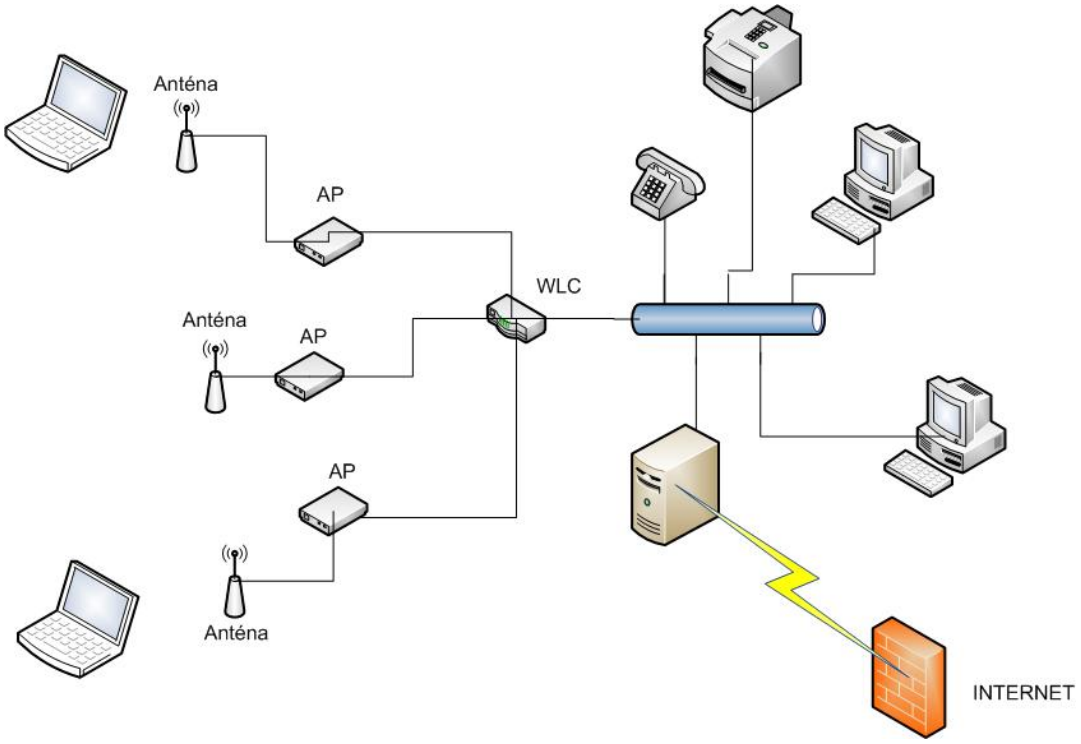
Signál by měl pokrývat veškerý prostor zasedací místnosti a zároveň přilehlý prostor pro občerstvení, oddělený od zasedací místnosti celoskleněnými dveřmi.



Obrázek 9 - Pokrytí přízemí Wi-Fi signálem centrály PČS

Třetí, a poslední access point, který má zajistit pokrytí signálem ve dvou kancelářích v přízemí, bude umístěn nad vstupní dveře. Tento AP pokryje dostatečně silným signálem obě dvě kanceláře a navíc i chodbu mezi kancelářemi a velkou zasedací místností. Zaměstnanci tak budou moci přejít z kanceláře do zasedací místnosti bez nutnosti odpojení a následného opětovného připojení do bezdrátové sítě.

Oba access pointy v přízemí by měly být nastaveny na první Wi-Fi kanál.



Obrázek 10 - Schematické znázornění rozložení sítě ve společnosti

4.4 Výběr hardwaru

S ohledem na to, že společnost doposud využívá výhradně síťové prvky značky Cisco, je vhodné u této značky zůstat i v případě rozšiřování na bezdrátovou sít. Každý výrobce dokonce udává, že pokud má být zajištěna kompatibilita všech prvků v síti, je doporučeno, aby všechny tyto prvky spadaly pod jednu značku.

