UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

BAKALÁŘSKÁ PRÁCE

2017 David Kožený

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Návrh a správa bezdrátové sítě

David Kožený

Bakalářská práce

2017

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**David Kožený**
Osobní číslo:	**I13158**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Návrh a správa bezdrátové sítě**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem bakalářské práce je navrhnout bezdrátovou síť umožňující připojení PC klientům a mobilním zařízením. Připojení koncových zařízení bude ověřováno pomocí Radius server. Teoretická část práce popíše technologie a služby použité v navržené síťové infrastruktuře. Praktická část bude obsahovat: návrh infrastruktury, popis použitých prvků, podrobný popis zpráv mezi Radius servrem a klienty.

Rozsah grafických prací:

Rozsah pracovní zprávy: **35**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. Vyd. 1. Brno: CP Books, 2005. ISBN 80-251-0791-4.
MikroTik Wiki. Mikrotik IPS IDS [online]. MikroTik, 1996, 2014 [cit. 2015-12-09]. Dostupné z URL: <http://wiki.mikrotik.com/wiki/Mikrotik_IPS_IDS>.

Vedoucí bakalářské práce: **Ing. Soňa Neradová, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **31. října 2016**

Termín odevzdání bakalářské práce: **12. května 2017**

Univerzita Pardubice Česká republika

L.S.

Ing. Zdeněk Němec, Ph.D.
děkan

Mgr. Josef Horálek, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2017

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 27. 04. 2017

podpis autora
David Kožený

PODĚKOVÁNÍ

Chtěl bych zde poděkovat vedoucímu bakalářské práce Ing. Soně Neradové Ph.D. za zadání zajímavé a podmětné práce, její rady, čas a péči, kterou mi věnovala při řešení veškeré problematiky. A také všem respondentům, kteří mi poskytli potřebné informace.

ANOTACE

Obsahem práce je návrh bezdrátové sítě, která umožní připojovaní PC klientů a mobilních zařízení. Připojování koncových zařízení je ověřováno pomocí Radius serveru. Práce popisuje použité služby, použité technologie a komunikaci mezi klienty a Radius Serverem.

KLÍČOVÁ SLOVA

Radius server, klient, bezdrátové sítě, technologie, služby

TITLE

Design and management wireless networks

ANNOTATION

The content of the thesis is a wireless network design that allows the connection of PC clients and mobile devices. The connection of the end devices has been verified by the Radius server. This work describes used services, used technologies and communication between clients and Radius Server.

KEYWORDS

Radius server, client, wireless, technology, services

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

AAA	Authentication, Authorization and Accounting protocol
AD	Active Directory
AES	Advanced Encryption Standard
AES-CCM	Advanced Encryption Standard- Counter with CBC-MAC
AES-GCM	Advanced Encryption Standard - Galois Counter Mode
AP	Access Point
CAPsMAN	Controlled Access Point system Manager
CCMP Protocol	Counter Cipher Mode with Block Chaining Message Authentication Code
CIFS	Common Internet File System
DES	Data (Digital) Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol over LAN
CHAP	Challenge-Handshake Authentication Protocol
CHAPv2	Challenge-Handshake Authentication Protocol version 2
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IEEE-SA	Institute of Electrical and Electronics Engineers Standards Association
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardisation

ISP	Internet service provider
LAN	Local Area Network
MAC	Media Access Control
MD5	cryptographic hash function
MIC	Message Integrity Code
NAS	Network Attached Storage
NTLM	NT LAN Manager
NTLMv2	NT LAN Manager version 2
OS	Operating System
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
PMK	Pairwise Master Key
PSK	Pre-shared Key
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RC4	Rivest Cipher 4
RFC	Request For Comments (standard)
SMB	Server Message Block
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security

TTLS	Tunnelled Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus
VLAN	Virtual LAN
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fifelity
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access version 2
WPS	Wi-Fi Protected Setup
WS	Windows Server

0 ÚVOD

Bezdrátové sítě se staly nedílnou součástí našich životů. Dnes jsou bezdrátové sítě ve většině domácností, které vlastní notebook nebo chytrý telefon. Dříve byly bezdrátové sítě rozšířené pouze ve firmách, které měly dostatek finančních prostředků na pořízení těchto zařízení. Hlavním důvodem rozvoje bezdrátových sítí byla potřeba volného pohybu a připojení zařízení ze všech dostupných prostor. S přibývající potřebou bezdrátového připojení roste počet útoků na zabezpečení sítě, proto je nezbytnou součástí co nejbezpečnější nastavení sítě.

Začátek práce je věnován bezpečnosti sítě, kde je uveden přehled bezpečnostních zásad se zásadami zabezpečení sítí VPN a zásadami pro práci s hesly. Je zde vysvětlena technologie AAA s protokolem Radius a protokolem TACACS+. Popis Radius protokolu obsahuje podrobné znázornění komunikačních zpráv, které zasílá nebo přijímá Radius server od přístupového bodu případně klienta. Dále se práce zabývá zabezpečením bezdrátových sítí, popisem vývoje zabezpečení, porovnáním základních druhů zabezpečení včetně základního autentizačního protokolu EAP a jeho komunikačních zpráv. Následuje krátké vysvětlení algoritmů šifrování v bezdrátové komunikaci, Samby a protokolu SMB.

Praktická část práce obsahuje návrh síťové infrastruktury, nastavení prvků a funkcionalit. Jedním z úkolů bylo vytvořit podrobný popis zpráv mezi Radius servrem a klienty. V přílohách jsou uložena jednotlivá nastavení.

1 BEZPEČNOST SÍTĚ

Na zabezpečení sítě se často zapomíná nebo mu není věnováno dostatek prostředků. V dnešní době jsou běžné pokusy o napadnutí firemních sítí bez ohledu na to, zda mají cenná data. Proto je nutné dodržet alespoň ty nejdůležitější bezpečnostní zásady. Kontrolovat, komu je umožněn přístup do sítě a zvážení, jaká obdrží přístupová práva. Nikdy nesmíme umožnit uživateli přístup do celé sítě a už vůbec ne ke všem datům. (THOMAS,2005, s. 68)

1.1 Přehled bezpečnostních zásad

- Chraňte data na úrovni souborů a adresářů pomocí přístupových práv.
- Chraňte sítové prvky umístěním mimo dosah nepovolaným osobám.
- Přenosná zařízení jako například notebooky chraňte šifrováním.
- Nedovolte lidem využívat váš počítač pod vaším účtem.
- Nevypínejte bránu Firewall ani antivirové programy.
- Nevstupujte na nebezpečné stránky a neotevírejte podezřelé emaily.

