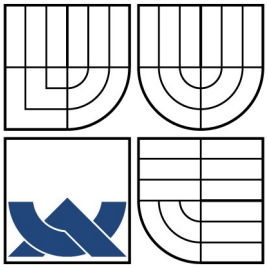
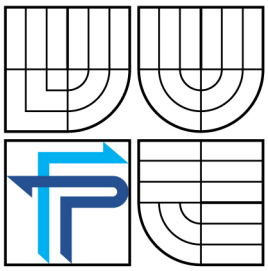


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUT OF INFORMATIC

PROBLEMATIKA BEZDRÁTOVÝCH SÍTÍ

WIRELESS NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — DUŠAN BRADÁČ
AUTHOR

VEDOUCÍ PRÁCE — DOC. ING. MILOŠ KOCH CSC.
SUPERVISOR

BRNO 2009

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

ANOTACE BAKALÁŘSKÉ PRÁCE:

Tato práce se zabývá problematikou bezdrátových sítí. Navrhuje výstavbu přístupového bodu (hledání místa, ekonomickou část a technickou část). Následně navrhuje řešení klientských stanic (typ zařízení, způsob instalace, finanční a technickou část). A v poslední řadě se zaměřuje na servisní činnost ve smyslu údržby a renovace jak přístupového bodu, tak klientské části.

ANNOTATION:

This document generally concerns of wireless networks. This job suggest building-up access point (surching for the place, economic part and technical part). Consequently suggest solutions clients stations (type of facilities, way of installations, financial and technical parts). Lastly it focus on servis in sence of repairs and renovation both access point and clients part.

KLÍČOVÉ SLOVA:

wi-fi, WEP, WPA, Access point, IEEE 802.11, VPN, zabezpečení

KEYWORD:

wi-fi, WEP, WPA, Access point, IEEE 802.11, VPN, security

BIBLIOGRAFICKÁ CITACE PRÁCE:

Bradáč, D. Problematika bezdrátových sítí. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2009. 35 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. 121/200 Sb. O právu autorském a o právech souvisejících s právem autorským).

V Brně dne:

……

podpis

OBSAH:

1) ÚVOD:

V dnešní době, kdy je vše závislé na počítačích a internetu nalezneme mnoho způsobů, jak se k intenetu připojit. Jednou z nejrozšířenějších možností se stal tzv. bezdrátový přenos dat. Ve stručnosti jde o spojení klienta s poskytovatel za pomocí bezdrátové sítě, neboli vzduchem bez tažení jakéhokoliv kabelu. Tento druh připojení se stal velmi žádaným z důvodu velkého množství poskytovatelů, což zlepšuje šanci na nalezení pro nás nejvhodnějších podmínek připojení, dále také kvůli své dostupnosti, protože šance na to, že by některý dům ve městě nebyl pokryt signálem alespoň jednou firmou je velmi malá. Nemusíme být tedy vázáni na možnost připojení jen těch míst, kde jsou natahané kabely např. od kabelové televize. Další skvělou možností využití bezdrátového přenosu je v dnešní době připojení notebooků. Jelikož totiž všechny moderní notebooky mají v sobě zabudovanou bezdrátovou kartu, tak se nám naskýtá možnost připojit náš notebook za pomocí bezdrátové sítě a tím nám odpadne zbytečné tahání kabelů přímo až k počitači a tím jecho fixní umístnění na jednom místě.

2) VYMEZENÍ PROBLÉMU A CÍLE PRÁCE:

V této práci se budu zabývat problémem, kdy se firma poskytující internetové služby rozhodne rozšířit pole působnosti a nebo tato firma teprve vzniká a řeší problém s pokrytím vybraného města bezdrátovou sítí. Zaměřím se tedy na problém, jak z místa, kde firma sídlí dostaneme pomocí bezdrátového přenosu internet na požadované místo. Dále budu řešit probém výstavby přístupového bodu na tomto místě pro šíření signálu ve vybraném městě. Poté se zaměřím na řešení klientských stanic samotných a to jak už na připojování za pomoci kabelu, tak i domácí WiFi sítě. Také se podívám na problémy s rušením a bezpečností bezdrátových sítí. A v poslední řadě se budu zabývát servisem jak přístupového bodu, tak klientských stanic.

3) TEORETICKÁ VÝCHODISKA PRÁCE:

3.1. Frekvenční pásma:

V dnešní době máme na výber více frekvenčních pásem, ve kterých můžeme přenášet data, takže by jsme se měli v první řadě rozhodnout, které z těchto pásem budeme my využívat. Máme na výběr pásmo 2,4GHz, 5GHz a 10GHz. Tyto tři by se dali považovat za nejrozšířenější, existujou i další, ale ty nás teď nebudou zajímat, protože pro ty už by jsme potřebovali speciální licenci. Kdežto tyto pásma jsou tzv. bezlicenční.

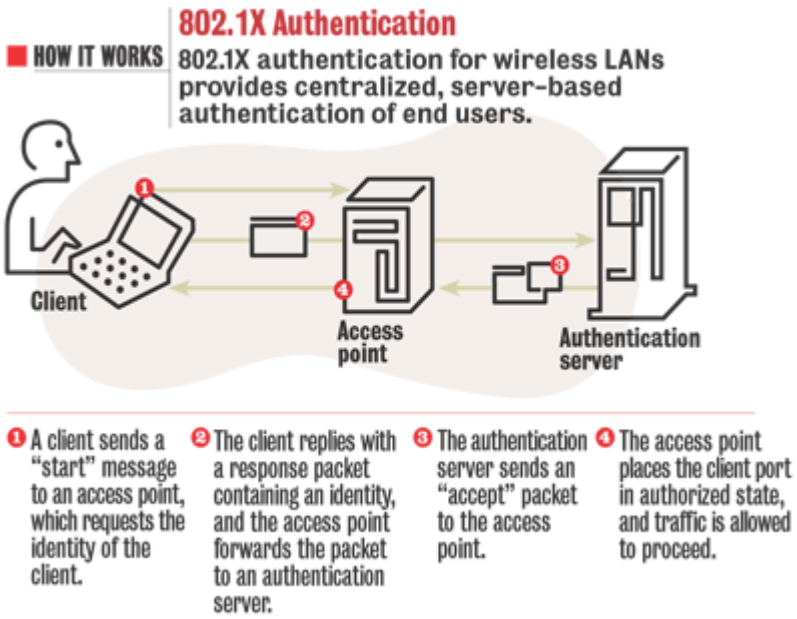
Pokud chceme, aby naše firma měla dobré jméno, málo reklamací a servisů, tak by jsme měli rovnou pásmo 2,4GHz zavrhnout. Je to z toho důvodu, protože toto pásmo už je zastaralé a v některých městech už je přehlcené. Na tomto pásmu můžeme využívat pouze 13 kanálů pro přenos dat a pokud se objeví dvě zařízení pracující na stejném kanálu, tak se objevuje vzájemné rušení.

