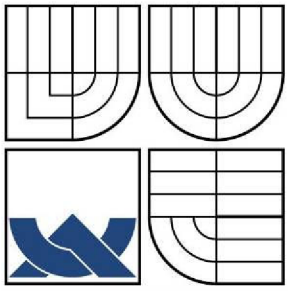
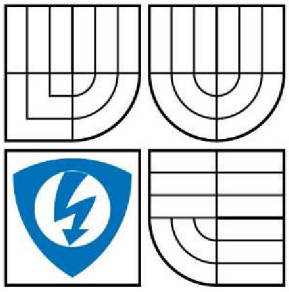


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKACNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH ŘEŠENÍ AUTENTIZACE A AUTORIZACE V BEZDRÁTOVÝCH LOKÁLNÍCH SÍTÍCH

CONCEPT OF AUTHENTICATION AND AUTHORIZATION IN WIRELESS LOCAL NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — MICHAL ČÍŽEK
AUTHOR

VEDOUCÍ PRÁCE — DOC. ING. KAREL BURDA, CSC.
SUPERVISOR

BRNO 2008

ANOTACE

Tato práce pojednává o dostupných principech a metodách autentizace a autorizace v bezdrátových lokálních sítích. V první části je uveden přehled dostupných metod autentizace, jejich krátký popis a zhodnocení jejich použitelnosti pro malé a středně velké sítě. Druhou část tvoří návrh autentizace a autorizace pro školní bezdrátovou síť o třech přístupových bodech, popis konfigurace systému Mikrotik RouterOS a serveru FreeRadius. Práce končí praktickým ověřením návrhu a zhodnocením použitelnosti v praxi.

Klíčová slova: autentifikace, autentizace, autorizace, tarifikace, radius, AAA, hotspot, wlan

ABSTRACT

This thesis is about available priciples and methods of authentication and authorization in wireless local area networks. First part is about available methods of authentication with short description each of them and usage analysis for small and middle-sized wireless networks. There is a project of authentication and authorization for school wireless network of three access points in the second part of the thesis, including description of Mikrotik RouterOS configuration and FreeRadius configuration. In the end of the thesis there is a project tests and usage analysis.

Keywords: authentification, authentication, authorization, accounting, radius, AAA, hotspot, wlan

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: Michal Čížek

Bytem: Malátova 2417/31, 400 11, Ústí nad Labem

Narozen/a (datum a místo): 14. 7. 2008, Ústí nad Labem

(dále jen „autor“)

a

2. Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií

se sídlem Údolní 244/53, 602 00, Brno

jejímž jménem jedná na základě písemného pověření děkanem fakulty:

prof. Ing. Kamil Vrba, CSc.

(dále jen „nabyvatel“)

Čl. 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
   - □ disertační práce
   - □ diplomová práce
   - □ **bakalářská práce**
   - □ jiná práce, jejíž druh je specifikován jako

   .....

   (dále jen VŠKP nebo dílo)

Název VŠKP:	Návrh řešení autentizace a autorizace v bezdrátových lokálních sítích
Vedoucí/ školitel VŠKP:	doc. Ing. Karel Burda, CSc.
Ústav:	Ústav telekomunikací
Datum obhajoby VŠKP:	

VŠKP odevzdal autor nabyvateli v*:

- □ tištěné formě – počet exemplářů …….
- □ elektronické formě – počet exemplářů …….

* hodící se zaškrtněte

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizovaní výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti
   - □ ihned po uzavření této smlouvy
   - □ 1 rok po uzavření této smlouvy
   - □ 3 roky po uzavření této smlouvy
   - □ 5 let po uzavření této smlouvy
   - □ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: ……

…….. ……

Nabyvatel Autor

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma NÁVRH ŘEŠENÍ AUTENTIZACE A AUTORIZACE V BEZDRÁTOVÝCH LOKÁLNÍCH SÍTÍCH jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

podpis autora

PODĚKOVÁNÍ

Děkuji vedoucímu bakalářské práce doc. Ing. Karlovi Burdovi, CSc. za velmi užitečnou metodickou pomoc a cenné rady při zpracování bakalářské práce.

Obsah

1 Úvod

Bezdrátové lokální sítě se dnes využívají v různých oblastech. Setkáme se s nimi jak v domácnostech či kancelářích, tak ve velkých firmách o stovkách přístupových bodů a tisícovkách uživatelů. S rostoucím využitím se zvyšují také nároky na bezpečnostní opatření, řízení přístupu do sítě a důvěrnost přenášených dat.

Pří návrhu bezdrátové sítě je důležité věnovat dostatečný čas volbě správné metody autentizace a autorizace uživatelů sítě. Není snadné zvolit takovou metodu, která uspokojí všechny požadavky na konkrétní realizaci.

Prvním cílem této práce je porovnání dostupných metod a řešení autentizace a autorizace v bezdrátových lokálních sítích a zhodnocení jejich použitelnosti pro malé a středně velké sítě. Druhým cílem je na základě získaných teoretických znalostí navrhnout řešení autentizace a autorizace ve výše uvedených sítích včetně praktického ověření návrhu.

Práce by měla poskytnout nadhled nad danou problematikou, popsat základní principy řešení a usnadnit navrhovateli volbu správné autentizační metody pro konkrétní síť. Dále by měla ukázat možnosti autentizace a autorizace na síťové vrstvě pomocí HotSpot brány s využitím RADIUS serveru včetně praktického ověření. Podobných informací v ucelené podobě je na internetu a v literatuře nedostatek. Proto jsem přesvědčen, že práce může být základem pro řadu řešení v praxi.

2 Autentizace v bezdrátových sítích

2.1 Význam autentizace

Autentizace v bezdrátových sítích je proces, při kterém se posuzuje, zda-li je síťové zařízení/uživatel žádající o přístup k síti oprávněným uživatelem sítě. Při autentizaci se posuzuje identita uživatele/síťového zařízení a jeho případné další údaje. Dalšími údaji mohou být např. hesla, tokeny, digitální certifikáty apod. Na základě úspěšné autentizace je následně uživateli/síťovému zařízení povolen přístup do sítě [10].

2.2 Metody autentizace v bezdrátových sítích

2.2.1 Open System

Tento typ autentizace neposkytuje žádnou úroveň zabezpečení. Jakmile nějaké zařízení zažádá o přihlášení, přístupový bod přihlášení dovolí, aniž by prováděl jakákoli ověření. Tento způsob autentizace je jako jediný vyžadován standardem IEEE 802.11 u všech zařízení, a proto je dosaženo maximální kompatibility zařízení různých výrobců. Tento způsob lze využít ve veřejných bezdrátových sítích, kde není vyžadováno žádné zabezpečení. Vhodné použití může být také v kombinaci s metodou autentizace na síťové vrstvě.

2.2.2 Filtr MAC adres

Velké množství přístupových bodů podporuje funkci filtrování MAC adres. MAC (Medium Access Control) adresa je fyzická adresa síťového zařízení, kterou využívají protokoly linkové vrstvy. MAC adresa má sloužit jako jedinečný identifikátor síťového rozhraní, nicméně ji lze snadno měnit v operačním systému. Délka MAC adresy je 48 bitů a zapisuje se hexadecimálně, nejčastěji ve formátu XX:XX:XX:XX:XX:XX .
Filtrace MAC adres funguje tak, že na přístupovém bodu je nadefinován seznam MAC adres (někdy nazýván jako Access List), které smí/nesmí daný přístupový bod přihlásit do sítě. V takovém případě probíhá kontrola MAC adresy u každé žádosti o přihlášení do sítě a na základě porovnání se seznamem MAC adres je danému zařízení přístup umožněn nebo zamítnut. Pokud bychom chtěli tento způsob autentizace použít ve větší bezdrátové síti o několika desítkách přístupových bodů a stovkách klientů, bylo by velmi administrativně náročné udržovat a aktualizovat stejný seznam MAC adres, zvlášť na každém přístupovém bodu.
Tento způsob neposkytuje vysokou úroveň zabezpečení přístupu do sítě, neboť lze snadno prolomit odposlechnutím komunikace a změnou MAC adresy v operačním systému. Tato metoda nezajišťuje šifrování komunikace mezi přístupovým bodem a klientem.

2.2.3 WEP – Shared Key

WEP (Wired Equivalent Privacy) je metoda zabezpečení bezdrátové sítě, která je součástí standardu IEEE 802.11. WEP se stará o autentizaci zařízení, které žádají o přístup k bezdrátové síti a zajišťuje šifrování komunikace mezi klientem a přístupovým bodem. Jak již vyplývá z názvu, cílem metody je přinést ekvivalentní důvěrnost dat tradičním kabelovým sítím. Tento cíl bohužel nebyl naplněn, neboť metoda obsahuje několik závažných slabin, díky kterým lze WEP prolomit během několika minut. WEP nelze doporučit pro dlouhodobé zabezpečení bezdrátové sítě. V případě, že není možnost použít dokonalejší metodu zabezpečení, doporučuje se často měnit statický sdílený klíč.

2.2.3.1 Autentizace

WEP používá pro autentizaci i šifrování komunikace statický sdílený klíč o velikosti 40 bitů nebo 104 bitů. Tento klíč se používá pro symetrické šifrování dat a musí být stejný pro klienta i přístupový bod.

Autentizace probíhá v následujících krocích:

1. Klientská stanice pošle žádost o autentizaci přístupovému bodu
2. Přístupový bod pošle klientovi výzvu s nezašifrovaným textem
3. Klientem přijatý nezašifrovaný text zašifruje pomocí nastaveného WEP klíče a pošle přístupovému bodu další žádost o autentizaci s přiloženým zašifrovaným textem.
4. Přístupový bod přijatý text rozšifruje pomocí svého nastaveného WEP klíče a porovná jej s původně zaslaným nezašifrovaným textem. Pokud se oba texty shodují, znamená to, že klient používá stejný klíč jako přístupový bod a může být autentizován.
5. Přístupový bod na základě porovnání textu pošle klientovi zprávu o úspěšné/neúspěšné autentizaci a v případě úspěchu přihlásí klienta do sítě. Následně je WEP využíván pro šifrování komunikace mezi klientem a přístupovým bodem.

2.2.3.2 Šifrování

Pro šifrování je používán šifrovací algoritmus RC4. Standardní 64-bitový WEP funguje tak, že spojí 40-bitový statický sdílený klíč s 24-bitovým inicializačním vektorem a pomocí algoritmu RC4 je vytvořena posloupnost, která je potom logicky sečtena s nešifrovanými daty. Inicializační vektor se dynamicky mění pro každý rámec a je posílán v otevřené formě. Pokud bude dvakrát za sebou poslán stejný paket, výsledná šifra se bude lišit. 40-bitový statický sdílený klíč se nikdy nepřenáší mezi klientem a přístupovým bodem. Pro lepší zabezpečení lze použít 128-bitový WEP, kde je 104 bitů určeno pro statický sdílený klíč a 24 bitů pro inicializační vektor.

2.2.3.3 Bezpečnostní rizika

Při použití WEP jak pro autentizaci, tak i pro šifrování se vystavujeme bezpečnostnímu riziku. Díky použití statického klíče, který se v čase nemění, lze WEP snadno prolomit. Protože se používá 24-bitový inicializační vektor, existuje pouze cca 16 miliónů kombinací šifrování stejného rámce. Stačí odchytit několik set tisíc paketů a pomocí některého z programů dostupných na internetu (např. WEPCrack) lze získat použitý statický sdílený klíč. Použití 128-bitového WEP pouze prodlužuje dobu potřebnou pro získání statického sdíleného klíče.

2.2.4 WPA PSK

WPA (Wi-Fi Protected Access) byl vytvořen primárně pro využití standardu 802.1X/EAP – využití autentizačního serveru pro autentizaci a distribuci dynamických klíčů. Existuje však také druhá varianta WPA PSK (Pre Shared Key), která funguje podobně jako WEP, ale odstraňuje jeho zásadní bezpečnostní nedostatky. U WPA PSK se používá protokol TKIP (Temporal Key Integrity Protocol), který používá stejně jako WEP algoritmus RC4, ale klíč má místo 40 bitů délku 128 bitů s 48 bitovým inicializačním vektorem. Protokol TKIP přináší oproti WEP dvě zásadní výhody. TKIP řeší automatické střídání šifrovacích klíčů v čase, proto je každý paket, přenášený mezi přístupovým bodem a klientem, šifrován jiným šifrovacím klíčem. Přispívá k tomu také

použití 48 – bitového inicializačního vektoru. TKIP používá oproti WEP lepší způsob zajištění integrity zpráv MIC (Message Integrity Check - zvaný "Michael") [1].
WPA PSK poskytuje dostatečné zabezpečení malých bezdrátových sítích v domácnostech nebo kancelářích. Je vhodné jej použít tam, kde není třeba autentizačního serveru.