1.2 Zásady pro práci s hesly

- Nesdělujte své heslo ostatním lidem.
- Nepište si hesla na papíry a nevytvářejte nápovědu k heslům jako například: „Jméno mého psa“.
- Pravidelně měňte heslo ideálně jednou za tři měsíce.
- Heslo nesmí být možné najít ve slovníku.
- Heslo musí být složeno z minimálně 8 znaků a musí mít zvolenou vhodnou strukturu tzn. minimálně tři kombinace z těchto čtyř kombinací: (0-9), (a-z), (A-Z), (~-#).

1.3 Zásady zabezpečení sítí VPN

- Šifrujte připojení do privátní sítě.
- Ověřujte pomocí digitálního certifikátu.
- Autentizujte uživatelé.
- Uživatelé s oprávněním přístupu přes VPN nesmí umožnit přístup neoprávněným osobám.

1.4 Standardy ISO

Mezi základní ISO standardy patří:

- ISO / IEC 27001: 2013 řízení bezpečnosti informací.
- ISO / IEC 27002 kybernetická bezpečnost.

V České republice od roku 2015 platí Zákon č. 181/2014 Sb. o kybernetické bezpečnosti. Zákon stanovuje, jakým způsobem má být kybernetická bezpečnost zajišťována a jak mají být řešeny bezpečnostní incidenty. Poslanecká sněmovna schválila letos v dubnu novelu zákona o kybernetické bezpečnosti. Novela rozšiřuje působnost stávajícího zákona na další skupiny provozovatelů nebo správců IT technologií.

2 TECHNOLOGIE AAA

Je to protokol zabývající se počítačovou bezpečnosti, AAA znamená authentication, authorisation and accounting protocol. V českém jazyce termín označuje autentizační, autorizační a účtovací protokol. (THOMAS,2005, s. 103)

2.1 Autentizace

Mezi nejbezpečnější autentizační metody patří používaní uživatelského jména a hesla. Tento proces není náročný na uživatele z důvodu, že uživatelské jméno zůstává po celou dobu neměně a heslo se mění podle implementace bezpečnostních zásad. Autorizační proces má pouze potvrdit, jestli je uživatel tím, za koho se vydává. (THOMAS,2005, s. 104)

2.2 Autorizace

Autorizace znamení povolení nebo zamítnutí služeb přihlášenému uživateli. Autorizační proces například udělí práva zápisu na sítové disky, které patří uživateli na základě autentizace. (THOMAS,2005, s. 104, 105)

2.3 Účtování

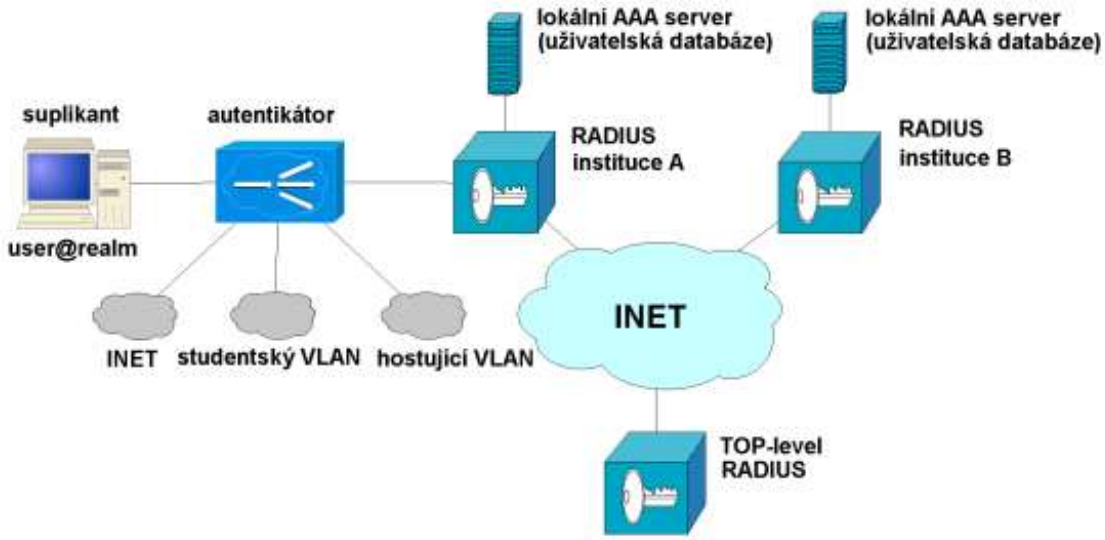
Účtovaní znamená sledovaní využívaných služeb uživatelem. Tyto informace bývají často využívaný pro správu sítě nebo jako další kroky pro zabezpečení sítě. (THOMAS,2005, s. 105)

2.4 Protokol Radius

Radius protokol byl vytvořen v roce 1997 společnosti Merit Network ve spolupráci s Livingston Enterprises. Aktuálně je definován v dokumentací RFC 2865 a RFC 2866. Cílem systému Radius bylo vytvoření centrálního místa pro ověření uživatelů. Uživatelé by se ověřili na centrálním serveru a byl by jim umožněn přístup k požadovanému systému nebo službě. Zároveň při pokusu kontaktovat požadovaný systém by centrální server vrátil zprávu, zda se požadovaný systém povedlo nebo nepovedlo kontaktovat. V roce 1999 se společnost Microsoft zasadila o specifikaci vlastností, protokol byl postupně rozšiřován a nyní podporuje většinu autentizačních protokolů: PAP, CHAP, MS-CHAPv2, EAP-MD5, EAP-TLS, PEAP, EAP-TTLS, EAP-SIM atd. Pojem Radius je u nás známí ve spojení s institucí eduroam, která využívá Radius server s ověřovacím protokolem 802.1x. Instituce nevyužívá jen jeden Radius server, ale několik serveru, které jsou mezi sebou propojeny.

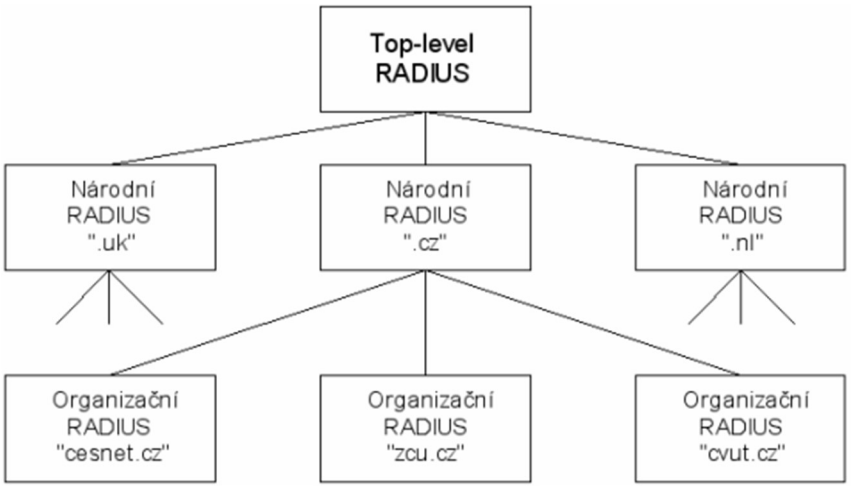
Základní funkce Radius serveru:

1. Ověření uživatelů nebo zařízení, než je umožněn přístup do sítě.
2. Autorizace uživatelů nebo zařízení pro konkrétní sítové služby.
3. Sledovaní využití těchto sítových služeb a účtů uživatelů.