Zbyly nám tedy dvě pásma a to 5GHz a 10GHz. Co se týká přístupových bodů, já by jsem se přikláněl k použití pásma 10GHZ, protože zvládá větší přenos dat a tím pádem se jen tak nepřetíží. Také se dá spojit na větší vzdálenosti a tím pádem můžeme spojit i dvě velmi vzdálená města. Na spojení přístupového bodu a klientské stanice nám postačí pásmo 5GHz, které má oproti pásmu 2,4GHz kanálu mnohem více a tím pádem je šance, že by nás někdo rušil opravdu malá a když už by se to stalo, tak můžeme přepnout na jiný kanál.

Až nám pásmo 10GHz nebude stačit, můžeme přejít i některé z licencovaných pásem, například na pásmo 11GHz. V tom případě ale budeme muset požádat nějakou firmu, která se tím zabývá, aby nám spoj v tomto pásmu vybudovala. Navíc budeme muset zaplatit za licenci, díky které budeme moci toto pásmo využívat.

3.2. Způsob vedení uživatelů:

Dalším důležitým faktorem určitě bude to, jakým způsobem si budeme vést seznam klientů. Nejjednodušší způsob a při tom určitě i nejefektivnější bude zavedení RADIUSU (*Remote Authentication Dial In User Service),* který nám velmi usnadní práci s klientskými účty. V tomto RADIUSU si velmi šikovně nastavíme pro danného uživatele přihlašovací jméno a heslo pomocí kterého se bude tento uživatel připojovat na naši síť. Také si zde nastavíme do jaké rychlostní skupiny bude uživatel patřit, což znamená, jakou maximální přenosovou rychlost může docílit. Tím získáme velmi dobrý přehled o všech zákaznících, jejich uživatelských jménech a heslech, rychlostech a také jejich přidělených IP adresách atd. Samozřejmě by se to dalo udělat i bez tohoto RADIUSU, ale tím by jsme ztratili dokonalý přehled o všem, tudíž by bylo nejlepší, hned v počátcích implementovat tento RADIUS a tím si do budoucna ulehčit práci.



RADIUS systém

3.3. Síla antén:

Při našem rozhodování, jaké antény použijeme na náš přístupový bod a hlavně u klientských stanic, nesmíme zapomenout na sílu antén. Ta se udává v decibelech (dB) a nejrozšířenější jsou antény o síle 13-23 dB. Nám bude toto rozmezí také stačit, protože pokud ani s anténou o síle 23 dB nebudeme mít u zákazníka signál, je lepší tuto přípojku nerealizovat, kvůli velkým problémům se signálem. Při zhoršeném počasí by mohl mít tento zákazník velké problémy se stabilitou připojení.

3.4. Standard IEEE 802.11

Standard pro bezdrátové sítě IEEE 802.11 vznikl v červenci roku 1997 a ke své činnosti využívá bezlicenční pásmo od 2,4 do 2,4835 GHz. Maximální přenosová rychlost definovaná tímto standardem (2 Mbit/s) byla nedostačující a stejně tak se ukázalo být nedostačující i zabezpečení přenosu. Proto k původnímu standardu vzniklo několik nových doplňků, které jeho nedostatky upravují.

3.4.1 Dopňky standardu IEEE 802.11

IEEE 802.11a - Doplněk IEEE 802.11a byl schválen v roce 1999 a na rozdíl od IEEE 802.11 pracuje v pásmu 5 GHz s výrazně vyšší přenosovou rychlostí - 54 Mbit/s. Pro její dosažení se poprvé v paketových komunikacích používá ortogonální multiplex s kmitočtovým dělením (*Orthogonal Frequency Division Multiplex*, OFDM), který se dosud používal pouze ve systémech jako DAB (*Digital Audio Broadcasting*) nebo DVB (*Digital Video Broadcasting*) určených pro distribuci digitálního zvuku a videa. Výhoda IEEE 802.11a oproti původnímu standardu není pouze ve vyšší rychlosti, ale také v použitém kmitočtu, protože kmitočtové pásmo 5 GHz je méně vytížené než pásmo 2,4 GHz a také dovoluje využití více kanálů bez vzájemného rušení (IEEE 802.11a nabízí

až osm vzájemně nezávislých a nepřekrývajících se kanálů).

IEEE 802.11b - Doplněk IEEE 802.11b vznikl v roce 1999 a poskytuje vyšší přenosové rychlosti v pásmu 2,4 GHz, a to až 11 Mbit/s. Pro jejich dosažení využívá nový způsob kódování, tzv. doplňkové kódové klíčování (*Complementary Code Keying*, CCK) s použitím DSSS (*Direct Sequence Spread Spectrum*) na fyzické vrstvě. Doplněk specifikuje, že podle momentálního rušení prostředí se dynamicky mění rychlost: 11 Mbit/s, 5,5 Mbit/s, 2 Mbit/s či 1 Mbit/s.

IEEE 802.11c - Tento doplněk řeší práci komunikačních mostů (*Bridge*) v rámci podvrstvy MAC (*Media Access Control*) a doplňuje mezinárodní normu IS 10038 (IEEE 802.1d) o transparentních mostech. Doplněk byl schválen v roce 1998.