2.2.5 WPA EAP

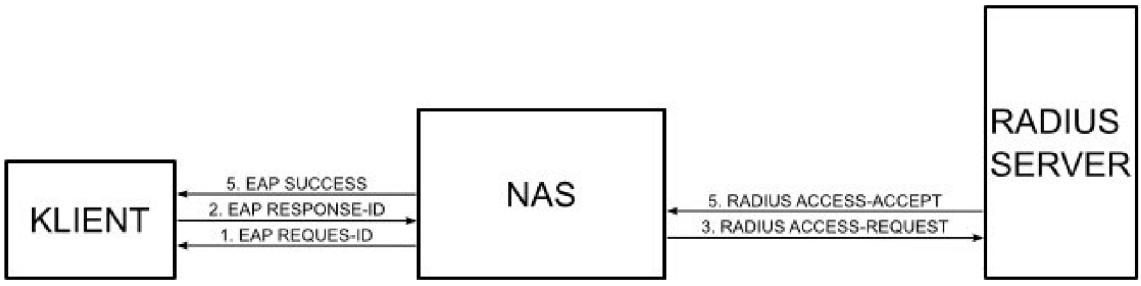
WPA v módu EAP (Extensible Authentication Protocol) funguje podle standardu 802.1X, což je obecné bezpečnostní řešení pro sítě LAN.
Pro použití WPA je třeba, aby v síti běžel autentizační server (např. RADIUS), který obsahuje databázi zařízení/uživatelů, jenž mají povolen přístup k určitým částem sítě. Autentizační server se v použití s WPA EAP stará o autentizaci uživatelů a distribuci unikátních šifrovacích klíčů pro každého autentizovaného klienta [2].

Protokol EAP podporuje řadu autentizačních mechanismů, přičemž WPA oficiálně využívá 5 z nich:

- EAP-TLS,
- EAP-TTLS/MSCHAPv2,
- PEAPv0/EAP-MSCHAPv2,
- PEAPv1/EAP-GTC.
- EAP-SIM.

EAP lze použít také v novějším WPA2. WPA-EAP je vhodné pro rozsáhlejší firemní bezdrátové sítě. Využití autentizačního serveru představuje snadnou správu většího počtu uživatelů a dovoluje využít více autentizačních metod dohromady.

2.2.5.1 Princip autentizace podle standardu IEEE 802.1X



Obr. 2.1: Komunikace síťových prvků při autentizaci podle IEEE 802.1X.

Jednotlivé kroky:

1. Jakmile NAS (Network Access Server) zjistí přítomnost klienta, vyšle mu žádost o identifikační údaje – EAP REQUEST-ID.
2. Klient pošle identifikační údaje uživatele zpět NASu pomocí zprávy EAP RESPONSE-ID.
3. NAS přijatou zprávu EAP RESPONSE-ID přeposílá RADIUS serveru v paketu RADIUS ACCESS-REQUEST.
4. RADIUS server ověří uživatele porovnáním identifikačních údajů se svou databází. Na základě toho pak vyšle paket RADIUS ACCESS-ACCEPT v případě úspěšné autentizace. V případě neúspěchu posílá RADIUS ACCESS-REJECT.
5. NAS následně přepošle zprávu EAP SUCCESS/FAILURE obsaženou v přijatém RADIUS paketu klientovi.

6. V případě úspěšné autentizace je pro daného uživatele otevřen daný port a jsou mu zpřístupněny dané síťové zdroje [4].

2.2.5.2 Autentizační metody EAP

2.2.5.2.1 EAP-TLS

EAP-TLS (EAP – Transport Layer Security) je definováno v RFC 2716. Metoda využívá ověření klientského certifikátu, který musí mít každý uživatel k dispozici pro úspěšné přihlášení do sítě.
Pokud by chtěl útočník proniknout do sítě, musel by nejdříve odcizit soukromý klíč některého z oprávněných uživatelů. Toto potenciální nebezpečí se dá minimalizovat využitím tzv. smart karet (smartcards), které obsahují soukromý klíč každého uživatele. Smart karty fungují tak, že daný soukromý klíč se nikdy nedostane mimo kartu. Veškeré kryptografické operace probíhají uvnitř karty, a proto nelze uživateli odcizit soukromý klíč, aniž by byla odcizena smart karta. Odcizení nebo ztrátu smart karty uživatel snáze pozná a může včas zneplatnit svůj certifikát, a tak zamezit jeho zneužití [3].
Třebaže je tato autentizační metoda jen málo užívána, je považována za jednu z nejbezpečnějších metod EAP autentizace. Tato metoda je podporována řadou výrobců hardware a software.

2.2.5.2.2 EAP-TTLS/MSCHAPv2

Metoda EAP-TTLS/MSCHAPv2 (EAP - Tunneled TLS / Microsoft Challenge Authentication Handshake Protocol) využívá šifrovaného tunelového spojení mezi autentizačním serverem a klientem přímo. Výhoda je v tom, že není vyžadován certifikát na straně klienta.
V první fázi je klientem ověřen certifikát autorizačního serveru a volitelně může autentizační server ověřit certifikát klienta. Klient i autentizační server si v této fázi určí způsob šifrování a klíč, kterým bude šifrována další komunikace. Díky tomu může přijít fáze 2, kdy autentizační server vytvoří šifrovaný tunel ke klientovi [8]. Vlastní autentizace už probíhá přes šifrovaný tunel, kdy se použije MSCHAPv2.
Šifrovaný tunel mezi klientem a autentizačním serverem představuje ochranu před některými útoky na autentizační mechanismus (např. man-in-the-middle).

2.2.5.2.3 PEAPv0/EAP-MSCHAPv2

PEAP je založen na velmi podobném principu jako EAP-TTLS, opět není vyžadován certifikát na straně klienta. Tato metoda je oproti EAP-TTLS velmi podporována velkou škálou zařízení a softwaru různých výrobců. Existují klientské i serverové implementace od Cisco Systems, Microsoftu, MAC OS X, Linuxu a opensource.
Například podporu v systému Microsoft Windows nalezneme od verze WIN 2000 SP4.
PEAP verze 0 podporuje pouze autentizační metodu MSCHAPv2.

2.2.5.2.4 PEAPv1/EAP-GTC

Metoda PEAPv1/EAP-GTC (PEAPv1/EAP-Generic Token Card) byla později vytvořena Cisco System a měla za cíl podporovat i jiné autentizační metody než MSCHAPv2. Použití s EAP-GTC funguje tak, že autentizační server zašle klientovi text a očekává od klienta, aby na základě přijatého textu vygeneroval odpověď pomocí bezpečnostního tokenu. S podporou PEAPv1 se bohužel nesetkáme u žádného systému od Microsoftu.

2.2.5.2.5 EAP-SIM

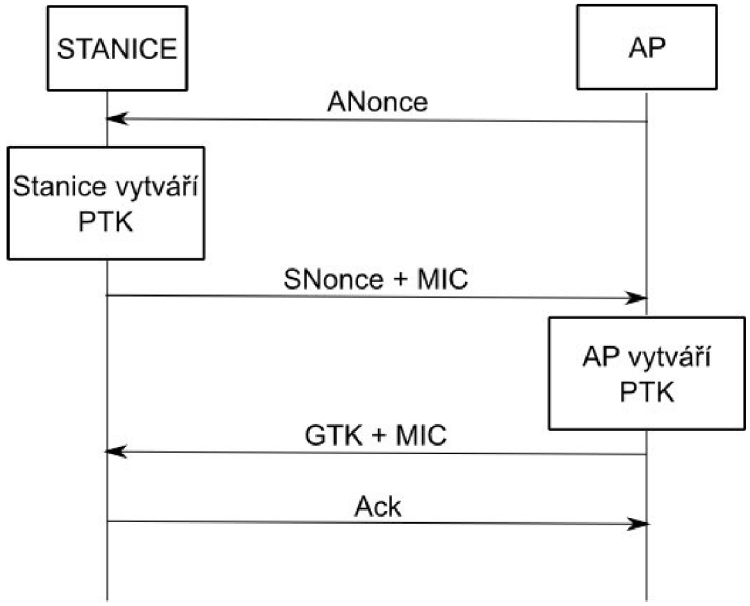
Tato metoda se používá v GSM (Global System of Mobile Communications). Metoda je založena na principu výzva-odpověď (challenge-response). Na SIM kartách funguje

algoritmus A3/A8 pro autentizaci a derivaci klíče. Autentizační server zašle klientovi náhodné 128-bitové číslo jako výzvu. SIM karta zvolí algoritmus (specifikovaný operátorem) a použije přijaté náhodné číslo a tajný klíč uložený na SIM kartě k výpočtu 32-bitové odpovědi a 64-bitového klíče, který lze použít pro šifrování komunikace [4].

2.2.6 WPA2 – IEEE 802.11i

Jedná se o plnou implementaci standardu IEEE 802.11i – kompletní bezpečnostní mechanismus pro bezdrátové sítě. Oproti WEP a WPA používá WPA2 nový algoritmus AES (Advanced Encryption Standard). WPA2 může fungovat v režimu PSK nebo stejně jako u WPA lze u WPA2 využít všechny výhody EAP autentizace. Distribuce šifrovacího klíče probíhá na základě tzv. čtyřcestného handshake (The Four-Way Handshake) [2], [11].

Dřívější sdílený klíč PMK (Pairwise Master Key) už není v čtyřcestném handshake použit. Místo něj se používá jiný klíč zvaný PTK (Pairwise Transient Key). PTK je vygenerován spojením atributů: PMK, Access Point nonce (Anonce), Station nonce (Snonce), MAC adresy AP a MAC adresy stanice. Z výsledného spojení je následně vytvořen hash. Ve čtyřcestném handshake se používá také GTK (Group Temporal Key), který se používá pro dešifrování multicastového a broadcastového přenosu. Výměnu zpráv při čtyřcestném handshake znázorňuje obrázek Obr. 2.2 .

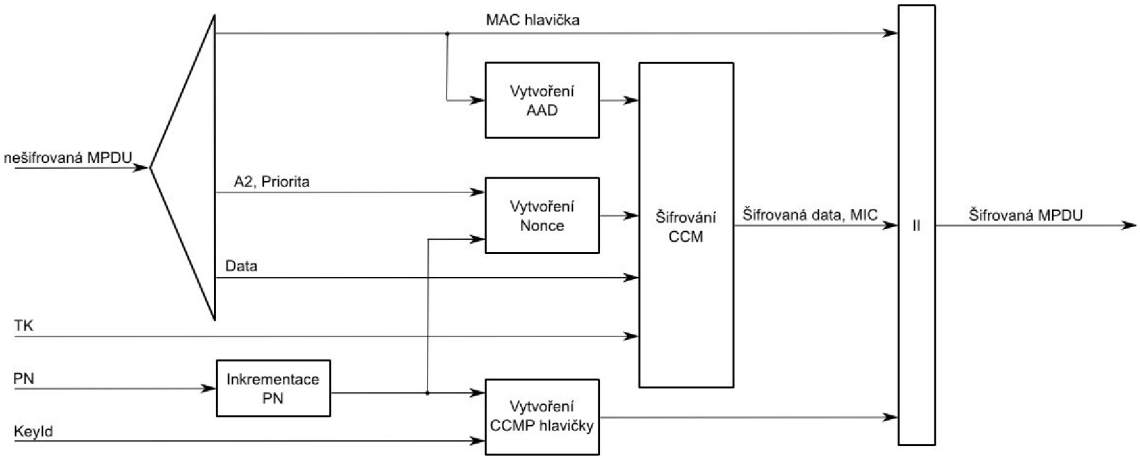


Obr. 2.2: Čtyřcestný handshake.

Pro šifrování podle standardu 802.11i je použit protokol CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). Protokol TKIP lze ve WPA2 také použít, nicméně se jeho použití nedoporučuje [11].

WPA2 v kombinaci s EAP v dnešní době představuje nejvyšší úroveň zabezpečení. Řešení je vhodné především pro středně velké firemní sítě o několika přístupových bodech a desítkách až stovkách uživatelů. Autentizační server umožňuje centrální správu uživatelů. Pro malou firmu či domácnost bych zvolil řešení WPA-PSK nebo WPA2-PSK s šifrováním AES CCM, které nevyžaduje autentizační server.

