Bezdrátová síť v polouzavřeném prostředí

Jan Kasprzak, Fakulta informatiky MU Brno <kas@fi.muni.cz>

Abstrakt

Při budování počítačových sítí může být někdy překážkou nutnost pokládat metalickou nebo optickou kabeláž a takto „pevně“ připojovat síťová zařízení. Naštěstí existují technologie, pomocí kterých lze používat prostředky sítě i bez pevného kabelového připojení – bezdrátové sítě. *Cílem této přednášky je poskytnout jemný úvod do problematiky bezdrátových sítí a popsat jednu konkrétní bezdrátovou síť, se zaměřením na bezpečnostní rizika použité technologie.*

1. Bezdrátové sítě

Pro konstrukci bezdrátových sítí je k dispozici několik druhů přenosových cest, využívajících nějakou formu elektromagnetických vln:

- **Rádiové sítě** – obvykle v pásmu krátkých vln, příkladem jsou amatérské rádiové sítě (*hamradio*).
- **Mikrovlnné sítě** – frekvence nad 100 MHz. Tyto sítě mají v případě potřeby dobrou směrovost, takže je možno budovat dvoubodové spoje bez rizika vzájemného rušení i ve stejném frekvenčním pásmu. Naopak nevýhodou je špatná průchodnost překážkami (budovy, zemský povrch).
- **Optické spoje** – obvykle realizovány laserovým spojem, dvoubodové. Výhodou je přenosová rychlost až stovky Mbit/s. Nevýhodou je citlivost k atmosférickým vlivům (mlha, sníh, déšť).
- **Infračervené spoje** – podobné vlastnosti jako u optíckých, lepší odolnost proti mlze (ale nikoliv proti sněhu nebo dešti).

2. Mikrovlnné sítě

Omezujícím faktorem mikrovlnných sítí jsou frekvenční pásma, protože celková šířka pásma je omezená. Přidělování přenosových frekvencí v České republice má na starosti Český telekomunikační úřad (ČTÚ). Tento úřad přiděluje volné frekvence a zároveň určuje způsob jejich využití. Mikrovlnné sítě jsou buďto v tzv. *licenčních pásmech*, kde je daná frekvence v daném místě přidělena jen jednomu subjektu a je pro něj vyhrazena. Příklady licenčních pásem jsou pásma 3,5 GHz, 26 GHz a 28 GHz, využívaná pro sítě FWA (fixed wireless access) nebo pásma 900 MHz a 1800 MHz pro sítě GSM.

Pro volný provoz je vyhrazeno tzv. *bezlicenční pásmo* 2,4 GHz, které je možno využívat při omezeném výkonu vysílače na základě generálního povolení ČTÚ. Celková šířka tohoto pásma je 83 MHz (čili frekvence 2400–2483 MHz). Podobně je definováno bezlicenční pásmo i v jiných zemích s tím, že šířka tohoto pásma se může mírně lišit.

3. Technologie pro bezdrátové sítě

Pro provozování bezdrátových sítí v bezlicenčním pásmu je k dispozici několik technologií. Jde jednak o proprietární technologie jako například zařízení BreezeNet izraelské firmy BreezeCom nebo technologie firmy Proxim, a jednak o technologie postavené na otevřených standardech.

Asi nejslibněji pro budování bezdrátových LAN menšího a středního rozsahu se jeví rodina protokolů IEEE 802.11. Z ostatních protokolů pro bezdrátové sítě v bezlicenčním pásmu připomenu ještě protokoly BlueTooth.