IEEE 802.11d - Doplněk IEEE 802.11d upravuje IEEE 802.11b pro jiné kmitočty s cílem umožnit nasazení těchto sítí v místech, kde pásmo 2,4 GHz není dostupné. Doplněk byl schválen v roce 2001.

IEEE 802.11e - Doplňuje podporu pro kvalitu služeb (*Quality of Service*, QoS) pro zajištění přenosu hovorového signálu, obrazu apod. IEEE 802.11e doplňuje sítě definované IEEE 802.11a/b/g a nahrazuje stávající metody pro přístup k médiu: DCF (*Distributed Coordination Function*) a PCF (*Point Coordination Function*). Nově použité přístupové metody jsou: EDCF (*Enhanced DCF*) a HCF (*Hybrid Coordination Function*). Doplněk navíc zajišťuje zpětnou kompatibilitu se zařízeními, které nejsou podporou pro QoS vybaveny.

IEEE 802.11F - Doplněk IEEE 802.11F vylepšuje mechanismus předávání stanic (*Roaming*) při přechodu mezi dvěma rádiovými kanály nebo z jedné sítě do sousední s připojením k jinému přístupovému bodu. Protokol IAPP (*Inter-Access Point Protocol*) umožňuje spolupráci přístupových bodů od různých výrobců. Doplněk byl schválen v roce 2003.

IEEE 802.11g - Dopněk IEEE 802.11g je obdobou IEEE 802.11a s tím rozdílem, že je specifikován pro pásmo 2,4 GHz, stejně jako IEEE 802.11b. Pro

dosažení vyšší rychlosti, až do 54 Mbit/s, se používá na fyzické vrstvě OFDM, a navíc se používá DSSS pro zpětnou kompatibilitu s IEEE 802.11b. Pro modulaci se používá podle hodnoty odstupu signálu od šumu QPSK, BPSK, 16-QAM či 64-QAM. Podporované rychlosti v závislosti na modulaci jsou následující: 54 Mbit/s (64-QAM), 48, 36 a 24 Mbit/s (16-QAM), 18 a 12 Mbit/s (QPSK), 9 a 6 Mbit/s (BPSK). Další rychlosti jsou stejné jako u 802.11b: 11 Mbit/s (CCK), 5,5Mbit/s (CCK), 2 Mbit/s (DQPSK) a 1 Mbit/s (DBPSK). Doplněk byl schválen v roce 2003.

IEEE 802.11h - Doplněk IEEE 802.11h vylepšuje řízení využití kmitočtového spektra (výběr kanálu a řízení vysílacího výkonu). Evropští regulátoři požadují pro schválení produktů IEEE 802.11a použití dynamického výběru kanálu (*Dynamic Channel Selection*) pro venkovní i vnitřní komunikaci a řízení vysílacího výkonu (*Transmit Power Control*) u zařízení pracujících v pásmu 5 GHz. Doplněk schválený v roce 2003 doplňuje právě tyto parametry do IEEE 802.11a.

IEEE 802.11i - Doplňuje lepší zabezpečení IEEE 802.11 sítí. Místo WEP (*Wired Equivalent Privacy*) používá nový způsob šifrování AES (*Advanced Encryption Standard*). Doplněk byl schválen v roce 2004.

IEEE 802.11j - Doplněk schválený v roce 2004 umožňuje použití pásma 4,9 – 5 GHz pro nasazení WLAN v Japonsku.

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

IEEE 802.11m - Dokumenty vydané ostatními skupinami jsou skupinou IEEE 802.11m kontrolovány a jsou upravovány případné nesrovnalosti nebo chyby v původních specifikacích.

IEEE 802.11n - Skupina IEEE 802.11n studuje různé možnosti nastavení parametrů fyzické vrstvy a MAC podvrstvy pro zvýšení datové propustnosti. Mezi tyto možnosti patří použití více antén, změny kódovacích schémat a změny MAC protokolů. Aktuální cíl skupiny je přenosová rychlost minimálně 100 Mbit/s nad MAC vrstvou. Navíc má IEEE 802.11n zajistit vyšší dosah se zachováním co největší rychlosti a zvětšit odolnost proti rušení.

IEEE 802.11p - První podpora mobility pro připojení rádiových stanic v automobilech k pevným bezdrátovým přístupovým bodům.

IEEE 802.11r - Doplněk MAC pro rychlejší předávání uživatelů (*Roaming*) mezi přístupovými body v rámci ESS (*Extended Service Set*) pro aplikace v reálném čase (např. pro telefonní služby).

IEEE 802.11s - Zavádí podporu topologie tzv. mesh sítě s použitím automatické konfigurace. Každý klient bude zároveň přístupovým bodem a naopak. Tato technologie se označuje jako multi-hopping (přenos přes několik mezilehlých zařízení).

IEEE 802.11.2 - Návrh pro vytvoření souboru metrik, metodik pro měření a podmínek pro testování zařízení WLAN.

IEEE 802.11u - IEEE 802.11u specifikuje spolupráci s externími sítěmi.

IEEE 802.11v - IEEE 802.11v vytváří jednotné rozhraní pro management zařízení v bezdrátové síti. Stanice budou moci provádět funkce managementu zahrnující monitoring a konfiguraci buď centralizovaně, nebo distribuovaně prostřednictvím mechanismu na druhé vrstvě. Přispívá také k rekonfiguraci stávající MIB (*Management Information Base*), která obsahuje informace o měření kvality média.

IEEE 802.11w - Rozšíření stávající MAC vrstvy o mechanismy na podporu integrity dat, autenticity zdroje dat, utajení dat a ochrany před útoky typu replay pro vybrané rámce určené pro management. Cílem je zvýšení zabezpečení rámců pro management.

Standard IEEE 802.11 se dočkal mnoha doplňků a podle všeho se jich ještě pár objeví, protože se jedná o čím dál tím víc využívanou službu.