Cisco je celosvětově uznávaná společnost, jejíž výrobky se zaručují vysokou kvalitou zpracování a dlouholetou tradicí v oboru IT. Zaměstnanci každé firmy na světě mohou projít různými kurzy a získat tak celou řadu certifikátů, vypovídajících o úrovni seznámení se nejen s jednotlivými produkty Cisco, ale i s širokou problematikou sítí. Na základě těchto certifikátů potom mohou být uplatňovány slevy na zboží dodávané společností Cisco. V PČS zaměstnanci IT oddělení několik certifikátů Cisco již získali. Proto se hardware může vybírat přímo na stránkách Cisco. Dá se předpokládat, že konečná cena bude mnohem nižší než uvedená doporučená cena (v řádu desítek procent).

K realizaci bezdrátové sítě ve společnosti bude nutné použít centralizované řízení, tzn., že všechny AP mají téměř nulovou inteligenci a všechny informace předávají přímo na řízení bezdrátové sítě (WLC – Wireless LAN Controller). WLC tedy představuje „mozek“ celé

bezdrátové sítě. Komunikace mezi WLC a AP je realizována po šifrovaných kanálech (trunk). Výhodou tohoto řešení je centralizovaná správa konfigurací jednotlivých AP, možnost vytvoření několika vzájemně nezávislých WLAN, možnost řízení výkonů jednotlivých antén a sledování jiných než firemních Access Pointů v síti. [8]

Jako WCL byl vybrán typ Cisco AIR-WLC4402-12-K9 v provedení splňujícím evropské normy pro radiokomunikaci ETSI. Tento typ WLC obsahuje dva 1 GB ethernetové porty a má licenci na podporu dvanácti AP. Jelikož bude mnou navrhovaná síť obsahovat celkem tři AP, je zde poměrně velká rezerva v případě, že se firma rozhodne bezdrátovou síť ještě v budoucnu rozšiřovat. [18]

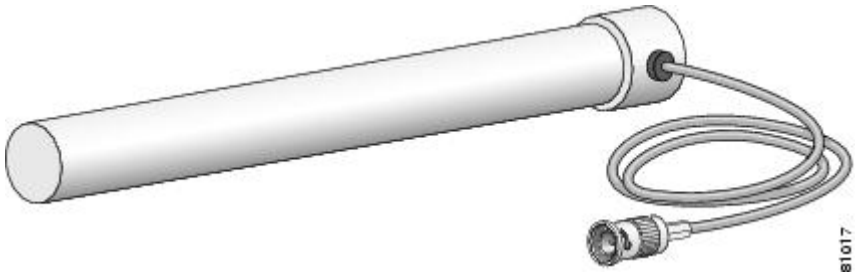
Obrázek 11 - Cisco AIR-WLC4402-12-K9 [18]

Jak již bylo řečeno, v navrhované bezdrátové síti by měly být použity celkem tři AP. Na stránkách Cisco byl vybrán jako vhodný typ Cisco AIR-LAP1252G-E-K9, který podporuje nejen 802.11a/g, ale i 802.11n. Proto by se v budoucnu, v případě přechodu na 802.11n, nemusela nakupovat nová zařízení, pouze by se připojily nové antény k těmto. Řada Cisco Aironet 1250 podporuje i napájení pomocí ethernetové infrastruktury PoE (PoE+). [14]

Obrázek 12 - Cisco AIR-LAP1252G-E-K9 [14]

Další nedílnou součástí navrhované bezdrátové sítě jsou antény, které nejsou součástí výše uvedeného typu AP. Jelikož budova, ve které má být síť realizována, má obvodové zdi z železobetonu o šířce téměř 1 m, není zapotřebí se zabývat příliš směrovostí antén, protože přes tyto zdi by Wi-Fi signál neměl projít. V případě, že by se přece jen signál přes některou ze zdí dostal ven (max. na jednotky desítek centimetrů), firma disponuje kamerovým systémem, pomocí kterého by byl případný narušitel okamžitě odhalen.