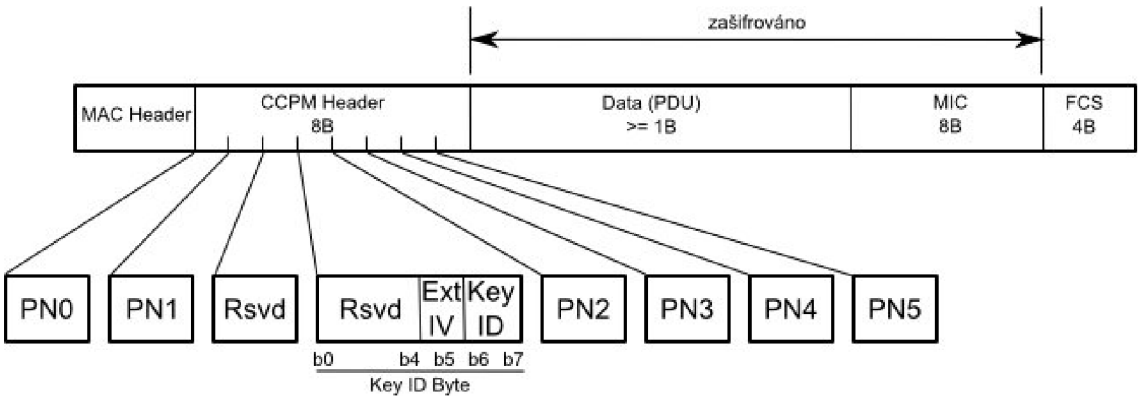
2.2.6.1 Postup šifrování dat pomocí CCMP



Obr. 2.3: Blokové schéma šifrování CCMP.

1. Nejprve se inkrementuje PN (48-bitové číslo paketu), aby bylo docíleno unikátního čísla pro každou MPDU (Medium Access Control Protocol Data Unit). Dočasný klíč (Temporal Key) je pro každé PN jiný.
2. Informace v hlavičce MPDU - MAC header se použijí pro vytvoření dodatečných autentizačních dat (AAD – Aditional Autentication Data) pro vytvoření pro CCM.
3. Vytvoří se blok CCM Nonce těchto údajů: PN, A2 (Adresa 2 v MPDU), Priority (pole priority v MPDU).
4. Do 8-bajtové CCMP hlavičky se umístí PN a Identifikátor klíče (Key Identifier).
5. Pomocí šifrování CCM se z dočasného klíče, AAD, Nonce a nešifrovaných dat z MPDU vytvoří zašifrovaná data a MIC (Message Integrity Check - zvaný “Michael”).
6. Poskládá se zašifrovaná MPDU z původní hlavičky MPDU, z hlavičky CCMP, ze zašifrovaných dat a MIC [11].

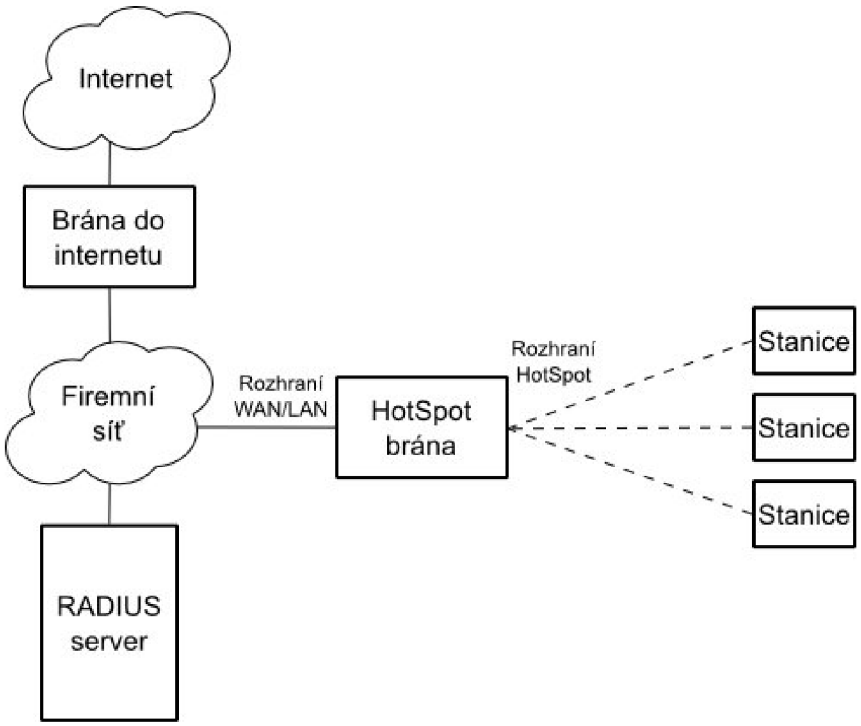
2.2.6.2 Struktura CCMP rámce



Obr. 2.4: Struktura CCMP rámce.

2.2.7 Brána HotSpot

Jedná se o systém, který na rozdíl od předchozích metod nepracuje na linkové vrstvě, nýbrž na vrstvě síťové. Tento rozdíl představuje na jedné straně nevýhodu v tom, že nelze zamezit přihlášení stanice k přístupovému bodu, na straně druhé má díky síťové vrstvě spoustu možností. Je tu možnost kombinace autentizačních metod na obou vrstvách.



Obr. 2.5: Topologie lokální sítě s HotSpot bránou a RADIUS serverem.

HotSpot brána nejčastěji funguje jako rozhraní mezi dvěmi sítěmi – lokální a veřejnou. Hlavním cílem HotSpot brány je autentizace a autorizace uživatelů, kteří žádají o přístup k síťovým zdrojům (např. firemní síť, internet). HotSpot brána má za úkol poskytnout uživateli službu definovanou různými parametry (např. délka poskytnutí služby, rychlost připojení atd.), dále má za úkol sbírat informace o využívání služby. Může pracovat s lokální databází uživatelů, kdy jsou jednotliví uživatelé a sesbíraná data o poskytnuté službě uložena na lokálním disku daného zařízení. Ve větších podnikových sítích ale není vhodné takové decentralizované řešení. Udržování stejné databáze uživatelů na všech přístupových bodech je příliš náročné na správu. Je žádoucí, aby databáze uživatelů byla udržována a spravována na jednom místě, kde se budou také uchovávat informace o využívání služeb jednotlivými uživateli. Z toho důvodu se používá centrální autentizační server a protokol RADIUS (Remote Authentication Dial In User Service).

Výhodou HotSpot brány je velice snadná autentizace uživatelů. Na klientský počítač není třeba instalovat žádný certifikát, dodatečný software a není třeba provádět složitou konfiguraci operačního systému. Pro přihlášení stačí uživateli běžný internetový prohlížeč podporující http/https protokol, což přináší nezávislost na operačním systému uživatele.

HotSpot bránu lze použít v malých i středně velkých sítích, kde je vyžadován veřejný přístup k firemní síti nebo internetu. Přihlášení na přístupový bod je umožněno všem, ale přístup k síťovým zdrojům je umožněn teprve po úspěšném přihlášení. Takto lze realizovat například placený přístup k internetu v kavárně. Další uplatnění může být

třeba ve škole, kdy je umožněn přístup do školní sítě a internetu umožněn pouze studentům a zaměstnancům. Ve výše popsaných případech by bylo administrativně příliš náročné vydávat osobní certifikáty, smart karty každému uživateli. Je téměř nemožné zvolit takovou autentizační metodu, aby nebylo předem vyloučeno použití software či zařízení nějakého výrobce, který zrovna danou autentizační metodu nepodporuje. Použití brány HotSpot ve spojení s autentizací Open System na linkové vrstvě umožňuje dosažení maximální kompatibility.

2.2.7.1 Postup autentizace uživatele na HotSpot bráně

1. Získání IP adresy
    - Jakmile se připojí k přístupovému bodu nové zařízení, je třeba přidělit mu IP adresu. Přidělení bývá nejčastěji realizováno serverem DHCP, který je na stejném lokálním síťovém rozhraní jako HotSpot brána. Pokud je uživatelské zařízení správně nakonfigurováno, zažádá si o přidělení IP adresy a DHCP server poskytne jednu z volných IP adres dané podsítě. HotSpot brána neřeší jak uživatel IP adresu získal.
2. Zobrazení výzvy k zadání přihlašovacích údajů
    - Jakmile uživatel otevře internetový prohlížeč a zadá požadavek na nějakou internetovou stránku. HotSpot brána detekuje, že se jedná o nepřihlášeného uživatele a automaticky jej přesměruje na přihlašovací stránku. Tato stránka může být libovolně upravena pro konkrétní užití. Ve většině případů obsahuje výzvu k zadání jména a hesla. Přesměrování je ve směrovači provedeno přesměrováním veškerých HTTP a HTTPS požadavků na přihlašovací stránku uloženou lokálně na daném směrovači nebo jinde v síti.
3. Ověření údajů a povolení/zamítnutí přístupu
    - Uživatel na přihlašovací stránce zadá nejčastěji jméno a heslo, které HotSpot brána porovná se svou lokální databází, nebo tyto údaje přepošle autentizačnímu serveru. V případě, že jsou přihlašovací údaje shodné s údaji uvedené v databázi uživatelů, je uživateli povolen přístup k daným síťovým zdrojům.

2.2.7.2 Síťové zdroje dostupné bez přihlášení

HotSpot brána může umožnit nepřihlášeným uživatelům přístup k vybraným síťovým zdrojům. Toto lze například využít, pokud chce provozovatel sítě umožnit volný přístup na firemní stránky, kde je nabídka služeb, případně možnost objednání atd. Daná doména nebo IP adresa je potom vyňata z automatického přesměrování na přihlašovací stránku a je na ní umožněn volný přístup.

2.3 Porovnání jednotlivých metod autentizace

Tab. 2.1: Porovnání metod autentizace v bezdrátových sítích.

Metoda Autentizace	Výhody	Nevýhody	Vhodné použití
open-system	Standard 802.11 vyžaduje tuto metodu pro všechna zařízení – plně kompatibilní	Žádná úroveň zabezpečení	Veřejné sítě, které nevyžadují zabezpečení a omezení přístupu V kombinaci dalšími metodami autentizace
Filtr MAC adres	Snadné řešení omezeného přístupu na AP	Snadné prolomení, lze měnit MAC adresu Složitá administrace	Vhodné pro malé domácí bezdrátové sítě Tam kde není vyžadováno šifrování bezdrátové komunikace
WEP – shared-key	Podpora ve starších zařízeních	Velmi malá úroveň bezpečnosti Snadné prolomení	Jako krátkodobé řešení pro malé sítě, v případě nedostupnosti WPA V kombinaci dalšími metodami autentizace
WPA-PSK	Mnohem bezpečnější řešení než WEP Dynamické střídání klíčů	Nepodporují starší zařízení	Menší sítě – kanceláře, domácnosti Tam kde není možné / nutné využívat autorizační server
WPA-EAP	Podpora autentizačního serveru Podpora více autentizačních metod Každá stanice může šifrovat jiným klíčem	Nízká podpora v dostupných zařízeních Vyšší náklady na implementaci Složitější přihlášení do sítě pro uživatele	Malé i středně velké firemní bezdrátové sítě Pokud jsou žádány pokročilé autentizační metody - smart karty, osobní certifikáty atd.
WPA2 - IEEE 802.11i	Vysoká bezpečnost Podpora šifrování multicast a broadcast provozu Podpora autentizačního serveru	Nepodporují starší zařízení	Malé i středně velké firemní bezdrátové sítě Pokud jsou žádány pokročilé autentizační metody - smart karty, osobní certifikáty atd. Pokud vyžadována vysoké zabezpečení sítě a šifrování
Brána HotSpot	Snadné pro uživatele Podpora autentizačního serveru Množství nastavení parametrů služby Pracuje na síťové vrstvě	Nezajišťuje šifrování komunikace Nelze zakázat připojení stanice k AP	Malé, středně velké bezdrátové sítě s vysokou kompatibilitou, dynamickou správou uživatelů Tam kde není vyžadováno šifrování bezdrátové komunikace Veřejné přístupové body

3 Autorizace v bezdrátových sítích

3.1 Význam autorizace

Autorizace v bezdrátových sítích je proces, při kterém jsou uživatelům žádajícím o přístup k síťovým zdrojům přidělena práva a omezení k využívání specifických služeb sítě. Při autorizaci se rozhoduje, zda-li má uživatel, příp. síťové zařízení, právo přistupovat k určitým segmentům sítě. Dále mohou být pro konkrétního uživatele určeny různé parametry určující povahu poskytovaných služeb sítě.
Proces autorizace následuje po úspěšné autentizaci uživatele, a proto úspěšná autentizace uživatele nemusí nutně znamenat, že mu bude služba poskytnuta. Při autorizaci se může zvažovat mnoho různých podmínek např. aktuální čas, den v týdnu, místo využití služby nebo stav systému. Jedním z příkladů může být případ, kdy se uživatel řádně autentizoval, ale nemá zaplacené žádné služby na daném přístupovém bodu, proto mu je přístup k síti zamítnut [9].

3.1.1 Obecný princip autorizace uživatele

1. Po úspěšné autentizaci uživatele zjistí autentizační server ve své databázi, jaká práva a parametry služby mají být uživateli nastaveny.
2. Autentizační server posílá práva a parametry pro daného uživatele NASu (Network Access Server) společně s informací o úspěšné autentizaci.
3. NAS následně provede patřičné nastavení (např. pravidla firewallu), zajišťující síťová práva pro daného uživatele a umožní tak uživateli využívat službu definovaných parametrů.