3. Radius

Radius (*Remote Authentication Dial In User Service*, česky *Uživatelská vytáčená služba pro vzdálenou autentizaci*) je vlastně AAA protokol (*autentizace, autorizace a správa účtů*) používaný pro správu a přístup k síti. Můžeme ho používat jak lokálně tak i jako vzdálený přístup. U některých typů připojení je vyžadováno uživatelské jméno a heslo, které je posláno do tzv. NAS službou (Network Access Server) přez službu PPP (Point-to-Point Protocol). Poté je předána RADIUS serveru k ověření pravosti dat, pokud jsou data správná, RADIUS server přidělí IP adresu nebo rozsah IP adres a také další nastavení pro daný účet. Například rychlost, omezení na stáhnutá data atd.

RADIUS byl původně vyvinut společností Livingston Enterprises pro jejich PortMaster série Network Access Servers a později (1997) zveřejněny jako RFC 2058 a RFC 2059 (současné verze jsou RFC 2865 a RFC 2866). Nyní existuje několik komerčních a open-source RADIUS serverů. Vlastnosti se liší, ale většina umožňuje dohledávat uživatele v textových souborech, LDAP serverech, různých databázích a podobně. Účtovací informace se mohou zapisovat do textových souborů, různých databází, přeposílat na externí servery a podobně. SNMP je často používáno pro vzdálené monitorování. RADIUS proxy servery jsou používány pro centrální správu a mohou přepisovat RADIUS pakety za běhu (z bezpečnostních důvodů, nebo pro překlady mezi dialekty jednotlivých výrobců).

4) ANALÝZA PROBLÉMU A SOUČASNÉ SITUACE:

4.1 Seznámení s firmou:

V mojí práci se nezaměřím na konkrétní firmu, ale použiji fiktivní firmu, která mi pomůže názorně předvést veškeré problémy a jejich řešení. Řekněme, že máme firmu poskytující internetové služby, která je na trhu zhruba rok. Tato firma je zisková, ale její zisk není nějak závratný, protože nemá tolik zákazníků. Tím pádem se firma rozhodne, že se pokusí expandovat do sousedního města, aby zvýšila svůj počet klientů.

4.2. Rozbor požadavků firmy:

Firma by velmi ráda rozšířila své pole působnosti ne vedlejší města, čímž by získala více zákazníků a tím i vyšší zisky. Hlavním požadavkem firmy je, co nejefektivněji pokrýt svým signálem vybrané město a to za pomoci co nejmenšího počtu přístupových bodů. Dále aby provoz tohoto přístupového bodu byl co nejméně nákladný finančně i co se týče údržby. Dalším požadavkem firmy je instalace klientských stanic tak, aby jejich finanční část nebyla příliš velká, ale aby zařízení bylo spolehlivé s co možná nejméně servisy. Dále by firma zavedla nějaký systém, díky němuž by v případě servisu bylo vše vyřízeno rychle a spolehlivě.

5) NÁVRH PŘÍSTUPOVÉHO BODU:

5.1. Vhodné místo:

Jelikož jsme se rozhodli používat pro šíření našeho signálu bezdrátovou sít, musíme najít vhodné místo, kam umístníme náš přístupový bod neboli Access point (dále jen AP). Pokud se jedná o vesničku, nebo menší město, můžeme se zkusit porozhlédnout po nějakém blízkém kopci, na kterém můžeme často nalézt staré vodárny a podobné zařízení. Pokud nic takového není, tak je třeba zkusit štestí na nejvyšší budově ve městě, což z pravidla bývají školy nebo úřady. V některých případech můžeme narazit i na několika patrovou bytovku, která bývá nejvhodnějším místem.

Pokud se jedná o nějaké větší město, budeme se zřejmě muset porozhlédnout po více místech, protože z jednoho místa asi zteží pokryjeme celé město. Většinou ale stejně platí pravidlo, že nikdy nepokryjeme 100% část vybraného města. Vždy se najde nějaké hluché místo, ke kterému se náš signál prostě a jednoduše nedostane. Pokud ale pokryjeme naším AP alespoň 80% města, tak jsme náš úkol splnili.

Nejdůležitější podmínkou při hledání našeho nového přístupového bodu je určitě to, zda-li teda z něj je vidět větší část města, ale hlavně také to, zda-li z něj máme přímou viditelnost na naši základnu, od kud bude náš internet příjmat. V případě přístupového bodu není ani tak důležité, abychom na naši základnu viděli pouhým okem, ale to, zda-li na cestě mezi naší základnou a novým přístupovým bodem není nějaká překážka jako například strom, budova atd.

V případě, že bychom měli v cestě nejakou tu překážku, máme ještě možnost zkusit se porozhlédnout ze všech možných míst na vybraném přístupovém bodě, nebo také můžeme postavit dost vysoký stožár na to, abychom se přez danou překážku dostali. Tento způsob řešení je většinou ale nepraktický a také i nemožný, protože majitel objektu nedovolí postavit na střeše obrovský stožár.

5.2. Spojení základny a nového AP:

Jakmile nalezneme vhodné místo pro náš nový AP s přímou viditelností na základnu, můžeme se pustit do výstavby spoje. Při budování takovéhoto spoje budeme potřebovat dva protikusy stejných antén pracujících v pásmu 10GHz. Jednu nainstalujeme na základnu a druhou na přístupový bod. Poté už nám stačí obě stranz na sebe zamířit tak, aby měli co nejlepší signál a tím i kvalitní přenos. Většina těchto 10GHz antén má ukazatel síly signálu, pomocí kterého je zaměřování vcelku jednoduché a postačí nám na něj zhruba hodinka.

