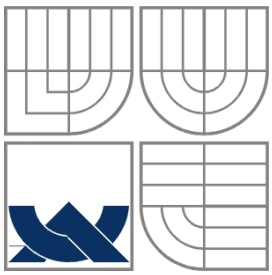
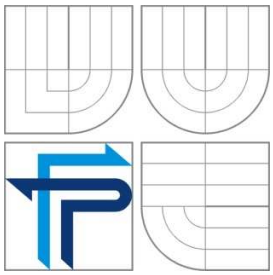


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

PROBLEMATIKA BEZDRÁTOVÝCH SÍTÍ

WIRELESS FIDELITY NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR‘S THESIS

AUTOR PRÁCE
AUTHOR

PAVEL PAROLEK

VEDOUCÍ PRÁCE
SUPERVISOR

doc. Ing. MILOŠ KOCH, CSc.

BRNO 2009

Abstrakt

Obsahem mé bakalářské práce je realizace ověřování identity uživatele RADIUS serverem v bezdrátové síti, který je provázaný s MySQL databází a tím zjednodušení správy databáze uživatelů.

Abstract

My bachelor's thesis contains realization of user authentication by RADIUS server in wireless network, where server is connected to MySQL database. By that we will achieve better management of user database.

Klíčová slova

Wi-Fi, Linux, RADIUS, PHP, MySQL, 802.1X, bezdrátová síť

Keywords

Wi-Fi, Linux, RADIUS, PHP, MySQL, 802.1X, wireless network

Bibliografická citace

PAROLEK, P. *Problematika bezdrátových sítí.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2009. Vedoucí bakalářské práce doc. Ing. Miloš Koch, CSc.

Problematika bezdrátových sítí

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením svého vedoucího bakalářské práce. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

……
Pavel Parolek
29. květen 2009

Poděkování

Rád bych poděkoval vedoucímu mé práce, doc. Ing. Miloši Kochovi CSc. za rady vedoucí k vypracování této práce. Také bych rád poděkoval panu Zdeňku Švarci, za pomoc při výběru tématu a za technický dozor, a nakonec svým blízkým za podporu.

Obsah

1 Úvod

Připojení k internetu se stalo nedílnou součástí většiny domácností a mnozí konektivitu s celým světem považují za stejně důležitou, jako například připojení k inženýrským sítím. A není se čemu divit, kvalitní konektivita nám zprostředkovává téměř neomezený výběr činností. Ať už se jedná o pouhou zábavu, nebo hledání nových poznatků, přátel, ale i pracovních příležitostí.

Vysoká poptávka po rychlém a levném připojení do celosvětové sítě dala možnost vzniku celé řadě poskytovatelů internetu. Jejich nabídky, ceny, technologie, ale i uživatelské základny jsou velmi různorodé a mohou se výrazně lišit v závislosti na lokalitě. Nalezneme zde rozsáhlé sítě společnosti Telefonica O2, založené na telefonních rozvodech a technologiích ADSL a ISDN. Připojení odkudkoliv mohou také zprostředkovat mobilní operátoři, kteří se předhánějí v nabídkách výhodnějších podmínek a balíčků. Významní poskytovatelé jsou také společnosti vlastnící rozvody kabelové televize, které nalezneme v každém větším městě. Ale vůbec nejvýznamněji se na konektivitě českých domácností podílejí lokální poskytovatelé bezdrátového připojení do sítě internet.

Těchto lokálních poskytovatelů je celá řada a dnes se nachází téměř v každém městě či vesnici jedna nebo i více společností. Víme ale, jak kvalitně je zajištěna bezpečnost těchto sítí? A když není, jaké by měli poskytovatelé učinit kroky, aby bezpečnost jejich sítí a tím pádem i klientů byla dostatečná?

2 Vymezení problému a cíle práce

Malí a středně velcí poskytovatelé bezdrátového internetu velmi často využívají své přístupové body pro databázi klientských účtů. S každým novým přístupovým bodem se zvyšuje decentralizovanost databáze a její správa se stává velmi obtížná a časově náročná.

Cílem této bakalářské práce je poukázat na alternativní řešení správy databáze uživatelských účtů a zvýšení bezpečnosti celé sítě pomocí implementace protokolu IEEE 802.1X. Má práce zahrnuje návrh jak hardwarových zařízení, kompatibilní se standardem IEEE 802.1X, tak i softwarového vybavení databázového a autentizačního serveru.

Výstupem tedy bude softwarové a hardwarové řešení, které centralizuje databázi uživatelských účtů a významně zvýší bezpečnost celé sítě.

3 Teoretická východiska práce

3.1 IEEE 802.11

Standard IEEE 802.11 byl ustanoven mezinárodním standardizačním institutem IEEE v roce 1997 za účelem sjednotit technologie od různých výrobců na bezdrátový přenos dat. Do této doby bylo pásmo 2,4 GHz využíváno několika výrobci, kde každý měl vlastní technologii bezdrátové sítě, vzájemně však nebyli mezi sebou kompatibilní. Mezi nejrozšířenější patřil BreezeNete od stejnojmenného izraelského výrobce.

Tento standard využívá nelicencované pásmo 2,4 GHz. Toto pásmo bylo vymezeno jak americkým regulátorem FCC, tak evropským ETSI pro průmyslové, vědecké a lékařské účely. Mimo jiné v tomto pásmu operují mikrovlnné trouby, bezdrátové telefony, ale i Bluetooth zařízení, proto mohou tyto zařízení rušit bezdrátový přenos.

Standard nespecifikuje technologii nebo implementaci, ale pouze popisuje fyzickou a MAC (Media Access Control) vrstvu.

Standard specifikuje tři alternativní technologie fyzické vrstvy: (1)

- infračervený přenos
- FHSS – Frequency-hopping spread spectrum
- DSSS – Direct-sequence spread spectrum

FHSS je jedna z metod přenosu v rozprostřeném spektru. Její princip spočívá v přeskakování mezi několika frekvencemi při přenosu bitu nebo bitů. Datová zpráva je tak vyslána na mnoha nosných frekvencích. Vysoké spolehlivosti je dosaženo tím, že nepotvrzené nebo chybně přenesené rámce se znovu přenesou s jinou nosnou frekvencí.(2)

DSSS pracuje tak, že každý jednotlivý bit určený k přenosu je nejprve nahrazen určitou početnější skupinou bitů. Díky této redundanci je signál rozprostřen do větší části spektra a je více odolný vůči rušení. (3)

Standard počítal i s použitím infračerveného spektra, ale tento model se neujal a nahradil ho standard IrDA.

Maximální rychlosti dosahovali 2 Mbps, nebo 1 Mbps při použití infračerveného spektra. Již v roce 1997 bylo jasné, že tyto přenosové rychlosti budou nedostačující a proto se standard dočkal několika revizí.

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	

Tabulka 2.1 – Přehled standardů IEEE 802.11 (4)

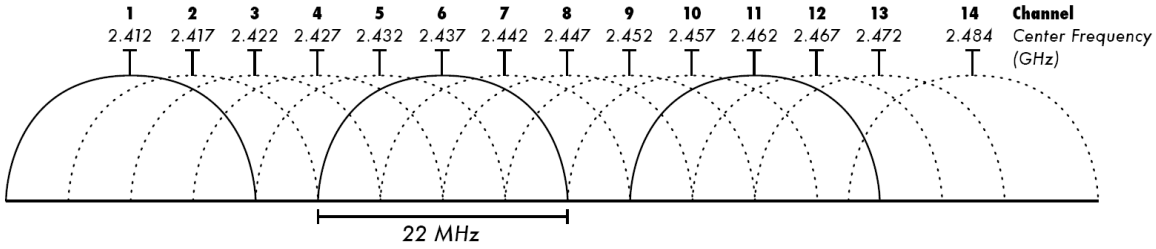
3.1.1 IEEE 802.11b

IEEE 802.11-1999 nebo také 802.11b je jedním z doplňků standardu IEEE 802.11, který navýšil přenosovou rychlost ze stávajících 2 Mbps na 11Mbps při použití stejného frekvenčního pásma. Tato specifikace se pod obchodním názvem Wi-Fi rozšířila do celého světa.

802.11b opouští infračervené spektrum i frequency hopping používá již jen DSSS modulaci. I když se uvádí maximální rychlost 11 Mbps, díky této modulaci je výrazná část přenosové rychlosti využita na prevenci chyb a rušení. Typická reálná přenosová rychlost dosahuje maxima 5 Mbps. I tak se jedná o výrazné zvýšení přenosové rychlosti

a to vzájemně se snížením ceny zařízení vedlo k rychlému rozšíření standardu 802.11b jako konečnou technologii pro bezdrátové sítě.

Aby mohlo pracovat v jedné lokalitě několik bezdrátových zařízení nezávisle na sobě a vyhnula se vzájemnému rušení, standard 802.11b a 802.11g definuje v pásmu 2,4 GHz několik přenosových kanálů. Celkem se jedná o 14 kanálů, vzdálených 5 MHz od sebe (s výjimkou 12 MHz mezery mezi kanály 13 a 14). Protože ale pro přenos dat je potřeba 25MHz široká mezera, zařízení pracující na sousedních kanálech se mohou rušit. (5)



Obrázek 2.1 – Rozložení kanálů v přenosovém pásmu (5)

Z obrázku 2.1 vidíme, že v tomto spektru mohou komunikovat pouze tři zařízení, aniž by se jakkoliv ovlivňovaly. Některé státy si vytvářejí vlastní regulace použití kanálů. V severní Americe lze využít pouze kanály 1 až 11, v Japonsku všechny, ale čtrnáctý kanál pouze pro standard 802.11b. Ve zbytku světa jsou pak přístupny kanály 1 až 13. (5)

Dosah tohoto standardu bývá typicky 30 metrů v budově. Venkovní spoje dokážou fungovat i na vzdálenosti několika kilometrů. Pokud se vzdálenost zvyšuje nebo roste zarušení pásma, zařízení postupně snižují přenosovou rychlost z 11 Mbps na 5,5, pak 2 a nakonec na 1 Mbps pomocí technologie Adaptive Rate Selection. Tímto se dají vyřešit potíže se slabým signálem mezi dvěma zařízeními.