Zdroj: zpracováno dle(EDUROAM,2016)

Obrázek 1 – Příklad připojení zařízení do sítě eduroam.



Obrázek 2 – Struktura sítě eduroam

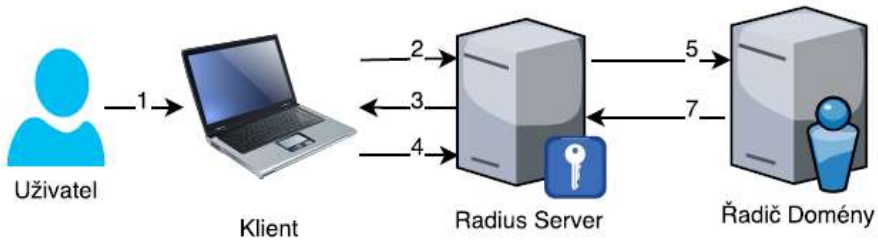
Zdroj: zpracováno dle (EDUROAM,2016)

2.4.1 Protokol NTLM

Je to autentizační protokol, který je využíván v sítích pužívající operační systémy Windows. U systému Windows 7 nebo novějšího systému s aktivní podporou od společnosti Microsoft[1] se používá verze NTLM2-Session, která kombinuje původní verzi NTLM protokolu a zabezpečení z verze NTLMv2. Nová verze využívá 128bit s MD5 šifrovaní hesla. NTLM je složeno z názvu domény, uživatelského jmena a hash hesla.

Komunikace přes NTLM:

1. Uživatel zadá doménu, uživatelské jméno a heslo.
2. Na klientovy se vypočte kryptografické hash a heslo se zahodí. Klient odešle uživatelské jméno serveru.
3. Radius server vygeneruje 16bajtové náhodné číslo a zašle jej klientovy (žádost).
4. Klient zašifruje toto číslo svým hash heslem a odešle serveru (odpověď).
5. Server odešle na řadič domény uživatelské jméno, žádost, která byla zaslána klientovy a odpověď kterou obdržel od klienta.
6. Řadič domény použije uživatelské jméno k získání hash hesla uživatele. Heslo bude vyhledáno v databáze uživatelů.
7. Řadič domény porovná šifrované objekty, a pokud jsou shodné zašle zprávu „authentication is successful“ a tím získá klient přístup do sítě.



Obrázek 3 – Komunikace přes protokol NTLM

Zdroj: vlastní

[1] Dostupná z: https://msdn.microsoft.com/cs-cz/library/cc236621.aspx(20.04.2017)

2.4.2 Popis zpráv mezi radiu serverem a klientem

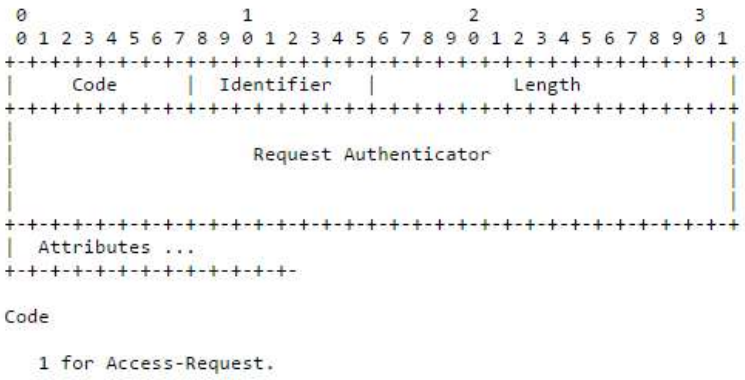
Radius server stěně jako autentizační metoda EAP komunikuje pouze pomocí čtyř typů zpráv.

Access-Request-Požadavek o přístup

Zpráva musí obsahovat uživatelské jméno a heslo nebo heslo metodou CHAP. Zároveň musí obsahovat identifikační údaje přístupového bodu NAS IP adresu nebo NAS jméno, ideálně obojí. V případě obdržení špatných informací je odeslána zpráva přístup zamítnut. Příklad požadavku o přístup:

```
rad_recv: Access-Request packet from host 192.168.30.155 port 59499,
id=10, length=194
      User-Name = "skola-upce\\kozeny"
      NAS-Identifier = "f09fc2331510"
      NAS-Port = 0
      Called-Station-Id = "F2-9F-XX-XX-15-10:Internal"
      Calling-Station-Id = "2C-56-DC-AB-C6-74"
      Framed-MTU = 1400
      NAS-Port-Type = Wireless-802.11
      Connect-Info = "CONNECT 0Mbps 802.11b"
      EAP-Message = 0x02de001c0161672d6565c6b726976736b79
      Message-Authenticator = 0xe97ef3c5839f68d88545105bc26fd
```

Pole identifikátoru se změní jen, pokud se změní atributy žádosti, aby zůstal paket platným. V případě, že se nezmění identifikátor, jde o opakované vysílání žádosti. Seznam atributu se postupně zvětšuje podle požadavků Radius serveru.

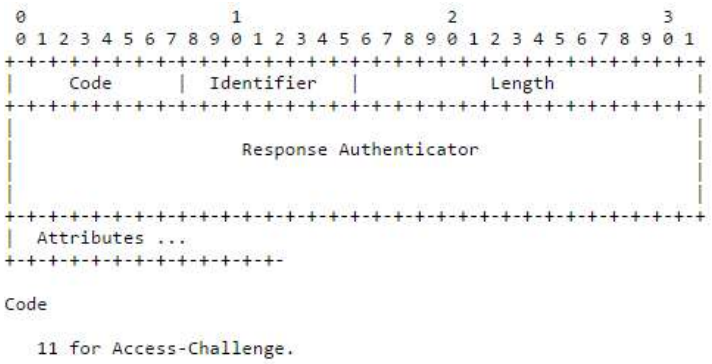


Obrázek 4 – Struktura paketu Access-Request .

Zdroj: zpracováno dle (WILLENS,2016)

Access-Challenge-výzva se změnou

Zpráva obsahuje požadavek na změnu nebo doplnění informací podle požadavků Radiu serveru. Seznam atributu je zvýšen o požadovanou informaci.