Pro velkou zasedací místnost v přízemí je vhodné použít větší dipólovou anténu, aby bylo pokrytí prostor bezdrátovým signálem dostatečné ve všech požadovaných místech. Typ Cisco AIR-ANT2506 je všesměrová anténa pracující na frekvencích 2,4 až 2,84 GHz se ziskem 5,2 dB. U této antény je limitujícím prvkem délka přívodního kabelu (0,91 m). AP tak bude muset mít možnost připevnění na zeď (strop) v bezprostřední blízkosti antény. [16]



Obrázek 13 - Cisco AIR-ANT2506 [16]

Ve dvou přízemních kancelářích a v prvním patře, kde má být pokryta malá školící místnost bude použit větší počet menších antén. Konkrétně by se mělo jednat o všesměrové antény typu Cisco AIR-ANT2422DG-R. Jde o 13 cm dlouhou dipólovou anténu, schopnou pracovat na frekvencích 2402-2495 MHz. Anténa se připojuje pomocí RP-TNC plug, tzn., že je zapojena přímo na konektor přístupového bodu. Z toho vyplývá, že tento typ antény je určen pouze pro vnitřní použití, na rozdíl od předchozí antény, jež může být použita jak pro venkovní, tak i pro vnitřní prostory. [15]

Obrázek 14 - Cisco AIR-ANT2422DG-R [15]

Posledním prvkem, který by měl být použitý při realizaci bezdrátové sítě, je GLC-T. Ten funguje jako modulární metalický gigabitový port, prostřednictvím něhož lze WLC (i jiná

zařízení) připojit ke stávající kabelové síti. Jde o hot-swap modul, tzn., že je možné ho za chodu zařízení vyjmout nebo naopak vložit.

Obrázek 15 - Cisco GLC-T

4.5 Cenová kalkulace

Tabulka 4 - Přehled prvků určených pro realizaci návrhu

Prvek	Typ	Počet	Jednotková cena
WLC	AIR-WLC4402-12-K9	1	$9 995
AP	AIR-LAP1252G-E-K9	3	$1 249
Anténa	AIR-ANT2506	1	$159
Anténa	AIR-ANT2422DG-R	4	$19
Modul	GLC-T	2	$395
Celková cena			$14 767

Jednotkové ceny jsou udávány v amerických dolarech, protože jsou získány z oficiálního katalogu Cisco. Jak bylo řečeno dříve, tyto ceny jsou nejvýše možné pro prodej. Podle certifikátů, které získali zaměstnanci PČS, dají se očekávat konečné ceny zhruba o 30% nižší.

V kalkulaci nejsou uváděny korunové položky (kabely, konektory), které by při realizaci také byly využity.

Závěr

Protože se bezdrátové sítě vyvíjejí prakticky neustále, je složité veškeré detaily zachytit najednou. Z toho důvodu byla problematika pojata spíše od základních pojmů.

Během navrhování bezdrátové sítě byla ve všech prostorách, které mají být pokryté Wi-Fi signálem, zohledněna konstrukce budovy i samotných místností. Pozornost byla věnována znemožnění připojení se k firemní síti z okolních prostranství, ale zároveň dosažení požadované úrovně pokrytí v daných místnostech.

Návrh splňuje požadavek na garantovanou minimální přenosovou rychlost 11 Mb/s ve všech primárně pokrytých prostorách. Dostatečně silný Wi-Fi signál sahá i do prostor chodeb a přilehlých kanceláří, což bylo firmou kladně přijato.

Vysoká cena je vyvážena vysokou spolehlivostí a garancí zabezpečení firmou Cisco. Technika, která byla pro společnost navržena, splňuje veškeré normy podle ETSI a je plně připravena na budoucí přestavbu z 802.11g na 802.11n, s vynaložením minimálních nákladů.