4. Bezdrátové sítě podle IEEE

Původní standard IEEE 802.11 (dokončený v roce 1997) definoval přenosovou rychlost až 2 Mbit/s. V současné době se používá jeho kompatibilní rozšíření IEEE 802.11b. Toto rozšíření definuje přenosové rychlosti 1, 2, 5,5 a 11 Mbit/s. Hlavní nevýhodou standardu IEEE 802.11b je, že na rozdíl od původního IEEE 802.11 nedefinuje dostatečně striktně požadavky na přenosové zařízení, takže zařízení podle 802.11b od různých výrobců nemusí být nutně navzájem kompatibilní. Tento problém vyřešili výrobci vytvořením sdružení WECA a zavedením de facto standardu a certifikace s názvem Wi-Fi (*wireless fidelity*). Označení Wi-Fi pak zajišťuje i kompatibilitu zařízení mezi různými výrobci.

Protokol IEEE 802.11b definuje tři druhy fyzické vrstvy – jedna z nich je pro infračervené pásmo, ostatní dva pro mikrovlnný přenos. V mikrovlnných sítích se používá rozprostřeného spektra, a to buďto metodou Direct Sequence Spread Spectrum (DSSS) nebo Frequency Hoping Spread Spectrum (FHSS). Přístup ke sdílenému médiu je řízen metodou CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) a používají se rámce kompatibilní s IEEE 802.1 čili ethernetem.

Pro použití sítí Wi-Fi lze v České republice použít 11 nezávislých přenosových kanálů v pásmu 2,4 GHz, přičemž norma definuje až 15 kanálů. Některé kanály jsou dostupné jen v zemích, kde generální povolení (nebo jeho ekvivalent) definuje širší bezlicenční pásmo.

Na stejném pásmu je možno provozovat několik navzájem nezávislých sítí. Jednotlivé sítě jsou navzájem rozlišeny svým jménem, tzv. ESSID. Protokol IEEE 802.11b definuje i automatickou volbu přenosové rychlosti podle kvality signálu – protokol ARS (*automatic rate selection*).

5. Režimy činnosti sítě Wi-Fi

Počítač v síti Wi-Fi může fungovat v jednom ze dvou režimů. Prvním z nich je tzv. ad-hoc mód, kdy se počítač může spojit s jiným počítačem bez nutnosti mít nějaké další aktivní síťové prvky. Takto může komunikovat každý s každým, jen za předpokladu, že každý každého opravdu slyší. Druhý režim činnosti se nazývá *managed* (spravovaný) a vystupuje v něm nové zařízení s názvem *access point* (dále budu občas používat zkratku AP). Komunikace pak probíhá tak, že každý komunikuje s access pointem, který pak data předává jinému účastníkovi. Access point může být i spojen s jiným AP pomocí běžného „drátového“ ethernetu, nebo dokonce i bezdrátově (tomuto se říká *roaming AP*).

6. Bezpečnostní aspekty sítí Wi-Fi

Bezdrátová síť je ještě více než metalické kabely přístupná odposlechu. Součástí normy je proto i šifrování na úrovni linkové vrstvy. Šifrování zajišťuje WEP (*wireless encryption protocol*), k šifrování se používá algoritmus RC4 v 64-bitové formě (40 bitů klíč a 24 bitů inicializační vektor) nebo 128-bitové formě (104 bitů klíč a 24 bitů inicializační vektor). Druhá varianta bohužel není dostupná mimo USA, čili celý slavný WEP nemá v našich podmínkách valného významu[1].

Dále je nutno připomenout, že v podstatě nelze omezit fyzický přístup k síti. Jakýkoli počítač v dosahu signálu některého AP z naší sítě má jednak možnost poslouchat co tento AP vysílá a jednak mu i zasílat svá data. Nelze tedy přístup omezit třeba na jednu budovu nebo jen na určitá „zaregistrovaná“ zařízení. Některé access pointy nicméně mají do jisté míry možnost omezit přístup na základě MAC adresy zařízení. Toto ovšem není standardizováno a tak při zavádění omezení na množinu fyzických adres jsme odkázáni na ty AP, které toto podporují (a pokud možno na jednoho výrobce, abychom měli možnost tento přístup nějak rozumně konfigurovat). Přitom ale nezískáváme nijak velkou úroveň zabezpečení, protože mnohé Wi-Fi karty umožňují softwarově nastavit svoji MAC adresu.