3.1.2 Příklady některých síťových práv a parametrů služeb

- Povolení přístupu do určitých segmentů sítě,
- Přidělení adresy z určitého rozsahu IP adres, NAT 1:1, mapování portů,
- Specifická pravidla směrování provozu,
- Nastavení přenosové rychlosti, QoS,
- Délka poskytnuté služby,
- Limity přenesených dat [9].

4 Autentizační server

4.1 Význam autentizačního serveru

Autentizační server je síťové zařízení používané pro řízení přístupu do sítě. Součástí autentizačního serveru je databáze uživatelských identit a hesel, (případně certifikátů, klíčů, algoritmů pro tokeny apod.) potřebných pro identifikaci uživatelů, kteří žádají o přístup do sítě.

4.2 AAA server

Autentizační server bývá nejčastěji spojen dohromady s autorizačním a tarifikačním serverem - tzv. AAA server (Authentication, Authorization, Accounting server). Ten pak poskytuje centralizované řešení pro řízení přístupu, nastavení parametrů síťových služeb a tarifikaci. AAA server by neměl být implementován jako součást jiných síťových prvků. Měl by fungovat jako samostatné síťové zařízení.
Nejrozšířenějším protokolem autentizačních serverů je protokol RADIUS, (Remote Authentication Dial-In User Service) vyvinutý společností Livingston Enterprises (později Lucent). Za druhý nejrozšířenější protokol lze považovat TACACS+ , (Terminal Access Controller Access-Control System Plus) vyvinutý Ciscem.
Mezi nejznámější komerční implementace patří např. EVOLYNX, z open source implementací se nejvíce používá FreeRadius.

4.3 Protokol RADIUS

Protokol RADIUS pracuje podle modelu klient – server. Jako klient je zde považován NAS (Network Access Server) – síťové zařízení zajišťující služby uživatelům.
NAS může být např. přístupový bod nebo směrovač. NAS při autentizaci předává identifikační údaje uživatele RADIUS serveru a podle přijatých informací od RADIUS serveru poskytuje uživateli služby sítě.
Pro výměnu zpráv mezi NASem a RADIUS serverem je použit UDP protokol. Důvodem je jeho jednoduchá implementace, navíc způsob UDP komunikace lépe vyhovuje potřebám autentizace uživatelů. Oficiální port, na kterém RADIUS server standardně naslouchá, je 1812.
RADIUS server může pracovat také jako proxy – klient pro další nadřazené RADIUS servery. Komunikace mezi NAS a RADIUS serverem probíhá šifrovaně díky sdílenému tajnému klíči (Secret), který musí znát obě strany a nikdy není posílán po síti [6].

4.3.1 Obecný princip RADIUS autentizace a autorizace

1. Uživatel poskytne klientovi (NAS) autentifikační informace – uživatelské jméno (username) a heslo (password).
2. Jakmile NAS obdrží od uživatele jméno a heslo, vytváří tzv. Access-Request zprávu, která obsahuje uživatelské jméno, heslo, identifikátor NASu, a port ID. Heslo je zašifrováno pomocí algoritmu RSA Message Digest Algorithm MD5. Následně je zpráva odeslána příslušnému RADIUS serveru po síti. Pokud od RADIUS serveru nepřijde odpověď do určité doby, je zpráva odeslána znovu. Takto se to opakuje několikrát. Pokud po specifikovaném počtu opakování nedostane NAS odpověď od daného RADIUS serveru, může zprávu poslat dalšímu RADIUS serveru v pořadí, jestliže takový server existuje. Autorizačních serverů může být několik.
3. Po přijmutí požadavku RADIUS server zkontroluje, zda-li má tajný klíč k NASu, od kterého požadavek přišel. Pokud takový klíč neexistuje, pak je

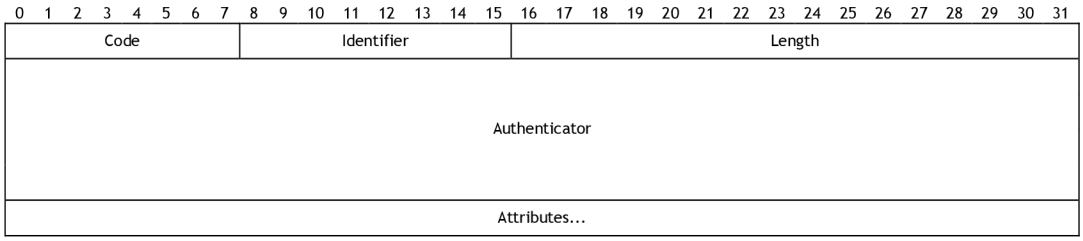
požadavek tiše zahozen (Silently Discard). To znamená, že RADIUS server neodešle žádnou odpověď. Každé zahození požadavku by mělo být na serveru zaznamenáno do logu.

4. V případě, že RADIUS server ověří NAS podle tajného klíče, pokusí se najít v databázi uživatelů požadované uživatelské jméno a ověřit uživatele podle daných údajů. Nejčastěji to bývá právě heslo.
5. Pokud nejsou splněny podmínky (např. nesouhlasí heslo), pak server odesílá zprávu Access-Reject, která požadavek zamítá a NAS službu uživateli neposkytne. Server může k požadavku přiložit i zprávu, kterou NAS zobrazí uživateli jako důvod zamítnutí požadavku.
6. Pokud jsou splněny všechny podmínky pro autorizaci uživatele, pak může server odeslat buď hned zprávu Access-Accept, nebo nejprve odeslat zprávu Access-Challenge a požádat NAS, aby vyzval uživatele k zadání odpovědi na požadavek serveru. Access-Challenge lze využít například při ověření uživatelů pomocí smart karet. Zprávu Access-Accept server odesílá pouze v případě, že jsou splněny všechny podmínky pro autorizaci uživatele. Zpráva Access-Accept obsahuje všechny potřebné konfigurační parametry, podle kterých NAS nastaví službu uživateli [6].

4.3.2 Druhy RADIUS paketů

- Access-Request,
- Access-Accept,
- Access-Reject,
- Access-Challenge.

4.3.3 Struktura RADIUS paketu



Obr. 4.1: Struktura RADIUS paketu.

4.3.4 RADIUS atributy

RADIUS atributy zajišťují specifické autentizační, autorizační informace a konfigurační detaily RADIUS požadavků a odpovědí.

Atribut se skládá z:

- Typu (Type) [1B],
- Délka (Length) [1B] – určuje délku atributu včetně typu a hodnoty,
- Hodnota (Value) [nB] – hodnota atributu. Počet bajtů a formát jsou dány typem a délkou atributu. Hodnota může být typu text, string, address, integer nebo time.

Příklady Atributů:

- User-Name – posílán v paketu Access-Request,
- Reply-Message – text zobrazovaný uživateli,

- Session-Timeout – omezení délky relace uživatele,
- NAS-Identifier – identifikátor NASu.

4.3.5 RADIUS tarifikace

RADIUS server umožňuje tarifikaci uživatelů (Accounting) - evidenci spotřebovaných zdrojů daného NAS uživatelem. Databáze accounting může sloužit např. pro vyúčtování služeb uživatelům nebo jako přehled o využívání zdrojů na jednotlivých NASech. V accounting databázi nalezneme informace o každém využití služby NASu – relaci (session). Každá relace má svůj začátek a konec. Pokud to NAS podporuje, může mít uživatel několik paralelních či seriových relací [7].

Příklady položek accounting databáze:

- RadAcctId (id záznamu v databázi RADIUS serveru),
- AcctSessionId (id relace),
- AcctUniqueId (unikátní id relace),
- UserName (jméno uživatele),
- Realm (oblast),
- NASIPAddress (IP adresa NASu),
- NASPortId (id portu na kterém relace probíhala),
- NASPortType (typ portu, na kterém relace probíhala),
- AcctStartTime (datum a čas začátku relace),
- AcctStopTime (datum a čas ukončení relace),
- AcctSessionTime (délka relace v sekundách),
- AcctInputOctets (počet bajtů, které byly přijaty od uživatele),
- AcctOutputOctets (počet bajtů, které byly poslány uživateli),
- AcctTerminateCause (důvod ukončení relace),
- FramedIPAddress (přidělená IP adresa uživateli).

4.3.5.1 Obecný postup RADIUS tarifikace

1. NAS vygeneruje paket typu Accounting Request - začátek tarifikace (Accounting Start) na začátku poskytování služby uživateli a pošle jej RADIUS serveru. Součástí paketu jsou informace o datu, čase, typu služby atd.
2. RADIUS server pošle NASu potvrzení o přijetí paketu.
3. Ve chvíli, kdy je uživateli ukončeno poskytování služby, vygeneruje NAS paket typu Accounting-Request - konec tarifikace (Accounting Stop) a pošle jej RADIUS serveru společně s informacemi o dané relaci.
4. RADIUS server pošle NASu potvrzení o přijetí paketu.
5. V případě, že NAS neobdrží potvrzení o přijetí paketu od RADIUS serveru, opakuje poslání znovu. Pokud několikrát neobdrží potvrzení, může Accounting-Request poslat následujícímu RADIUS serveru v pořadí, pokud takový server existuje [7].

5 Výběr vhodné metody autentizace

Při výběru vhodné metody autentizace a autorizace je potřeba zvážit konkrétní situaci z hlediska:

- požadované úrovně zabezpečení,
- dostupných finančních prostředků,
- kompatibility s různými operačnímy systémy a síťovými adaptéry různých výrobců.

Z popsaných metod autentizace a jejich porovnání je zřejmé, že nejvyšší úroveň bezpečnosti poskytuje autentizace a šifrování pomocí WPA2 podle standardu IEEE 802.11i s šifrováním dat AES CCMP.Nejlépe s využitím EAP, autorizačního serveru a osobních certifikátů, případně smart karet. Takové řešení je však značně nákladné a hodí se především pro větší firemní sítě.
Pro domácnosti, kde je kladen důraz na nízké finanční náklady, je nejvhodnější použití WPA PSK nebo WPA2 PSK.
Existují však také případy, kdy nelze předem vyloučit použití různých síťových adapterů a operačních systémů. Vzniká problém nekompatibility. Tento problém řeší autentizace pomocí brány HotSpot, u které pro úspěšnou autentizaci postačí jakýkoliv webový prohlížeč. Pro představu uvádím několik situací, kde je vhodné zvolit autentizaci pomocí brány HotSpot:

- vzdělávací zařízení,
- úřady,
- zdravotnická zařízení (nemocnice, zdrav. střediska, lázeňská zařízení),
- kavárny, restaurace,
- nádraží, letiště.

V těchto případech má bezdrátová síť často několik přístupových bodů a mohou ji využívat kromě zaměstnanců také zákazníci, pacienti, studenti apod. Uživatelé bývají náhodní a nelze po nich požadovat instalaci certifikátů.

Pro demonstraci řešení autentizace a autorizace jsem zvolil právě výše uvedenou situaci, která je podle mého názoru někde uprostřed mezi malou bezdrátovou sítí o jediném přístupovém bodu a rozsáhlou sítí o desítkách až stovkách přístupových bodů. Následovat bude praktický návrh řešení určeného pro dvoupatrovou školní budovu o třech přístupových bodech.

6 Praktický návrh řešení autentizace a autorizace

6.1 Stanovení požadavků

Požadavky jsou:

- pokrytí společných prostor chodby v každém patře a ředitelny bezdrátovým signálem,
- připojení bezdrátové sítě do internetu,
- vytvoření uživatelských účtů pro každého učitele s omezenou šířkou pásma 2048/512 kbps,
- vytvoření uživatelských účtů pro studenty s omezenou šířkou pásma 2048/256 kbps,
- vytvoření uživatelského účtu guest pro náhodné návštěvníky s omezenou šířkou pásma 1024/256 kbps,
- umožnění správci školní sítě centrálně spravovat účty.

6.2 Výběr vhodného HW a SW řešení

Pro realizaci bezdrátové sítě WLAN jsem zvolil síťové prvky od společnosti Mikrotik, jelikož jsem je měl k dispozici ze zaměstnání. Jedná se o HW platformu Mikrotik RouterBoard 133, na které běží síťový operační systém Mikrotik RouterOS. Druhým důvodem pro volbu těchto prvků byla jejich přijatelná cena. Jeden WLAN router se dá pořídit za cenu okolo 3000Kč. Výhodou operačního systému Mikrotik RouterOS je, že v sobě zahrnuje systém HotSpot brány a podporu RADIUS serveru.

WLAN router se zkládá z těchto součástí:

- Mikrotik RouterBoard 133,
- miniPCI Wireless karta CM9 s chipsetem Atheros 5214,
- minipigtail,
- všesměrová anténa,
- CASE pro RB133,
- napájecí adaptér 18V.

Obr 6.1: HW platforma Mikrotik RouterBoard 133.