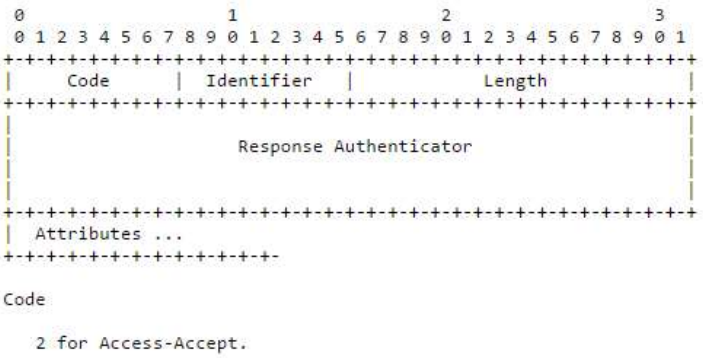


Obrázek 5 – Struktura paketu Access-Challenge.

Zdroj: zpracováno dle (WILLENS,2016)

Access-Accept-přístup povolen

Zpráva je kopii požadavku o přístup, obsahuje pouze jiný kód zprávy a povoluje přístup k sítí.

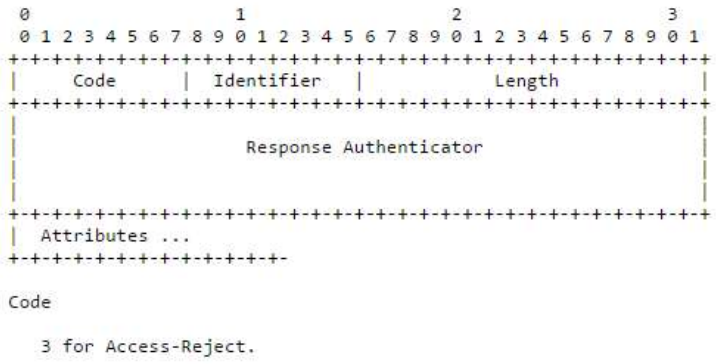


Obrázek 6 – Struktura paketu Access-Accept.

Zdroj: zpracováno dle (WILLENS,2016)

Access-Reject-přístup zakázán

Pokud, není některá hodnota z atributu správná pak Radiu serveru okamžitě odpovídá zamítnutím přístupu. Zprava je kopii požadavku o přístup pouze s jiným kódem zprávy.



Obrázek 7 – Struktura paketu Access-Reject.

Zdroj: zpracováno dle (WILLENS,2016)

2.5 Protokol TACACS+

Předchůdcem je protokol TACACS, který je nejstarším AAA protokolem. Protokol byl využíván pro autentizaci v sítích, pomocí IP protokolu. Vznikl pro potřebu řízení přístupu v síti ARPANET (předchůdce dnešního internetu). Protokol TACACS+ je proprietárním protokolem firmy Cisco. Na rozdíl od svého předchůdce, který byl využíván v transportní vrstvě protokolu UDP tak TACACS+ využívá TCP protokol a šifruje celé pakety. Všechny protokoly z rodiny TACACS provádějí autentizaci uživatelů a bez zadání správného uživatelského jmena a hesla je zakázán přístup k síti. (THOMAS,2005, s. 107)

3 BEZDRÁTOVÉ SÍTĚ

Bezdrátové sítě nám zajištují spojení klientů s vnitřní sítí bez použití sítových kabelů. Připojení zajištuje radiokomunikační zařízení, které komunikuje s klienty pomocí rádiových vln. Každé bezdrátové zařízení se musí řídit domluvenými komunikačními standardy IEEE 802.11. Standard je znám pod komerčním označením Wi-Fi. Signál je podle standardu šířen s frekvencí 2,4GHz nebo 5GHz. Ve městech bývá lepší využívat frekvenci 5GHz, protože pásmo nebývá zarušeno.

3.1 Rozdělení Bezdrátových sítí podle typu zabezpečení

Zabezpečení bude rozděleno na WEP, WPA-TKP, WPA-AES, WPA2 s implementaci standardu IEEE802.11i, WPS a filtrováním MAC adres. Porovnám zabezpečení typu WEP, WPA, WPA2

3.1.1 Zabezpečení WEP

Protokol WEP funguje na symetrickém principu, kde pro dešifrování i šifrovaní je používán stejný klíč, který je nejčastěji 40bitový. Tento klíč používají i všichni připojení uživatelé, pro autentizaci spolu s tím použijí i svou MAC adresu. Protokol ověřuje totožnost sítové karty nikoli uživatele, a to je jeho slabinou. Protokol WEP není považován za bezpečný v případě, že bude dostatečný provoz v síti, tak se podaří útočníkovi pomocí monitorování sítě odchytit dostatečný počet paketů pro útok na klíč. Po odchycení dostatečného množství paketů se útočníkovi povede klíč prolomit. Bývá to zhruba do 2 minut (zaleží na provozu sítě). Proto není toto zabezpečení od roku 2001 považováno za bezpečné. (HOLEČEK,2013; TRAPANI,2011)

3.1.2 Zabezpečení WPA-TKP a WPA-AES

Protokol WPA vznikl, aby nahradil nedostatky protokolu WEP. Protokol TKIP opravuje nedostatky protokolu WEP a to tak, že využívá dynamickou správu šifrovacího klíče. Později byly nalezeny slabiny šifry RC4, z které TKIP vychází, a tak se zabezpečení WPA-TKIP stalo nebezpečným. WPA-TKIP lze dnes prolomit do 30 minut. WPA bylo později vylepšeno šifrováním AES místo původního TKIP šifrování a pojmenováno jako WPA-AES, které je považováno za bezpečné. Některá zařízení nepodporuji AES šifrování. Šifrování vyžaduje vetší výpočetní výkon, a proto starší zařízení nejsou schopna podporovat tento typ šifrování. Integritu dat zajištuje algoritmus MIC. Pro autentizaci můžeme využívat PSK nebo protokol 802.1x s autentizačním serverem, který podporuje protokoly typu EAP. (VANHOE,2011)

3.1.3 Zabezpečení WPA2

Protokol WPA2 plně implementuje standard IEEE802.11i, který zajišťuje komplexní bezpečnost bezdrátových sítí. Standard rozšiřuje původní WPA tím, že kompletně odstraňuje algoritmus RC4 a nahrazuje ho algoritmem AES a zároveň odstraňuje algoritmus MIC pro počítání rámců a nahrazuje ho algoritmem CCPM. Pro autentizaci můžeme využívat PSK nebo protokol 802.1x s autentizačním serverem, který podporuje protokoly typu EAP.

Zabezpečení WPA2 je povinné pro všechny zařízení certifikovaná jako Wi-Fi od března 2016.

Protokol IEEE 802.1x

Protokol využívá tři základní komponenty:

- **supplicant –** je uživatel nebo klient, který žádá o ověření.
- **autentizační server –** ověřovací server například Radius server.
- **ověřovatel –** zařízení mezi klientem a ověřovacím serverem (přepínač nebo přístupový bod).