3.1.2 IEEE 802.11g

Standard rozšiřující 802.11b vznikl v roce 2003, je zpětně kompatibilní a pracuje ve stejném frekvenčním pásmu 2,4GHz. Došlo však k výraznému navýšení přenosové rychlosti na teoretických 54 Mbps, v reálu tento standard dosahuje rychlostí do 20 Mbps. Vzdálenosti jsou podobné jako u specifikace 802.11b.

Došlo také ke změně modulace. U rychlostí standardu 802.11b (tedy 11, 5,5, 2 a 1 Mbps) z důvodů kompatibility zůstává DSSS, ale u vyšších rychlostí (konkrétně 54, 48, 36, 24, 18, 12, 9 a 6 Mbps) je nově použito OFDM modulační schéma. (6)

V dnešní době se jedná o nejpoužívanější standard pro bezdrátové sítě v uzavřených prostorách. Donedávna byl také hojně využíván (spolu s 802.11b) lokálními poskytovateli internetu pro připojení svých klientů do celosvětové sítě. Díky rostoucí saturaci přenosového pásma byly specifikace nahrazeny standardem 802.11a.

3.1.3 IEEE 802.11a

Tato specifikace vznikla v roce 1999. Používá v jádru stejný protokol jako původní standard, ale pracuje v pásmu 5 GHz a používá OFDM modulaci. Tato modulace byla později využita i v pásmu 2,4 GHz ve standardu 802.11g, a proto obě specifikace např. sdílí přenosovou rychlost.

Původně tento standard popisoval 12/13 vzájemně se nepřekrývajících kanálů – 12 pro použití uvnitř budov, 4/5 z dvanácti pro použití ve venkovních prostorách pro spoje na dlouhou vzdálenost. Některé státy však toto pásmo rozšířily o kanály ze standardu 802.11h a tím se zajistily dalších 12/13 kanálů. Stejně jako u 802.11b/g se může lišit povolení vysílat na některých kanálech. V tomto případě jsou však rozdíly příliš velké a proto je zde nebudu vypisovat. Tyto restrikce si hlídají sami výrobci a tak by se nemělo stát, že koupíme produkt, který vysílá i v zakázaných kanálech.

Díky vyšší pracovní frekvenci dosah je o něco menší než u specifikací 802.11b/g. Signál nedokáže proniknout tak daleko, protože je snadno pohlcován všemi pevnými překážkami v cestě. Na druhou stranu vyšší frekvence vylučují rušení od zařízení typu

mikrovlnných trub, bezdrátových telefonů, Bluetooth zařízení atp., takže ve výsledku je specifikace 802.11a spolehlivější než 802.11b/g. (7)

3.1.4 Alternativní specifikace bezdrátových sítí

Nové bezdrátové technologie, které se ucházejí o místo nástupce stávajících specifikací 802.11a/b/g.,přinášejí vyšší kmitočty, vyšší rychlosti a doufejme, že i vyšší spolehlivost.

3.1.4.1 IEEE 802.16 - WiMAX

Specifikace zaměřená na venkovní sítě vznikla v roce 2002. Definovala tuto technologii na frekvenčních pásmech 10-66 GHz při rychlostech dosahující 134 Mbps, nutná je ovšem přímá viditelnost obou koncových bodů. O rok později byla vydána revize 802.11a, která definuje frekvenční pásmo 2-11 GHz. Dokáže fungovat na vzdálenosti 40-70 km. Rychlost však klesá na polovinu oproti původní specifikaci. Při použití nižších frekvencí odpadá nutnost přímé viditelnosti. (8)

3.1.4.2 IEEE 802.11n

Jedná se o další vylepšení standardu 802.11. Specifikace „n“ pracuje na frekvencích 5 a 2,4 GHz s teoretickou maximální propustností až 600 Mbps a maximálním dosahem uvnitř budov až 300 metrů.

Takto velké rychlosti jsou dosaženy spojením dvou nepřesahujících kanálů do jednoho a implementace MIMO technologie. Tato technologie používá několik antén pro několikanásobný příjem/vysílání. Spoléhá přitom na odražené signály, které dorazí až po přijetí signálu v přímé viditelnosti. Tyto odražené signály jsou ve specifikacích 802.11a/b/g brány jako rušení a snižují kvalitu přenosu.

V současné době jsou většinou v prodeji zařízení specifikace 802.11n Draft2, které pracují na frekvenci 2,4 GHz, což není pro použití spojení kanálů ideální. Maximální teoretická propustnost je 300 Mbps, ale reálné testy dosáhly pouze rychlosti 170 Mbps. (9)

3.2 Topologie bezdrátových sítí

Bezdrátová zařízení dokáží vystupovat v několika různých rolích v závislosti na požadavky struktury sítě nebo na schopnostech samotného zařízení. Bezdrátové sítě mají ve standardech nadefinovány dva základní typy sítí. Jedná se o sítě Ad-hoc a infrastrukturní sítě.

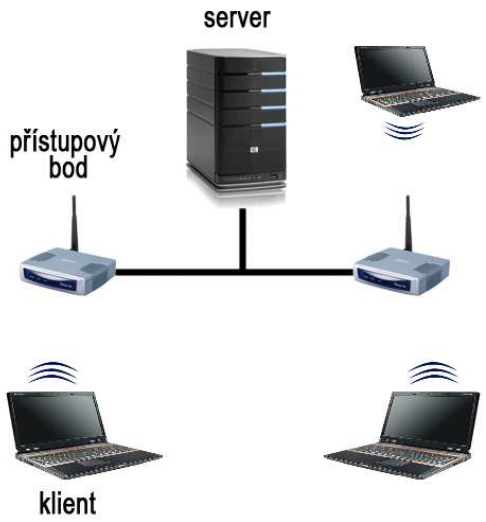
3.2.1 Ad-hoc

“Sítě ad-hoc se někdy rovněž nazývají nezávislé sítě, to z toho důvodu, že jednotlivé stanice v takové síti spolu komunikují přímo podle potřeby, a tedy nezávisle na nějakém prostředníkovi. Z toho vyplývá, že pokud spolu stanice chtějí komunikovat, musí být ve vzájemném radiovém dosahu. Pro menší síť s několika stanicemi vzdálenými pár metrů od sebe je to vhodné komunikační schéma, ale je zřejmé, že sítě s více počítači nebo sítě v členitějších a rozlehlejších prostorách, kde princip vzájemného nebo radiového dosahu nemůže být vždy zajištěn, takto realizovat nelze“ (10, str. 7)

Obrázek 2.2 – Příklad Ad-hoc sítě

3.2.2 Infrastrukturní sítě

Daleko rozšířenější jsou infrastrukturní sítě. Klient se připojí pouze k jednomu nejbližšímu přístupovému bodu (Access Point, AP) a má přístup ke všem prostředkům sítě. Přístupový bod přeposílá požadavky mezi jednotlivými klienty nebo zpřístupňuje klientovi zbytek sítě, ať už bezdrátové, tak metalické. Přístupový bod se umisťuje do takových míst, aby poskytl svým klientům nejlepší pokrytí a tím i bezproblémový bezdrátový přístup do sítě. Sám může být, a často taky bývá, spojen např. metalickým kabelem se zbytkem sítě. (11)



Obr. 2.3 – Příklad infrastrukturní sítě

Díky tomu, že tedy klient tedy komunikuje pouze s jedním přístupovým bodem, je velmi vhodné použití směrových antén s větším ziskem a tím pokrýt daleko rozsáhlejší oblasti. Této vlastnosti lze také využívat při spojích na velkou vzdálenost mimo budovy, kdy se použije úzce směrová anténa.

3.3 Bezpečnost bezdrátových sítí

S bezdrátovými sítěmi velmi úzce souvisí jejich bezpečnost. Protože se signál šíří vzduchem, je téměř nemožné fyzicky zabezpečit bezpečnost přenosu. Útočník se tak může zkoušet připojovat k přístupovému bodu, odposlouchávat datový přenos mezi přístupovým bodem a jeho klienty atp. a stačí mu k tomu pouze být poblíž přístupového bodu. U poskytovatelů bezdrátového připojení to mohou být stovky metrů, u domácností nebo kanceláří se jedná o desítky metrů – např. v zaparkovaném autě před domem nebo kanceláří.

Z logiky bezdrátového přenosu dat téměř nemůžeme zabránit odposlouchávání, nebo útoku na přístupový bod. Lze však útočníkovi znemožnit, nebo alespoň velmi ztížit, zpětné přečtení a analýzu datového přenosu aplikací některé formy šifrování přenosu mezi klientem a přístupovým bodem.

3.3.1 WEP

WEP, neboli Wired Equivalent Privacy (česky soukromí ekvivalentní drátovým sítí), je nejstarší forma zabezpečení bezdrátových sítí a je součástí standardu IEEE 802.11 z roku 1999.

