VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

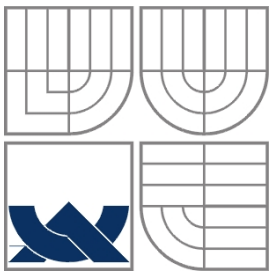
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

NÁVRH BEZDRÁTOVÉ LAN SÍTĚ S LOKALIZACÍ

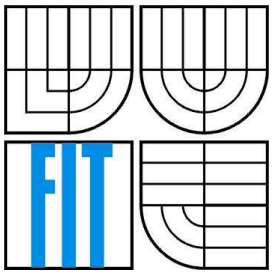
SEMESTRÁLNÍ PROJEKT
SEMESTRAL PROJECT

AUTOR PRÁCE Bc. Jiří Žiška
AUTHOR

BRNO 2007



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

NÁVRH BEZDRÁTOVÉ LAN SÍTĚ S LOKALIZACÍ

A DESIGN OF WIFI LAN WITH LOCALIZATION

SEMESTRÁLNÍ PROJEKT
SEMESTRAL PROJECT

AUTOR PRÁCE — Bc. Jiří Žiška
AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Matoušek, Ph.D.
SUPERVISOR

BRNO 2008

Návrh bezdrátové LAN sítě s lokalizací

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením Ing. Petra Matouška.
Další informace mi poskytl Ing. Tomáš Novák (Cisco systems ČR).
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

……
Jiří Žiška
4. ledna 2007

Poděkování

Rád bych na tomto místě poděkoval zejména Ing. Petru Matouškovi za vedení diplomové práce, rady, konzultace a věcné připomínky.
Dále bych rád poděkoval firmě Unis Computers za poskytnutí tématu a možnosti pracovat na tomto projektu i dalších projektech, které vedli ke zvýšení praktických znalostí v této oblasti.
V neposlední řadě bych chtěl poděkovat zástupcům firmy Cisco Systems za podklady, konzultace a rady při řešení tohoto projektu.

Abstrakt

Tématem této diplomové práce je návrh bezdrátové sítě WiFi s lokalizací bezdrátových zařízení jako jsou přenosné počítače, aktivní RFID čipy nebo mobilní telefony a terminály s podporou WiFi. Návrh vychází ze skutečného projektu.
Tato síť bude postavena na komponentách firmy Cisco systems, která má rozsáhlý program výrobků pro takové sítě. Jako aplikace je v tomto projektu uvažován software a RFID čipy od firmy AeroScout, která spolupracuje s firmou Cisco systems.

Klíčová slova

Cisco Unified Wireless Network, LWAPP, LAP, lokalizace, kontrolér, triangulace, RF Fingerprint, RFID, bezdrátová síť, WiFi, TDoA, WCS, Location Appliance, Guest Access, AeroScout, PanGo.

Abstract

The subject of this Master's thesis is Centralized Wireless Network (WiFi) with localization of laptops, active RFID chips or mobile phone and mobile terminals with WiFi feature. Design of network is derived from really project.
The network is design with Cisco Systems products program "Cisco Unified Wireless Network". I select AeroScout software and RFID chips for this project. AeroScout is a company, which cooperate with Cisco Systems.

Keywords

Cisco Unified Wireless Network, LWAPP, LAP, localization, controller, triangulation, RF Fingerprint, RFID, wireless network, WiFi, TDoA, WCS, Location Appliance, Guest Access, AeroScout, PanGo.

Citace

Žiška Jiří: Návrh bezdrátové LAN sítě s lokalizací. Brno, 2008, diplomová práce, FIT VUT v Brně.

Obsah

1 Úvod

Bezdrátové sítě WiFi jsou jednou z nejrychleji se rozvíjejících se oblastí počítačových sítí. Zejména velké rozšíření mobilních počítačů způsobil velkou poptávku po připojení k síti a Internetu bez drátů. Nyní se s těmito sítěmi můžeme setkat téměř na každém kroku. Proč proto tuto technologii nevyužít k dalším účelům.

Lokalizace v bezdrátových sítích WiFi začíná být aktuální zejména tam, kde je velký pohyb osob, vybavení nebo zboží, jako např. v nemocnicích, na letištích ve skladech nebo ve velkých továrnách. Je již několik firem, které se touto možností lokalizace zabývají, avšak já jsem si pro vypracování tohoto dokumentu vybral pouze jednu firmu – Cisco systems. Důvod pro toto rozhodnutí je celkem zřejmý. Cisco je v současné době lídrem trhu v oblasti počítačových sítí, včetně bezdrátových sítí. Druhým důvodem je také ta skutečnost, že tyto sítě buduji a tak je pro mne jednodušší vypracovat projekt na dané téma a získat k tomu potřebné podklady a zkušenosti.

Centralizované bezdrátové sítě byly vytvořeny za účelem snadnější zprávy rádiového vysílání (dále jen RF). Existuje více typů. V druhé kapitole popíši jednotlivé typy centralizovaných bezdrátových sítí, jejich vlastnosti, výhody a nevýhody. Zmíním se také o některých mýtech, které tyto sítě provázejí.

Další kapitola se už zaměří na komponenty centralizovaných sítí, které budu využívat při návrhu. Tedy sítí Cisco. Popíši, k čemu jednotlivé komponenty slouží, zda jsou pro danou síť nezbytné či nikoliv. Zmíním se o způsobu komunikace mezi komponentami těchto sítí. Ke konci kapitoly vypracuji návrh topologie bezdrátové sítě, která bude dále rozvinuta v další kapitole.

Kapitola zabývající se studií proveditelnosti bude koncipována tak, jak je předkládána zákazníkovi. Proto budou texty určeny pro laickou veřejnost. Popíši v nich způsob měření, vyhodnotím měření a provedu konečný návrh sítě pro pilotní projekt s odhadem na celý projekt.

Pátá kapitola bude informovat o průběhu realizace a změnách, které při realizaci budou provedeny. Důvodem ke změnám budou zejména počty komponent sítě. Jelikož je projekt vypracován pouze na základě vzorkového měření v pilotní části projektu, proto zcela jistě dojde k nějakým změnám.

V předposlední kapitole bude zhodnocen celý projekt. Bude porovnán s původním návrhem a výsledky měření. Dále bude zhodnocena funkčnost a možnosti dalšího využití.

2 Centralizované bezdrátové sítě WiFi

Centralizované bezdrátové sítě WiFi jsou takové sítě, jejichž přístupové body (dále jen AP) nemají vlastní logiku. Veškerá jejich logika je součástí tzv. kontrolérů, které řídí veškeré RF parametry, ale i rozdělení zátěže, rozdělení uživatelů do VLAN, zabezpečení sítí, aj.

Hlavní výhodou je přizpůsobivost takové sítě. V podstatě se celá síť chová jako jeden přístupový bod. AP v takové síti se vzájemně ruší jen velmi málo. S tím souvisí i větší rychlost roamingu nejen mezi přístupovými body na jednom kontroléru, ale také mezi kontroléry.

Neméně důležitou výhodou je větší bezpečnost. Pokud je proveden útok na některou část sítě a „škůdce“ je zablokován v dané části sítě, pak je zablokován i ve zbytku sítě.

Další výhodou těchto sítí je jednoduchost konfigurace, což je ale vykoupeno horší diagnostikou problémů v síti. Proto je obtížné např. určit, proč některý přístupový bod nepracuje správně, proč se nemůže připojit ke kontroléru, apod.

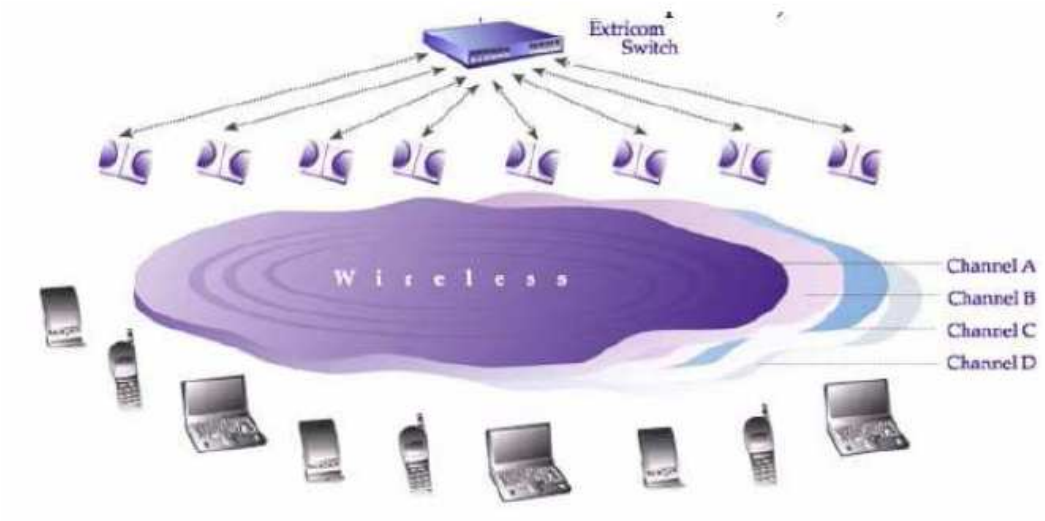
Velmi často je zajištěna také redundance na úrovni AP. Pokud dojde k výpadku jednoho AP, ostatní AP zvýší vysílací výkon (v rámci povolených limitů) tak, aby vzniklá „díra“ v pokrytí byla co nejmenší. Některé sítě zaručují také redundanci na úrovni kontrolérů.