Protokol 802.1x definuje přístup k síti a zabraňuje přístupu neautorizovaném klientům. Autentizační server ověří klienta předtím, než mu jsou zpřístupněny jakékoli služby. Neoprávněným klientům je přístup k síti zakázán. Pokud není klient ověřen tak standart řízení přístupu povoluje přístup přes protokol EAPOL na portu, kde je klient připojen. Po úspěšném ověření klienta je povolen přístup k síti. (FIEDLER,2004)

Stavy portu přepínače:

- **force-authorized – přístup do sítě je povolen bez nutnosti autorizace.**
- **force-unauthorized – všechny pokusy klienta o autorizaci jsou ignorovány.**
- **auto – autorizace 802.1X zapnuta.**

3.1.4 Zabezpečení přes WPS

Zabezpečení pomocí protokolu WPS je velice jednoduché spočívá v tom, že router poslouchá, jestli se některé zařízení nesnaží připojit. Zařízení, která se chtějí připojit, zasílají osmimístný kód, který je rozdělen do dvou částí po čtyřech číslicích. Router jim následně odpoví, jestli byl zadaný kód správný nebo ne. Bohužel odpověď obsahuje informace i o tom jaké byly první dvě číslice z každé části. Útočníkovi pak zbývá odhalit dvě číslice z první části a jednu číslici z druhé časti což je 10^4+10^3 kombinací. Útočníkovi se proto do několika hodin podaří tento osmimístný kód prolomit.

3.1.5 Blokování odesílaní SSID

Je nejjednodušším typem zabezpečení je velice jednoduché na nastavení, ale lze také velmi snadno prolomit, přesto může útočníka odradit od útoku. Síť se v seznamu zobrazuje jako „skrytá síť“ a zdá se, že pro připojení je nutné zadat název sítě.

3.1.6 Filtrovaní MAC adres

Každá sítová karta v počítači má svou jedinečnou identifikační adresu MAC. Tuto adresu můžeme zapsat do routeru a tím zamezíme připojení komukoli, kdo bude mít jinou adresu MAC. Pokud k vám přijde návštěva, budete muset každou MAC adresu přidat do routeru, a to je nevýhodou řešení filtrovaní přes MAC adresy.

3.1.7 Porovnání zabezpečení bezdrátových sítí

Tabulka 1 – Porovnání zabezpeční bezdrátových sítí

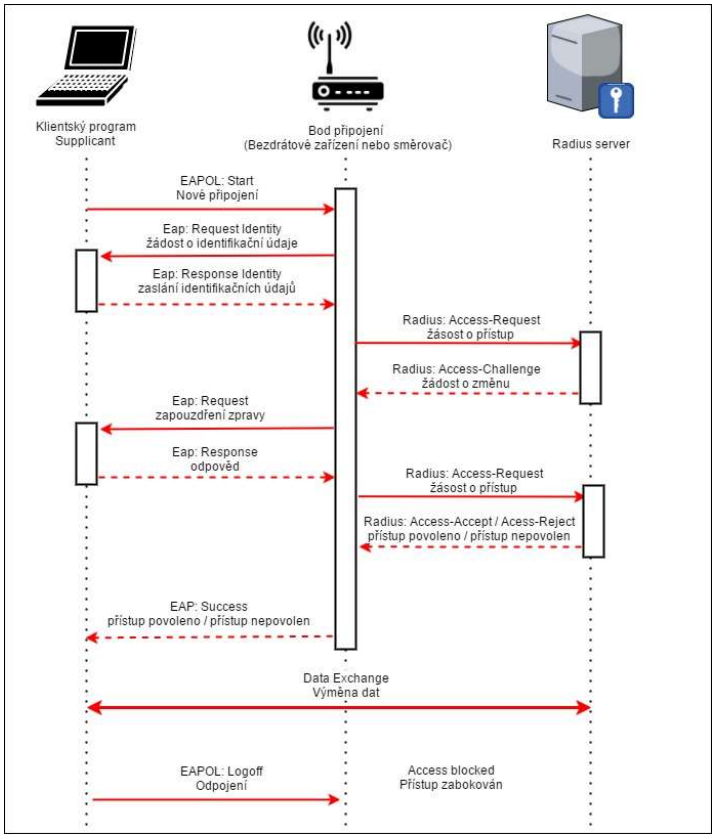
Metoda	Ověření identity	Síla šifry	Použ. pro domácí a malé sítě	Použ. pro podnikové sítě
WEP	žádné	slabší (WEP-RC4)	dobré, avšak relativně slabé	nedostatečné
WPA (PSK)	slabší (předem sdílený klíč)	dobrá (TKIP-RC4)	velmi dobré	slabé
WPA2 (PSK)	slabší (předem sdílený klíč)	výborná (AES-CCMP)	velmi dobré	slabé
WPA (plná)	dobré (IEEE 802.1x)	dobrá (TKIP-RC4)	velmi dobré	dobré
WPA2 (plná)	dobré (IEEE 802.1x)	výborná (AES-CCMP)	výborné	velmi dobré

Zdroj: zpracováno dle (FIEDLER,2004)

3.2 Autentizační protokol EAP

EAP je to autentizační protokol, který umožnuje zasílat pouze zprávy typu:

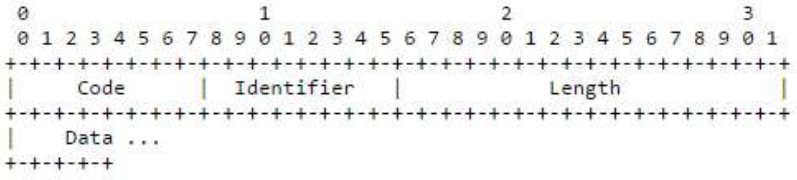
- **Request** (žádost o identitu),
- **response** (odpověď s identitou),
- **success** (úspěšné ověření),
- **failure** (neúspěšné ověření).



Obrázek 8 – Příklad komunikace s využitím protokolu EAP

Zdroj: vlastní

V současnosti definováno nejméně 20 různých EAP metod, které se lišící typem šifrovaní nebo zapouzdřování paketů.

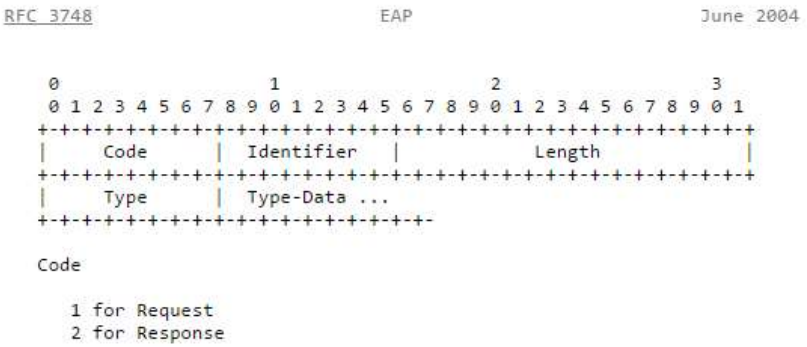


Obrázek 9 – Základní struktura EAP paketu.