5.1.1. Rodiný domek:

Pokud narazíme na rodiný domek, který je na velmi vhodném místě a zároveň je dost vysoký na to, aby z něj byla vidět větší část města, tak se můžeme pokusit postavit náš přístupový bod zde. Jelikož budeme muset nějak přesvědčit majitele tohoto domku, aby si nechal na něm udělat náš přístupový bod, budeme muset nabídnout nějake výhody. Nejčastěji se to řeší tak, že se danému člověku nabídne internet zdarma, dále se nechá namontovat počítadlo zpotřebované elektrické energie, abychom mohli doložit, kolik náš přístupový bod zpotřeboval energie a poté ji uhradit. Pokud s tímto bude majitel souhlasit, pak už tedy jen stačí nainstalovat naše antény. Instalaci provedeme tak, že nejlépe někam na půdu vyvedeme elektriku, do které následně zapojíme věškeré elektrické zařízení jako napájení pro naše antény, SWITCH atd. Tyto věcy umístníme do plastové krabice, kterou necháme na nějakém dobře dostupném místě, kvůli případným servisům. Dále veškeré vybavení, které na půdě nechame označíme nálepkou „majetek firmy XXX“, čímž zabráníme neoprávněnému vniknutí do našeho zařízení.

5.1.2. Školy, obecní uřady, kostely atd.:

Pokud se nám žádný rodiný domeček nehodí, což býva velmi často, tak příjdou na řadu budovy jako škola, obecní úřad a někdy i například kostel. V případě školy a úřadu se většinou postupuje stejně jako u rodiného domku. Nabídne se internet zdarma a plus placení zpotřebované energie. Co se týče kostela, tak tady je to složitější, zde

budeme muset zřejmě navrhnout nějaký plán řešení, který poté předložíme správci daného kostela. On tento plán přednese na vyšších místech a pokud se vše schválí, tak nám nic nebrání ve výstavbě našeho přístupového bodu. Jedinou podmínkou u takovýchto budov bývá, aby antény nebylo příliš vidět, což se dá obvykle udělat tak, že naše antény umístníme do prostoru se zvony a nasměřujeme je tak, aby vysílali signál přes okenice. Nebo můžeme naše antény také natřít stejnou barvou, jakou má kostel a tím pádem budou splívat.

5.3. Finanční stránka:

V případě přístupového bodu se nám nevyplatí šetřit kde se dá, ba naopak. Je lepší investovat do zařízení více peněz, protože nám to pak velmi často ulehčí servis. Co se týče spoje mezi náší domovskou základnou (sídlo firmy) a přístupovým bodem, velmi dobré řešení bývá použití SVM zařízení (SDM10-DE), které můžou přenášet rychlost 25Mbps (Megabit per second), což by nám mělo pro začátek stačit. Pokud si ale myslíme, že budeme potřebovat více, můžeme použít zařízení ALCOMA, které dosahují mnohem vyšších přenosových rychlostí. V našem pásmu 10GHz je to až 155 Mbps. Je tedy na nás, jak moc velkou rychlost budeme přenášet a podle toho se rozhodnout, jaké zařízení pořídit. Pokud se rozhodneme pro SVM zařízení, mluvíme tu o částce něco kolem 200 000,-Kč, zatímco pokud se rozhodneme pro ALCOMA zařízení, cena se nám vyšplhá zhruba na dvojnásobek.

SVM zařízení

ALCOMA zařízení

5.4. Technická stránka:

Jak už jsem napsal výše, pro přístupový bod bude nejvhodnější použít pásmo 10GHz. Je tím myšlono spojení našeho hlavního spoje, většinou sídlo firmy a daného přístupového bodu. Pásmo 10GHz použijeme proto, protože umí přenášet vyšší rychlosti a hlavně je umí přenášet na mnohem větší vzdálenosti. Pro samotné šíření signálu po vybraném městě už použijeme pásmo 5Ghz, protože by bylo již zbytečné

vyhazovat tolik peněz za 10Ghz zařízení. Pásmo 5GHz nám bohatě postačí. Na šíření

signálu použijeme jednu nebo dvě všesměrové antény a dále sektorové antény. Někdo

by si mohl říct, na co nám budou dvě stejné všesměrové antény, ale musíme taky myslet na to, že každá tato všesměrová anténa bude připojena k nějakému typu zařízení, které v sobě bude mít nastavení našeho přístupového bodu a na tyto zařízení nesmíme připojit neomezené množství zákazníků. Ono by to teoreticky šlo, ale daný přístupový bod by byl potom velmi přetížený a my by jsme nemohli našim zákazníkům zaručit tu rychlost, kterou jsme slibíli. Pro zařízene s nastavením našeho acces pointu bych doporučil zařízení MikroTik, má velice pokročilé rozhraní a opravdu mnoho funkcí. U sektorových antén už nemusíme dávat dvě stejné na jeden směr, protože je velmi malá pravděpodobnost, že by jsme všechny zákazníky připojovali na jeden access point. Použijeme jich zkrátka tolik, abychom pokryli všechny části města.

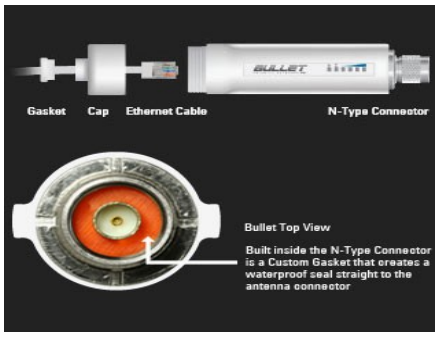
Všesměrová anténa

Sektorové antény

6) KLIENTSKÁ STANICE:

6.1. Vhodný typ zařízení:

Co se týka klientské stanice, tak tady by bylo asi rozumné vybýrat typ zařízení podle situace. Pokud budeme například připojovat zákazníka, který je dost vzdálen od našeho přístupového bodu, tak by bylo asi rozumné, aby tento zákazník měl nainstalováno nějaké výkonější zařízení, protože by jinak mohli nastat komplikace a to určitě nechceme. Naopak v případě zákazníka, který je od našeho přístupového bodu vzdálen velmi málo, by zas bylo hloupé dávat nějaké výkonné zařízení, protože by nám zaprvé bralo většinu signálu a za druhé by to bylo zbytečné. Rozhodně by pro nás bylo nejideálnější, kdybychom našli takové zařízení, které se dá libovolně měnit podle toho, jak my zrovna potřebujeme. Zde bych doporučil zařízení od firmy Ubiquiti, která má velký výběr sortimentu. Například nám by stačilo zařízení od této firmy s označením Bullet, které se dá připojit pomocí PigTailu (spoj mezi samotnou anténou a zařízením) k libovolné anténě.