V případě potřeby se díky navrhované bezdrátové síti mohou okamžitě zaměstnanci v zasedací místnosti připojit jak k internetu, tak i do vnitropodnikové sítě intranet a vyhledat si informace, které v danou chvíli potřebují.

Pokrytím kanceláří IT oddělení se dosáhlo toho, že správce sítě má prostřednictvím svého notebooku stále k dispozici webové rozhraní WLC, pomocí něhož může řešit problémy vzniklé v rámci celé sítě.

Seznamy

Seznam literatury

[1] BARKEN, L. *Wi-Fi: jak zabezpečit bezdrátovou síť*. vyd. 1. Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3.

[2] BRISBIN, S. *Wi-fi: postavte si svou vlastní wi-fi síť*. vyd. 1. Praha: Neocortex, 2003. 248 s. ISBN 80-86330-13-3.

[3] KÖHRE, T. *Stavíme si bezdrátovou síť Wi-Fi.* vyd. 1. Brno: Computer Press, 2004. 295 s. ISBN 80-251-0391-9

[4] PUŽMANOVÁ, R. *Bezpečnost bezdrátové komunikace: Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G.* vyd. 1. Brno: Computer Press, 2005. 179 s. ISBN 80-251-0791-4

[5] ZANDL, P. *Bezdrátové sítě WiFi: Praktický průvodce*. vyd. 1. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

---

[6] BAILEY, D. *New enhanced PoE standard lacks punch*. [2008]. [cit. 2010-05-09] Dostupný z: http://www.itnews.com.au/News/106975,new-enhanced-poe-standard-lacks-punch.aspx

[7] BENTON, K. *The Evolution of 802.11 Wireless Security*. [online]. [2010]. [cit. 2010-05-20] Dostupný z: http://itffroc.org/pubs/benton_wireless.pdf

[8] BOUŠKA, P. *Centrální řízení WiFi sítě*. [online]. [2007]. [cit. 2010-05-21] Dostupný z: http://www.samuraj-cz.com/clanek/cisco-wlc-1-centralni-rizeni-wifi-site/

[9] BOUŠKA, P. *Cisco WiFi - základní principy a protokoly*. [online]. [2009]. [cit. 2010-04-15] Dostupný z: http://www.samuraj-cz.com/clanek/cisco-wifi-zakladni-principy-a-protokoly/

[10] BOUŠKA, P. *OSI model*. [online]. [2007]. [cit. 2010-02-10] Dostupný z: http://www.samuraj-cz.com/clanek/osi-model/

[11] BOUŠKA, P. *Počítačové sítě a jejich typy*. [online]. [2010]. [cit. 2010-02-11] Dostupný z: http://www.samuraj-cz.com/clanek/pocitacove-site-a-jejich-typy/

[12] BOUŠKA, P. *VLAN - Virtual Local Area Network*. [online]. [2010]. [cit. 2010-02-11] Dostupný z: http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

[13] *Campus Area Network*. [online]. [2010]. [cit. 2010-03-20] Dostupný z: http://www.javvin.com/networkingterms/CampusAreaNetwork.html

[14] *Cisco Aironet 1250 Series Access Point Data Sheet*. [online]. [2010]. [cit. 2010-05-15] Dostupný z: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/ps8382/product_data_sheet0900aecd806b7c5c.html

[15] *Cisco Aironet 2.4-GHz Dipole Antenna (AIR-ANT2422DG-R)*. [online]. [2010]. [cit. 2010-05-15] Dostupný z: http://www.cisco.com/en/US/docs/wireless/antenna/installation/guide/an2422dg.html

[16] *Cisco Aironet Omnidirectional Mast Mount Antenna (AIR-ANT2506)*. [online]. [2010]. [cit. 2010-05-15] Dostupný z: http://www.cisco.com/en/US/docs/wireless/antenna/installation/guide/ant2506.html

[17] *Cisco Enhanced Power over Ethernet*. [online]. [2010]. [cit. 2010-02-10] Dostupný z: http://www.cisco.com/en/US/prod/switches/epoe.html