Velmi časté je tvrzení, že taková síť má jednodušší návrh než běžná síť tvořená autonomními AP. Toto tvrzení je však nepravdivé, jelikož pro optimální funkci je třeba dbát kvalitního návrhu, zejména je-li síť navrhována pro využití lokalizace. Nekvalitní návrh se většinou promítne také do ceny takové sítě nejen díky vyššími počtu AP, ale také z toho plynoucího vyššího počtu kontrolérů.

Obecně můžeme rozdělit centralizované bezdrátové sítě na 2 typy – centralizované sítě na vlastním distribučním systému (DS) a centralizované bezdrátové sítě na LAN / WAN.

2.1 Centralizované bezdrátové sítě na vlastním DS

Centralizované bezdrátové sítě na vlastním DS jsou takové sítě, u kterých je AP připojeno ke kontroléru dedikovanou linkou (vlastním kabelem). Struktura těchto bezdrátových sítí je znázorněna na Obr. 1.

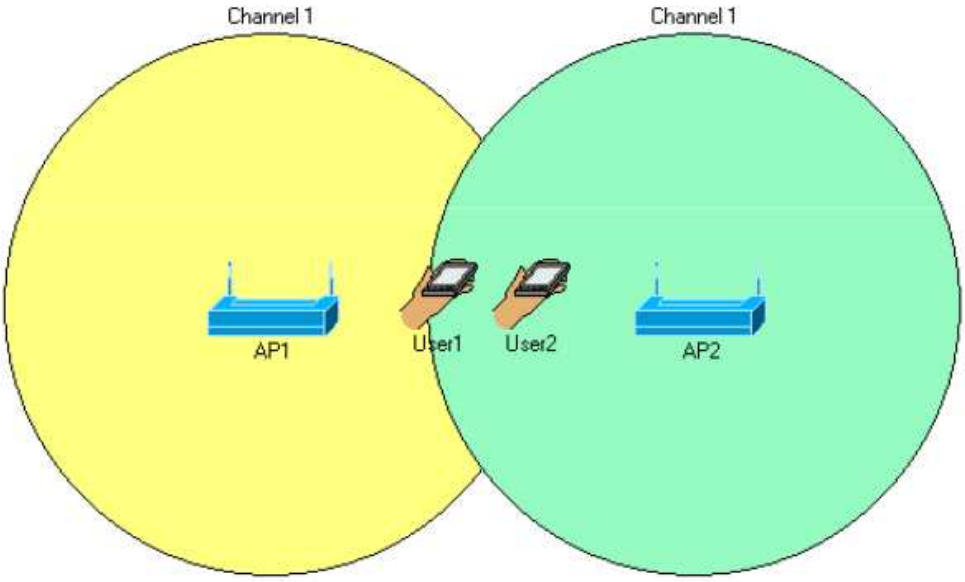


Obr. 1 - Struktura sítí firmy Extricom

Přístupové body těchto sítí obvykle mají více rádiových modulů, které mohou pracovat současně. Obvykle také mohou pracovat všechny přístupové body na stejném rádiovém kanálu. Díky tomu je možno u 4 rádiových AP dosáhnout až 4 násobné propustnosti (každý klient se připojí na jedno rádio). V praxi však tohoto nelze dosáhnout, jelikož obvykle v pásmu 2,4 GHz bývá některý kanál již obsazen. Navíc na stejném kanálu mohou pracovat přístupové body pouze tehdy, pokud je v síti velmi málo klientů. Jakmile je více klientů na hranici mezi přístupovými body, dochází ke snižování rychlosti až na polovinu.

Toto tvrzení dokazuje Obr. 2. Na tomto obrázku jsou vyznačeny 2 AP vysílající na stejném kanále a 2 klienti, kteří jsou na pomyslné hranici Při současném využití sítě oběma klienty může dojít ke třem variantám.

1) Jeden přístupový bod sníží výkon a ke druhému se připojí oba klienti. V takovém případě dojde ke snížení rychlosti na zhruba polovinu.
2) Každý klient je připojen k jednomu přístupovému bodu a oba vysílají současně. V takovém případě je velké vzájemné rušení a přenosová rychlost jde velmi razantně dolů. Dochází také k častému opakování přenosu z důvodu poškození dat a může docházet i k výpadkům spojení. Ke vzájemnému rušení dochází i pokud obě AP sníží výkon na hranici potřebnou k připojení klienta. V takovém případě je stále velmi špatný parametr SNR (signal to noise ratio, česky nazývaný kvalita signálu – odstup signálu od šumu).
3) Každý klient je připojen k jednomu přístupovému bodu a při komunikaci dochází k časovému multiplexu. Tato možnost je nejpravděpodobnější. Pokud vysílají oba přístupové body, střídají se tak, aby nebyl žádný z klientů ve výhodě. Pokud vysílají klienti, síť se pro ně tváří jako jeden přístupový bod. Tedy dochází k „boji“ o médium jako by byly připojeni k jednomu AP. Rychlost je opět poloviční – stejně jako by byli oba klienti na jednom AP.



Obr. 2 - Problematika bezdrátových sítí na vlastním DS

Předchozí princip také dokazuje, že i v těchto sítích je potřeba udělat kvalitní návrh. Při prezentaci jednoho ze systémů pracujícím na vlastním DS nám bylo zástupci firmy řečeno, že pokud je některá část budovy špatně pokryta, je možné vzít AP a umístit ho kdekoliv v dané lokalitě při zachování stejné kvality sítě. Což ovšem, jak dokazuje předchozí příklad, může být pravda jen v případě velmi malé hustoty uživatelů. Při větším počtu AP je také větší počet hranic mezi jednotlivými AP a tudíž se snižuje rychlost.

Hlavní nevýhodou je chybějící redundance na úrovni kontrolérů. Je zde riziko, že pokud dojde k poruše kontrolérů je celá část sítě nefunkční. Při obvyklém použití bezdrátových sítí to nemá žádné rozsáhlé důsledky, ovšem v případě použití např. ve skladech nebo továrnách, kde se používají bezdrátové čtečky čárových kódů to má velké ekonomické důsledky.

Neméně závažnou nevýhodou je nutnost budovat vlastní infrastrukturu pro tyto sítě. S tím souvisí také prostorové omezení přístupových bodů vzhledem ke kontrolérům. Kabeláž je tvořena klasickými UTP5e kabely, proto maximální délka je 100m od kontroléru. Je možné využít i tzv. extendéry (dalo by se říci, že to je klasický repeater – opakovač), které zvýší délku na max. 200m od kontrolérů. To má obvykle za důsledek větší počet kontroléru s 8 porty nebo nevyužité porty v 24 portových kontrolérech.

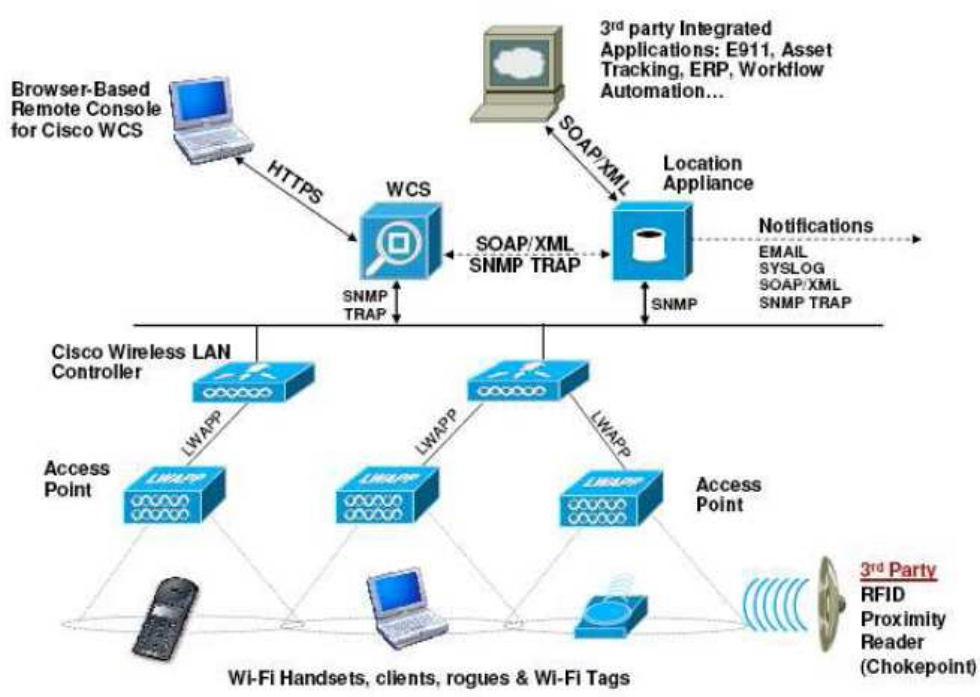
Sítě pracující na vlastním DS vyrábějí firmy Extricom a Belden.

2.2 Centralizované bezdrátové sítě na LAN / WAN

Tyto sítě, jak již název kapitoly napovídá, využívají ke komunikaci mezi kontroléry a AP klasickou LAN síť nebo mohou komunikovat i přes WAN. Důvodem je unicastová komunikace na L2 i L3 vrstvě ISO / OSI modelu. To zaručuje zejména univerzálnost sítě, ale také redundanci na úrovni kontrolérů. V případě výpadku trasy je většinou otevřena nová trasa díky STP (spanning-tree protokolu).

Další výhodou těchto sítí je modularita a možnost využití dalších služeb. Je možné postavit síť jen z kontrolérů a AP a později doplnit další kontroléry, systém poskytující společnou správu nad kontroléry nebo produkty pro využití lokalizace.