Zdroj: zpracováno dle (MICROSOFT,2004)

3.2.1 Zprávy typu Request a Response

Jako první se vždy musí odeslat paket se žádostí a následně je možné přijmout odpověď. Není možné přijmout odpověď bez předem zaslané žádosti. Pokud nebude přijata odpověď v časovém limitu, který má paket se žádostí nastaven. Opakuje se zaslání žádosti znovu, starý paket s odpovědí je automaticky zahozen. Jednotlivé žádosti o identitu jsou mezi sebou odlišeny identifikátorem a je povoleno zaslat maximálně 256 paketů se žádostí o identitu.

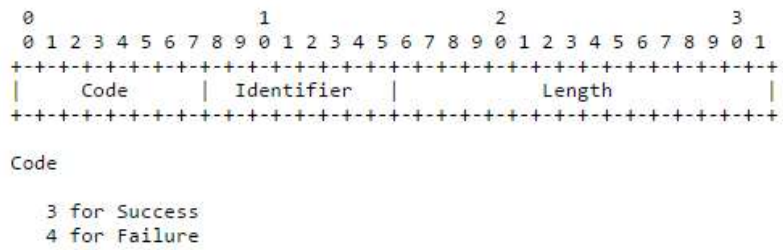


Obrázek 10 – Struktura paketu Request a Response.

Zdroj: zpracováno dle (MICROSOFT,2004)

3.2.2 Zprávy typu Success a Failure

Pokud byla obdržena zpráva s odpovědí identity od klienta, tak klientovy musí být vždy zaslána zpráva o potvrzení nebo odmítnutí autentizace. Existuje však jedna výjimka. Odpověď nebude zaslána v případě ztráty připojení klienta. Zároveň pakety nemůžou být zaslány, dokud to zvolený typ metoda EAP nepovolí. V případě, že zařízení neobdrží potvrzení nebo odmítnutí autentizace, bude komunikace se zařízením ukončena jako ztráta paketu EAP a celé ověření se musí opakovat.



Obrázek 11 – Struktura paketu Success a Failure.

Zdroj: zpracováno dle (MICROSOFT,2004)

3.3 Použité algoritmy šifrování v bezdrátové komunikaci

Jednou z důležitých úloh zabezpečení přenášených dat je jejich šifrování. Slovem šifra nebo šifrování je označován kryptografický algoritmus, který převádí čitelnou zprávu neboli prostý text na její nečitelnou podobu neboli šifrový text. Vývoj bezdrátových sítí se odráží i v implementovaných algoritmech šifrování.

DES je symetrická bloková šifra s nedostatečnou délkou klíče. Algoritmus byl používán od roku 1972 a v 90. letech byl prolomen hrubou silou[2]. V roce 2002 byl nahrazen šifrováním AES. Algoritmus DES se stále využívá například pro zabezpečení aplikací nebo informací, které nemají vysokou materiální hodnotu.

3.3.1 Šifrování TKIP

TKIP je stejně jako protokol WEP založený na algoritmu RC4, účelem protokolu TKIP bylo napravit všechny nedostatky protokolu WEP. Problémem protokolu TKIP je že umožňuje vkládat pakety do šifrované komunikace, jedná se tak o tzv. Beck-Tews útoky. Proto je tento algoritmus považován za prolomený a není doporučováno ho používat.

3.3.2 Šifrovaní AES

AES je symetrická bloková šifra s pevnou délkou bloků, šifrování vyžaduje větší výpočetní výkon. AES nahrazuje dříve používanou šifru DES. Algoritmus používá i vláda Spojených států amerických. Šifrovací metodu lze prolomit pouze hrubou silou[2]. Tento problém lze lehce ošetřit, pokud použijete silné heslo. Heslo bude obsahovat všechny znaky bezpečného hesla. Šifra se používá pro zabezpečení bezdrátových sítí typu WPA2 a WPA. Všechna zařízení vyrobená po roce 2006 musí podporovat tuto šifrovací metodu.

Tabulka 2 - Typy šifrovaní AES

aes128	AES(128bitový klíč)
aes192	AES(192bitový klíč)
aes256	AES(256bitový klíč

Zdroj: zpracováno dle (IBM,2004)

[2] Hádáním hesla z připraveného seznamu.

3.4 Samba

Samba je programový balík dostupný v rámci GNU licence umožňující přístup k souborům a tiskovým službám v sítích složených ze zařízení s podporou protokolů SMB/CIFS. Je nezávislá na operačním systému, tzn. Linux/Unix/Windows. Snadno tak lze sdílet soubory, typicky mezi Linuxem a Windows.

3.4.1 SMB

Síťový protokol běžící na aplikační vrstvě a pracující na principu klient-server a využívající technologie NetBIOS. Byl vyvinut firmou IBM, později převzat a zdokonalen Microsoftem. Samba implementuje sítový protokol SMB, který využívá autentizační protokol NTLM, který slouží pro připojování klientů k Active Directory. Protokol CIFS je moderní nadstavba SMB, která na rozdíl od SMB nepoužívá pro překlad názvů NetBIOS, ale DNS. Aktuální protokol využívá kryptovací algoritmus AES-GCM. Microsoft zároveň ke každé verzi vydává obsáhlou dokumentaci, kde vysvětluje dopodrobna všechny náležitosti spojené s novou verzí a zároveň jaké změny provedl.

Tabulka 3 – Verze SMB v systémech Windows

OS	Windows 10 WS 2016 TP2	Windows 8.1 WS 2012 R2	Windows 8 WS 2012	Windows 7 WS 2008 R2	Windows Vista WS 2008	Previous versions
Windows 10 WS 2016 TP2	**SMB 3.1.1**	**SMB 3.0.2**	**SMB 3.0**	SMB 2.1	SMB 2.0.2	SMB 1.x
Windows 8.1 WS 2012 R2	**SMB 3.0.2**	**SMB 3.0.2**	**SMB 3.0**	SMB 2.1	SMB 2.0.2	SMB 1.x
Windows 8 WS 2012	**SMB 3.0**	**SMB 3.0**	**SMB 3.0**	SMB 2.1	SMB 2.0.2	SMB 1.x
Windows 7 WS 2008 R2	SMB 2.1	SMB 2.1	SMB 2.1	SMB 2.1	SMB 2.0.2	SMB 1.x
Windows Vista WS 2008	SMB 2.0.2	SMB 2.0.2	SMB 2.0.2	SMB 2.0.2	SMB 2.0.2	SMB 1.x
Previous versions	SMB 1.x	SMB 1.x	SMB 1.x	SMB 1.x	SMB 1.x	SMB 1.x