“WEP používá k šifrování zpráv symetrickou šifru RC4 - princip spočívá v tom, že se odesílána zpráva na vysílači zašifruje nějakým klíčem, a přijímač ji stejným klíčem rozšifruje. Tento klíč musí být znám jak vysílající stanici, tak přijímací (ve standardu se jedná o 40-bitový klíč).

Aby to nebylo tak jednoduché, klíč se expanduje na délku stejnou jako má vysílaná zpráva, a to pomocí tzv. inicializačního vektoru. Jedná se o 24-bitový pseudonáhodný sled znaků, který se na straně vysílače přidá k tajnému klíči (tím vzniká 64-bitová "šifra", se kterou se pak zašifruje zpráva) a také se pošle (nijak

nezakódovaný! - toto patří mezi jednu z hlavních nevýhod WEPu) přijímači, aby ten ho mohl přidat ke svému tajnému klíči a tento složený klíč pak použít pro dešifrování.“[12]

Dnes je již toto zabezpečení nedostatečné a útočník je schopný zjistit klíč během několika minut odposlouchávání komunikace mezi dvěma body, a proto se WEP nedoporučuje používat.

3.3.2 Filtrování MAC adres

Každé síťové rozhraní je od výrobce vybaveno fyzickou (MAC) adresou. Jedná se o jednoznačný identifikátor síťového rozhraní, ať už se jedná o kabelový ethernet, nebo bezdrátová zařízení např. Wi-Fi nebo Bluetooth . Skládá se ze 48 bitů a nejčastěji ji můžeme vidět zapsanou ve tvaru 01:23:45:67:89:ab. (13)

Protože tato adresa je z pohledu uživatele neměnná, lze ji využít v bezdrátových sítích pro autorizaci uživatelů. Přístupový bod obsahuje databázi povolených fyzických adres síťových rozhraní, které mají povolení přihlásit se do sítě. Síťová rozhraní s jinými adresami se do sítě nepřipojí.

V dnešní době však není problém MAC adresu u některých zařízení změnit přímo v nastavení zařízení, nebo utilitou zamaskovat původní adresu a vydávat ji za jinou. Proto se jedná o nedostatečné zabezpečení a osobně bych ho doporučil pouze do domácností, kde zabrání náhodnému útočníkovi.

3.3.3 WPA

WPA, neboli Wi-Fi Protected Acces (česky Wi-Fi chráněný přístup) je druh zabezpečení bezdrátových sítí. Vznikl jako náhradník WEPu, který se díky svým bezpečnostním chybám stal snadno prolomitelný.

WPA vychází ze standardu IEEE 802.11i a je navržen s ohledem na zpětnou kompatibilitu. Stejně jako u zabezpečení WEP je zpráva šifrována pomocí RC4 se

[12] STEJSKAL, Petr. *Bezdrátové sítě – Wi-Fi, Bezpečnost* [online]. 2009. [cit. 2009-04-10]. Dostupné z WWW: <http://www-kiv.zcu.cz/~simekm/vyuka/pd/zapocty-2003/wi-fi/index.php?id=5>

128bitovým klíčem a 48bitovým inicializačním vektorem. Přidává však protokol TKIP, který umožňuje dynamicky měnit použité klíče. Dále nahrazuje kontrolní součet CRC-32 bezpečnější metodou MIC – Message Integrity Code, konkrétně algoritmem Michael. Ten v sobě obsahuje ochranný mechanismus, který detekuje pokus o útok a dočasně zablokuje komunikaci s útočníkem.

WPA2 je pak kompletní implementací standardu IEEE 802.11i. Přidává novou šifru CCMP, která vychází z AES a je momentálně neprolomena. (14)

3.3.3.1 Distribuce klíčů

WPA/WPA2 byl navržen s ohledem jak na korporátní sféru, tak malé lokální sítě. Dokáže využít standard 802.1X pro výměnu klíčů pomocí protokolu EAP, nebo lze fungovat i s předem vyplněným klíčem – pre-shared key, PSK.

Použití	WPA	WPA2
Enterprise	Autentifikace: IEEE 802.1X/EAP Šifrování: TKIP/MIC	Autentifikace: IEEE 802.1X/EAP Šifrování: AES-CCMP
Pesronal	Autentifikace: PSK Šifrování: TKIP/MIC	Autentifikace: PSK Šifrování: AES-CCMP

Tabulka 2.1 – Přehled typů zabezpečení ve WPA/WPA2 (14)

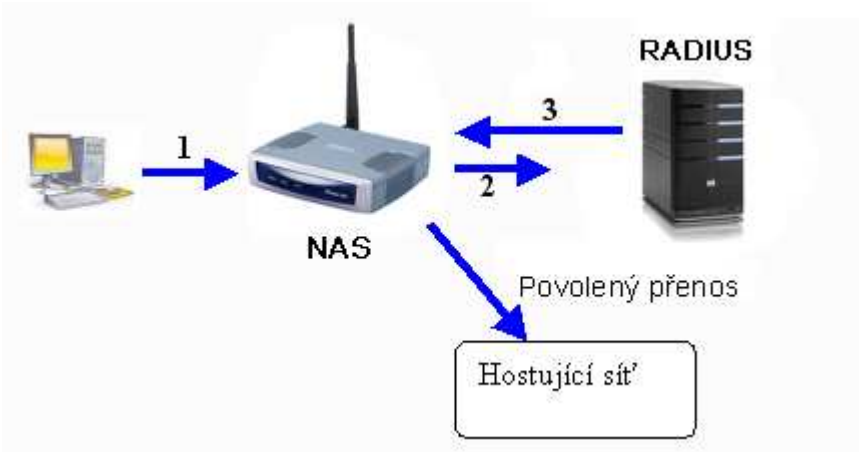
3.3.4 IEEE 802.1X

IEEE 802.1X je standard pro zabezpečení fyzického přístupu do sítě. Byl zprvu vyvinut pro řízení přístupu v metalických sítích, kdy u velmi rozsáhlých sítí nemáme pod kontrolou každou přípojku, ale je velmi vhodný pro řízení přístupu i v bezdrátových sítích. Komunikace probíhá pomocí EAP protokolu.

“Ověřování v bezdrátové síti provádí přístupový bod pro klienty na základě jejich výzvy, pomocí seznamu nebo externího autentizačního systému, založeného na serveru Kerberos nebo RADIUS, Remote Authentication Dial In User Service. Pouze ověřený uživatel má přístup k síti.“ (10, str. 134)

3.3.4.1 Postup autentizece klienta do sítě

1) Klient vyšle žádost o autentizaci na svůj přístupový bod – Network Access Server, NAS jednotka, která odpoví dotazem na totožnost klienta
2) Klient zašle své identifikační údaje NAS jednotce, ta je přepošle na RADIUS server, kde proběhne ověření totožnosti uživatele,
3) NAS jednotka je informována o výsledku autentizace:
   a. Pokud byla autentizace úspěšná, NAS jednotka povolí komunikaci klienta se zbytkem sítě podle specifikací RADIUS serveru.
   b. Neúspěšná autentizace znamená zablokování komunikace s klientem, vyjma EAP protokolu.



Obrázek 2.4 – Postup autentizace klienta do sítě

“802.1x používá k šifrování datové komunikace pro každé autentizované zařízení dynamické klíče. Tyto klíče jsou známy pouze danému zařízení, mají omezenou životnost a využívají se k šifrování rámců na daném portu, dokud se zařízení neodhlásí nebo neodpojí.“ (10, str. 134)

3.4 RADIUS

Remote Authentication Dial In User Service – RADIUS – je síťový protokol poskytující AAA. Byl vyvinut společností Livingston Enterprises v roce 1991, ale později dosáhl IETF standardů.

Tato technologie je široce využívaná poskytovateli internetu pomocí vytáčeného připojení, nebo xDSL. Tato technologie však nachází čím dál větší oblibu mezi poskytovateli bezdrátového připojení.

3.4.1 AAA

Authentication, Authorization and Accounting (česky autentizační, autorizační a účtovací) protokol slouží k ověření uživatelské identity a monitoring využívaní sítě uživatelem.

3.4.1.1 Authentication – autentizace

Autentizace znamená ověření identity uživatele, nebo síťového zařízení. Autorizace je provedena předložením identifikátoru a jeho porovnání s identifikátorem na serveru. Tímto identifikátorem mohou být hesla, digitální certifikáty atp.

3.4.1.2 Authorization – autorizace

Autorizace je přidělení přístupu k službě nebo službám na základě úspěšné autentizace. Také definuje službu poskytnutou uživateli: může poskytovat IP adresy, šifrování, stanovit přenosové rychlosti, ale také časově omezit přístup.

3.4.1.3 Accounting – účtování

Účtováním v AAA protokolu rozumíme sledování využití síťových služeb uživatelem. Toto lze využít např. pro analýzu vytížení částí sítě, plánování, účtování, atp. Většinou se sledují informace o časech připojení.

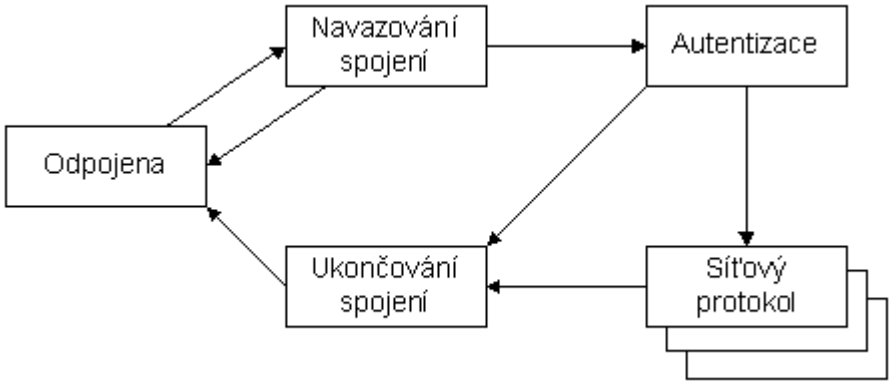
3.4.2 PPP

Komunikace mezi zařízením uživatele a NAS jednotkou probíhá pomocí Point-to-Point Protokolu (PPP). Poskytuje autentizaci, šifrování přenosu a kompresi dat na linkové vrstvě.