Struktura centralizovaných sítí Cisco je zobrazena na Obr. 3. Jejími hlavními prvky jsou „odlehčené“ přístupové body (LAP – Lightweight Access Points) a kontroléry, které jsou jádrem celého systému.



Obr. 3 - Struktura centralizovaných bezdrátových sítí Cisco

Nespornou výhodou je také L2 i L3 roaming. L2 roaming v rámci jednoho kontroléru je rychlejší než u řešení s autonomními AP. Díky vzájemné spolupráci kontrolérů je i roaming klienta mezi kontroléry rychlejší. Na rozdíl od autonomního řešení je zde umožněn i L3 roaming. Uživatel po přechodu od AP v jedné L3 síti k AP v druhé L3 síti zůstává virtuálně členem původní sítě. Tzn.

zůstane mu nejen IP adresa, ale i práva z původní sítě. Veškerý jeho provoz je posílán IP tunelem do původní sítě.

Krom řízení LAP lze kontroléry využít i k řízení bezdrátových MESH sítí.

Snad jedinou výhodou jsou u těchto sítí kanálová omezení, která jsou stejná jako u klasických WiFi. Z technického hlediska nelze ovládat síť na jednom kanále.

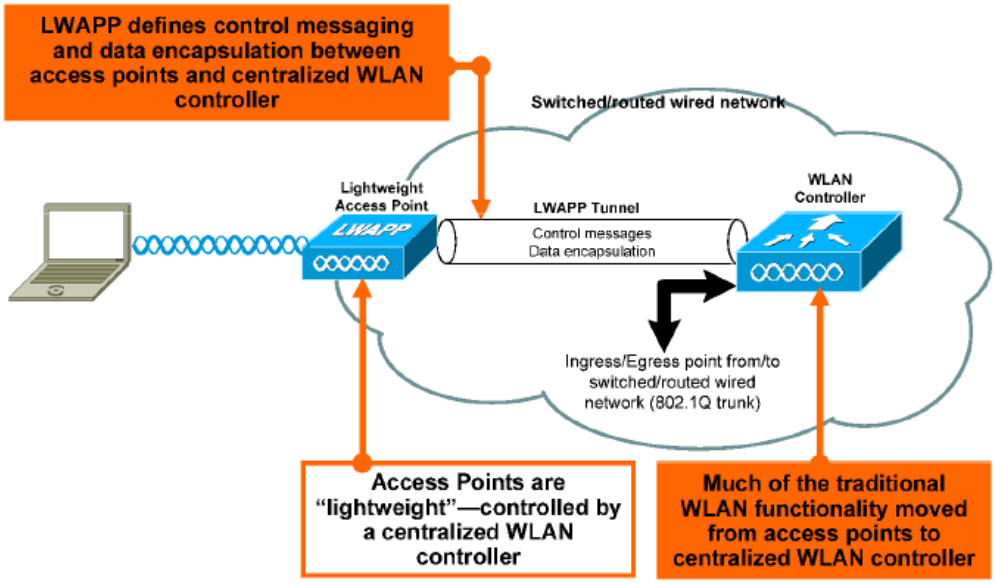
Vývojem a produkcí těchto sítí se zabývá nejen firma Cisco, ale také firma HP.

3 Komponenty centralizovaných sítí Cisco

Jak již jsem zmínil v předchozí kapitole, centralizované sítě Cisco jsou modulární. Základem těchto sítí jsou LAP a kontroléry. Samozřejmostí jsou také klientská zařízení.

3.1 Přístupové body

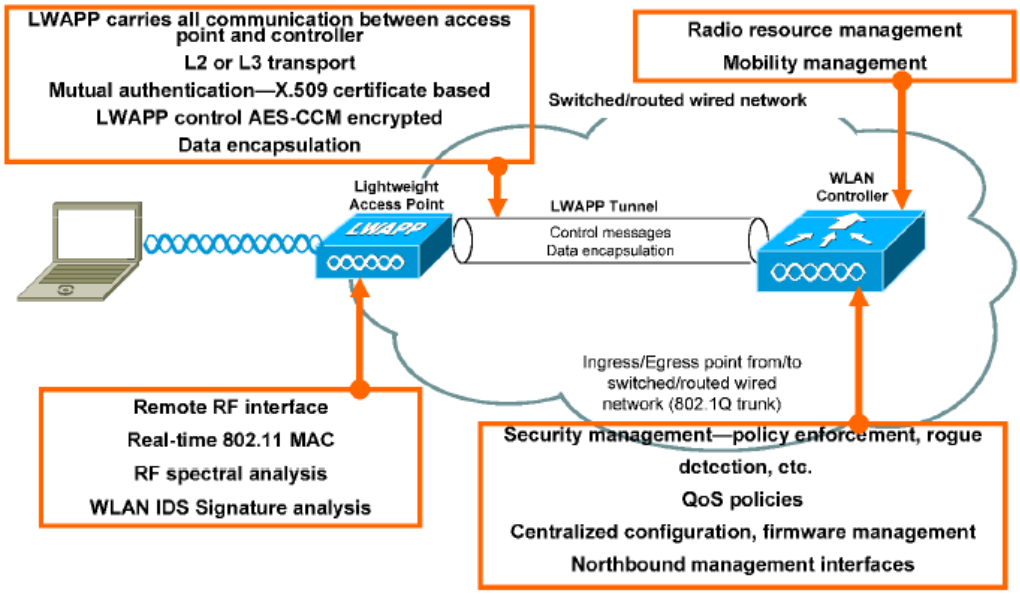
Přístupové body (LAP … Lightweight Access Point), jak již jsem zmínil, jsou zařízení, která sama neřídí rádiové vysílání. Jsou řízena kontroléry, se kterými komunikují skrz LWAPP tunel (LightWeight Access Points Protocol). Lze jim nastavit pouze základní hodnoty (IP adresu, masku a IP adresy kontrolérů) pro komunikaci po ethernetu.



Obr. 4 - Komunikace skrz LWAPP tunel

LWAPP je v současné době proprietární protokol firmy Cisco, ale pracuje se na jeho standardizaci. Tento tunel je vytvořen v klasickém ethernetu, a jelikož většina komunikace je formou

unicastu, tak pracuje skrz L2 i L3 vrstvu ISO / OSI modelu. Při komunikaci jsou přenášeny nejen řídící informace (UDP / 12223), ale i data (UDP / 12222) šifrovaná pomocí AES-CCMP (Advanced Encryption Security – Counter CBC-MAC Protocol … rozšíření AES používané také v 802.11i). Autentizace ke kontrolérům je prováděna pomocí X.509 certifikátů.



Obr. 5 - Komunikace skrz LWAPP tunel

Skrz LWAPP tunel je přenášen také firmware. Přístupové body mají stejnou verzi firmware, jakou mají kontroléry. Vždy když se liší verze firmware kontrolérů a verze firmware přístupových bodů, je stažen a nainstalován firmware z kontrolérů.

Existuje několik způsobů, pomocí kterých nalezne LAP kontrolér, ke kterému se přihlásí:

- Pomocí zpráv na broadcastu L2 vrstvy ISO / OSI modelu
- Pomocí zpráv, které vysílají okolní LAP vzduchem (OTAP … Over-The-Air Provisioning)
- Manuální konfigurací 3 IP adres kontrolérů do LAP
- Pomocí parametru DHCP (option 43) … lze pouze pro jeden typ přístupových bodů v dané síti
- Přes DNS (LAP se ptá na *CISCO-LWAPP-CONTROLLER.localdomain)*

Pokud nalezne v síti více kontrolérů, připojuje se podle následujících pravidel (dle pořadí):

- Z manuálně konfigurovaných IP adres
- Ke kontroléru, který je označen jako „master“
- Ke kontroléru, který je nejméně vytížen

V sortimentu firmy Cisco je jedna série, která je vyráběná pouze ve verzi LAP. Tato série nese označení LAP1000 series.

Některé série přístupových bodů lze konvertovat z autonomních AP na LAP (i opačným směrem). Tyto přístupové body jsou vhodné, pokud se předpokládá postupný přechod na centralizovanou síť později. Některé vlastnosti těchto LAP jsou potom omezené (např. počet SSID na

jednom přístupovém bodu je po konverzi na LAP snížen z 16 BSSID na polovinu). Konverzi lze provést u AP1100, AP1130AG, AP1200, AP1240AG a AP1300 series.

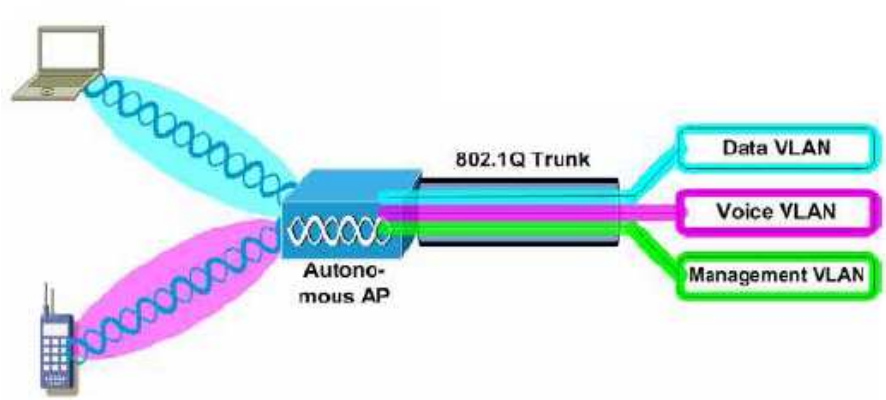
Některé přístupové body nelze konvertovat. Jsou to zejména bridge a některé starší přístupové body (AP350, AP1120).