6.2.1 HW platforma RouterBoard 133

Jedná se o embedded počítač postavený na procesoru MIPS32 4Kc 175 Mhz. Deska dále obsahuje:

- 32MB paměti SD RAM,
- 64 nebo 128 MB NAND paměti pro uložení operačního systému a dat,
- 3x 10/100 Mbit/s Fast ethernet porty, přičemž jeden z portů podporuje POE,
- 3x miniPCI sloty,
- RS232 port,
- Mini - PC speaker,
- Napájecí konektor,
- 2x konektor pro případné ventilátory.

Zvolený RouterBoard není příliš výkonný. Nicméně pro menší počet připojených uživatelů a datové toky do cca 7 Mbit/s je plně dostačující.

6.2.2 Síťový operační systém Mikrotik RouterOS

Mezi základní funkce systému patří:

- Firewall a NAT,
- Směrování (statické i dynamické – RIP, BGP, OSPF),
- Správa datové přenosové rychlosti a podpora QoS,
- Brána Hotspot,
- Tunelovací protokoly (PPTP, L2TP, PPPoE, IPIP, EoIP),
- Ipsec,
- Proxy server,
- DHCP server, klient, relay,

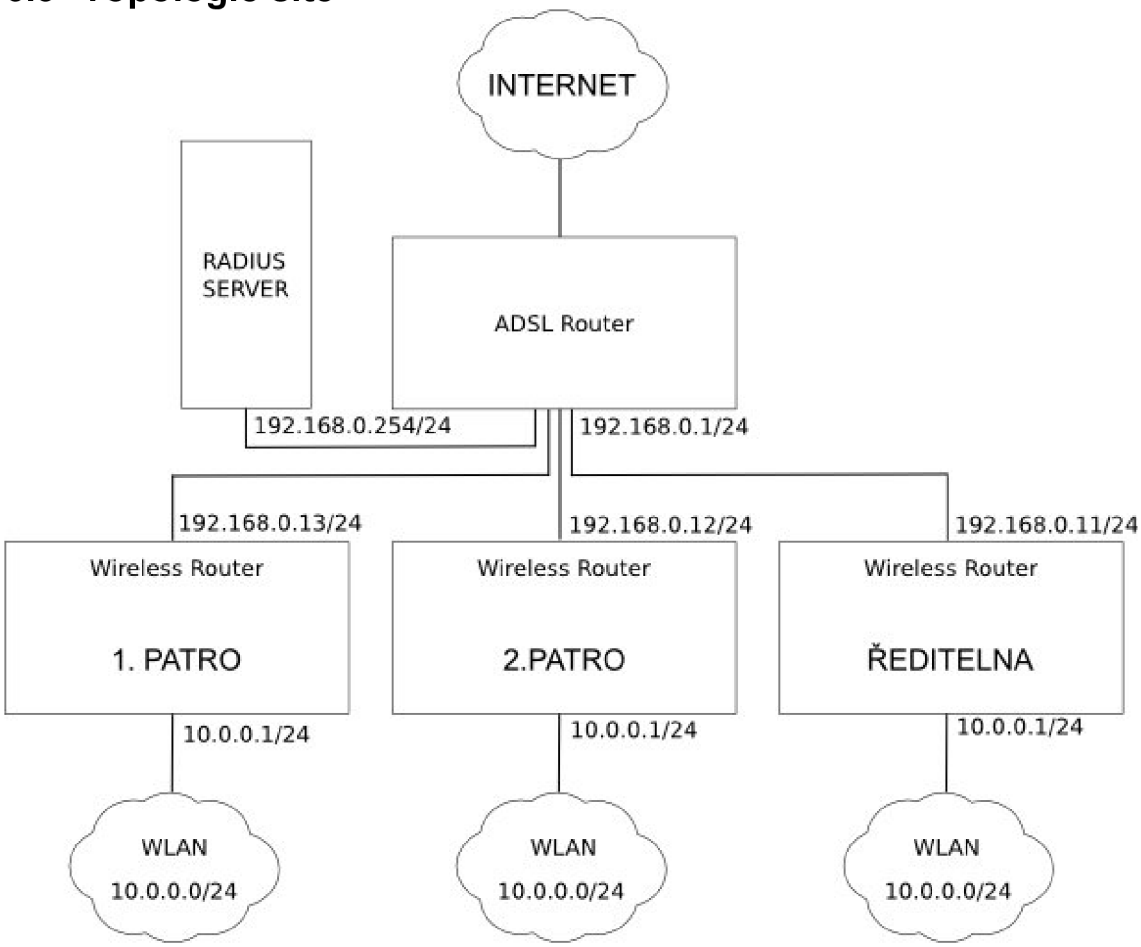
- NTP klient, server,
- DNS cache,
- Monitorování a Accounting IP přenosů,
- SNMP server,
- MNDP kompatibilní s CISCO CDP,
- Síťové nástroje (ping, traceroute, bandwidth test, ping flood, telnet SSH, packet sniffer),
- Podpora Wireless (802.11 a/b/g Access point, station, bezpečnost WEP, WPA),
- Podpora síťových mostů – Bridge.

Operační systém RouterOS lze nainstalovat na jakýkoliv počítač architektury x86 nebo na embedded počítače RouterBoard architekturou MIPS. RouterOS podporuje velké množství síťových prvků. HW platforma RouterBoard 133 se prodává již s nainstalovaným systémem RouterOS a licencí LEVEL 4.

6.2.3 FreeRadius

Jedná se o opensource balík aplikací zahrnující především server, klient a další související nástroje. FreeRadius balík bývá standardní součástí různých operačních systémů, navíc jsou k dispozici kompletní zdrojové kódy. FreeRadius využívá řada telekomunikačních operátorů. Jsou podporovány funkce jako RADIUS proxy, load balancing, různé druhy databázových systémů. Přičemž různé třídy autentizačních požadavků mohou pracovat s různými databázemi, stejně tak tarifikace může pracovat s různými databázemi a zálohováním.
Systém podporuje řadu autentizačních metod, dokáže provádět konfiguraci klientů pomocí velkého množství parametrů. Jednotlivé nestandardní parametry jsou uvedeny ve slovníkových souborech určených pro zařízení různých výrobců, samozřejmě včetně Mikrotik RouterOS.

6.3 Topologie sítě



Obr 6.2: Topologie sítě.

6.4 Databáze uživatelů

Pro databázi uživatelů jsem použil MySQL server běžící na stejném počítači společně s FreeRadius serverem. Databázi uživatelů lze snadno spravovat lokálně i vzdáleně po sítí. O správu databáze se může starat jakýkoliv externí program.

6.4.1 Pravidla přidělování uživatelských jmen

Uživatelská jména pro učitele:

- ucitel.<příjmení učitele><pořadové číslo v případě shodného příjmení>.

Uživatelská jména pro studenty:

- student.<příjmení studenta><pořadové číslo v případě shodného příjmení>.
- guest

6.5 Konfigurace přístupových bodů

Konfigurační soubory jednotlivých AP (ředitelna, 1. patro, 2. patro) jsou na přiloženém CD.

6.5.1 Import konfigurace

Konfigurace Mikrotik RouterOS:

- vyresetujeme router do výchozího nastavení (příkazem reset-configuration),
- nakopírujeme konfigurační soubor (<nazev>.rsc) pomocí ftp do routeru,
- v konzoli importujeme příkazem import <nazev>.rsc,

- pokud se konfigurace nepovede, je potřeba ručně upravit chybu ve skriptu. Toto může nastat v případě, že provádíme konfiguraci na novější (nebo i starší) verzi Mikrotik RouterOS,
- konfiguraci můžeme zkontrolovat pomocí utility WinBox.

6.6 Konfigurace FreeRadius serveru

6.6.1 Konfigurační soubory

FreeRadius jsem nakonfiguroval tak, že využívá lokální MySQL databázi uživatelů, hesel, skupin, autorizačních a autentizačních atributů namísto textových souborů. Toto řešení je vhodné zejména pro snadnou správu uživatelů pomocí libovolné aplikace nad databází MySQL. Pro autentizaci se využívá metoda http-pap. Tarifikace (Accounting) je nasměrován také do MySQL databáze. Nastavení pro klienty (NAS) je v souboru clients.conf.

Konfigurace FreeRadius serveru je provedena úpravou těchto konfiguračních souborů:

- freeradius.conf,
- dictionary,
- /dict/dictionary.mikrotik.my,
- clients.conf,
- sql.conf.

Uvedené konfigurační soubory jsou na přiloženém CD. Ostatní konfigurační soubory mohou zůstat tak, jak byly vytvořeny při instalaci FreeRadius.

6.6.2 Struktura MySQL databáze FreeRadius

MySQL databáze pro FreeRadius obsahuje tyto tabulky:

- **nas** – klienti NAS,
- **radacct** – tarifikace (accounting),
- **radcheck** – uživatelská jména a hesla,
- **radgroupcheck** –atributy společné pro jednotlivé skupiny uživatelů,
- **radgroupreply** – atributy odesílané zpět NASu společné pro jednotlivé skupiny uživatelů,
- **radpostauth** – v našem případě nevyužitá,
- **radreply** – atributy zasílané zpět NASu pro konkrétní uživatele (zde lze nadefinovat speciální autorizační parametry pro konkrétní uživatele. Tyto parametry mají vyšší váhu než parametry pro skupinu v tabulce radgroupreply,
- **usergroup** – přiřazení uživatelů do skupin.

Struktura MySQL databáze včetně testovacích dat je na přiloženém CD.

6.7 Praktické ověření návrhu

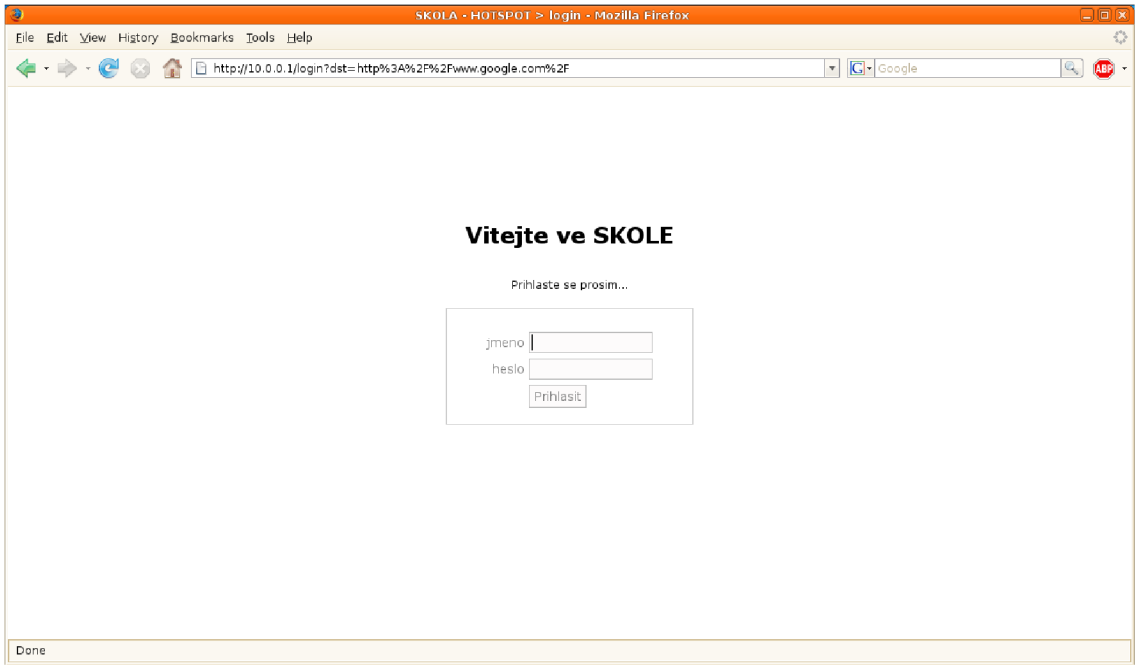
Praktické ověření jsem provedl se svým notebookem a operačním systémem Gentoo Linux. Pracoval jsem s AP ředitelna. Pro ověření správného nastavení v Access Pointu jsem použil grafický konfigurační nástroj pro Mikrotik RouterOS – WinBox, který je pouze pro Windows, nicméně běží bez problému i v Linuxu pomocí Wine. Server FreeRadius jsem nainstaloval na stolní počítač s operačním systémem Debian Linux.

6.7.1 Přidělení adresy pomocí DHCP

Po zapnutí a naběhnutí Access Pointu jsem se s notebookem připojil na SSID SKOLA. DHCP server mi přidelil IP adresu 10.0.0.253, masku 255.255.255.0, výchozí bránu 10.0.0.1 a DNS server 10.0.0.1.