Součástí tohoto protokolu jsou dva služební protokoly (15)

- LCP sloužící k navázání spojení a autentizaci stanic
- Skupina protokolů NPC pro samotný přenos dat

Protokol LCP se používá ještě před tím, než se vůbec uvažuje o tom, jaký síťový protokol na lince poběží. Při navazování komunikace linka postupně projde stavy navazování spojení, autentizace, aplikace síťového protokolu až po ukončení spojení, jak je to znázorněno na obr. 2.5 (15)



Obrázek 2.5 – Navazování komunikace (15)

3.4.3 PAP

Password Authentication Protocol (PAP) je jednoduchý autentizační protokol pro přihlášení uživatele do sítě, používá se v protokolu PPP. Autentizační data jsou zaslána v nešifrované podobě, tudíž při odposlouchávání paketů lze jednoduše zjistit přihlašovací údaje uživatele.

Pokud je tento protokol použit k autentizaci uživatele pomocí RADIUS serveru, hesla se přenáší jako MD5 otisk, který zvyšuje bezpečnost. (15)

3.4.4 CHAP

Challenge Handshake Authentication Protocol (CHAP) řeší nedostatky svého předchůdce – PAP. Klient i server mají definovaný stejný klíč symetrické šifry. CHAP autentizuje klienta pravidelně v náhodných intervalech. (15)

Autentizace probíhá ve třech krocích:

1) Po navázání spojení server pošle „challenge“ zprávu klientovi, obsahující náhodný řetězec
2) Klient odpoví MD5 otiskem zaslaného řetězce

3) Server porovná MD5 otisk ve zprávě se svým otiskem. Pokud jsou shodné, autentizace klienta je úspěšná.

3.4.5 EAP

Extensible Authentication Protocol (EAP) je univerzální autentizační protokol často používaný v bezdrátových sítích, ale není jimi omezen a dokáže fungovat i v metalické síti. Technologie zabezpečení WPA a WPA2 používají některé EAP metody jako své autentizační mechanizmy. Celkem lze vybírat asi z čtyřiceti EAP metod. Přiblížím zde jen ty metody, které jsou podporovány RADIUS serverem. (16)

3.4.5.1 EAP-MD5

Tato metoda je založena na MD5 otisku hesla a je tedy náchylná na slovníkový útok. Tato metoda poskytuje pouze autentizaci klienta se serverem, ale ne naopak, což ji dělá zranitelnou útokem typu man-in-the-middle. (16)

3.4.5.2 LEAP

LEAP je proprietální EAP metoda vyvinutá společností Cisco Systems. Používá modifikovanou verzi MS-CHAP, protokol, kde uživatelské údaje nejsou zvlášť chráněné. V roce 2004 byla vydána utilita ASLEAP, která zneužívá tyto nedostatky, a proto se tato metoda nedoporučuje používat. (16)

3.4.5.3 EAP-TLS

EAP – Transport Layer Security je otevřený standard, široce podporovaný mezi výrobci bezdrátových zařízení. I přes to, že jeho bezpečnost je velmi silná a je považován za nejbezpečnější EAP metodu, je zřídkakdy nasazován. Pracuje jak s certifikáty, tak s uživatelskými údaji, takže pro útočníka i znalost hesla uživatele neznamená proniknutí do sítě. (16)

3.4.5.4 EAP-TTLS

EAP-Tunneled Transport Layer Security rozšiřuje EAP-TLS metodu. Uživatel již nemusí mít certifikát od certifikační autority, stačí mít tento certifikát na serveru. To velmi zjednodušuje vybudování zabezpečení, protože certifikát nemusí být instalován na každém klientském zařízení. (16)

3.4.5.5 PEAP

PEAP vznikl spojením úsilí společností Cisco Systems, Microsoft a RSA Security jako otevřený standard. Je široce podporovaný a nabízí dobré zabezpečení. Ve svém návrhu je podobný EAP-TTLS, vyžadující certifikát jen na straně serveru. S klientem je pak vytvořen zabezpečený tunel, chránící celý autentizační proces. I když přišel na trh později než EAP-TTLS, velmi rychle se rozšířil. (16)

3.5 Debian GNU/Linux

Debian GNU/Linux je distribuce operačního systému. Tento operační systém používá jádro Linuxu a je vyvíjen jako nekomerční projekt velkým množstvím dobrovolníků z celého světa. Jedná se o nejrozšířenější linuxovou distribuci vůbec.

Zakladatelem distribuce Debian je Ian Murdock. Utvářel se v letech 1994 – 1995, přičemž v roce 1995 proběhlo portování na různé hardwarové architektury. V roce 1996 vyšla první stabilní verze. (17)

3.5.1 Verze distribuce

Vývojáři udržují tři hlavní verze své distribuce. Těmto verzí odpovídají i instalační balíčky softwarových aplikací v repozitářích.

3.5.1.1 Stable

Stabilní verze distribuce. Všechen software obsazený v této distribuci je otestovaný, odladěný a bez závažných chyb. Vyznačuje se perfektní stabilitou, ale verze aplikací mohou být zastaralé. Nejnovější verze této distribuce je verze 5.0.1 (lenny), vydána 11. dubna 2009.

3.5.1.2 Testing

Testovací distribuce. Obsahuje balíčky, které ještě čekají na přijetí do „stable“ verze. Uživatelé se mohou setkat s chybami. Tato verze distribuce se hodí pro domácí nebo kancelářské využití, neboť obsahuje nejnovější verze aplikací a není nutná 100% stabilita.

3.5.1.3 Unstable

Distribuce, ve které probíhá aktivní vývoj Debianu, je velmi nestabilní. Z tohoto důvodu je vhodná jen pro vývojáře, nebo nadšence.

Dále existují verze *oldstable*, která sdružuje staré verze „stable“ aplikací a verze *experimental*, která se používá výhradně k pokusům. Aplikace jsou v ní zpravidla z verze „unstable“.

3.5.2 Systém repozitářů

Balíčkovací systémy pracují velmi úzce se systémem repozitářů. Repozitář je sklad, kde jsou uloženy softwarové balíčky. Může se jednat o lokální adresář, fyzicky disk, nebo celý server. V těchto repozitářích balíčkovací systém vyhledává vhodné verze aplikací podle pokynů uživatele. Stejně jako u verzí distribuce samotného systému, i zde jsou aplikace rozděleny na verze stable, testing a unstable. Pro rovnoměrnou zátěž sítě jsou repozitáře umístěny po celém světě a uživatel si určuje, v kterých repozitářích mu bude balíčkovací systém vyhledávat

3.5.3 Aplikace

Debian, jakožto unixový derivát, dokáže instalovat aplikace z centrálních repozitářů, které jsou umístěny na internetu. Pomocí balíčkovacího systému je uživatel schopný spravovat velmi jednoduše všechny nainstalované aplikace, instalovat nové, popř. updatovat na nové verze. Balíčkový systém bývá specifický pro různé linuxové distribuce.

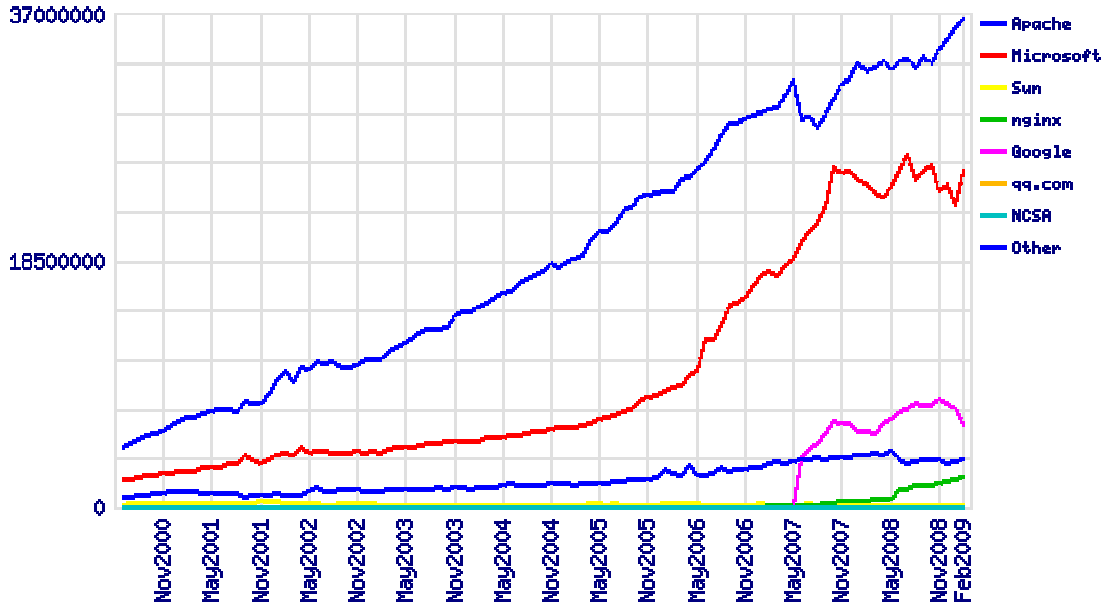
Distribuce Debian používá ATP – Advanced Packaging Tool. ATP je souhrn několika programů – atp-get, apt-cache, atp. Díky tomuto balíčkovacímu systému je uživatel schopný vyhledávat v repozitářích, aktualizovat aplikace, instalovat a odebírat aplikace nebo rovnou aktualizovat celý systém na novou verzi.