3.2 Kontroléry

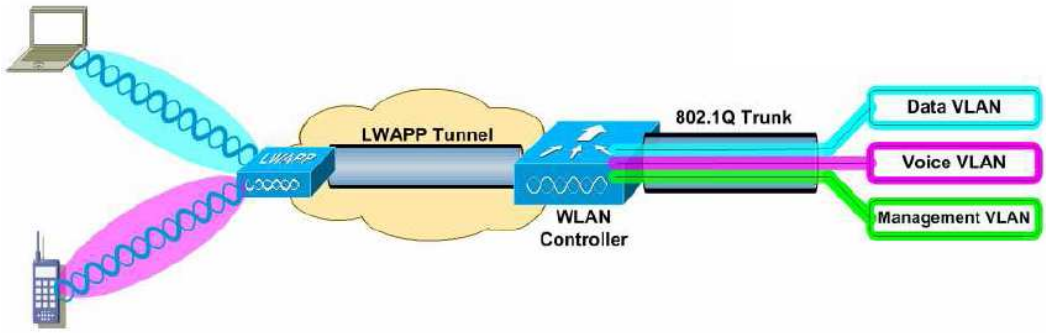
Kontroléry jsou „mozkem“ celého systému centralizovaných bezdrátových sítí Cisco. Spolu s LAP jsou nezbytnou součástí těchto sítí.

Řídí všechny přístupové body v síti, jejich vysílací výkon a kanál. Pokud je to možné, snaží se rozdělit klienty tak, aby byla vyrovnaná zátěž na jednotlivých přístupových bodech. Klienti bezdrátové sítě nekomunikují s přístupovými body, ale jsou spojeni s kontroléry. Veškerá autentizace a zabezpečení bezdrátové sítě probíhá mezi kontroléry a bezdrátovými klienty. Také rozdělení do VLAN je řešeno až na kontrolérech. Proto nemusí být všechny bezdrátové VLAN šířeny skrz celou síť, ale pouze tam kde je potřeba a ke kontrolérům.

Řízením rádiového vysílání (kanál a výkon) lze pokrýt i výpadky některého z přístupových bodů (pokud je síť správně navržena).



Obr. 6 - VLAN s autonomními AP



Obr. 7 - VLAN v centralizovaných bezdrátových sítích

Kontroléry se vyrábějí ve 3 variantách.

- Standalone (2100 series, 4400 series) … kompletní HW + SW, který je funkční bez dalšího HW
- Moduly (do síťového přepínače L3 c3750, routery) … nejsou schopny pracovat samostatně
- WiSM modul (síťový přepínač L3 catalyst 6500) … nejvyšší řada kontrolérů

Jednotlivé modely se dále rozdělují podle počtu LAP, které mohou řídit. Nejnižší řadou je 2100 series, která řídí max. 6 LAP. Nejvyšší řadou je WiSM modul (až 300 LAP). Zajímavostí je, že WiSM modul jsou v podstatě 2 kontroléry 4404 (umí řídit pouze 100 LAP) i přes to však dokáží řídit více LAP. Výhodou může také být, že pokud nedojde k poruše společné části pro obě jednotky WiSM modulu, pak je WiSM modul schopný dále řídit 150 LAP.

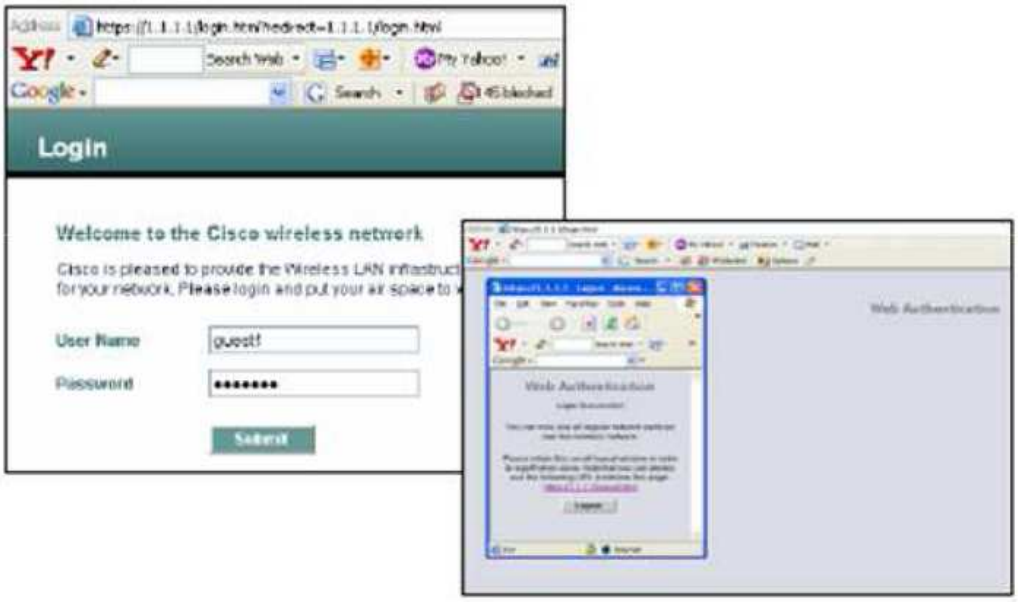
Jelikož LAP hledají kontroléry a asociují se k nim podle postupu popsaného v předchozí kapitole, je možné budovat sítě s redundancí „n+1“, kde „n“ je počet potřebných kontrolérů a „1“ je redundantní kontrolér s počtem licencí jako největší kontrolér (s největším počtem licencí).

Kontroléry se mohou sdružovat a vzájemně spolu komunikují v rámci domén. V sítích Cisco existuje doména pro roaming a RF doména. Obvykle se však síť konfiguruje tak, aby obě domény byly stejné.

V RF doméně spolupracují kontroléry na konfiguraci rádiového vysílání, takže se ve výsledku chovají jako jeden přístupový bod (vzájemně se snaží nerušit se). Max. počet kontrolérů v RF doméně je 20.

Roaming doména je určena pro snazší přechod v rámci odlišných L3 sítí ISO / OSI modelu mezi kontroléry (i uživateli). Pokud uživatel přechází mezi kontroléry v různých L3 sítích, pak je vytvořen tunel, který zajistí, že uživatel zůstává v původní L3 síti a tudíž nemusí měnit IP adresu. Jeho provoz je pak symetricky (u nových kontrolérů i nesymetricky) posílán skrz IP tunel. Do roaming domény je možné připojit až 24 kontrolérů.

Jednou z funkcí kontroléru je i tzv. Guest Access. Je to přístup do sítě po autentizaci ve webovém formuláři. Tento způsob přihlašování do sítě není příliš bezpečný díky útokům „Men in the Middle“, proto je vhodné ho používat pouze pro přístup do Internetu a nejlépe v kombinaci s časově omezenými přihlašovacími údaji. Naopak značnou výhodou je jednoduchost konfigurace z důvodu otevřené sítě, díky čemuž se dá použít pro hosty firemní sítě (odtud název guest access). Hosté nemusí nic konfigurovat, kontroléry povolí DHCP a DNS provoz.



Obr. 8 - Příklad Guest Access

Na rozdíl od řešení Cisco s autonomními AP lze použít dynamické přidělování VLAN pomocí RADIUS serveru v sítích se zabezpečením WPA. V sítích s autonomními AP je problém s šifrovacím klíčem WPA při změně VLAN.

3.3 Wireless Control Systém (WCS)

WCS je softwarové serverové řešení, které umožňuje správu a dohled nad kontroléry. Není nutnou součástí centralizovaných sítí Cisco, ale při použití více než jednoho kontroléru je vhodné tuto aplikaci dokoupit.

Hlavním úkolem WCS je vytváření a správa konfiguračních šablon. Mezi konfigurační šablony patří také účty „Guest Access“, které lze spravovat pomocí účtu typu Lobby Ambasador. Tento účet umožňuje pouze správu uživatelských účtů pro tento způsob přístupu do sítě, proto je možné jej použít i pro vybrané zaměstnance firmy. Rozhraní přidávání účtů je intuitivní a tudíž není obtížné zaučit zaměstnance na přidávání těchto účtů. Nevýhodou však zůstává nutnost použití pouze prohlížeče Internet Explorer a některé malé chybičky ve formulářích (jako nutnost celého data apod.).

Další úkolem WCS je monitoring sítě. Tato aplikace umožňuje nejen zobrazit bezpečnostní rizika, informace o útocích a poruchy v síti, ale také o těchto událostech informovat pomocí e-mailu. Licence se prodává ve dvou provedeních

- WCS Base
- WCS Location

Druhá zmíněná, jak již název napovídá, umožňuje lokalizaci v sítích. Na rozdíl od verze „base“ umožňuje lokalizaci pomocí RF fingerprint, ale jen jednoho klienta v reálném čase (v případě lokalizace v bezdrátových sítích Cisco platí reálný čas = 1 až 2 minuty zpoždění). Verze „base“ umožňuje zobrazit pouze asociaci k přístupovému bodu.

3.4 Location Appliance

Je dalším HW produktem pro rozšíření lokalizace. Při použití location appliance je nutné použít také WCS Location. V této kombinaci je pak umožněna lokalizace mnoha klientů v reálném čase. Současně lze sledovat více než 10 tis. bezdrátových zařízení.

Cisco Location Appliance je také vybaveno vlastním API rozhraním pro připojení aplikace 3. Strany. Tyto aplikace dále rozšíří zejména komfort, ale také využití lokalizace v bezdrátových sítích.