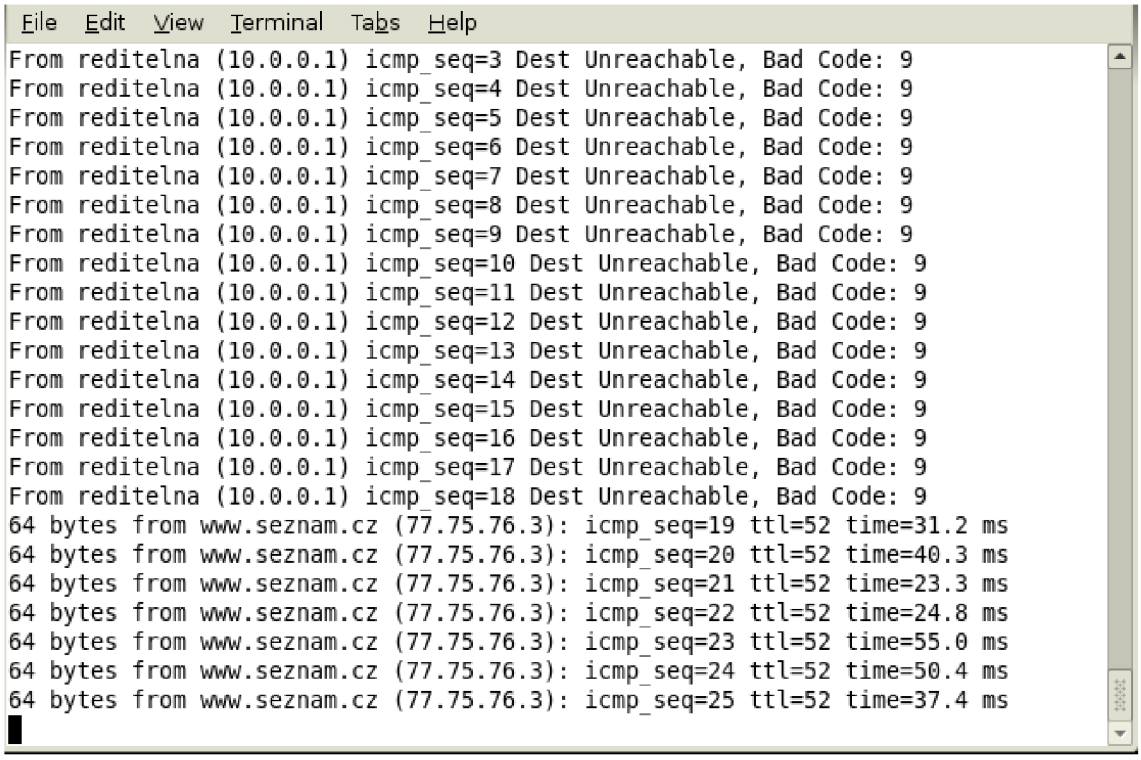
6.7.2 Přihlášení do sítě – autentizace a autorizace

Otevřel jsem terminál a začal jsem pomocí ping testovat odezvu na server seznam.cz. Jak je vidět z obr. 6.4., komunikace na server seznam.cz byla blokována na AP reditelna a vracela se odpověď Dest Unreachable, Bad Code: 9 (pro windows – cílová síť není dostupná).
V dalším kroku jsem otevřel internetový prohlížeč Mozilla Firefox a do adresního řádku jsem zadal adresu http://www.google.com. Požadavek na server google.com byl přesměrován na adresu http://10.0.0.1/login?dst=http%3A%2F%2Fwww.google.com%. Zobrazila se přihlašovací stránka (načtená přímo z AP reditelna) s výzvou k zadání uživatelského jména a hesla viz.obr. 6.3.



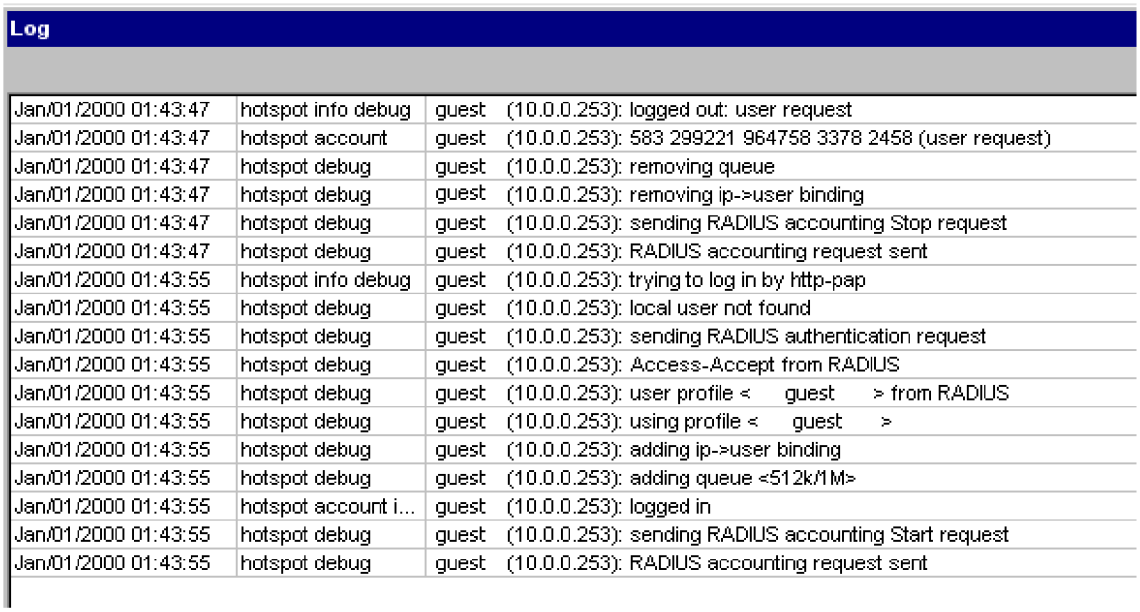
Obr. 6.3: Přihlašovací stránka.

Po zadání uživatelského jména guest a hesla guest jsem byl úspěšně přihlášen. Dále se v prohlížeči objevila původně zadaná stránka http://www.google.com. Úspěšné přihlášení jsem ověřil v otevřeném terminálu, kde stále probíhal ping na server seznam.cz. V okamžiku přihlášení do sítě začaly ICMP pakety procházet a vracely se odpovědi od serveru seznam.cz viz. obr. 6.4.



Obr. 6.4: Odezva ping z notebooku na seznam.cz před a po přihlášení.

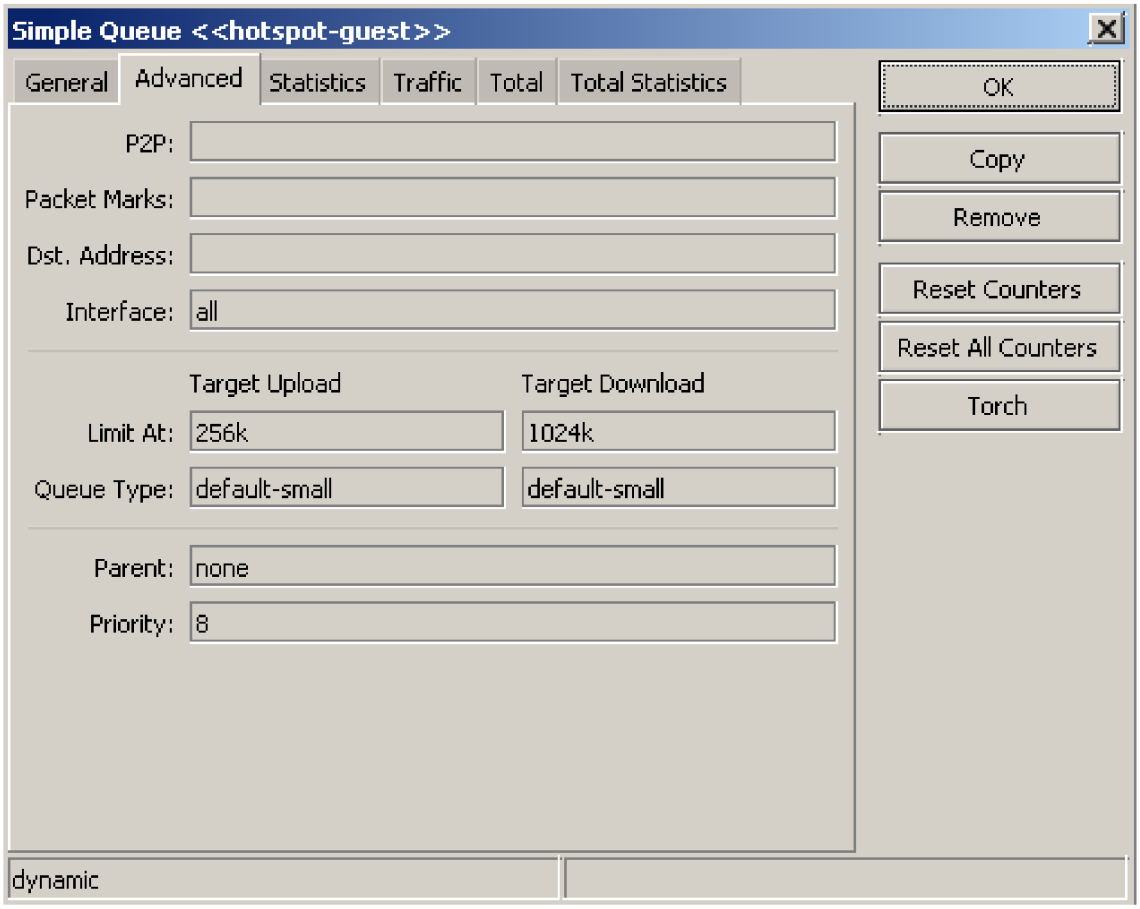
Procedura, která se odehrála v čase mezi odesláním přihlašovacích údajů a přihlášením, je vidět z logu RouterOS na obrázku Obr. 6.5. K odeslání přihlašovacích údajů došlo v čase 01:43:55 – pokus o přihlášení pomocí http-pap. Následovala kontrola, zda-li uživatel guest je uveden v lokální databázi na Access Pointu. Tam uživatel nalezen nebyl, a proto HotSpot brána poslala požadavek authentication request na server RADIUS. RADIUS server ověřil uživatele guest podle jména a hesla, následně zaslal zpět Access Pointu paket Access-Accept, včetně parametru Mikrotik-Group, který říká, že má být pro uživatele guest použit profil guest. HotSpot brána následně vytvořila podle profilu guest dynamická pravidla ve firewallu a frontu simple queue s požadovanými parametry připojení. V tu chvíli byl uživatel guest přihlášen. Následovalo zaslání paketu Radius-Accounting-Start směrem do RADIUS serveru, kde se přidal záznam do tabulky radacct. Ze záznamů v logu je vidět, že celá procedura autentizace a autorizace proběhla v průběhu jedné vteřiny, takže ji uživatel guest ani nepostřehl.



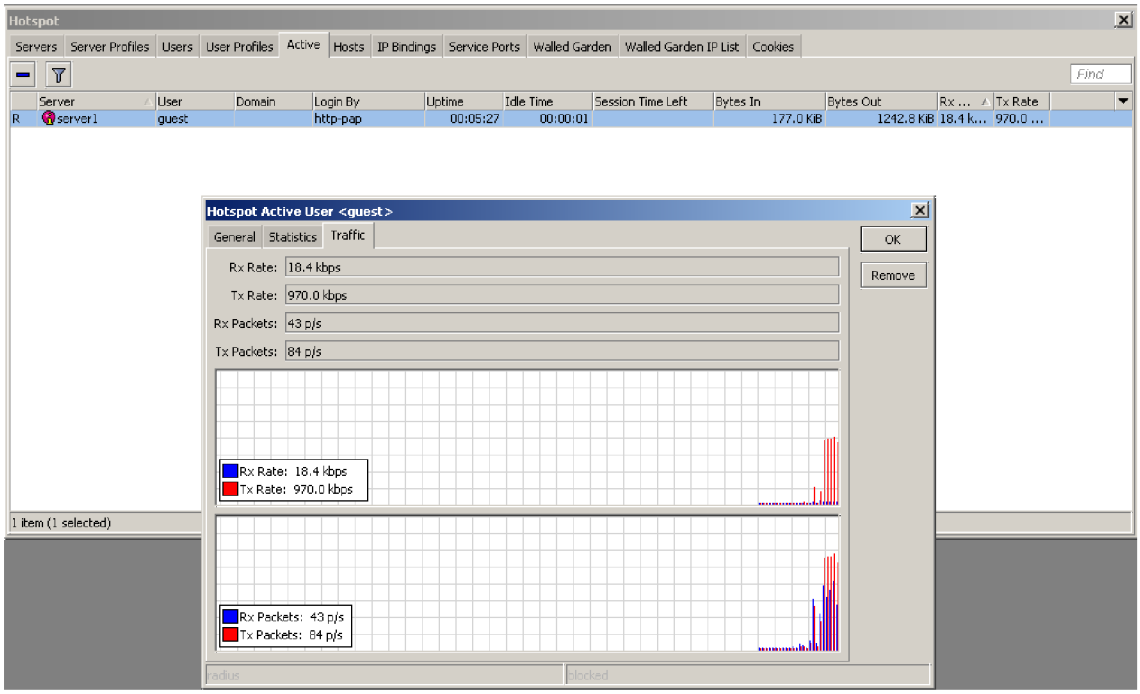
Obr. 6.5: Záznamy v logu RouterOS v průběhu přihlášení uživatele guest .