Obrovskou výhodou balíčkovacího systému je hlídání si závislostí balíčků. Tzn., že tento systém ví, jaké jsou v systému nainstalované balíčky a pokud nově instalovaná aplikace pro svůj běh potřebuje nějaký jiný balíček, který v systému chybí, nabídne jej okamžitě také ke stáhnutí.

3.5.3.1 Apache HTTP Server

Apache HTTP Server (dále jen Apache) je softwarový webový server. Je vyvíjen jako open source a dokáže fungovat na celé řadě platforem od domácích spotřebičů, přes mobilní telefony a síťová zařízení, až po velké serverové farmy. Nejrozšířenější jsou však jeho linuxové mutace. (18)

Vznikl v roce 1995 a od té doby jeho popularita stále roste. V počátcích nahradil Netscape Communications Corporation web server, v roce 1997 běžel na 57% všech serverů a v roce 2005 byl nasazen na 69%. I dnes je Apache nerozšířenějším webovým serverem vůbec. (19)



Graf 2.1 – Celkový počet nasazených serverových řešení (19)

Apache je silně modulární systém, jehož schopnosti lze velmi lehce rozšířit doinstalováním patřičného modulu. Ty mohou být od programovacího jazyka po autentizační schémata. Mezi oblíbené skriptovací jazyky patří např. PHP, Python, Perl. Zabezpečovací moduly dokážou např. SSL.

3.5.3.2 MySQL

MySQL je relační databázový systém. Je vydáván pod dvěmi licencemi: bezplatnou licencí GPL a komerční placenou licencí. Jejími autory jsou Michael Widenius a David Axmark, dnes je vlastníkem společnost Sun Microsystems. Tato společnost byla na počátku tohoto roku odkoupena společností Oracle Corp.

Využívá SQL – Structured Query Language – strukturovaný dotazovací jazyk pro práci s daty v relační databázi.

Stejně jako Apache je MySQL multiplatformní a lze jej tak snadno implementovat na celou řadu operačních systémů. V kombinaci s nulovou cenou se z něj stal nejrozšířenější databázový systém.

MySQL je většinou instalován v kombinaci s Apache a PHP a tvoří tak základ většiny webových serverů. (20)

3.5.3.3 FreeRADIUS

FreeRADIUS je open source implementace RADIUS serveru a e distribuován pod GPL licencí. Opět lze provozovat na celé řadě různých platforem a operačních systémech. Jedná se o škálovatelný systém, který podle dokumentace dokáže fungovat i v sítích o milionech uživatelích. Podporuje celou řadu autentizačních protokolů.

FreeRADIUS svůj vývoj započal v roce 1999, přičemž ostrá verze spatřila světlo světa v roce 2001. Od té doby vychází nová verze každých pár měsíců. Nejnovější verze je verze 2.1.4 z dubna 2009.

4 Analýza problému a současné situace

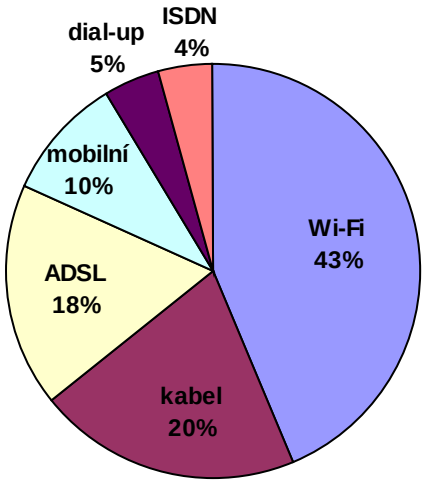
4.1 ČR jako Wi-Fi velmoc

Českou republiku bychom mohli označit za Wi-Fi velmoc. Téměř polovina všech připojených domácností v ČR se na internet dostává díky některému z mnoha poskytovatelů Wi-Fi připojení.

Proč tomu tak je? Český Telekom se v letech 2001-3 bezhlavě držel zastaralé a předražené ISDN technologie, která v podstatě nenabízela klientům žádný výraznější přínos od klasického vytáčeného připojení. ADSL bylo v nedohlednu a tak hlad zákazníků po stálém, rychlém a levném připojení dal možnost vzniku obrovskému množství lokálních poskytovatelů bezdrátového připojení k internetu.

Zavedením ADSL technologie se trend neobrátil. ADSL přineslo FUP – Fair User Policy – měsíční datové limity, nutnost placení poplatků za telefonní linku, i když ji klient nepotřeboval. Vedle toho byla nabídka bezdrátového internetu stále lepší řešení.

Dnes je technologie ADSL již více konkurenceschopná, ale stále zaostává za bezdrátovým připojením, které je čím dál populárnější. Dle průzkumu Českého telekomunikačního úřadu Wi-Fi připojení k internetu používá 44% dotázaných. V minulém roce to bylo 38% a ještě o rok dříve jen 28%. Dnes je podíl bezdrátového připojení asi dvakrát vyšší, než je evropský průměr. (22)



Obrázek 3.1 – internetové připojení domácnosti v roce 2009 (22)

4.2 Decentralizace databází uživatelů

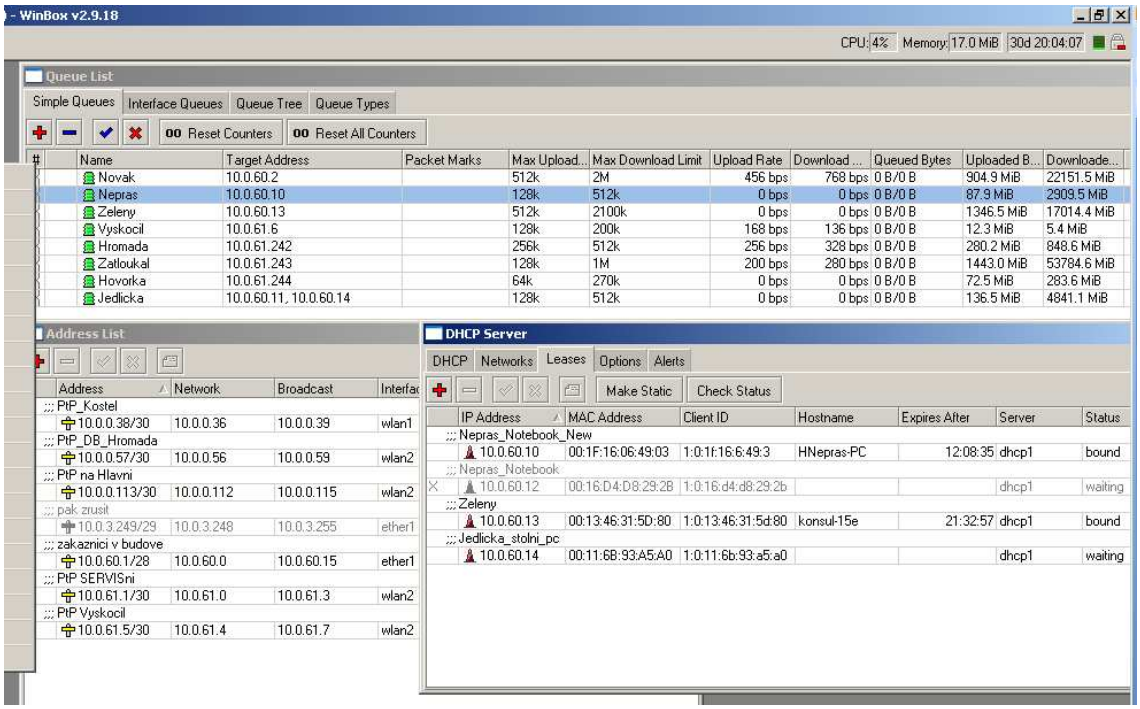
Velký rozmach Wi-Fi poskytovatelů sebou přinesl i rychlý rozvoj infrastruktury bezdrátových sítí. Bezdrátové sítě lze nyní najít téměř v každé obci a pokrytí je i v těch nejvzdálenějších koutech republiky.

Poskytovatelé bezdrátového připojení k internetu musí spravovat desítky přístupových bodů, aby se jejich klienti mohli připojit. Na každý takový bod přistupuje několik uživatelů a poskytovatel musí zajistit, aby se na něj nedostal nikdo jiný. Z vlastní zkušenosti vím, že velká část poskytovatelů k tomu využívá samotné přístupové body a možnosti operačních systémů těchto bodů.

Velmi rozšířeným zařízením pro přístupové body jsou RouterBOARDy od společnosti MikroTik, které dokáží spravovat několik málo desítek uživatelů. Takových přístupových bodů může mít poskytovatel několik a na každém je malá databáze uživatelů, kteří mají přístup právě na tento bod, o kus dál je jiný přístupový bod s dalšími uživateli a o další kus další.

S každým novým přístupovým bodem roste decentralizace uživatelské báze a správa uživatelských účtů se pak stává noční můrou v době, kdy se např. hromadně

mění tarify. Mohou vznikat také bezpečnostní rizika, když např. při správě jedné části databáze se zapomene „zamknout“ přístupový bod a zůstane otevřený pro všechna připojení.