Podporuje akce aktivních RFID tagů a funkce vyvolané pomocí tzv. chokepointu (bude vysvětleno později).

S použitím Location Appliance je lokalizace určena spíše pro správce sítě a administrátory, ne pro personál. Důvodem je méně intuitivní prostředí a typy účtů.

Umožňuje jen základní dělení uživatelů do skupin a je vhodná spíše pro použití uvnitř budov.

3.5 Software třetích stran

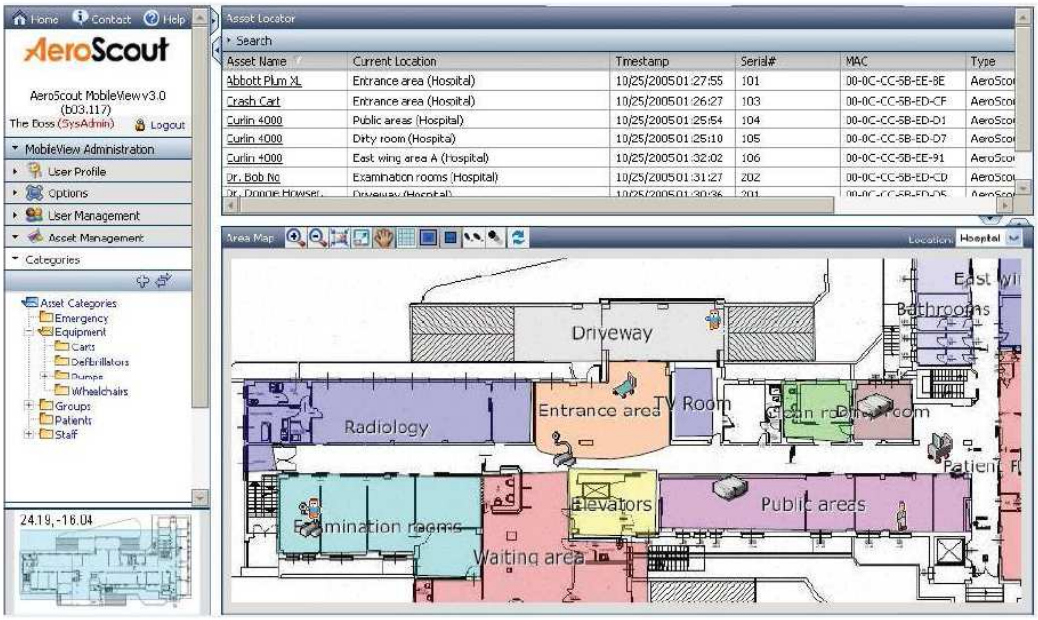
Software 3. Strany je (obvykle) serverová aplikace, která je prostředníkem mezi Location Appliance a personálem firmy využívající lokalizaci. Na jedné straně komunikuje s Location Appliance přes API rozhraní. Na straně druhé s klientem pomocí webového rozhraní.

Cisco úzce spolupracuje s firmami PanGo a AeroScout, ale výrobců lokalizačního software, který je schopný spolupracovat s Location Appliance je více.

3.5.1 Software AeroScout MobileView

Software firmy AeroScout se jmenuje AeroScout MobileView. Rozšiřuje schopnosti lokalizace zejména o „user friendly“ uživatelské rozhraní pro personál firmy (bez použití JAVA). Dokáže rozdělit prostor i bezdrátové klienty na více skupin a těmto skupinám přiřadit akce (např. objekt opustil prostor apod.). Srovnání vlastností AeroScout MobileView s vlastnostmi Location Appliance je v tab. 1.

Obr. 9 - Blokové schéma AeroScout MobileView



Obr. 10 - Příklad lokalizace v AeroScout MobileView

	Cisco 2700 / WCS	AeroScout MobileView
User	IT & Network Manager	Business User – Nurse, Material Manager, Ops Exec
Value	Determine location; find rogue clients and tags	Track and manage critical business assets
Logic	Find asset X	Business rules and alerts based on asset X's location (enter/exit, overflow, dwell, workflow, etc.)
Grouping	Basic	Advanced asset management and categorization
Environment	Indoor	Adds outdoor data

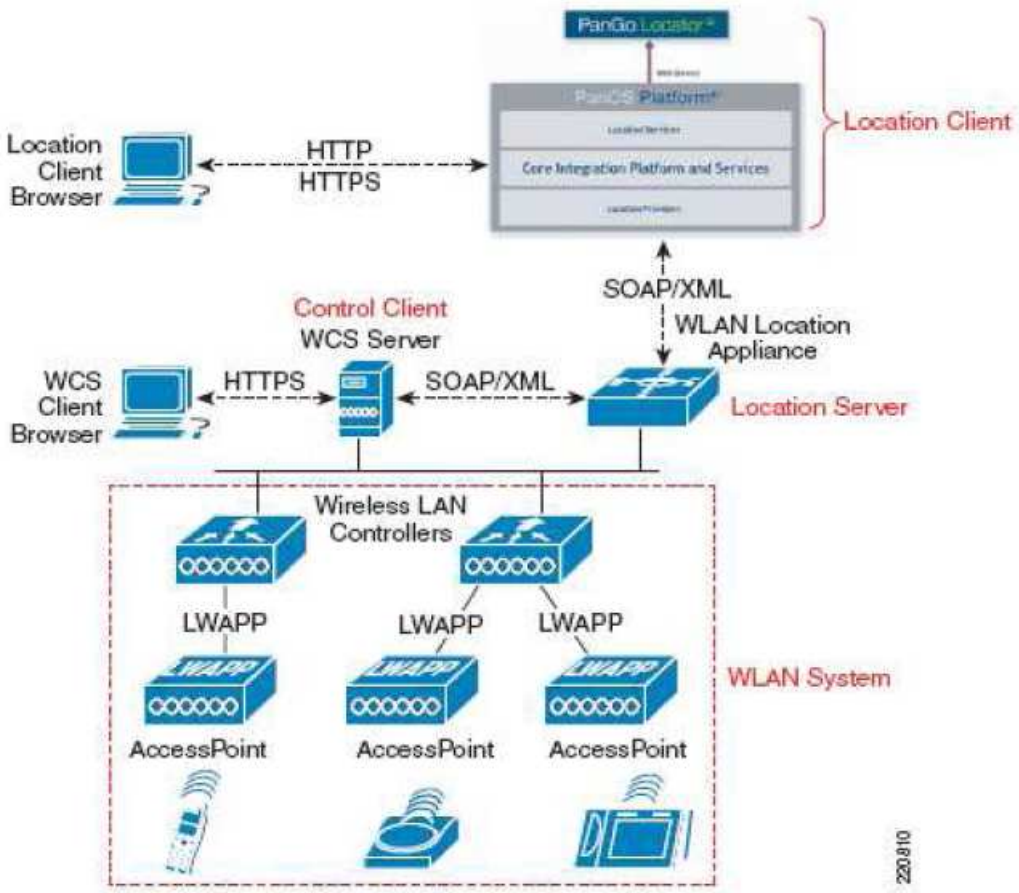
Tab. 1 - Srovnání vlastností Location Appliance a AeroScout MobileView

Vlastnosti:

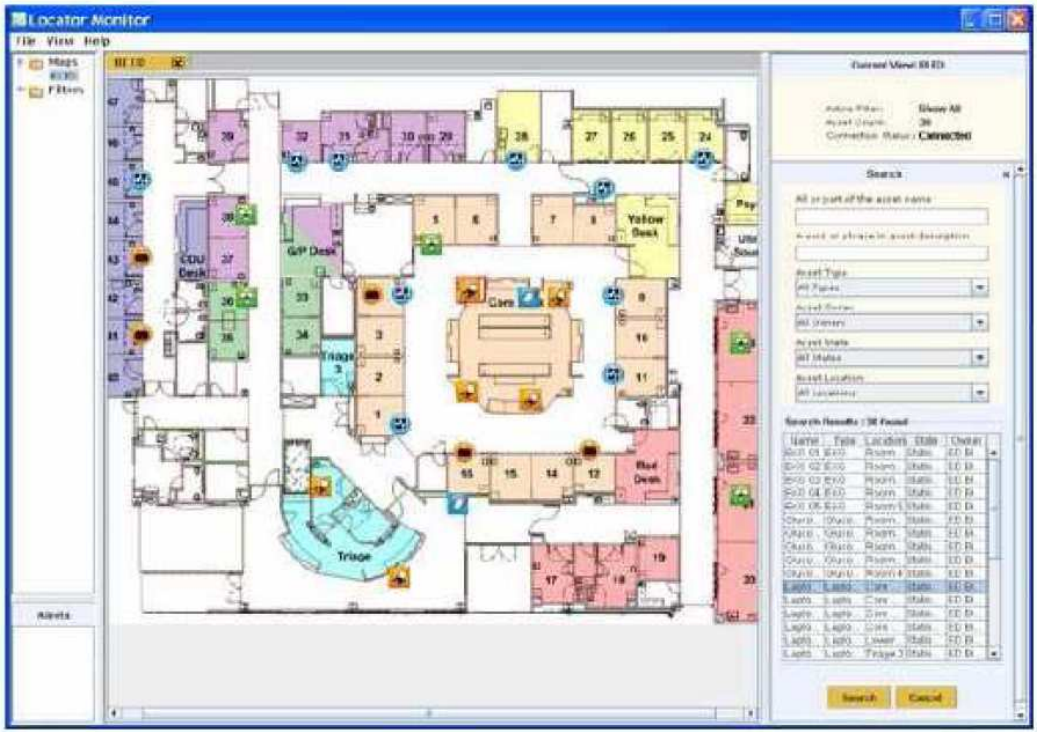
- HW / SW požadavky:
  - OS Windows 2003 server
  - Database: Oracle 9,2i / MS-SQL 2005
  - JBoss 3.2.7
  - Paměť: 2 GB
  - Procesor: 2,8 Ghz
- Webové rozhraní bez JAVA
- Spolupracuje s Cisco Location Appliance
- Modularita

3.5.2 Software PanGo Locator

PanGo vyrábí software pro lokalizaci s názvem PanGo Locator. Tento software vyžaduje ke své funkci serverovou aplikaci PanOS.