[1] Toto tvrzení není jen teoretické – pro vzorové řešení hledejte program AirSnort :–)

7. Praktická implementace

Na Fakultě informatiky MU jsme vybudovali bezdrátovou síť, pokrývající téměř celou budovu a přilehlé prostory. Jedním z cílů bylo pochopitelně vyzkoušet novou slibnou technologii v praxi, pokud možno při velké zátěži. Velkou zátěž sítě lze vygenerovat poměrně jednoduše – pustíte do sítě studentský provoz :–). Primárně jsme se tedy snažili pokrýt prostory, ve kterých se zdržují studenti. Chodby, nádvoří fakulty, učebny, atrium a podobně. Vedlejším efektem mělo také být snížení zátěže již tak přetížené počítačové haly, sloužící hlavně pro volný nerozvrhovaný provoz. Bezdrátová síť je také využívaná v průběhu konferencí, které se v budově FI konají.

Při těchto požadavcích ale také bylo cílem udržet rozumnou míru bezpečnosti. Jde o připojení k akademické síti, a toto připojení nemůže být přístupné úplně komukoli. Šlo tedy také o to, aby byli uživatelé aspoň nějakým způsobem autentizováni a vůbec aby byla síť zajištěna proti „špatně zkonfigurovaným“ počítačům.

Pro konstrukci bezdrátové sítě jsme zvolili standard IEEE 802.11b Wi-Fi, zejména pro jeho otevřenost, nízkou cenu a vysokou dostupnost příslušných zařízení. Přístupové body i většina bezdrátových karet je značky Lucent Orinoco, nicméně zkoušeli jsme interoperabilitu i se zařízeními jiných výrobců, a to jak na místě access pointů, tak na místě klientských adaptérů.

Poměrně zásadní při pokrytí rozsáhlejších prostorů je volba topologie sítě. Protože z bezpečnostního hlediska nelze doporučit připojování pevných i bezdrátových stanic na jednu síť, je třeba zvolit nějaké jiné řešení. Za ideální považuji vyhradit samostatný segment pouze pro připojení access pointů a bezdrátových stanic. Ne vždy ale lze svést přípojné kabely od jednotlivých AP do stejného switche. Jedna z možností je využít AP v roaming režimu (což ale sníží šířku pásma celé bezdrátové sítě). My jsme použili jiný přístup – z každého AP je veden 100baseTX spoj do nejbližšího switche, a pro bezdrátovou síť je vytvořen samostatný VLAN (podle IEEE 802.1q). Do tohoto VLANu jsou pak připojeny pouze ty porty switche, do kterých jsou zapojeny bezdrátové AP.

Pro pokrytí budovy FI jsme použili 14 přístupových bodů Lucent AP-500 a OR-1000, každý s jednou tyčovou anténou se ziskem 6 dB. Přístupový bod na nádvoří je vybaven 10 dB anténou. Fyzická bezpečnost aktivních prvků je řešena tak, že jsou umístěny vždy pod stropem v kanceláři, dírou ve zdi je pak veden krátký koaxiální kabel k anténě na chodbě.

8. Přístupové body Lucent Orinoco

Aktivní prvky sítě tvoří – jak již bylo řečeno – přístupové body Lucent Orinoco. Hardwarově jde o zařízení s jedním 100baseTX portem a dvěma PCMCIA/CardBus sloty. Do těchto slotů lze umístit standardní karty Orinoco. Jeden AP tak může mít až dvě nezávislá rozhraní.