Obrázek 3.2 – Administrace uživatelských účtů na přístupovém bodě

Proč tomu tak je? Dle mého názoru poskytovatelé jsou příliš pohodlní na to, aby hledali a implementovali nová řešení a to i v případě, že se jim přímo nabízí a investice do něj jsou minimální.

4.3 Absence šifrování

Velkým bezpečnostním rizikem je nepoužívání šifrování přenosu dat. Většina poskytovatelů své zákazníky nechrání šifrováním. U domácností je tato situace lepší a nezabezpečenou domácí síť je daleko obtížnější najít.

Důvodem u poskytovatelů z počátku mohl být výkonový deficit zařízení přístupových bodů a nekompatibilita klientských zařízení. Přesto, že se dnes masivně přešlo na 5GHz pásmo a vyměnila se klientská zařízení, bezpečnost přenosu se výrazně nezvýšila.

5 Vlastní návrh řešení

5.1 Serverové aplikace

5.1.1 Debian

Na výběr byla celá řada linuxových distribucí, ale vzhledem k tomu, že velká část vychází právě z distribuce Debian, byla zvolena tato distribuce. Tento operační systém byl také zvolen pro jeho obrovskou stabilitu a velkou uživatelskou základnu, takže v případě nějakých potíží nebude těžké najít řešení. Vybrána byla poslední „stable“ verze 5.0.1 s kódovým označením *lenny*, aby se předešlo chybám v neodladěných verzích.

Při instalaci se nabízí několik variant této distribuce, které se liší nainstalovanými aplikacemi. Lze si vybrat mezi přednastavenými konfiguracemi např. pro desktopové prostředí, databázový server, webový server atp. Pro zvýšení bezpečnosti bych však doporučil instalovat pouze základní verzi a jednotlivé verze aplikací doinstalovat později. Předejde se tak tomu, že na serveru poběží nějaká služba, kterou uživatel nainstaloval v rámci instalace systému, běží v defaultním nastavení a dává možnost útoku na server.

5.1.2 MySQL

MySQL bude sloužit pro databázi uživatelů, jejich autentizační a autorizační údaje a sběr accountingových dat. Pro *lennyho* je dostupná stabilní verze 5.0.51a.

Pro účely RADIUS serveru je vhodné vytvořit novou databázi a uživatele s přístupem do této databáze. Aplikace FreeRADIUS obsahuje SQL skript na vytvoření všech potřebných tabulek. Skript se nachází v */etch/freeradius/sql/mysql/schema.sql*. Po jeho spuštění vznikne v databázi osm tabulek.

5.1.2.1 Struktura databáze

Aplikace FeeRADIUS využívá tyto tabulky:

- radacct – sběr accountingových dat
- radcheck – autentizační údaje uživatele
- radgroupcheck – autentizační údaje skupiny
- radgroupreply – autorizační údaje skupiny
- radreply – autorizační údaje uživatele
- usergroup – přiřazuje uživatele do skupin
- radpostauth – záznamy přihlašování
- nas – definice NAS jednotek

Celé schéma funguje tak, že uživatel se pokusí autentizovat. Autentizační údaje se vyberou z tabulky *radcheck*, pokud je autentizace úspěšná, server vybere z tabulek *radreply* a *radgroupreply* autorizační údaje a pošle je NAS jednotce. Záznam o přihlášení se zapíše do *radpostauth* a NAS jednotka posílá accountingová data od uživatele, které se zaznamenávají do tabulky *radacct.*

5.1.3 Apache HTTP server a PHP

HTTP server není nezbytně nutný, ale velmi zjednodušuje administraci. Je dostupný pro *stable* distribuci Debianu ve verzi 1.3.34. HTTP je vhodné kombinovat se skriptovacím jazykem PHP, dostupným ve verzi 5.

Doinstalováním balíčku *phpmyadmin* lze spravovat MySQL serverovou aplikaci pohodlně z internetového prohlížeče. Také se otevírá možnost přistupovat do databáze pomocí vlastních PHP skriptů.

5.1.3.1 PHP skripty

V příloze lze nalézt několik jednoduchých PHP skriptů na správu uživatelů v databázi. Jedná se o přidání uživatele do databáze, odstranění uživatele a vyhledávání v databázi.

5.1.4 FreeRADIUS

Stěžejní aplikace, dostupná ve *stable* verzi 2.0.4, zabezpečující celý autentizační proces. Je široce konfigurovatelná pomocí textových konfiguračních souborů. Lze například definovat, odkud bude brát autentizační údaje – databázové systémy SQL, Kerberos, nebo pouze textový soubor, nastavení zabezpečení, atp.

Konfigurační soubory jsou velmi dobře zdokumentovány a každé nastavení je v nich pečlivě popsáno.

5.1.4.1 radiusd.conf

Hlavní konfigurační soubor aplikace, který ovlivňuje její chování. Zahrnuje nastavení přístupových práv aplikace, výpisů logů, zahrnutí jednotlivých modulů, počet vláken aplikace atp.

5.1.4.2 clients.conf

V tomto konfiguračním souboru definujeme IP adresy jednotek, kterým chceme poskytnout přístup k serveru. Kromě IP adresy se NAS jednotka musí prokázat heslem - *secret*, které se definuje také zde.

Příklad konfigurace NAS jednotky:

```
client 192.168.3.2 {
       secret          = 123aaa
       shortname       = MT_hlavni_trida_8
       nastype         = mikrotik
}
```

5.1.4.3 users.conf

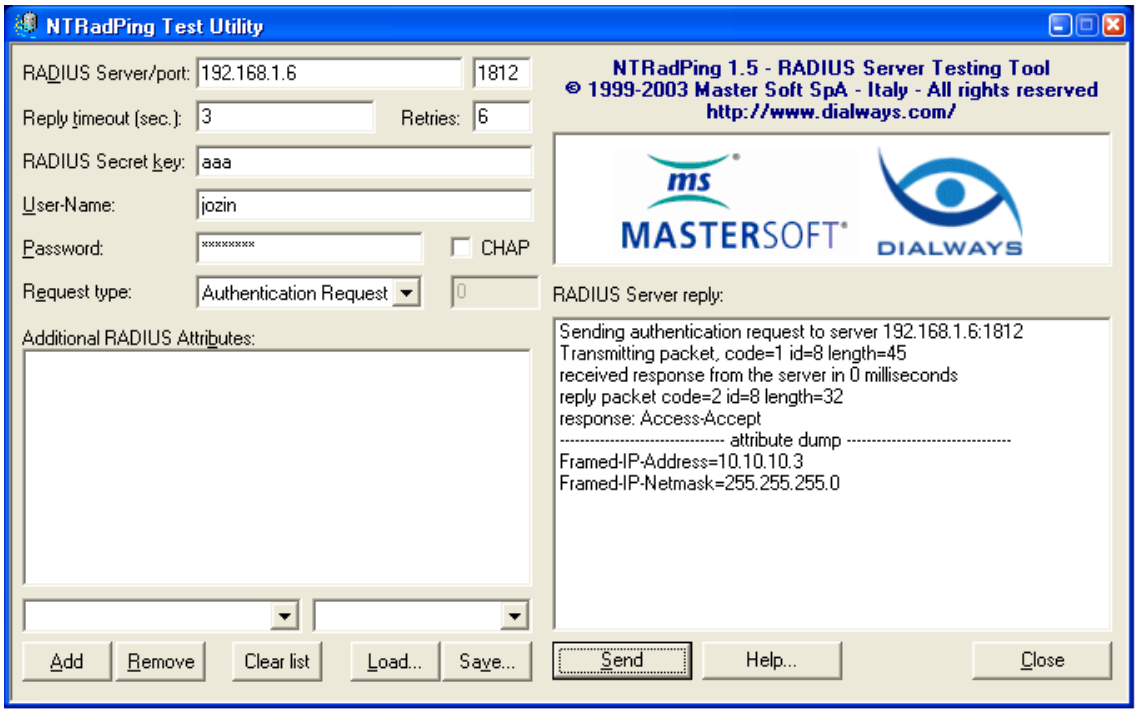
Soubor, ze kterého je možné brát autentizační a autorizační údaje. Zde bych doporučil nechat pouze jednoho testovacího uživatele nebo tento soubor nepoužívat.

5.1.4.4 sql.conf

V tomto souboru se definuje nastavení SQL databáze. Je nutno nastavit adresu SQL serveru a autentizační údaje pro přístup do databáze. Pokud byl použit skript *schema.sql*, není nutné zde nic jiného měnit. Je tu ale možnost definovat kompletní nastavení tabulek pro nestandardní databáze.

5.1.4.5 Ověření funkčnosti

Pro ověření funkčnosti lze použít volně dostupnou aplikaci NTRadPing. Na screenshotu této aplikace je vidět úspěšný pokus o autentizaci. Server běžící na adrese *192.168.1.6:1812* potvrdil autentizaci uživatele „*jozin*“ a zaslal autorizační údaje s IP adresou a maskou podsítě.



Obrázek 4.1 – Příklad úspěšné autentizace pomocí NTRadPing

5.2 Hardwarová řešení

Mnou navrhované řešení si žádá kompatibilní síťová zařízení. Velkou výhodou však je, že tato technologie je široce podporována ve většině zařízení. Také starší nekompatibilní zařízení jsou velmi rychle nahrazována novějšími z důvodů vysokého zarušení 2,4 GHz pásma, v kterém tyto starší přístroje pracují.