Obr. 11 - Schéma lokalizace se software PanGo



Obr. 12 - Lokalizace s PanGo Locator

3.6 Klienti bezdrátových sítí

Klienty v bezdrátových sítích netvoří v dnešní době jen přenosné počítače, ale i bezdrátové VoIP telefony, mobilní terminály se čtečkami čárových kódů a samozřejmě aktivní RFID čipy pro lokalizaci v bezdrátových sítích.

Většina přenosných počítačů v dnešní době používá bezdrátové standardy 802.11b/g, ale počet přenosných počítačů, které používají standard 802.11a (resp. v EU 802.11h) valně přibývá. Proto je vhodné stavět nové sítě i s podporou tohoto standardu.

U bezdrátových VoIP telefonů je situace podobná jako u přenosných počítačů. Rozdílem je, že bezdrátové VoIP telefony podporující pásmo 802.11a se dostali na trh až začátkem loňského roku. I Cisco má ve své nabídce jeden takový telefon, který nese označení 7921G.

Obr. 13 - Cisco IP Phone 7921G

Vlastnosti Cisco IP Phone 7921G:

- Standard 802.11 a/b/g
- Mobilita
- 6 linek
- Zkrácené telefonní volby
- Upravitelná hlasitost a melodie vyzvánění
- Automatická odpověď
- Vibrační vyzvánění
- Konference
- Autentizace a WPA šifrování
- QoS
- Standard 802.11h (použitelnost v Evropě)
- Šetření energií
- Zabudovaná anténa

Stejně jako v předcházejících případech je nabídka mobilních terminálů pracující ve standardu 802.11a velmi malá. V současné době je nabízí pouze firma Symbol Technology.

Aktivní RFID čipy na rozdíl od pasivních vysílají určitou informaci. Lze jim nastavit různé akce a přidat vlastnosti jako např. měření teploty apod.

Aktivní RFID čipy vyrábí opět více firem, ale opět se zmíním pouze o výrobcích firmy PanGo a AeroScout.

Na poli lokalizačního software je souboj těchto firem poměrně vyrovnaný. U aktivních RFID čipů je však AeroScout mnohem dále. Jeho sortiment v této oblasti je velmi rozsáhlý. Nabízí aktivní RFID čipy nejen s různými funkcemi, ale i s různým využitím, jako např. v podobě identifikačních karet pro zaměstnance. Výhodou je zejména dlouhá životnost baterie (až 3 roky), které jsou navíc vyměnitelné. Důvodem je, že čip nevysílá stále, ale jen v určitých intervalech. Lze nastavit i vysílání pouze po aktivaci pomocí ChokePointu. V současné době však vyrábí pouze chokepoint pracující v pásmu 2,4 GHz. Firma PanGo v současné době nabízí pouze jeden typ aktivního RFID čipu.

Obr. 14 - Příklady aktivních RFID čipů firmy AeroScout

Vlastnosti aktivních RFID čipů:

- Dlouhá životnost baterie (až 3 roky)
- Vyměnitelná baterie
- Široké možnosti připevnění
- V současné době pracují v pásmu 2,4 Ghz
- Rozsáhlá nabídka typů (zejména firma AeroScout)
- Využití ChokePoint nebo tlačítka k vyvolávání akcí
- Možnost programování zpráv
- Vodě odolnost
- Možnost verze se zabudovaným teplotním čidlem

3.7 ChokePoints

ChokePointy jsou poslední součástí lokalizace v bezdrátových sítích. Jejich význam je zejména tam, kde chceme vyvolat určitou akci na základě nějaké změny polohy. Typickou aplikací, kde se

chokepointy instalují jsou dveře. Po průchodu těmito dveřmi aktivují aktivní RFID čip a ten odešle zprávu, kterou má nastavenou. Obvykle má tato zpráva vyšší prioritu. Zpráv (v případě čipů AeroScout) může být 10 z nichž každá má délku max. 10 B. Událost zpracuje Location Appliance nebo software 3. strany.

ChokePointy pracují na frekvenci 125 kHz, proto musí mít RFID čipy zabudovaný také přijímač na této frekvenci.

4 Studie realizovatelnosti

4.1 Možnost rušení některých lékařských přístrojů

Všechna pásma využívaná v bezdrátových sítích jsou v nelicencovaném pásmu určeném pro volné vysílání. Proto je nepravděpodobné, že by funkce některého z lékařských přístrojů byla ovlivněna vysíláním přístupových bodů. Pokud by k takové situaci došlo, je vina jednoznačně na straně výrobce tohoto lékařského zařízení, jelikož zmíněná volná (bezlicenční) pásma jsou platná pro celou Evropu, Ameriku i Asii (kromě některých zemí zakazujících využití pásma 5,15 … 5,875).

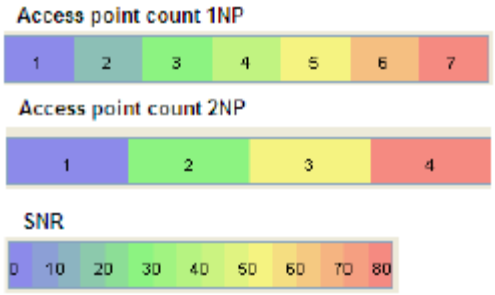
I přes to je nutné před případnou realizací projektu zvážit kontaktování výrobce přístrojů, které mohou ohrozit pacienta na zdraví nebo na životě. **U těchto výrobců je třeba zjistit, zda funkce jejich přístroje nemůže být ovlivněna vysíláním v pásmech 2,4 ... 2,480 GHz; 5,15 … 5,35 GHz; 5,47 … 5,875 GHz.**

4.2 Měření a vyhodnocení

V pilotní části projektu byl vznesen požadavek na změření části budovy C1, která má 3 podlaží. I když požadavky v zadání byly pouze v obecné rovině, síť byla navrhována a měřena s ohledem na další možnou rozšiřitelnost pro účely lokalizace a IP telefonie. Při měření byl zkušební přístupový bod nastaven na vysílací výkon s ohledem na možnou regulaci výkonu pomocí centralizovaného řešení Cisco.

K měření bylo využito programu Ekahau Site Survey. Tento program zaznamenává data získaná při měření. Výsledky měření vytvořené tímto programem jsou jen matematickým modelem, který program vytváří. Z toho důvodu jsou výsledky závislé i na nastavení programu a nemusí úplně přesně zobrazovat realitu. Ze zkušeností s tímto programem a předchozími měřeními mohu konstatovat, že obvykle jsou reálné výsledky lepší než jsou naměřené hodnoty. I přes to jsem při návrhu vytvořil určitou rezervu pro případ zhoršení podmínek v době realizace.

Při zhodnocení výsledků měření v tomto dokumentu budu využívat legendu zobrazenou na Obr. 15. Access point count jsou počty přístupových bodů, které pokrývají danou část patra. SNR je kvalita signálu při zobrazení vzájemného rušení a rušení cizími přístupovými body.



Obr. 15 - Legenda využívaná při zhodnocení výsledků měření

Při měření byla kontrolována také prostupnost signálu stropem. Výsledkem bylo, že strop má velký útlum, což je v tomto případě výhoda – nebudou se vzájemně rušit přístupové body v jednotlivých patrech.

Veškeré výsledky měření jsou zahrnuty v technickém návrhu.

4.2.1 1NP

V prvním patře nebylo naměřeno žádné rušení z cizího přístupového bodu. To návrh sítě, zvláště v pásmu 2,4 GHz, značně zjednodušuje.

Mapy budou doplněny se souhlasem zákazníka do dokončení diplomové práce. V současné době máme zakázáno šířit mapové podklady i výsledky měření na mapových podkladech.

Dle předchozích obrázků je patrné, že celé lůžková část patra je pokryta signálem s kvalitou lepší než 20 dBm. To zaručuje provoz všech bezdrátových zařízení v plné rychlosti (teoreticky 54 Mbps). Obr. zobrazuje informaci o tom, že celou lůžkovou část pokrývají 3 přístupové body. To je nutné v případě využití lokalizace.

I přes to bylo nutné přidat 1 přístupový bod z důvodu menšího maximálního výkonu navrhovaného přístupového bodu než u měřícího a potřeby rezervy ve vysílacím výkonu pro automatickou regulaci.

4.2.2 2NP

V druhém patře bylo naměřeno velmi slabé rušení na 6. kanálu. Tato skutečnost ovlivňuje návrh jen mírně, protože rušení se nachází jen v prostoru, kde mají 3 přístupové body dostatečný výkon a tím i odstup signálu od šumu (rušení).

Mapy budou doplněny se souhlasem zákazníka do dokončení diplomové práce. V současné době máme zakázáno šířit mapové podklady i výsledky měření na mapových podkladech.