6.7.3 Ověření správného nastavení parametrů připojení

Správné nastavení fronty a přihlášení uživatele jsem ověřil ve WinBoxu přihlášeného k AP reditelna. Z obrázků Obr. 6.6. a 6.7. je vidět správné nastavení fronty pro omezení rychlosti a záznam uživatele guest v seznamu aktivních, přihlášených uživatelů na HotSpot bráně. Následoval test rychlosti na http://rychlost.cz, kde jsem ověřil správné nastavení přenosové rychlosti pro uživatele guest viz. Obr. 6.8.

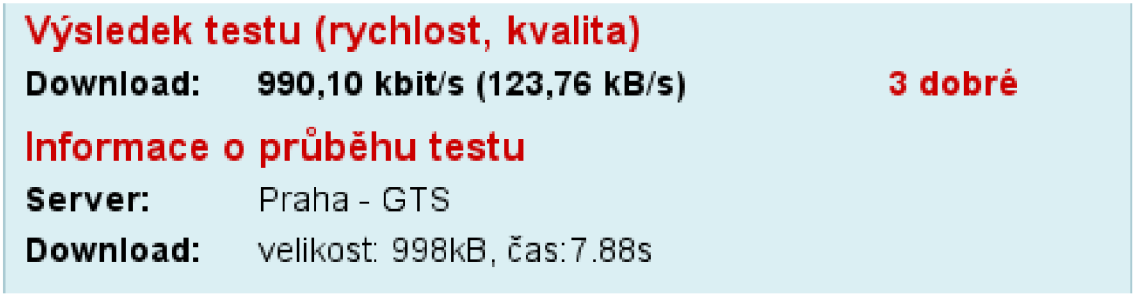


Obr. 6.6: Nastavení fronty Simple Queue pro uživatele guest.



Obr. 6.7: Záznam aktivního uživatele guest na HotSpot bráně a graf přenosové rychlosti v průběhu měření rychlosti na http://www.rychlost.cz.

Měření rychlosti připojení do internetu jsem provedl na serveru http://rychlost.cz viz. Obr. 6.8 a Obr. 6.9.

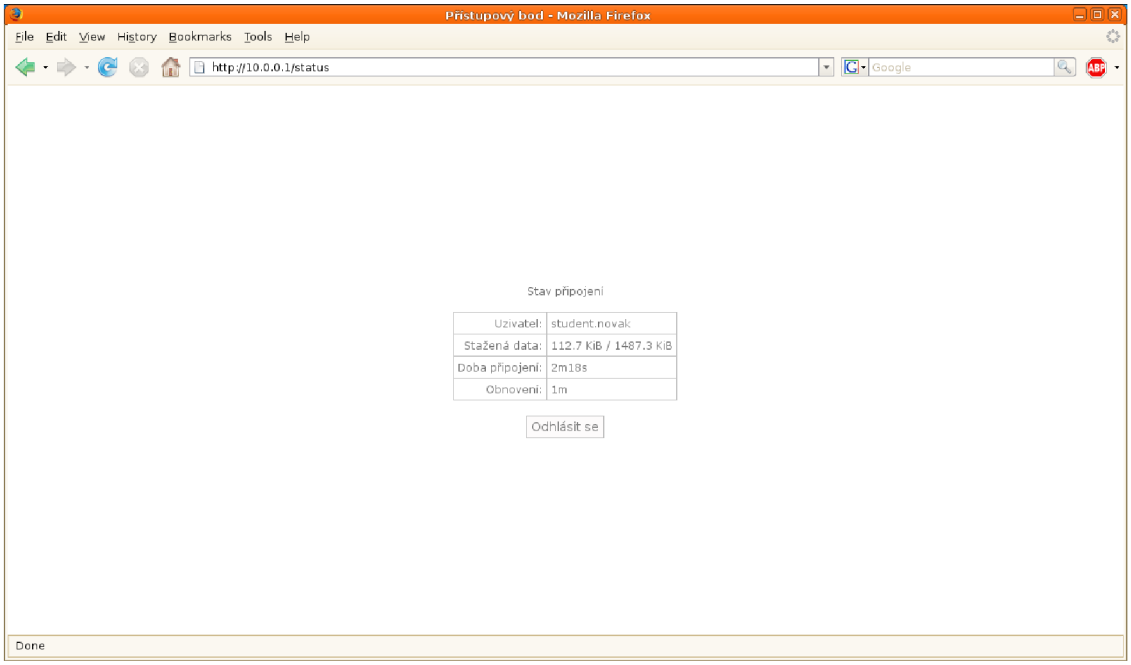


Obr. 6.8: Test rychlosti připojení pro uživatele guest.

Obr. 6.9: Test rychlosti připojení pro uživatele ucitel.novotna.

6.7.4 Stav připojení a odhlášení od sítě

HotSpot brána umožňuje zobrazení stavu připojení na adrese http://10.0.0.1/status. Jak je patrné z Obr. 6.10. na stránce nalezneme uživatelské jméno, přenesená data od začátku připojení, délku připojení a tlačítko pro odhlášení.

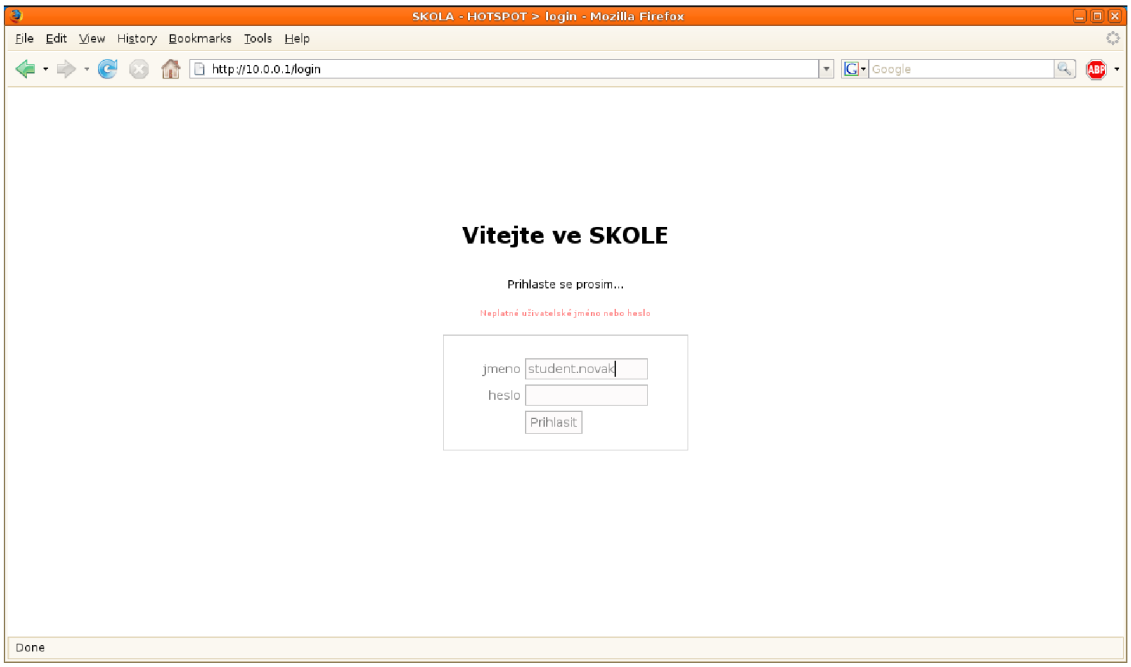


Obr. 6.10: Stránka se stavem připojení a tlačítkem pro odhlášení.

Dále jsem provedl odhlášení uživatele guest kliknutím na tlačítko odhlásit. Odhlášení proběhlo z pohledu uživatele okamžitě, nicméně v HotSpot systému proběhlo zrušení dynamické fronty simple queue, zrušení dynamických pravidel ve firewallu a do RADIUSu byl odeslán paket Radius-Accounting-Stop. Uživatel guest zmizel z tabulky aktivních uživatelů HotSpot brány.

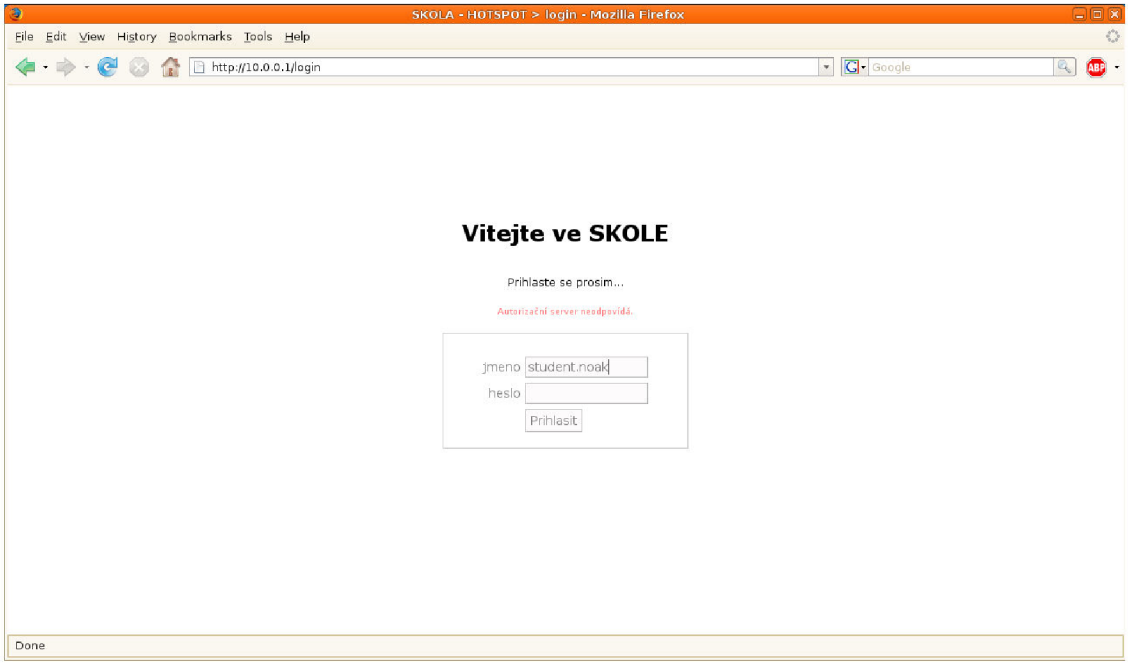
6.7.5 Neúspěšné přihlášení a ošetření výpadku RADIUS serveru

V dalším kroku jsem zkusil zadat neplatné uživatelské jméno, heslo a pokusil jsem se tak o neplatnou žádost o autentizaci. Jak je vidět na Obr. 6.11. HotSpot brána neumožnila přihlášení a vypsala chybové hlášení „Neplatné uživatelské jméno nebo heslo“. RADIUS server zaslal HotSpot bráně paket Access-Reject, což znamená, že žádost o přihlášení byla zamítnuta.



Obr. 6.11: Chybové hlášení při neplatném pokusu o přihlášení do sítě.

Dále jsem ověřil, jak se systém zachová při výpadku RADIUS serveru tím, že jsem server vypnul. Následně jsem do přihlašovací stránky zadal uživatelské jméno a heslo. Po krátké časové prodlevě (přibližně 1s)vyskočilo na přihlašovací stránce chybové hlášení „Autorizační server neodpovídá“ a přihlášení nebylo dovoleno viz. Obr. 6.12. V případě výpadku RADIUS serveru se tedy do sítě nikdo nepřihlásí. Pokud bychom toto chtěli řešit, lze instalovat záložní RADIUS server, který bude použit v případě, že primární server bude mimo provoz. Pro náš případ školní sítě je však použití jednoho RADIUS serveru dostačující.



Obr. 6.12: Chybové hlášení při nedostupném RADIUS serveru.

6.7.6 Tabulka Accounting na RADIUS serveru

Tab. 6.1: Záznamy z tabulky radacct na RADIUS serveru (jedná se o 4 řádky tabulky).