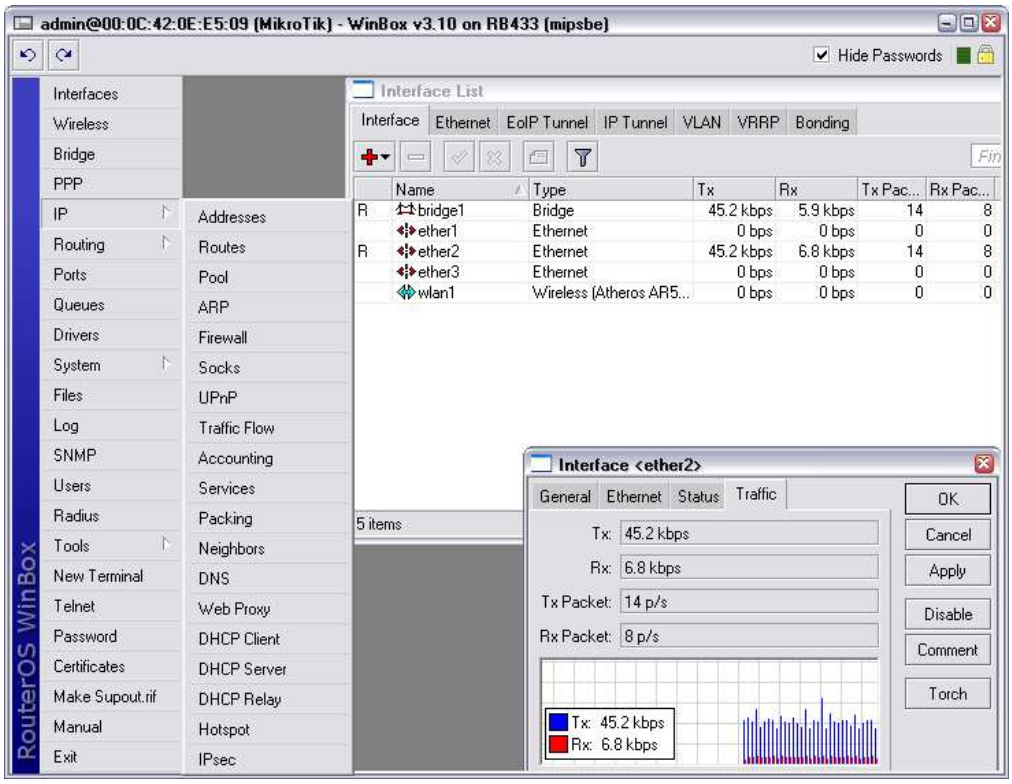
5.2.1 MikroTikls SIA

Společnost MikroTikls SIA, známá spíš jako MikroTik, vyvíjí síťová zařízení pro náročná nasazení. Mezi produkty patří základní desky RouterBOARD, které obsahují několik MiniPCI portů sloužící pro osazení bezdrátovými kartami dle výběru nasazení. Největší devizou je však operační systém RouterOS.

Tyto zařízení lze najít téměř u všech poskytovatelů bezdrátového připojení, proto implementace RADIUS autentizace nevyžaduje investici do inovace přístupových bodů, ale jenom změnu nastavení v systému zařízení.

5.2.1.1 RouterOS

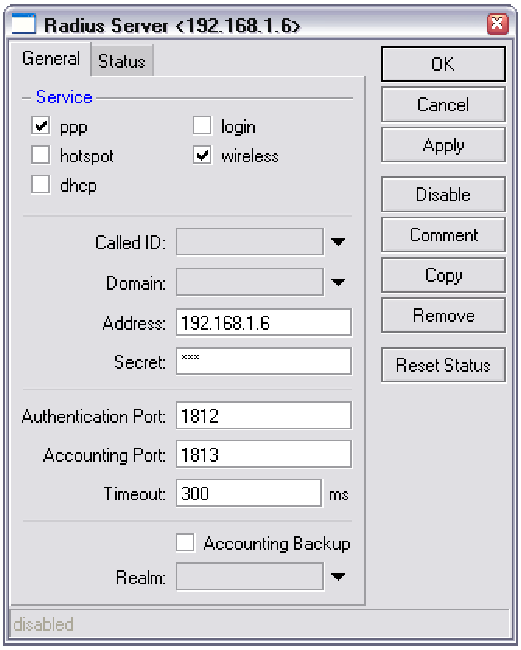
RouterOS slouží k velmi pokročilé administraci celého zařízení. Lze jej ovládat pomocí konzolových příkazů, ale také pomocí grafické utility WinBox.



Obrázek 4.2 – Grafické rozhraní WinBox

Možnosti tohoto systému jsou obrovské, od obyčejných schopností jako routování, DHCP serveru, firewallu přes uživatelské databáze, sledování vytížení sítě, omezování P2P provozu až po složité skriptování.

Pro účely autentizace uživatelů přes RADIUS serveru slouží menu Radius. Zde lze konfigurovat nastavení přístupu k RADIUS serveru. Je zde nutné definovat IP adresu serveru a heslo, port na autentizaci NAS jednotky, port na odesílání accountingových dat a služby, na kterých bude tento typ autentizace přístupný.



Obrázek 4.3 – Nastavení RADIUS serveru ve WinBoxu

5.2.1.2 Podporované atributy

Zařízení MikroTik mají vlastní slovník atributů, které dokáží přijímat od FreeRADIUS serveru. Tyto atributy slouží k nastavení služby uživateli a je nutné je definovat do tabulek *radreply* nebo *radgroupreply*. Mezi důležité parametry patří:

Žádost o autentizaci

- NAS-Identifier – identita NAS jednotky
- NAS-IPAddress – IP adresa NAS jednotky
- User-Password – šifrované heslo (použití u PAP autentizace)

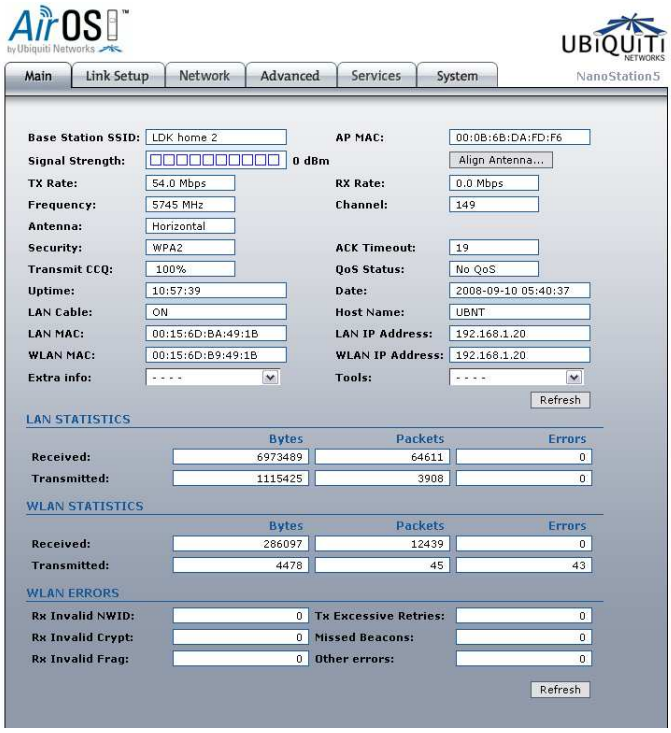
Úspěšná autentizace

- Framed-IP-Address – IP adresa uživatele
- Framed-IP-Netmask – maska podsítě uživatele

- Framed-Pool – rozsah adres, z kterého MikroTik přidělí adresu klientovi
- Mikrotik-Rate-Limit – rychlostní omezení pro uživatele, včetně nastavení „burst“ módu

5.2.2 NanoStation5

NanoStation5 je klientské bezdrátové zařízení vyrobené společností Ubiquity Networks. Pracuje pouze ve specifikaci 802.11a, má pouze jeden LAN port, který zároveň slouží pro napájení za použití technologie POE. Zároveň zařízení dokáže komunikovat nejrozšířenějšími bezpečnostními protokoly, včetně autentizace proti RADIUS serveru Tyto vlastnosti dělají zařízení naprosto ideální pro použití u klienta.



Obrázek 4.4 – Webové rozhraní síťového zařízení NanoStation5

Konfigurace se provádí přes webové rozhranní. Je nutno nastavit bezdrátové zařízení do módu *Station*, chová se tedy jako klientská stanice. Integrované vyhledávání přístupových bodů pak usnadní výběr toho správného. Při vyhledávání lze sledovat i výkyvy signálu a stanici tak přesněji zaměřit. Nastavením zabezpečení a autentizačních údajů je konfigurace u konce.

6 Závěr

Výrazný rozmach poskytovatelů bezdrátového připojení k internetu způsobil problematickou administraci a zabezpečení přístupových bodů.

Mnou navrhované řešení řeší problém složité správy databáze uživatelů v bezdrátových sítích zavedením autentizačního serveru typu RADIUS a také odpovídá na otázku zabezpečení přenosu dat mezi uživatelem a přístupovým bodem, která je tak opomíjená mezi poskytovateli bezdrátového připojení k internetu.

Toto řešení nabízí přístup přes webový prohlížeč k centrální databázi uživatelských účtů a tím obrovsky zjednodušuje administraci. Protože je databáze postavena na velmi rozšířené platformě MySQL, je zde možnost provázání této databáze i s řadou jiných služeb.

Velkou výhodou jsou také téměř nulové náklady, protože většina síťových zařízení je s touto technologií kompatibilní a serverové aplikace mohou běžet ve virtualizovaném prostředí fyzického serveru s výkonovou rezervou.