Z Obr. vyplývá, že opět skoro v celém prostoru 2NP je odstup signálu od šumu dostatečný pro připojení plnou rychlostí. Pouze v pravém dolním rohu by byla rychlost trochu omezena. To je dáno volbou kanálu při vyhodnocování měření a rušením v této části patra. V případě změny kanálů je rušení nižší a po přidání dalšího přístupového bodu je opět kvalita lepší. Prázdné místo při měření vzniklo z důvodu vynechání měření na pokoji JIP. Ze stejných důvodů jako na 1NP a z důvodu většího rušení je do návrhu přidán 1 přístupový bod oproti měření. Tedy celkový počet přístupových bodů na 2NP je 5.

Z Obr. je patrné, že většina patra je pokryta 3 až 4 přístupovými body. To dostačuje k využití lokalizace.

4.2.3 3NP

Třetí patro je podobné 2NP. Proto zde neproběhlo měření jako v předcházejících případech, ale jen bylo změřeno rušení. Obdobně jako na 2NP je zde rušení velmi mírné, avšak více roztáhnuté do celého patra. Nejvíce se rušení projevilo na kanálech 9-11 (podobné intenzity jako na 2NP). Na ostatních kanálech je rušení ještě menší.

Mapy budou doplněny se souhlasem zákazníka do dokončení diplomové práce. V současné době máme zakázáno šířit mapové podklady i výsledky měření na mapových podkladech.

Z měření 2NP a rušení na 3NP lze odvodit, že je opět vhodné použít 5 přístupových bodů.

4.3 Hierarchie a popis bezdrátové sítě

Technický návrh je postaven na základě výsledků měření v části C1.

Síť dle tohoto návrhu umožňuje připojení klientů nejen v pásmu 2,4 GHz, ale i 5 GHz. Je postavena pro připojení pacientů i zaměstnanců nemocnice tak, aby síť byla dobře zabezpečena proti úniku důvěrných dat a informací ze sítě nemocnice. V případě požadavku na rozšíření uživatelů (např. o studenty VŠ) lze síť dále rozšířit.

Rozmístění přístupových bodů je zvoleno s ohledem na budoucí možné rozšíření funkce sítě o lokalizaci nebo k využití bezdrátových IP telefonů.

4.3.1 Rozmístění přístupových bodů

Z jednotlivých měření vyplývá, že je nutné použít na patro 5 přístupových bodů. Výjimkou je 1NP, kde k pokrytí lůžkové části postačí 4 přístupové body. Přístupové body budou připevněny k podhledům na stropě. Napájení je řešeno po ethernetovém kabelu dle standardu 802.3af (PoE).

Mapy budou doplněny se souhlasem zákazníka do dokončení diplomové práce. V současné době máme zakázáno šířit mapové podklady i výsledky měření na mapových podkladech.

4.3.2 Zabezpečení bezdrátové sítě

Při řešení zabezpečení sítě je brána v úvahu zejména důvěrnost dat přenášených v rámci bezdrátového provozu, ale také jednoduchost přístupu k síti.

V tomto dokumentu bereme v úvahu pouze 2 typy uživatelů využívajících síť, ale je možné oddělit až 16 typů uživatelů.

4.3.2.1 Pacienti

Pacienti nesmí mít přístup do sítě nemocnice. Proto budou patřit do vlastní virtuální sítě (VLAN), která bude mít přístup pouze do Internetu. Tato VLAN začíná v kontrolérech a je zakončena na firewallu do Internetu.

Jelikož pacienti nebudou mít přístup k žádným citlivým informacím, není nutné zavádět žádné šifrování provozu. Přístup k Internetu bude omezen přihlášením přes webovou přihlašovací stránku v kontroléru. Přihlašovací údaje budou moci generovat zaměstnanci nemocnice (např. při příjmu pacienta) s platností na dobu určitou.

Tento způsob přístupu k Internetu zajišťuje, že pacienti nemusí nic složitě konfigurovat. Pokud mají přihlašovací údaje, pak se velmi snadno dostanou k Internetu.

Přístup pacientů k Internetu lze omezit také časově (pouze v určitý čas nebo po určitou dobu) nebo datově (na určitý objem přenesených dat).

4.3.2.2 Zaměstnanci

Zaměstnanci přistupují k citlivým údajům, které nesmí být přístupné cizímu uživateli. Proto je nutné provoz šifrovat pomocí WPA s šifrováním TKIP nebo WPA2 s AES. Z hlediska kompatibility s většinou karet je vhodnější volba WPA. Samotné šifrování s jedním šifrovacím klíčem (WPA-PSK) je nebezpečné z důvodu možnosti prozrazení klíče. V případě WPA-PSK by pak bylo nutné klíč měnit pro všechny uživatele. Proto je vhodnější využít některou z metod autentizace.

Pro tento případ jsou nejvhodnější (nejbezpečnější) metody EAP-FAST a PEAP. Obě metody mohou využívat přihlašování pomocí uživatelského jména a hesla a ověření protistrany (serveru) pomocí certifikátu. Autentizace vyžaduje autentizační server. Autentizační server byl zvolen Cisco

Secure Access Control Server (ACS) ve verzi 4.1, který umí autentizaci EAP-FAST i PEAP. Uživatelská jména a hesla budou využita z databáze LDAP (eDirectory).

Autentizaci pomocí metody EAP-FAST umí pouze ovladače bezdrátových síťových karet Cisco a Intel. Proto pro nepodporované karty na OS Windows 2000 a Windows XP lze zakoupit software 3. strany (Cisco Secure Services Client). PDA s OS Windows CE nebo Windows Mobile podporují autentizaci metodou PEAP.

4.4 Popis součástí bezdrátové sítě

4.4.1 Přístupové body

Bude využito přístupových bodů Cisco LAP1131AG (Lightweight access point), které umožňují připojit se k bezdrátové síti nejen v pásmu 2,4 GHz, ale i 5 GHz. To umožní využít všechny v současné době schválené standardy WiFi – 802.11 a/b/g.

Přístupové body budou napájeny po Ethernetovém kabelu (PoE), proto postačí pouze jeden kabel ke každému přístupovému bodu.

Obr. 1: Přístupový bod LAP1131AG

Vlastnosti:

- Integrované diversní všesměrové antény pro pásmo 2,4 GHz a 5 Ghz (3 dBi / 4,5 dBi)
- Regulace výkonu
- Rozsáhlé možnosti zabezpečení (WPA, WPA2, zabezpečení pomocí autentizace)
- Podpora více SSID s různým zabezpečením
- Příjemný vzhled
- Bezpečné upevnění
- Napájení po síti (PoE – 802.3af)

4.4.2 Přepínače

V rozvaděči na každém patře bude umístěn přepínač Cisco WS-C3560-24PS-S. K tomuto přepínači budou připojeny jednotlivé přístupové body. Tento přepínač obsahuje napájecí zdroj dle standartu 802.3af, proto bude také sloužit jako napájecí zdroj pro jednotlivé přístupové body.

Přepínač obsahuje dostatek portů i pro připojení přístupových bodů v části C2, proto nebude nutné v případě realizace bezdrátové sítě v části C2 nakupovat další přepínač.

Přepínač bude vybaven SFP modulem GLC-SX-MM= připojeným na stávající optickou páteřní síť.

Vlastnosti:

- 24 portů (10 / 100, half duplex / full duplex)
- Všechny porty mají zabudovaný napájecí zdroj PoE
- 2 SFP sloty použitelné pro připojení k metalické i optické síti rychlostí až 1Gbps
- Podpora VLAN, spanning-tree a dalších funkcí

4.4.3 Kontroléry

Návrh počítá se 2 kontroléry WLC4404 s licencemi pro 100 LAP (lightweight access point). Nepokrývají pouze přístupové body v tomto projektu (část C1), ale 2/3 předpokládaného počtu přístupových bodů pro celý areál.

Kontroléry budou umístěny v rozvaděči v serverovně a připojeny k Cisco Catalyst 4500 pomocí EtherChannel. To zajistí dostatečnou propustnost bezdrátové sítě.

Vlastnosti:

- 4 porty 1000Base-X
- 2 rozšiřující sloty
- Podpora VLAN, spanning-tree a dalších funkcí
- Podpora mnoha druhů autentizace (EAP-FAST, EAP-TLS, PEAP, LEAP, apod.)
- Podpora 802.11 a/b/g
- Podpora více SSID s různým zabezpečením
- Podpora WPA (TKIP), WPA2 (AES)
- Řízení 100 LAP
- Schopnost řízení AP přes L2 i L3 vrstvu

4.4.4 Embedded server

HW server bude sloužit pro provoz WCS. Bude v provedení do rozvaděče. Server bude umístěn v jedné ze serveroven a bude připojen k C4500.

Pokud by byla využita lokalizace, je vhodné zálohovat WCS server. V tom případě by musely být 2 servery umístěny v geograficky oddělených serverovnách, z nichž jeden by byl trvale vypnut a zapnul by se pouze v případě výpadku hlavního serveru.

Jeho konfigurace je dána požadavkem aplikace, která na něm bude provozována. OS bude Windows 2003 server.

Vlastnosti:

OS: Windows server 2003 R2 Standard edition, EN 5 CAL
Procesor: Intel Core Duo 2,4 GHz
Paměť: 2 GB
Pevný disk: 2x 72 GB SAS, 15 000 ot./min.
Optická mechanika: DVD-RW

4.4.5 Cisco Wireless Control System (WCS)

Cisco Wireless Control System (WCS) není nezbytnou součástí, pokud není třeba používat lokalizaci, avšak je vhodné jej využít, pokud je v síti více kontrolérů. Pomáhá navrhovat, spravovat a monitorovat rozsáhlé bezdrátové sítě.