AP Orinoco lze konfigurovat dvěma způsoby: konfigurace přes sériovou konzolu vyžaduje přímé připojení. Druhá možnost je konfigurace pomocí SNMP (za předpokladu že AP již má svoji IP adresu). Pro naše účely je velmi pozitivní, že výrobce dodává konfigurační program pro Linux. Tento program má příkazové rozhraní podobné směrovačům Cisco, čtení a ukládání konfigurace ale probíhá přes SNMP. Tímto způsobem je možné rozumně implementovat i dávkové kopírování podobných konfigurací na všechny AP v síti (liší se zde pouze IP adresa a kanál na kterém AP vysílá).

Pro zabezpečení sítě poskytují AP Lucent Orinoco několik prostředků. Šifrování protokolem WEP je spíše jen pro naplnění standardu, ale není dostatečně silné pro praktické použití. Bezdrátová síť na FI šifrování nepoužívá, abychom nevyvolávali falešný pocit bezpečí. Dalším zajímavým prostředkem je autentizace MAC adres protokolem Radius. Tuto vlastnost také síť FI nevyužívá – hardwarovou adresu lze příliš snadno změnit. Pro zabezpečení vlastního AP má Lucent Orinoco dvě vlastnosti: Jde o omezení SNMP přístupu na seznam IP adres, ale hlavně o omezení SNMP pouze na datagramy, přicházející z jednoho rozhraní. Pokud tedy SNMP povolíme pouze z „drátového“ ethernetu, výrazně se tím omezí možnost kolemjdoucích uživatelů nějak konfiguraci sítě ublížit.

9. Konfigurace a zabezpečení bezdrátové sítě

Pro bezdrátovou síť je vyhrazen segment 256 IP adres. Z nich 128 je vyhrazeno pro router/firewall, přístupové body a další staticky připojené stroje, zbývajících 128 lze použít pro uživatelské stanice. IP adresy v tomto rozsahu přiděluje DHCP server, běžící na routeru/firewallu. Protože uživatelé v síti se mohou poměrně rychle střídat, přiděluje se IP adresa na nejvýše 10 minut (standardně jen 5 minut). DHCP server přiděluje kromě IP adresy a směrovacích informací také adresy DNS serverů.

Směrování bezdrátové sítě je řešeno routerem/firewallem (někdy používáme moderního pojmu „filtrující směrovač" :–), postaveném na OS Linux. Tento počítač má na starosti směrování mezi šesti fakultními sítěmi (včetně bezdrátového segmentu). Do tohoto počítače je optickou gigabitovou linkou zaveden 802.1q trunk z centrálního switche a směrování/filtrování probíhá v rámci jednoho fyzického rozhraní mezi jednotlivými VLANy[2].

Na firewallu je nastavena určitá minimální ochrana jednotlivých připojených přístupových bodů. Jedná se o statické ARP na odchozí straně, filtrování na základě MAC adresy na příchozí straně, plus filtrování provozu pouze na administrativní stroj (zasílání SNMP trapů, čtení statistik přes SNMP, konfigurace, atd).

Nově příchozí uživatel obdrží od DHCP serveru propůjčenou IP adresu a konfiguraci DNS, ale nemá téměř žádný přístup na síť. Mimo bezdrátový segment je na firewallu povolen pouze přístup na DNS servery protokolem DNS a přístup na administrativní server protokolem HTTPS. Uživatel se pak může spojit s administrativním serverem a autentizovat se buďto pomocí HTTP autentizace (pro uživatele z FI) nebo vyplněním formuláře s dočasným přístupovým jménem a heslem (může být generováno například pro účastníky konference, hosty a podobně). Autentizace je zabezpečena proti odposlechu protokolem HTTPS s opravdovým 128-bitovým šifrováním.

Po úspěšné autentizaci administrativní server zjistí přes SNMP z firewallu MAC adresu uživatele a spustí na firewallu zpřístupnění této adresy. Firewall pro tuto IP adresu nastaví statické ARP a zapne filtrování na MAC adresu. Zároveň z této IP adresy povolí přístup do vnějšího světa. Z hlediska „pevné" sítě FI jsou bezdrátoví klienti považováni za méně bezpečné a je k nim přistupováno z hlediska firewallu jako k libovolným jiným počítačům z vnějšího světa.