Jednou z mála nevýhod tohoto řešení oproti stávajícímu je složitější počáteční konfigurace a nutnost specializovaného serveru. Ale jinak je tato technologie připravená obsluhovat i několik desítek tisíc uživatelů.

Toto řešení najde své uplatnění i v případě nasazení sítí využívající optické spoje. Mnozí operátoři v hustě obydlených oblastech (např. sídliště) opouštějí od bezdrátových technologií a nasazují právě optiku. Přítomnost RADIUS serveru i v takové síti zajistí autentizaci klientů a zamezí přistup všem nepovolaným uživatelům i když budou mít fyzický přistup k přípojce. Přičemž úpravy na serverové části řešení jsou minimální a konfigurace probíhá pouze u klientských NAS jednotek

7 Seznam použité literatury

(1) *IEEE 802.11* [online]. 2009 [citováno 2.5.2009]. Dostupný z WWW: <http://en.wikipedia.org/wiki/IEEE_802.11#802.11-1997_.28802.11_legacy.29>

(2) *FHSS* [online]. 2009 [citováno 2.5.2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/FHSS>

(3) *Direct Sequence Spread Spectrum* [online]. 2009 [citováno 3.5.2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/DSSS>

(4) *IEEE 802.11* [online]. 2009 [citováno 2.5.2009]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/IEEE_802.11>

(5) *List of WLAN channels* [online]. 2009 [citováno 6.5.2009]. Dostupný z WWW: <http://en.wikipedia.org/wiki/List_of_WLAN_channels>

(6) *IEEE 802.11g-2003* [online]. 2009 [citováno 6.5.2009]. Dostupný z WWW: <http://en.wikipedia.org/wiki/IEEE_802.11g-2003>

(7) *IEEE 802.11a-2003* [online]. 2009 [citováno 6.5.2009]. Dostupný z WWW: <http://en.wikipedia.org/wiki/IEEE_802.11a-1999>

(8) *WiMAX* [online]. 2009 [citováno 8.5.2009]. Dostupný z WWW: <http://en.wikipedia.org/wiki/WiMAX>

(9) *Srovnání vybraných wireless technologií 2/2* [online]. 2009 [citováno 8.5.2009]. Dostupný z WWW: <http://pctuning.tyden.cz/srovnani_vybranych_wireless_technologii_22/wi-fi-aneb-wireless-fidelity>

(10) ZANDL, Patrick. *Bezdrátové sítě WiFi : praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

(11) STEJSKAL, Petr. *Bezdrátové sítě WiFi, stand. 802.11b/g* [online]. 2009 [citováno 8.5.2009]. Dostupný z WWW: <http://www-kiv.zcu.cz/~simekm/vyuka/pd/zapocty-2003/wi-fi/index.php?id=3>

(12) STEJSKAL, Petr. *Bezdrátové sítě – Wi-Fi, Bezpečnost* [online]. 2009. [citováno 9.5.2009]. Dostupný z WWW: <http://www-kiv.zcu.cz/~simekm/vyuka/pd/zapocty-2003/wi-fi/index.php?id=5>

(13) *MAC address* [online]. 2009 [citováno 9.5.2009]. Dostupný z WWW: <http://en.wikipedia.org/wiki/MAC_address>

(14) ŠUSTR, Matej. *Analýza bezpečnosti štandartu IEEE 802.11*. Diplomová práce. Slovenská technická univerzita v Bratislavě, Fakulta elektrotechniky a informatiky. 2007. vedoucí diplomové práce Ing. Martin Rakús, PhD.

(15) *Linková vrstva* [online]. 2009 [citováno 12.5.2009]. Dostupný z WWW: <http://www.cpress.cz/knihy/tcp-ip-bezp/CD-0x/4.html>

(16) *Extensible Authentication Protocol* [online]. 2009 [citováno 12.5.2009]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol>

(17) *A Brief History of Debian* [online]. 2009 [citováno 15.5.2009]. Dostupný z WWW: <http://www.debian.org/doc/manuals/project-history/ch-detailed.en.html>

(18) *About the Apache HTT Server Project* [online]. 2009 [citováno 15.5.2009]. Dostupný z WWW: <http://httpd.apache.org/ABOUT_APACHE.html>

(19) *February 2009 Web Server Survey* [online]. 2009 [citováno 16.5.2009]. Dostupný z WWW: <http://news.netcraft.com/archives/2009/02/18/february_2009_web_server_survey.html>

(20) *About MySQL* [online]. 2009 [citováno 16.5.2009]. Dostupný z WWW: <http://www.mysql.com/about/>

(21) *About the FreeRADIUS Project* [online]. 2009 [citováno 17.5.2009]. Dostupný z WWW: <http://freeradius.org/about.html>

(22) *ČTÚ: Češi nadprůměrně využívají bezdrátové připojení k internetu* [online]. 2009 [citováno 17.5.2009]. Dostupný z WWW: <http://www.ceskenoviny.cz/zpravy/ctu-cesi-nadprumerne-vyuzivaji-bezdratove-pripojeni-k-internetu/362056>

8 Přílohy

Příloha 1: Sada PHP skriptů pro přidání, vyhledávání a odstranění uživatelů z databáze

Příloha 2: MySQL skript pro naplnění databáze tabulkami

Příloha 2: MySQL skript pro naplnění databáze tabulkami (převzato z konfiguračních souborů aplikace FreeRADIUS)

```
CREATE TABLE radacct (
  RadAcctId bigint(21) NOT NULL auto_increment,
  AcctSessionId varchar(32) NOT NULL default '',
  AcctUniqueId varchar(32) NOT NULL default '',
  UserName varchar(64) NOT NULL default '',
  Realm varchar(64) default '',
  NASIPAddress varchar(15) NOT NULL default '',
  NASPortId varchar(15) default NULL,
  NASPortType varchar(32) default NULL,
  AcctStartTime datetime NOT NULL default '0000-00-00 00:00:00',
  AcctStopTime datetime NOT NULL default '0000-00-00 00:00:00',
  AcctSessionTime int(12) default NULL,
  AcctAuthentic varchar(32) default NULL,
  ConnectInfo_start varchar(50) default NULL,
  ConnectInfo_stop varchar(50) default NULL,
  AcctInputOctets bigint(12) default NULL,
  AcctOutputOctets bigint(12) default NULL,
  CalledStationId varchar(50) NOT NULL default '',
  CallingStationId varchar(50) NOT NULL default '',
  AcctTerminateCause varchar(32) NOT NULL default '',
  ServiceType varchar(32) default NULL,
  FramedProtocol varchar(32) default NULL,
  FramedIPAddress varchar(15) NOT NULL default '',
  AcctStartDelay int(12) default NULL,
  AcctStopDelay int(12) default NULL,
  PRIMARY KEY  (RadAcctId),
  KEY UserName (UserName),
  KEY FramedIPAddress (FramedIPAddress),
  KEY AcctSessionId (AcctSessionId),
  KEY AcctUniqueId (AcctUniqueId),
  KEY AcctStartTime (AcctStartTime),
  KEY AcctStopTime (AcctStopTime),
  KEY NASIPAddress (NASIPAddress)
) ;

CREATE TABLE radcheck (
  id int(11) unsigned NOT NULL auto_increment,
  UserName varchar(64) NOT NULL default '',
  Attribute varchar(32)  NOT NULL default '',
  op char(2) NOT NULL DEFAULT '==',
  Value varchar(253) NOT NULL default '',
  PRIMARY KEY  (id),
  KEY UserName (UserName(32))
) ;

CREATE TABLE radgroupcheck (
  id int(11) unsigned NOT NULL auto_increment,
  GroupName varchar(64) NOT NULL default '',
  Attribute varchar(32)  NOT NULL default '',
  op char(2) NOT NULL DEFAULT '==',
  Value varchar(253)  NOT NULL default '',
  PRIMARY KEY  (id),
  KEY GroupName (GroupName(32))
) ;
```

```
CREATE TABLE radgroupreply (
  id int(11) unsigned NOT NULL auto_increment,
  GroupName varchar(64) NOT NULL default '',
  Attribute varchar(32)  NOT NULL default '',
  op char(2) NOT NULL DEFAULT '=',
  Value varchar(253)  NOT NULL default '',
  PRIMARY KEY  (id),
  KEY GroupName (GroupName(32))
) ;

CREATE TABLE radreply (
  id int(11) unsigned NOT NULL auto_increment,
  UserName varchar(64) NOT NULL default '',
  Attribute varchar(32) NOT NULL default '',
  op char(2) NOT NULL DEFAULT '=',
  Value varchar(253) NOT NULL default '',
  PRIMARY KEY  (id),
  KEY UserName (UserName(32))
) ;

CREATE TABLE usergroup (
  UserName varchar(64) NOT NULL default '',
  GroupName varchar(64) NOT NULL default '',
  priority int(11) NOT NULL default '1',
  KEY UserName (UserName(32))
) ;

CREATE TABLE radpostauth (
  id int(11) NOT NULL auto_increment,
  user varchar(64) NOT NULL default '',
  pass varchar(64) NOT NULL default '',
  reply varchar(32) NOT NULL default '',
  date timestamp(14) NOT NULL,
  PRIMARY KEY  (id)
) ;

CREATE TABLE nas (
  id int(10) NOT NULL auto_increment,
  nasname varchar(128) NOT NULL,
  shortname varchar(32),
  type varchar(30) DEFAULT 'other',
  ports int(5),
  secret varchar(60) DEFAULT 'secret' NOT NULL,
  community varchar(50),
  description varchar(200) DEFAULT 'RADIUS Client',
  PRIMARY KEY (id),
  KEY nasname (nasname)
);
```