Ve verzi s Location licencí umožňuje najít aktuální polohu jednoho z bezdrátových uživatelů a ve spojení s Location appliance umožňuje dohled nad pohybem osob připojených k bezdrátové síti v reálném čase (reálný čas v řádu 1 minuty). Dále ve spojení s Location appliance umožňuje uchovávat historii pohybu osob.

WCS umožňuje vytvářet konfigurační šablony, monitorovat útoky na bezdrátovou síť a „podstrčené“ přístupové body.

WCS bude nainstalováno na serveru s OS Windows 2003 v provedení do rozvaděče. Tento server bude umístěn v rozvaděči v serverovně.

Vlastnosti:

- HW / SW požadavky:
  - Windows 2000 server
  - Windows 2003 server SP1
  - RedHat Linux AS / ES v4.0
  - Vmware ESX Server 3.0.1

- Procesor: Intel 3.06 GHz
- RAM: 960 MB
- HDD: 30 GB

- Kontroléry: 2000, 2100, 4100, 4400 series, WiSM, C3750G, WLCM, WLCM-E
- Přístupové body: LAP, MAP, RAP
- Integrovaná databáze
- S location licencí umožňuje lokalizaci 1 klienta
- S Cisco Location Appliance umožňuje real-time lokalizaci

4.4.6 Cisco Secure Access Control Server Solution Engine

Cisco Secure Access Control Server Solution Engine (ACS) je RADIUS server pro autentizaci pomocí různých metod EAP. Hlavním důvodem nasazení ACS je autentizace pomocí metody EAP-FAST, která je proprietárním řešením Cisco. ACS Solution Engine je jednotné řešení HW + SW ACS 4.1. Jelikož je ACS nezbytnou součástí pro přístup zaměstnanců do sítě nemocnice, musí být zálohován. Oba servery budou umístěny v geograficky oddělených serverovnách a připojeny k C4500.

Vlastnosti:

- HW:
  - Procesor: Intel P4 3,4 GHz, 2 MB cache
  - RAM: 1 GB
  - HDD: 80 GB SATA
  - CD/DVD combo
  - RS232 serial port, 3 USB 2.0
- Webové konfigurační rozhraní
- Připojitelné k LDAP, ODBC, OTP
- Podpora většiny autentizačních metod včetně EAP-FAST, PEAP

4.4.7 Cisco WLAN Location Appliance

Cisco WLAN Location Appliance má vlastní API, přes které může komunikovat se softwarem 3. strany (např. AeroScout nebo PanGo). Tento software umožňuje zobrazit klienty bezdrátové sítě na mapě, určit který klient volal o pomoc (pomocí tlačítka na RFID čipu) nebo kdo opustil daný prostor.

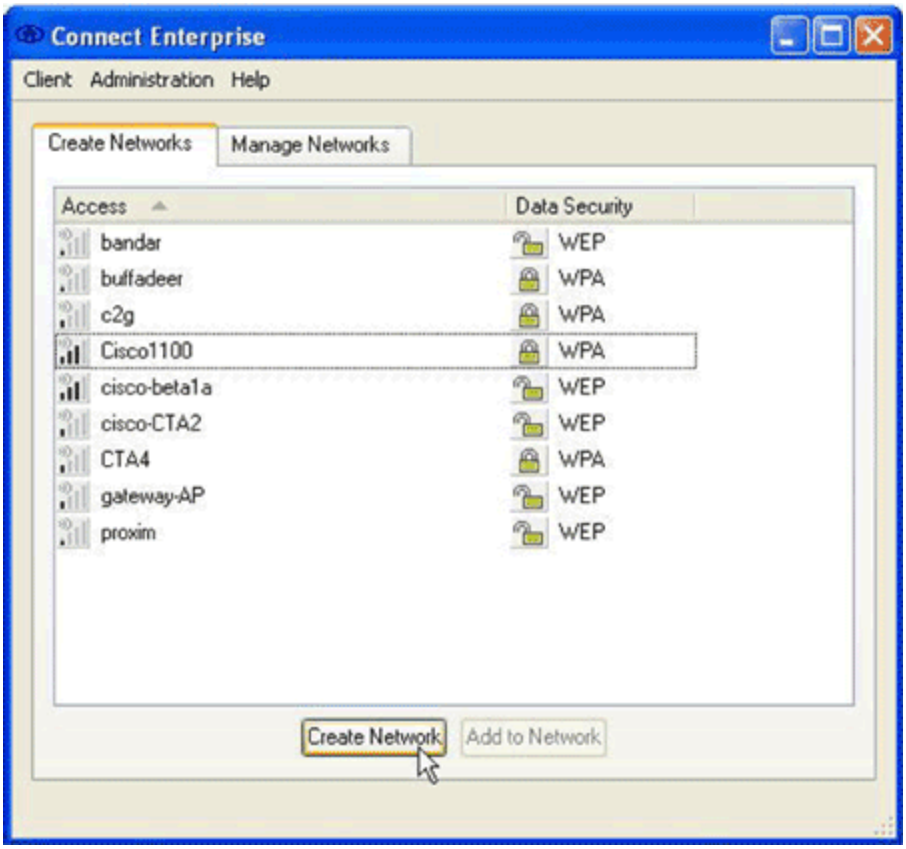
Součástí Cisco WLAN Location Appliance je i historie, která může sloužit k hledání chyb v signálu či ke kontrole pokusů o útok na bezdrátovou síť.

Vlastnosti:

- Spolupracuje s WCS Location licence a kontroléry sítě Cisco Unified Wireless Network
- Kompletní SW / HW řešení
- Uchovává historii (až 30 dní)
- Přes integrované SOAP / XML API spolupracuje se softwary 3. strany pro lokalizaci
- Spolupracuje s chokepoint a RFID čipy
- Pomáhá zajišťovat bezpečnost WLAN sítí

4.4.8 Cisco Secure Services Client

Je software, který je určený k autentizaci nekompatibilních zařízení k síti. Podporuje většinu typů autentizace včetně EAP-FAST a PEAP. Je určen pro OS Windows 2000 a Windows XP (podle neověřených informací nově i pro PDA s Windows CE).



Vlastnosti:

- Podpora většiny typů autentizace
- OS Windows XP / 2000
- Spolupracuje s bezdrátovými kartami přes NDIS rozhraní
- Časově neomezená licence pro 1 počítač

4.5 Shrnutí technického návrhu pro část C1

Všechny prvky, které jsou nutné umístěny v lokalitě C1 jsou povinné pro provoz bezdrátové sítě. Prvky, které by mohly ohrozit chod celé sítě jsou zálohovány tak, aby v případě výpadku některého z nich nebyla omezena funkčnost celé sítě.

Mezi volitelné součásti jsou zahrnuty prvky, které lze dokoupit a využívat v případě nekompatibility klientských zařízení nebo požadavků na další služby bezdrátové sítě jako např. lokalizace nebo IP telefonie. Některé prvky jsou taktéž zálohovány pro případ výpadku tak, aby daná služba nebyla omezena.

4.5.1 Povinné součásti pro pokrytí lokality C1

Název	Počet kusů
Přístupový bod LAP1131AG	140
Síťový přepínač C3560 s 24 porty PoE	15
SFP modul pro připojení k optické síti	15
Kontrolér pro bezdrátovou síť WLC4404 – 100 licencí	2
Kontrolér pro bezdrátovou síť WLC4402 – 50 licencí	1
SFP modul pro připojení k metalické síti	10
Cisco Wireless Control System (WCS) – Základ	1
WCS 100 location licencí	1
WCS 50 location licencí	1
Cisco Secure Access Control Server Solution Engine (ACS) (Autentizace pomocí EAP-FAST a PEAP)	2
Embedded server s OS Windows 2003 server pro WCS	1

4.5.2 Volitelné součásti

Název	Počet kusů	Využití
Cisco WLAN Location Appliance	2	K lokalizaci uživatelů nebo vybavení v reálném čase
Software AeroScout nebo PanGo	1	Software k určení pozice uživatelů nebo vybavení
RFID aktivní čip		Aktivní čip k označení zaměstnanců nebo vybavení nemocnice
Call manager (Cisco Call manager)	1	Server pro IP telefony
Cisco Hlasová brána	1	Slouží k převodu z IP telefonie na analogovou linku – k propojení s analogovou ústřednou
Cisco Wireless IP Phone 7921G		Bezdrátový IP telefon pro pásmo 2,4 Ghz a 5 GHz
Cisco Secure Services Client		Klient 3. strany pro autentizaci metodou EAP-FAST na Windows 2000 / XP (pro použití s jinými kartami než Intel a Cisco)

5 Závěr

V současné době mohu shrnout jen malou část práce. Informace, které uvádím v semestrální části diplomové práce jsou informace, které používám dnes a denně. Projekt, který zde prezentuji je však něčím výjimečný. Je to nejen největší projekt, který jsem navrhoval, ale je také jeden ze tří největších projektů v České republice. Žádný z podobných projektů v ČR nebyl doposud realizován v plném rozsahu (většinou z něj byla odstraněna část pro lokalizaci). Proto také doufám, že podobný osud nepostihne i tento projekt a zvláště že bude realizován do konce mého studia na FIT.

Literatura

[1] Alexander Bruce, 802.11 Wireless Network Site Surveying and Installation, Cisco Press, 2005.

[2] David Castenada, O.M.Aladair, C.Vinckier, *Business Case for Enterprise-Class Wireless LANs*, Cisco Press, 2006

[3] Různí autoři, *Datasheet's k produktům Cisco Unified Wireless Network*

[4] Různí autoři, *Prezentace pro partnery Cisco*

[5] Různí autoři, *Prezentace firmy Extricom*