RadAcctId	AcctSessionId	AcctUniqueId
1	809000b6	0de365ae6d377922
2	8050013f	ec77587fb3e37cc1
3	80a0006c	280eeae2e8f798e8
4	80c000b7	9389a8bd38d304f4

UserName	Realm	NASIPAddress
guest		192.168.0.11
guest		192.168.0.11
ucitel.novotna		192.168.0.11
student.novak		192.168.0.11

NASPortId	NASPortType	AcctStartTime
2147483647	Wireless-802.11	2008-05-11 10:34:25
2147483647	Wireless-802.11	2008-05-11 10:38:51
2147483647	Wireless-802.11	2008-05-11 10:42:54
2147483647	Wireless-802.11	2008-05-11 10:50:12

AcctStopTime	AcctSessionTime	AcctAuthentic
2008-05-11 10:37:29	184	
2008-05-11 10:40:02	71	
2008-05-11 10:48:27	333	
2008-05-11 10:52:50	158	

ConnectInfo_start	ConnectInfo_stop	AcctInputOctets
		2097274
		1117010
		2991102
		650329

AcctOutputOctets	CalledStationId	CallingStationId
896177	reditelna	00:1C:BF:4A:29:3C
251399	reditelna	00:1C:BF:4A:29:3C
1001127	reditelna	00:1C:BF:4A:29:3C
191305	reditelna	00:1C:BF:4A:29:3C

AcctTerminateCause	ServiceType	FramedProtocol
User-Request		
User-Request		
User-Request		
User-Request		

FramedIPAddress	AcctStartDelay	AcctStopDelay
10.0.0.253	0	0
10.0.0.253	0	0
10.0.0.253	0	0
10.0.0.253	0	0

7 Bezpečnostní rizika a jejich řešení

7.1 Možnost odposlechnutí hesla

Pokud používáme autentizaci http-pap, heslo je mezi počítačem uživatele a přístupovým bodem přenášeno v otevřené podobě. Pokud by se k síti někdo připojil a odposlechl by rámce nesoucí toto heslo, mohl by jej následně použít pro přihlášení do sítě. Pro navrhovanou školní síť jsem použil pouze http-pap, neboť v případě odposlechnutí cizího hesla nezíská útočník kromě možného rychlejšího připojení k internetu nic. Není tedy potřeba spravovat certifikační autoritu, vystavovat a instalovat certifikáty, případně nakupovat certifikáty od společností typu Verisign apod.

Pokud by bylo potřeba hesla chránit proti odposlechnutí a hrozilo by realné nebezpečí zneužití hesla, nabízí se nám několik řešení, přičemž dvě z nich lze snadno implementovat s FreeRadiusem i Mikrotik RouterOS. Místo http-pap můžeme použít http-chap, kdy bude heslo přenášeno jako MD5 hash. Toto řešení si vyžaduje konfiguraci RADIUS serveru tak, aby počítal s MD5 hashem místo otevřeného hesla. Dále je nuté, aby prohlížeč uživatele měl povolený javascript,čímž se zvyšuje pravděpodobnost nekompatibility v případě, že prohlížeč uživatele podporu nemá.

Druhou možností je použít SSL připojení mezi uživatelským počítačem a přístupovým bodem. Mikrotik RouterOS lze nakonfigurovat tak, aby používal https přístup na přihlašovací stránku. V takovém případě je heslo přenášeno šifrovaně a nelze jej odposlechnout.

7.2 Možnost odposlechnutí komunikace

Komunikace mezi počítačem uživatele a přístupovým bodem není šifrovaná, a proto lze snadno odposlechnout přenášená data. Většina služeb na internetu, kde se používají osobní či přístupové údaje, využívá https připojení a heslo je šifrováno vyšší aplikační vrstvou na straně prohlížeče uživatele. Pokud bychom však chtěli šifrovat kompletně celou komunikaci, nabízí se zde možnost vytvoření VPN tunelu z uživatelského počítače například na server, kde běží RADIUS, případně na samotný přístupový bod pomocí například OpenVPN nebo L2TP.

8 Závěr

V rámci své práce jsem popsal dostupné metody autentizace a způsoby autorizace uživatelů v lokálních bezdrátových sítích.

Z hlediska úrovně zabezpečení se zdá být nejvhodnější použití autentizační metody WPA2 podle standardu IEEE 802.11i s šifrováním dat pomocí AES CCMP, která poskytuje v dnešní době nejdokonalejší způsob zabezpečení bezdrátových sítí. Ve firemních sítích o větším množství uživatelů a přístupových bodů je vhodné zvolit autentizaci pomocí EAP a využít tak centrální řízení přístupu pomocí autentizačního serveru RADIUS. Úroveň zabezpečení lze maximalizovat použitím osobních certifikátů, tokenů nebo smart karet.

Pokud požadujeme, aby se do sítě mohly připojit zařízení různých výrobců a bylo tak dosaženo maximální kompatibility, pak je nejvhodnější využít autentizaci Open System na linkové vrstvy a přístup do sítě řídit na vrstvě síťové využitím HotSpot brány. Tento způsob lze využít např. v kavárnách, školních nebo firemních sítích, kde je vyžadováno uživatelsky jednoduché přihlášení do sítě bez nutnosti instalace dodatečného software či certifikátů. I v tomto případě lze využít RADIUS server pro centrální řízení přístupu do sítě.

Z hlediska úspory financí je pro zabezpečení malých sítí v domácnostech nebo kancelářích dostačující použití autentizace pomocí WPA2 PSK nebo WPA PSK s využitím šifrování AES CCMP nebo TKIP. V těchto případech není nutné využívat centrální RADIUS server, neboť konfiguraci jednotlivých uživatelů a klíčů lze provést přímo na přístupovém bodu.

Použití metod WEP - Shared Key nebo filtrace MAC adres pro autentizaci uživatelů nelze z hlediska bezpečnosti v žádném případě doporučit. Tyto metody lze snadno obejít, a proto nepředstavují téměř žádnou úroveň zabezpečení.

Pro praktický návrh autentizace a autorizace jsem zvolil situaci bezdrátové školní sítě o třech přístupových bodech. Pro tuto situaci je vhodné použití autentizace na síťové vrstvě pomocí brány HotSpot, protože není předem známo, jaký počítač, operační systém a síťový HW budou studenti, učitelé a náhodní návštěvníci školy používat. Pro přihlášení do sítě je potřeba jakýkoliv webový prohlížeč, kde uživatel vyplní své uživatelské jméno a heslo. Pro dané řešení nebylo třeba řešit otázku zabezpečení proti odposlechnutí hesla, neboť by útočník získal pouze rychlejší připojení k internetu a nemohl by heslo jinak zneužít. Pro jiné případy, kdy je zabezpečení hesla nutné, jsem uvedl možná řešení. Pro realizaci jsem zvolil síťové prvky společnosti Mikrotik s operačním systémem RouterOS. Volil jsem tak proto, že tento operační systém v sobě přímo obsahuje aplikaci HotSpot brány, podporuje RADIUS a spousty dalších užitečných funkcí. Jedná se o cenově dostupné řešení.

Zvolené zařízení Mikrotik RouterBoard 133 se ukázalo jako velmi stabilní řešení. Podle mého názoru by nebyl problém jej použit i v horších podmínkách (průmyslové aplikace). Výše uvedené zařízení umožňuje použití většiny autentizačních metod, o kterých jsem v této práci psal. Autentizace pomocí brány HotSpot se ukázala velmi použitelná a kompatibilní se spoustou síťových zařízení a operačních systémů. Navržená konfigurace Mikrotik RouterOS a FreeRadius serveru fungovala dobře. Přihlášení do sítě se mi podařilo s operačnímy systémy Linux, Windows XP, Windows Vista, Windows 98. Úspěšné přihlášení se mi podařilo i s mobilním telefonem iPhone. Přihlášení fungovalo bez problémů na prohlížečích Internet Explorer, Mozilla Firefox, Opera, Lynx a Safari.

Pro použití navrženého řešení v praxi je možné upravit přihlašovací stránku pro konkrétní řešení. Dále by bylo vhodné vytvořit nějakou jednoduchou aplikaci pro správu uživatelských účtů v MySQL databázi, díky čemuž by bylo velmi snadné přidávat, mazat a upravovat úživatelské účty. Pokud bychom umístili RADIUS server

někam do serverovny na veřejnou IP adresu, mohl by autentizovat a autorizovat uživatele třeba z celé republiky nezávisle na místě, kde se uživatel do sítě přihlašuje. Navržené řešení lze realizovat velmi levně (15 – 20 tisíc korun), pokud bychom realizovali podobnou aplikaci např. se síťovými prvky Cisco, náklady by vzrostly o několik desítek tisíc.
Jsem přesvědčen, že se můj návrh může stát základem autentizace a autorizace pro rozsáhlejší sítě.

Seznam literatury

[1] Wi-Fi Protected Access [online]. Poslední aktualizace 29. 4. 2003 [cit. 8. 12. 2007]. Dostupný z URL: <http://www.wifi.org/files/wp_8_WPA%20Security_4-29-03.pdf>.

[2] Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise [online]. Poslední aktualizace 1. 3. 2005 [cit. 8. 12. 2007]. Dostupný z URL: <http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf>.

[3] ADOBA, B, SIMON, D. PPP EAP TLS Authentication Protocol [online]. 1999 [cit. 2007-12-09]. Dostupný z WWW: <http://tools.ietf.org/html/rfc2716>.

[4] AWDUCHE, D, et al. Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) [online]. 2006 [cit. 2007-12-08]. Dostupný z WWW: <http://tools.ietf.org/html/rfc4186>.

[5] WHITING, D, et al. Counter with CBC-MAC (CCM) [online]. 2003 [cit. 2007-12-10]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc3610.txt>.

[6] RIGNEY, C, et al. Remote Authentication Dial In User Service (RADIUS) [online]. 2000 [cit. 2007-12-07]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc2865.txt>.

[7] RIGNEY, C, LIVINGSTON. RADIUS Accounting [online]. 2000 [cit. 2007-12-10]. Dostupný z WWW: <http://www.ietf.org/rfc/rfc2866.txt>.

[8] FUNK, Paul, et al. EAP Tunneled TLS Authentication Protocol Version 0 (EAP-TTLSv0) [online]. 2007 [cit. 2007-12-10]. Dostupný z WWW: <http://tools.ietf.org/wg/eap/draft-funk-eap-ttls-v0-02.txt>.

[9] Authorization [online]. 2005 , 6. 12. 2007 [cit. 2007-12-10]. Dostupný z WWW: <http://wiki.freeradius.org/Authorization>.

[10] Authentication [online]. 2005 , 6. 12. 2007 [cit. 2007-12-07]. Dostupný z WWW: <http://wiki.freeradius.org/Authentication>.

[11] IEEE Computer Society. 802.11i™ : IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks— Specific requirements [online]. 2004 [cit. 2007-12-08]. Dostupný z WWW: <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>.

Slovník

AAA server	Authentication, Authorization, Accounting server – server zajišťující Autentizaci, Autorizaci a Tarifikaci.
Access Point (AP)	(Přístupový bod) – síťové zařízení zajišťující bezdrátové spojení s lokální sítí.
Accounting	(Tarifikace) – záznam údajů o začátku, průběhu a konci každé relace (session), kterou uživatel uskuteční. Záznamy se často používají pro vyučtování služeb uživateli.
EAP	Extensible Authentication Protocol (rozšiřitelný autentizační protokol) – univerzální autentizační struktura, která se nejčastěji používá v bezdrátových lokálních sítích a v Point to Point připojeních. Definuje základní principy pro používání různých autentizačních metod. V současnoti jich je k dispozici přibližně 40.
HotSpot	Má více významů. V bezdrátových sítích představuje přístupový bod, pomocí něhož se lze připojit k síti WLAN. HotSpot brána je systém, který běží na přístupovém bodu a zajišťuje autentizace a autorizaci na síťové vrstvě.
HTTP-PAP	HTTP Password Authentication Protocol – protokol založený na principu ověření uživatelského jména a hesla.
MAC adresa	Medium Access Control adresa (adresa pro řízení přístupu k médiu) – identifikátor síťového rozhraní sítě ethernet, který má 48 bitů. Využívají ho protokoly spojové vrstvy modelu OSI.
MD5	Message Digest 5 – hashovací algoritmus používaný pro kontrolu integrity souborů a hashování hesel. Výstupní řetězec má délku 128 bitů.
NAS	Network Access Server (Síťový přístupový server) – zařízení (nejčastěji síťová brána), které má za úkol zpřístupňovat určité síťové zdroje určitým uživatelům/zařízením.
PSK	Pre-Shared Key (sdílený klíč) – tajný šifrovací klíč sdílený dvěma stranami, mezi nimiž má probíhat šifrovaná komunikace.
RADIUS	Remote Authentication Dial In User Service – je AAA protokol využívaný pro centrální autentizaci, autorizaci a tarifikaci pomocí autorizačního serveru.

SSID	Service Set Identifier – identifikátor bezdrátové sítě WLAN, který je v pravidelných intervalech vysílán bezdrátovým přístupovým bodem v rámcích beacon.
SSL	Secure Sockets Layer – vrstva vložená mezi transportní a aplikační vrstvu modelu OSI. Zajišťuje bezpečnou autentizaci a šifrování dat.

Obsah přiloženého CD

1. **/bp_2008_cizek_michal.pdf** – bakalářská práce ve formátu PDF
2. **/hotspot_html** – zdrojové kódy HTML stránek pro HotSpot bránu
3. **/mikrotik_config_files** – konfigurační soubory pro Mikrotik RouterOS
4. **/radius_config_files** – konfigurační soubory pro FreeRadius server
5. **/radius_db** – tabulky do MySQL databáze pro FreeRadius