Bezdrátové sítě v prostředí MU

David Rohleder, ÚVT MU

V minulém čísle Zpravodaje jsme se seznámili s rychle se rozvíjející oblastí bezdrátových sítí. Tento způsob připojení se stává velmi populární a čím dál dostupnější pro širokou univerzitní obec. Není tedy daleko doba, kdy budou uživatelé běžně vyžadovat takové připojení a to pokud možno co nejjednodušší formou.

Zavedení bezdrátové sítě ovšem přináší celou řadu problémů, které nebylo nutné řešit v případě klasických sítí. Mezi tyto problémy patří zejména:

- zajištění bezpečné komunikace ve snadno odposlouchávatelném prostředí
- zajištění autentizace a autorizace uživatelů tak, aby k síti měli přístup pouze oprávnění uživatelé
- vysledovatelnost různých problémů v tomto dynamicky se měnícím prostředí
- jednotná metoda přístupu k síti ve všech přístupových bodech sítě
- co největší interoperabilita

1 Možná řešení

Minule jsme si popsali jednotlivá možná řešení některých těchto problémů. Bohužel ne všechna zařízení podporují potřebné protokoly. Navíc řešením rozšiřitelné autentizace a autorizace se zabývají pouze protokoly, které implementuje jenom malá část existujících bezdrátových karet. Nebylo by tedy vhodné se vázat na protokoly typu WPA, EAP-TLS, 802.1X nebo 802.11i.

2 Existující bezdrátové sítě na MU

Fakulta informatiky se bezdrátovými sítěmi zabývá již delší dobu a implementovala svůj vlastní systém, který byl vyvinut jako součást pilotního projektu CESNETu. Fakulta informatiky je tak průkopníkem v nasazení bezdrátových sítí na univerzitě a jejich zkušeností jsme se snažili využít při vytváření naší koncepce celouniverzitní bezdrátové sítě. Systém používaný na FI autentizuje uživatele podle MAC adres bezdrátových síťových karet v kombinaci s přihlašováním prostřednictvím zabezpečené webové stránky. Tento způsob připojení k síti má ovšem své slabé stránky. Především, komunikace není šifrovaná a nejeví se jako dostatečně bezpečná pro všechny zamýšlené aplikace, autentizace MAC adresou nezajišťuje nezfalšovatelnost MAC adresy a následné zneužití připojení. Další nevýhodou je nutnost instalace autentizačního hardware přímo na vstupu do univerzitní sítě. V současnosti je tento systém v provozu v budově fakulty informatiky a v areálu přírodovědecké fakulty.

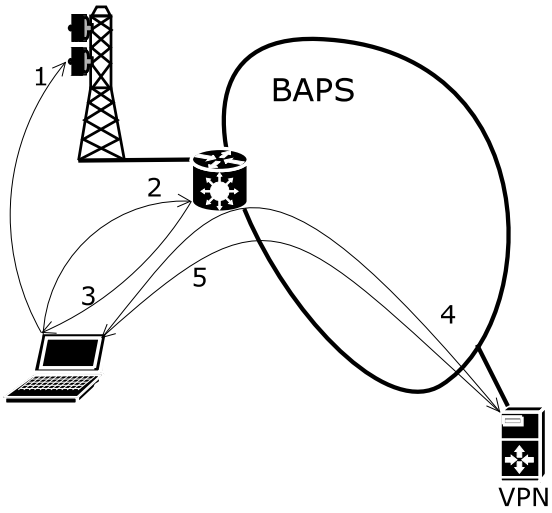
3 Alternativní řešení

Naším cílem bylo najít takové řešení, které by bylo možné zavést v každé přípojné lokalitě univerzitní sítě bez dodatečných nákladů na infrastrukturu a další správu. Nechtěli jsme jít cestou speciálních protokolů bezdrátových sítí, proto jsme se zaměřili na všeobecně rozšířené protokoly pro vytváření VPN (virtuálních privátních sítí). Tyto protokoly nám umožnily „tunelovat“ veškerý provoz do centrálního uzlu, ve kterém jsou zakončeny všechny tunely. Zároveň by se tím vyřešila otázka šifrování, autentizace a autorizace uživatelů počítačové sítě. Navrhované schéma zapojení je na obrázku 1.

4 Popis fungování

Jednotliví uživatelé se připojí pomocí bezdrátové karty k nejbližšímu přístupovému bodu. Komunikace není šifrovaná a není zabezpečená pomocí ESSID, takže k takové síti se může připojit kdokoliv. Následně je uživateli pomocí DHCP přidělena centrálním prvkem jeho IP adresa. Uživatelův přístup je nejbližším síťovým prvkem omezen na přístup k vytvoření autentizovaného a šifrovaného spojení s centrálním VPN serverem. Uživatel se autentizuje prostřednictvím centralizované databáze uživatelů a je mu vytvořeno spojení s novou IP adresou, jejíž pomocí už může plnohodnotně komunikovat se světem.

Jako tunelovací protokol přicházelo v úvahu několik variant. Asi nejstandardnější metoda by bylo použití IPSec, ale nabízely se i různé varianty typu L2TP nebo PPTP. Nakonec se ukazuje jako nejschůdnější použití protokolu PPTP, který je implementován na všech běžných počítačových platformách (ačkoliv se nám mnohem více



Obrázek 1: 1. notebook naváže spojení s bezdrátovou základnou; 2. notebook požádá o IP adresu pomocí protokolu DHCP; 3. je mu přidělena IP adresa; 4. uživatel požádá o navázání tunelu s VPN serverem MU; 5. VPN server MU vytvoří tunel a přidělí uživateli IP adresu, pomocí které bude přistupovat do Internetu.

zamlouvalo použití protokolu IPSec, není dostupný hlavně na platformách řady MS Windows 95-ME, což představovalo poměrně výrazný handicap v použitelnosti tohoto protokolu). V principu ovšem není problém rozšířit nabídku tunelovacích protokolů i o jiné, již zmíněné protokoly. Podrobnější informace o VPN serveru MU lze najít v článku v minulém Zpravodaji.

V současnosti je podle tohoto návrhu vybudována bezdrátová síť v CPS a na rektorátě MU. Toto řešení je možné poměrně jednoduše skloubit i se stávajícími řešeními vybudovanými na FI a PřF. Další výhodou tohoto řešení je možnost použití téměř libovolných přístupových bodů (protože na ně nejsou kladeny zvláštní požadavky) a bezdrátových karet, což může výrazně snížit cenu za vybudování této sítě.

Předpokládáme, že všechy přístupové body budou ve správě místních oddělení LVT, tak aby místní správci mohli jednoduše reagovat na požadavky svých uživatelů. Přesto je na místě varování, že jakékoliv připojování bezdrátových sítí musí projít schválením od příslušného LVT a různé načerno připojené přístupové body porušují pravidla používání univerzitní sítě.

5 Optimisticky laděný závěr

Postupně by se měla být bezdrátová síť rozšířit na co největší počet míst tak, aby co v největší míře pokryla požadavky uživatelů a přinesla jim co největší komfort při jejich práci se sítí Masarykovy univerzity. □