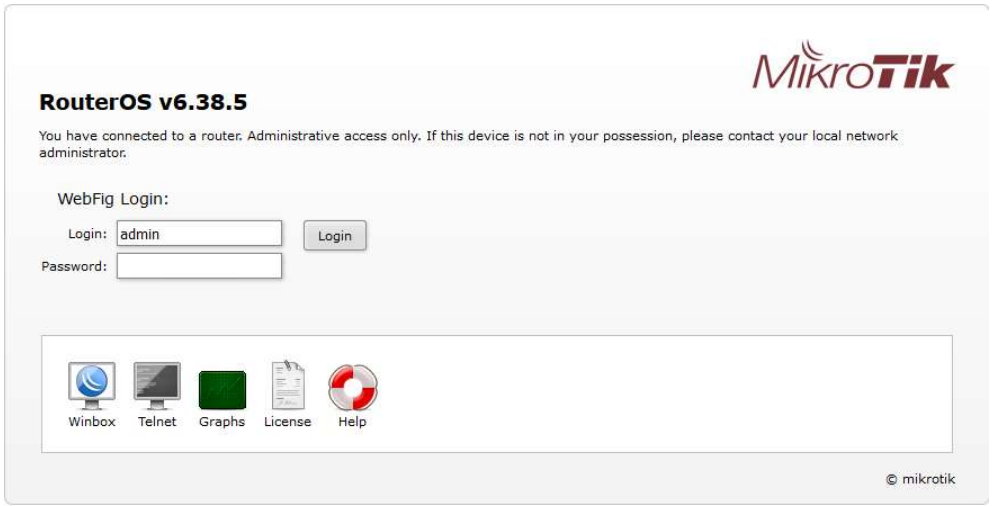
Zdroj: zpracováno dle (BARRETO,2015)

4 ZAŘÍZENÍ ZNAČKY MIKROTIK

Firma byla založena v roce 1996 v Lotyšsku pro vývoj směrovačů a bezdrátových ISP systémů. V roce 1997 vytvořila firma softwarový systém RouterOS, který poskytuje stabilitu a lehké ovládaní. Dále roku 2002 firma přešla na vlastní hardware, který pojmenovala RouterBOARD. Mikrotik nyní poskytuje softwarové i hardwarové řešení pro připojení domácností, ale i velkých firem k internetu. U nás je rozšiřováno povědomí o značce Mikrotik například firmou Tlapnet, která poskytuje připojení domácností. (MIKROTIK,2016)

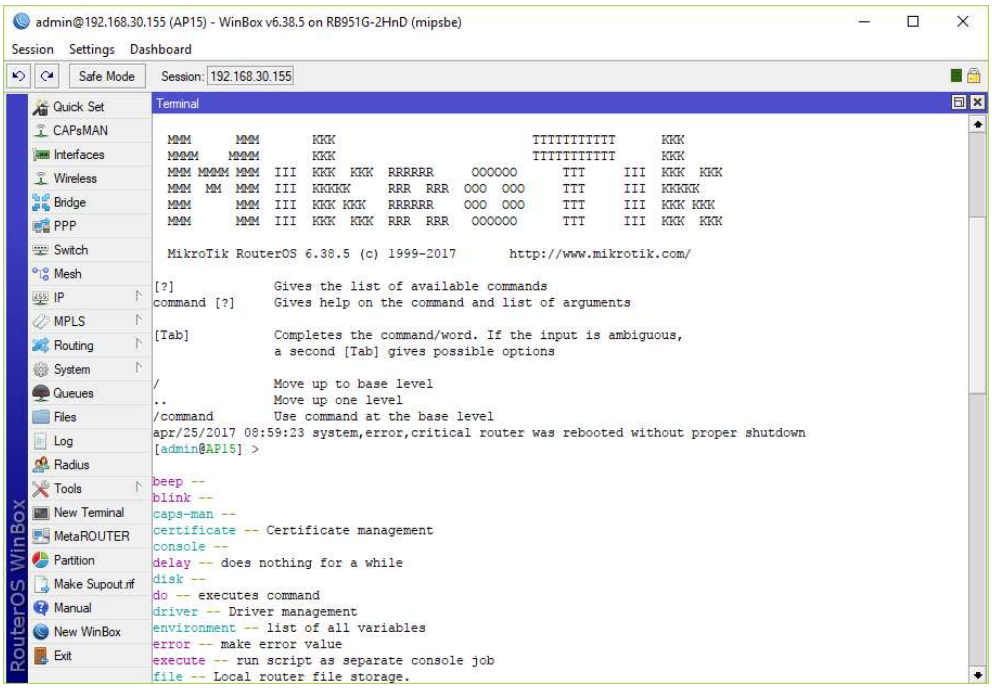
4.1 Připojeni k zařízení

Zařízení Mikrotik je možné spravovat přes Telnet, program Winbox a Webfig. Pro správu zařízení je nejlepší používat programu Winbox, který umožnuje připojení na MAC adresu zařízení nebo na IP adresu. Zároveň tento program umožňuje používat klasické terminálové funkce (viz. obrázek 13). Při používaní Webfig neboli webového rozhraní pro správu zařízení se stává, že se nastavená konfigurace správně neuloží. (MIKROTIK,2011)



Obrázek 12 – Možnosti správy zařízení Mikrotik

Zdroj: vlastní

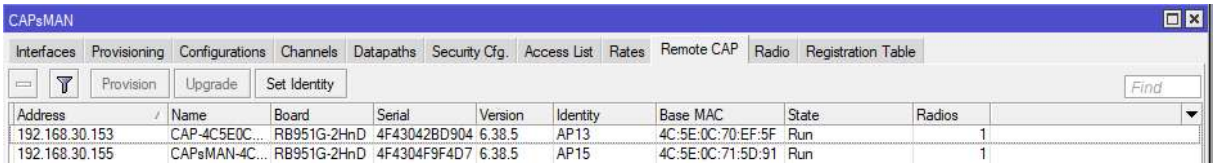


Obrázek 13 – Možnosti správy zařízení Mikrotik

Zdroj: vlastní

4.2 Modul CAPsMAN

Umožnuje centrální správu bezdrátových sítí. Modul spravuje veškerou bezdrátovou konfiguraci na jednotlivých AP zařízeních. Stará se také o ověřování klientů a případné předaní klienta na jiné AP zařízení. Zařízení mezi sebou provádí šifrovaní a dešifrovaní komunikačních dat, v závislosti na konfiguraci jsou data předána CAPsMANu pro centralizované zpracování. Modul umožnuje spravovat až 32 rozhraní na jednom zařízení. (MIKROTIK,2017)