Bullet

6.1.1 Rodiný domek:

V případě připojení rodiného domku musíme pouze zjistit, zda-li je z tohoto domu viditelnost na náš apod. Pokud by viditelnost nebyla, můžeme se ještě pokusit změřit sílu signálu, ale podle všeho nebude možné přípojku na tomto domku realizovat. V případě, že je viditelnost nebo síla signálu dobrá, bude nám už jen stačit, abychom nalezli vhodné místo na umístnění naší antény. V ideálním případě narazíme na dům, který má na vhodném místě anténí stožár, takže naši anténu umístníme právě na něj. V tomto případě ale musíme brát ohledet na jednu zásadní věc a to sice problém s rušením televizního signálu. Tento problém sice nenastává často, ale přesto jsou případy, kdy se rušení objevilo a proto bude lepší, když v případě, že naši anténu umístňujeme na anténí stožár zkontrolovat kvalitu TV obrazu. Jestliže bude vše v pořádku a žádné rušení se neobjeví, stačí už jen od naší antény svézt UTP kabel nejlépe přímo do místnosti, kde bude počítač. Zde zapojíme PoE (Power on Ethernet), což je napájení naší antény a z ní už jen vyvedeme UTP kabel k počítači. V dnešní době už ale nové domy anténí stožáry moc nemají, takže budeme muset hledat jiná řešení. Můžeme například využít komínu, na který navrtáme nějaký typ konzole a na ni umístníme naši anténu. V tomto případě

ale musíme zákazníka informovat o možném riziku, kdy jelikož budeme zasahovat do struktury komínu, můžeme narušit jeho funkčnost atd. Cesta k počítači je potom stejná jako u instalace an anténí stožár.

6.1.2 Vícebytové domy:

V případě, že realizujeme přípojku v domě, kde bydlí více lidí, se nám nevyplatí dávat samostatnou anténu pro každého nájemníka zvlášt. Proto využijeme možnosti, že některé dražší zařízení jsou schopny na sebe připojit více uživatelů, aniž by se navzájem nějak ovlivňovali. Každý zákazník bude mít svoji vlastní rychlost, IP adresu a své vlastní speciální uživatelské jméno. Při instalaci přípojky na takovýto dům musíme postupovat trochu jinak než v případě obyčejného rodiného domku. Naši anténu

umístníme se svolením správce domu bud na anténí stožár nebo opět na komín. Od antény svede UTP kabel tentokrát ne až k počítači, nýbrž na půdu. Zde musíme nějakým

způsobem získat elektrickou zásuvku. Pokud už tam nebude, budeme ji muset vytáhnout ze společných rozvodů. Dále na půdě nejlépe do plastové krabice umístníme PoE a tentokrát ještě navíc SWITCH, což je zařízení pro rozbočení signálu do více počítačů. Pak už jen vyvedeme z tohoto SWITCHE jednotlivé kabely do všech bytů, které od nás budou chtít připojit k internetu.

6.2. Způsob připojení

Při připojování zákazníků narazíme na další malý problém. A to sice ten, že jeden zákazník bude chtít připojit jeden stolní PC, další bude chtít připojit notebook a nebo někdo bude chtít připojit více počítačů jak stolních tak notebooků. Musíme být tedy připraveni an všechno a musíme počítat i s tím, že budeme síťovat i několik počítačů.

6.2.1 Kabeláž

Pokud se zákazník rozhodne, že bude chtít připojit PC jen kabelem, nastává nám další problém a to ten, jak UTP kabel od naší antény dostaneme až k počítači. Zde existuje několik možností. Pokud jde jen o jeden PC, je nejlepší svézt kabel od antény přímo až k PC, kde zapojíme PoE a od tud kabel přímo až k PC. Nejčastější způsob vedení kabelu bývá přez husý krky, kdy se velmi jednoduše dostaneme s kabelem až na půdu, kde už není takový problém pomocí vedení kabelu podél trámu dostat náš kabel až na místo, kde je umístněna anténa.

Ovšem můžeme narazit i na objekt, kde husý krky nejsou. Budeme tedy muset hledat jiné řešení. V případě, že místnost s počítačem je hned pod půdou, stačí nám vyvrtat otvor ve stropě, kterým náš UTP kabel povedeme. Jestliže by nebylo možné otvor ve stropě udělat, nebo místnost není přímo pod půdou, existuje ještě nouzové řešení. Můžeme kabel spustit přímo ze střechy objektu a pomocí uchytů jen přichytit k fasádě a otvorem ve zdi nebo případně okně se dostat do místnosti s PC.

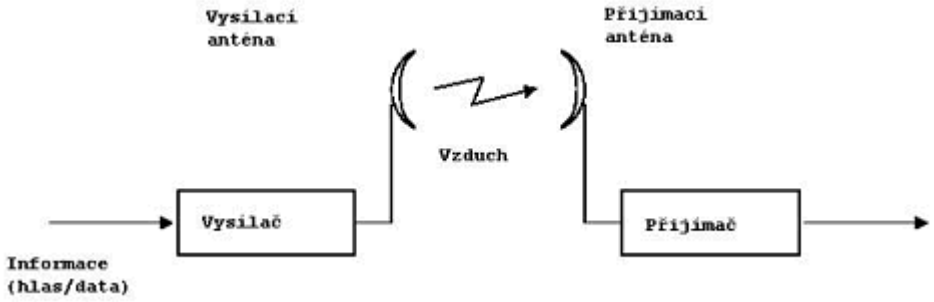
6.2.2. WiFi

Ve většině případů budeme ale muset připojit notebook nebo stolní PC za pomoci bezdrátové sítě WiFi. Při tomto řešení se nám vcelku výrazně usnadňuje práce a to proto, protože nemusíme dostat kabel přímo až do místnosti s PC. Stačí nám, pokud tam tedy je, na půdě elektrická zásuvka. Poté už jen instaluje WiFi router na místo, které je zhruba středem objektu, kvůli pokrytí všech částí.