[18] *Cisco Wireless LAN Controllers*. [online]. [2010]. [cit. 2010-05-15] Dostupný z: http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps6307/product_data_sheet0900aecd802570b0_ps6366_Products_Data_Sheet.html

[19] *How Does RADIUS Work?*. [online]. [2006]. [cit. 2010-04-15] Dostupný z: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800945cc.shtml

[20] *Hvězdicová topologie (strom)*. [online]. [cit. 2010-03-07] Dostupný z: http://site.the.cz/index.php?id=17

[21] GRIFFITH, E. *802.11i Security Specification Finalized*. [online]. [2004]. [cit. 2010-05-20] Dostupný z: http://securityworld.cz/securityworld/nac-rizeni-pristupu-k-siti-2163

[22] McMILLAN, R. *New attack cracks common Wi-Fi encryption in a minute*. [online]. [2009]. [cit. 2010-05-11] Dostupný z: http://www.networkworld.com/news/2009/082709-new-attack-cracks-common-wi-fi.html

[23] NOVÁK, L. *NAC: Řízení přístupu k síti*. [online]. [2009]. [cit. 2010-05-07] Dostupný z: http://securityworld.cz/securityworld/nac-rizeni-pristupu-k-siti-2163

[24] *Orthogonal Frequency-Division Multiplexing (OFDM)*. [online]. [2009]. [cit. 2010-05-08] Dostupný z: http://securityworld.cz/securityworld/nac-rizeni-pristupu-k-siti-2163

[25] ODVÁRKA, P. *Fyzická a linková vrstva ISO OSI*. [online]. [2000]. [cit. 2010-02-15] Dostupný z: http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=19#Physical

[26] ODVÁRKA, P. *Síťová a vyšší vrstvy referenčního modelu ISO OSI*. [online]. [2000]. [cit. 2010-02-15] Dostupný z: http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=1&clanekID=18

[27] PADMANABHAN, A. *Mobile & Wireless*. [online]. [2009]. [cit. 2010-04-15] Dostupný z: http://mobilewireless.wordpress.com/2008/03/01/an-overview-of-ofdm/

[28] *Perspektivní mobilní technologie – MIMO, HSPA+, LTE*. [online]. [2009]. [cit. 2010-05-07] Dostupný z: http://www.neu-mann.cz/mobilni-komunikace/mobilni-technologie/perspektivni-mobilni-technologie-mimo-hspa-lte/

[29] PETERKA, J. *Prezentační vrstva*. [online]. [2009]. [cit. 2010-05-25] Dostupný z: http://www.earchiv.cz/a92/a226c110.php3

[30] PETERKA, J. *Referenční model ISO/OSI - sedm vrstev*. [online]. [2009]. [cit. 2010-05-25] Dostupný z: http://www.earchiv.cz/a92/a213c110.php3

[31] *Počítačové sítě - Typy sítí dle technologie*. [online]. [cit. 2010-02-10] Dostupný z: http://site.the.cz/index.php?id=28

[32] *POE - Power Over Ethernet*. [online]. [2010]. [cit. 2010-02-10] Dostupný z: http://www.altair.org/labnotes_POE.html

[33] *Power over Ethernet Solutions*. [online]. [2010]. [cit. 2010-02-10] Dostupný z: http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns412/networking_solutions_package.html

[34] *Prstencová topologie (kruh).* [online]. [cit. 2010-03-07] Dostupný z: http://site.the.cz/index.php?id=18

[35] ŘEHÁK, J. *Co je to WiFi - úvod do technologie*. [online]. [2003]. [cit. 2010-05-10] Dostupný z: http://hw.cz/ethernet/wifi/wifi_co_to_je.html

[36] SHELDON, T. *RADIUS (Remote Authentication Dial-In User Service).* [online]. [2001]. [cit. 2010-04-15] Dostupný z: http://www.linktionary.com/r/radius.html