Přihlášení do bezdrátové sítě a povolení provozu na firewallu je časově omezeno, implicitní doba je 8 hodin. Aby nezůstávaly otevřené IP adresy na firewallu, testuje firewall periodicky každých 5 minut dostupnost všech zpřístupněných IP adres v bezdrátové síti (používá se ICMP echo, program `fping`). Pokud počítač dvakrát za sebou není dostupný, je daná IP adresa zablokována podobně jako byla ve výchozím stavu než se uživatel autentizoval. Podobně je IP adresa zablokována po vypršení platnosti autentizace (čili po 8 hodinách).

Firewall navíc kontroluje, jestli se uživatel nehlásí vícekrát. Vždy při zpřístupnění určité IP adresy a MAC adresy pro daného uživatele nejprve ruší připadná předchozí zpřístupnění pro stejnou IP adresu, pro stejnou MAC adresu nebo pro stejného uživatele.

10. Další vlastnosti bezdrátové sítě

Pro sledování provozu na bezdrátové síti používáme MRTG – sleduje se jak provoz sítě směrem k vnějšímu světu, tak i provoz na jednotlivých přístupových bodech. Firewall také umožňuje dočasné otevření bezdrátové sítě bez nutnosti autentizace na administrativním serveru (organizátoři některých konferencí považují přihlašování se k síti za příliš složité pro účastníky konference).

Zavedením takto autentizované sítě jsme získali i všestrannější prostředek než jen připojení k bezdrátové síti. Na tomto segmentu můžeme stejným způsobem realizovat i „drátové"

[2] Problematika gigabitového routeru/firewallu v síti FI by byla jistě tématem na samostatnou přednášku.

připojení, například pro účastníky konference, jejichž notebooky nedisponují bezdrátovými kartami. Zde je potřeba myslet na možnost fyzického poškození aktivních prvků například statickou elektřinou čí závadou na elektronice klientského počítače. Pro tyto účely proto obvykle vyhrazujeme starší 10Mbitový hub, který navíc od zbytku počítačové sítě elektricky oddělíme optickými mediakonvertory 10baseF na 10baseT.

11. Zkušenosti a problémy

Celkově lze říci, že bezdrátová síť v budově FI plní svůj hlavní původně zamýšlený účel – přístup pro studenty – vcelku dobře. Nicméně po zprovoznění sítě se objevily ve větší míře požadavky na přístup i pro zaměstnance. Zde nastaly jisté problémy, protože železobetonová konstrukce budovy FI není příliš prostupná pro mikrovlnnou síť a zaměstnanecké kanceláře jsou od antén na chodbách odděleny i několika stěnami. Částečně se problém podařilo vyřešit oddálením antén od stěn, v některých případech bude možná nutno zavést další přístupové body.

Jako problematické se také ukázaly situace, kdy počítač je v dosahu několika přístupových bodů. Podle druhu ovladače a síťové karty se pak stává, že počítač cyklicky přeskakuje mezi několika AP, což má za následek několikavteřinové výpadky sítě na příslušném počítači. Při nastavení na jeden konkrétní AP napevno zase nemůže počítač přecházet po budově.

S jistými bezpečnostními riziky by bylo možno použít i jiné řešení, například autentizace podle MAC adres protokolem Radius. Pro roli autentizující brány bezdrátové sítě, běžící pod Linuxem, existují i různé předpřipravené balíky softwaru. Naše řešení bylo motivováno tím, že jsme oba počítače (router/firewall i administrativní server s možností autentizovaného přihlášení) již provozovali. Při zprovoznění bezdrátové sítě jsme tedy jen přidali další VLAN na firewall a do páteřních switchů a zprovoznili autentizační aplikaci na administrativním serveru.