6.2.2.1 Dosah WiFi sítě

První otázka uživatele, který uvažuje o nasazení bezdrátové sítě, je: "Na jakou vzdálenost to vlastně funguje?" A odpověď? Není úplně jednoduchá a může se v závislosti na konkrétních podmínkách výrazně lišit. Na obrázku je vidět typický rádiový

systém. Vysílaná informace jde z vysílače do antény, následně pak v podobě elektromagnetických vln vzduchem do přijímače, kde je informace demodulována do své původní podoby.



Jelikož jde o přenos dat bezdrátově, musíme myslet na to, že každá překážka oslabuje sílu signálu. Například pokud budeme mít tlusté betonové zdi, může se nám stát, že signál na WiFi chytneme jen v okruhu pár metrů od routeru. Nemáme-li ale nějaký opravdu rozlehlý objekt, nebývá problém pomocí jednoho WiFi routeru pokrýt celý objekt. V některých místech samozřejmě nebude signál nejsilnější, ale ze zkušeností vím, že WiFi spojení funguje celkem spolehlivě i na 10% síly signálu.

6.2.2.2 Zabezpečení WiFi sítě:

Bezdrátová síť je na tom stejně jak počítač či router (nebo jiné síťové zařízení). Po zakoupení a instalaci není bezpečně nainstalována a je nutné ji dodatečně zabezpečit. Stejně jako například u routerů drátových, i ty bezdrátové jsou nainstalovány s "standardními" neboli defaultními hesly co dodává výrobce.

První krok zabezpečení je změna SSID (nýzev sítě) a nastavení nového přístupového jména a hesla a často i změna "defaultního" kanálu.

Neméně důležité je aktivování **WEP ochrany** - použití 128bitového zabezpečení

je doporučeno tam, kde máte karty podporující plných 128bitů. Každopádně postačí alespoň 40bitů. Bez ohledu na to, že WEP je "prolomitelný" je tato ochrana velmi důležitá. Aktivací WEP totiž zajistíte nemožnost volného anonymního přístupu "náhodným návštěvníkům" vaší sítě. WEP ochrana má možnost pouze hexadecimálního klíče, což znamená omezené množství znaků a také nemůžeme jako klíč použít slovo. Proto pokud budeme chtít mnohem složitější šifrování, budeme muset sáhnout po WPA

šifrování. Zde už můžeme mít v poctatě libovolně dlouhý klíč a hlavně můžeme použít i slova a ne jenom čísla.

WiFi routery často umožňují i **filtraci podle MAC adres** (adresa síťové karty "zadrátovaná" do hardware), takže v bezpečných sítích je dobré nastavit **seznam povolených MAC adres** - pokud "útočník" nebude mít tu správnou adresu, má smůlu. Zde ale můžete u větších sítí narazit na omezení počtu záznamů oprávněných MAC adres, nebo na složitost administrace na více routerech.

Pokud nastavíme tyto typy ochrany, mělo by to zamezit zneužití obyčejnými uživately. Pokud se na naši bezdrátovou sít bude chtít dostat někdo zkušený, zřejmě by po nějaké době uspěl, ale nemusíme se bát, protože šance na to, že by se do naší sítě někdo naboural je velmi malá.

6.2.2.3. Rušení

Bezdrátové sítě mají jeden velký problém a to ten, že vás může někdo rušit. Jelikož fungují na nějakém frekvenčním pásmu, kde je určitý počet možnych kanálů, tak se může stát, že dvě zařízení budou fungovat an stejném kanálu a tím pádem se budou navzáje ovlivňovat neboli rušit. U pásmá 2,4GHz, které se u WiFi routerů používá nejčastěji je toto rušení ještě výraznější. Pokud má například soused také WiFi router, který mu jede na stejném kanálu, tak se vám může velmi pravděpodobně stát, že se na vaší WiFi připojíte, ale síť bude velmi nestabilní a nebo velmi pomalá. Vaší jedinou možností je přeladit váš WiFi router na jiný kanál a doufat, že někdo další v okolí tento kanál už nevyužívá. Naštěstí u WiFi routerů není dosah až tak velký, aby vás mohl rušit například soused, co bydlí o tři domy vedle. Většinou vás může rušit jen nejbližší soused nebo soused naproti.

6.3. Finanční stránka

Co se týka finanční stránky u klientských stanic, tak v dnešní době seženeme opravdu velmi velké množství různých typů zařízení, takže bude už jen čistě na nás, co si vybereme a odzkoušíme v provozu. Cena se většinou pohybuje někde mezi 1000 – 5000,-Kč. V některých případech budeme nuceni postavit vlastní stožár na umístnění naší antény. V tom případě musíme počítat ještě s náklady na jeho výstavbu, což se pohybuje v rozmezí kolem 1000 – 4000,- Kč.

6.4. Technická stránka:

Z pohledu výstavby klientské stanice se budeme muset smířit s tím, že jelikož poskytujeme bezdrátový internet, tak všechny klientské stanice budou muset být umístněny někde ve venkovních prostorech, nejčastěji někde na střeše domu. Podmínkou bezdrátového připojení je totiž přímá vyditelnost na přístupový bod, tudíž nemůžeme antény instalovat do vnitřních částí domu.

7) SERVIS:

7.1. Způsob vedení zákazníků:

Pokud chceme mít rychlý a spolehlivý servis, budeme muset mít dobrý přehled o

zákaznících. Tudíž by bylo dobré si jednotlivé zákazníky vést v systemu například podle univerzálního uživatelského jména. Tím se nám ulehčí hledání zákazníka v systému a budeme mít velmi rychlý přehled o tom, co za zařízení daný zákazník má.