[37] STRÁNSKÝ, P. *Historie Wi-Fi aneb od FHSS k bezdrátu*. [online]. [2009]. [cit. 2010-04-20] Dostupný z: http://www.svethardware.cz/art_doc-E8854472EA5653EBC1257636003B03D0.html

[38] *WiGig Alliance Announces Completion of its Multi-Gigabit Wireless Specification*. [online]. [2010]. [cit. 2010-03-17] Dostupný z: http://wirelessgigabitalliance.org/news/814/

[39] *Wireless LAN Controller (WLC) FAQ*. [online]. [2010]. [cit. 2010-05-21] Dostupný z: https://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a008064a991.shtml

[40] *Základní schéma zapojení*. [online]. [cit. 2010-03-02] Dostupný z: http://www.rfelements.sk/buxus/generate_page.php?page_id=991

Seznam obrázků

Obrázek 1 - Průběh komunikace v rámci modelu ISO/OSI [10] 11
Obrázek 2 - Rozdělení sítí podle velikosti [11] 16
Obrázek 3 - Autentifikační mechanismus zabezpečovacího systému RADIUS [19] 28
Obrázek 4 - Úrovně bezpečnosti standardů IEEE [4] 28
Obrázek 5 - Polarizace antény [40] 32
Obrázek 6 - Půdorys prvního patra centrály PČS 34
Obrázek 7 - Půdorys přízemí centrály PČS 35
Obrázek 8 - Pokrytí prvního patra Wi-Fi signálem centrály PČS 38
Obrázek 9 - Pokrytí přízemí Wi-Fi signálem centrály PČS 39
Obrázek 10 - Schematické znázornění rozložení sítě ve společnosti 40
Obrázek 11 - Cisco AIR-WLC4402-12-K9 [18] 41
Obrázek 12 - Cisco AIR-LAP1252G-E-K9 [14] 41
Obrázek 13 - Cisco AIR-ANT2506 [16] 42
Obrázek 14 - Cisco AIR-ANT2422DG-R [15] 42
Obrázek 15 - Cisco GLC-T 43

Seznam tabulek

Tabulka 1 - Přehled vrstev modelu ISO/OSI [10] 14
Tabulka 2 - Srovnání vrstev modelů TCP/IP a ISO/OSI [10] 14
Tabulka 3 - Přehled standardů IEEE [37] 22
Tabulka 4 - Přehled prvků určených pro realizaci návrhu 43

Seznam použitých zkratek

AAA – Authentication, Authorization, and Accounting

AES – Advanced Encryption Standard

AP – Access Point

CAN – Campus Area Network

CCMP – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CUWN – Cisco Unified Wireless Network

DSSS – Direct-Sequence Spread Spectrum

ETSI – European Telecommunications Standards Institute

FHSS – Frequency-Hopping Spread Spectrum

IBSS – Independent Basic Service Set

IS – Informační systém – Information System

IT – Informační Technologie – Information Technology

ISO/OSI – International Standards Organization / Open System Interconnection

LAN – Local Area Network

LAP – Lightweight Access Point

MAC – Media Access Control

MAN – Metropolitan Area Network

MIC – Message Integrity Code

MIMO - Multiple-Input Multiple-Output

OFDM – Orthogonal Frequency-Division Multiplexing

PAN – Personal Area Network

PČS – Pojišťovna České spořitelny

PoE – Power Over Ethernet

PSK – Pre-Shared Key

RADIUS – Remote Authentication Dial In User Service

RJ-45 – Registered Jack – 45

SSID - Service Set IDentifier

TCP/IP - Transmission Control Protocol/Internet Protocol

TKIP – Temporal Key Integrity Protocol

VLAN – Virtual Local Area Network

WAN – Wide Area Network

WEP – Wired Equivalent Privacy

WEP2 – 802.11i

Wi-Fi – Wireless Fidelity (převzaté z High Fidelity – Hi-Fi)

WLAN – Wireless LAN

WLC – Wireless LAN Controller

WPA – Wi-Fi Protected Access