7.2. Způsob ohlášení závady:

Závadu zákazník ohlasí velmi jednoduše a to sice tak, že zavolá na naši firmu, uvede svoje celé jméno a adresu nebo svoje speciální uživatelské jméno. Jelikož se může stát, že zákazníkovy se porouchá naše připojení i mimo pracovní dobu, bylo by dobré mít například něco jako záznamník, na který zákazník nahraje svůj vzkaz a náš technik který bude mít pohotovost v daný den, si tento vzkaz co nejdříve vyposlechne a podle závažnosti problému ho začne řešit. Pokud se bude jednat o hlášení závady na přístupovém bodě, tak asi nejideálnější by bylo mít nějaký server, který bude hlídat všechny naše přístupové body a pokud by některý z nich přestal fungovat, tak by automaticky rozeslal například SMS všem technikům. Tím by bylo zajištěno, že se veškeré závady budou řešit velmi rychle a zvýší se spokojenost zákazníků.

7.3. Řešení problému

7.3.1 Probém na přístupovém bodě

Přístupový bod je pro nás velmi důležitý, pokud by přestal fungovat, ochromý to velmi výrazně naši síť. V situaci, kdy přístupový bod přestane fungovat, nebo-li spadne, musíme mít nějaký informační systém, který nás o tom informuje. Dá se to udělat pomocí již zmiňovaných SMS hlášení, ale určitě by bylo navíc ještě dobré, aby některý z našich servisních techniků měl pohotovost a sledoval průběžně dění na naší síti. V případě pádu našeho přístupového bodu by tedy mohl velice rychle reagovat a daný problém co nejrychleji vyřešit.

Někdy se může stát, že například vypadne jen proud na pár minut. V tomto případě by bylo zbytečné, aby náš servisní technik pokaždé jezdil kontrolovat náš

přistupový bod a proto bude nejrozumější, když náš AP připojíme ještě na baterie, které v případě výpadku proudu udrží alespon 30minut náš AP v chodu.

7.3.2. Problém na klientské stanici

Nejčastější servisy ovšem nebudou na našich přístupových bodech, ale na klientských stanicích. Je dobré tedy mít nějakou bezplatnou linku, kam můžou zákazníci v případě poruchy volat. Zhruba takových 80% problémů se dá vyřešit po telefonu na dálku. Našemu servisnímu technikovy stačí pouze uživatelské jméno klienta a podle toho si najde zařízení v systému, připojí se na něj a zjistí, zda-li je chyba někde na naší straně, nebo jestli náhodou není chyba na straně klienta například v zavirovaném PC. Velmi častým problémem bývají napájecí trafa k PoE, které se umí při velkých výkyvech napětí v elektrické síti přepálit a shořet. V tomto případě nám ovšem nezbývá nic jiného, než ke klientovi přijet osobně a napájecí zdorj vyměnit za nový.

Jelikož se naše firma snaží rozšířit do dalších měst, měli by jsme začít uvažovat o zvýšení počtu servisních techniků, protože čím dále od naší základny budeme mít pokrytí, tím složitější bude rychlý a spolehlivý servis. Proto by bylo dobré mít dostatek lidí na tuto funkci a vyvarovat se tak servisům trvajícím i několik dní nebo dokonce v nejhorším případě i týdnů.

8) ZÁVĚR:

Pokud se jako firma rozhodneme vybudovat nový přístupový bod pro rozšíření našeho pokrytí i na jiná města, musíme počítat s tím, že náklady na to nebudou malé, můžeme mít problém s nalezením vhodného místa, ale hlavně musíme počítat s tím, že budeme mít čím dál tím více servisu a proto by bylo asi dobré, abychom vyhledali nové

zaměstnance na pozici servisní technik. Dále se nám také zvednou náklady na údržbu našich spojů a zřejmě by jsme měli začít přemýšlet i navýšení naší kapacity rychlosti.

9) SEZNAM POUŽITÉ LITERATURY:

1) Zandl,P.: Bezdrátové sítě WiFi : praktický průvodce. Vyd. 1. Brno : Computer Press, 2003. 190 s. ISBN 80-7226-632-2

2) Barken,L.: Wi-Fi : jak zabezpečit bezdrátovou síť. Vyd. 1. Brno : Computer Press,

2004. 174 s. ISBN 80-251-0346-3

3) Brisbin, Shelly. Wi-fi : postavte si svou vlastní wi-fi síť.Praha: Neocortex, 2003. 248 s. ISBN 80-86330-13-3

4) MOLNÁR, Z. Efektivnost informačních systémů. 1. vyd. Praha: Grada, 2000. 142 s. ISBN 80-7169-410-X.75.

5) KÖHRE, Thomas. *Stavíme si bezdrátovou síť WI-FI*.
Vyd. 1. Brno : Computer Press, 2004. 295 s. ISBN 80-251-0391-9.

6) PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace : jak zabezpečit wi-fi, bluetooth, GPRS či 3G*. Vyd. 1. Brno : Computer Press, 2005. 179 s.
ISBN 80-251-0791-4.

10) SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ:

Frekvenční pásmo

2,4GHz

5GHz

10GHz

Access Point (přístupový bod)

RADIUS

Mbps

SWITCH

PoE

WEP

NAS

PPP

SEZNAM PŘÍLOH:

1) Přehled standardů IEEE 802.11

2) Fotky některých typů antén pro 5GHz

3) Porovnání odolnosti zapezpečení WEP a WPA

1) Přehled standardů IEEE 802.11

Standard	Rok vydání	Pásmo [GHz]	Maximální rychlost [Mbit/s]	Fyzická vrstva
původní IEEE 802.11	1997	2,4	2	DSSS a FHSS
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	OFDM
IEEE 802.11n	2009	2,4 nebo 5	600	MIMO
IEEE 802.11y	2008	3,7	54	

2) Fotky některých tzpů antén pro 5GHz

3) Porovnání odolnosti zapezpečení WEP a WPA

	WEP	**WPA**	**WPA2**
útok:	*odolnosť:*		
Man-in-the-middle	Dobrá	Lepšia	Najlepšia
Falošná autentizácia	Nedostačujúca	Najlepšia	Najlepšia
Na slabý kľúč	Nedostačujúca	Najlepšia	Najlepšia
Falšované pakety	Minimálna	Najlepšia	Najlepšia
Falošný prístupový bod	Minimálna	Lepšia	Lepšia