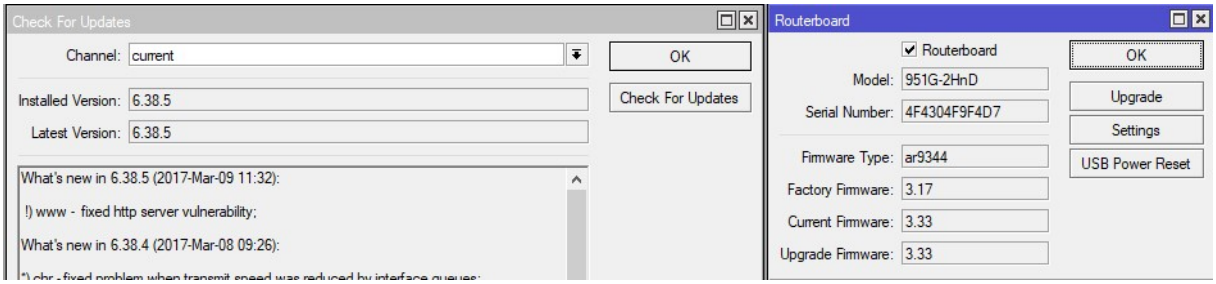


Obrázek 14 – Seznam spravovaných zařízení

Zdroj: vlastní

4.3 Způsoby aktualizace zařízení

Mikrotik pravidelně nabízí aktualizace operačního systému i firmwaru. Nejdříve je nutné aktualizovat operační systém a poté následně firmware. Po aktualizaci operačního systému nebo firmware je nutné zařízení vždy restartovat, pokud se tak nestane automaticky. Firmware řídí hardware, na kterém běží operační systém. (MIKROTIK,2017)



Obrázek 15 – Aktualizace operačního systému napravo a nalevo aktualizace firmwaru

Zdroj: vlastní

5 POROVNÁNÍ SÍŤOVÝCH PRVKŮ

Při volbě síťových prvků bylo důležité zaměření na požadavky, které musí zařízení splňovat. Zařízení musí mít možnost napájení přes ethernet, dále musí splňovat možnost ověřovaní klientů proti doméně a musí být schopné pracovat s více než čtyřmi logicky oddělenými sítěmi VLAN. Musí také umožnit vytvoření, alespoň pěti bezdrátových sítí, které mají svá unikátní jména. Posledním požadavkem je, aby zařízení bylo řízeno globálně a umožnovalo správu minimálně 8 zařízení.

Tabulka 4 – Porovnání sítových zařízení.

Zařízení	Poe	VLAN maximum	Klient maximum	Cluster maximum	SSID maximum	Cena od
Mikrotik RB951G-2HnD	**Ano**	**128**	**50**	**neomezeno**	**128**	**1500kč**
Mikrotik RB962UIGS	Ano	128	50	neomezeno	128	3000kč
Mikrotik RBcAP-2n	**Ano**	**128**	**50**	**neomezeno**	**128**	**1500kč**
CISCO WAP371	Ano	16	240	8	16	5100kč
CISCO WAP321	Ano	8	80	8	8	4200kč
TP-LINK EAP120	Ano	8	35	Kontrolní systém	8	2400kč
TP-LINK EAP220	Ano	16	35	Kontrolní systém	16	3000kč

Zdroj: vlastní

5.1 Zvolená zařízení pro bezdrátovou síť

Výběr značky Mikrotik byl ovlivněn zkušenostmi s jeho konfigurací a nenáročnou údržbou. Zařízení jsou cenově dostupná a nabízí rozsáhlé možnosti oproti ostatním zařízením jiných výrobců..

5.1.1 Popis zařízení RB951G-2HnD

Mezi integrované vybavení zařízení patří 600MHz procesor, 128MB RAM paměti, 2,5dBi anténa s frekvenci 2,4GHz a pět gigabitových portů LAN. Zařízení je možné napájet pomocí klasického konektoru nebo pomocí portu číslo 1, který umožnuje napájení přes ethernet. Mezi další vlastnosti patří: podpora IPv6, podpora norem 802.11b/g/n a možnost připojení zařízení USB.

Obrázek 16 – Zařízení RB951G-2HnD

Zdroj: zpracováno dle (ROUTERBOARD,2016)

5.1.2 Popis zařízení RBcAP-2n

Mezi integrované vybavení zařízení patří 650MHz procesor, 64MB RAM paměti, dvě 2dBi antény s frekvenci 2,4GHz a jedním napájecím ethernet portem. Mezi další vlastnosti patří: podpora IPv6 a podpora norem 802.11b/g/n.

Obrázek 17 – Zařízení RBcAP-2n

Zdroj: zpracováno dle (ROUTERBOARD,2016)

6 NÁVRH INFRASTRUKTURY

Návrh bezdrátového připojení je zaměřen na zabezpečení sítě, rozvržení umístění přístupových bodů, předávání klientu mezi přístupovými body, cenu zařízeních a jejich možnosti. Byla vybrána zařízení, která umožnují připojovaní klientů do sítě pomocí Radius serveru s ověřováním přes AD. Při volbě umístění zařízení bylo důležité pokrýt především kancelářské prostory a skladové prostory. Kancelářské prostory jsou pokryty zařízeními AP11, AP15 a AP10. Prostory skladu jsou pokryty zařízeními AP14 a AP12. Zařízení AP15 bylo zvoleno jako hlavní zařízení (master), které nastavuje ostatní zařízení na něj připojená. Ostatní zařízeni konfiguraci jen převezmou při spárovaní přes modul CAPsMAN.

Obrázek 18 – Rozvržení přístupových bodů

Zdroj: vlastní

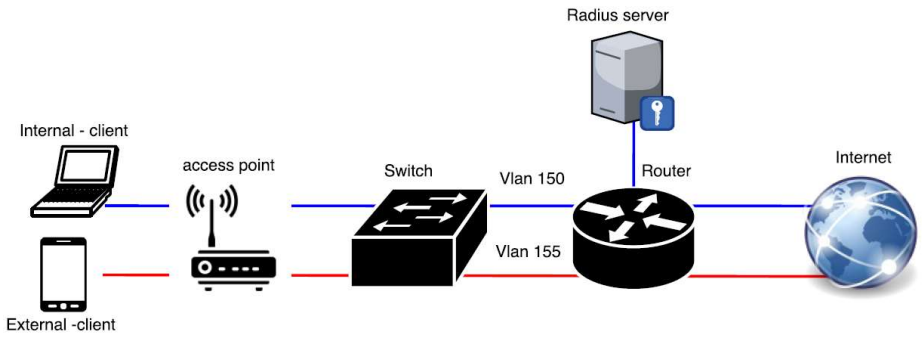
6.1 Rozdělení sítě

Bezdrátová síť je rozdělena na dvě skupiny. První skupina je pro mobilní zařízení a externí pracovníky. Druhá skupina je pro interní zařízení. Interní zařízení jsou ověřovaný přes Radius server, který ověří klienty pomocí doménového účtu. Síť je rozdělena na úrovni VLAN. VLAN-150 slouží interním zařízením a VLAN-155 slouží mobilním zařízením a zároveň externím zaměstnancům. Interní zařízení jsou k bezdrátové síti připojována automaticky, protože je na ně nastavení Wi-Fi aplikováno doménovou politikou.

Tabulka 5 – Nastavené zabezpečení.

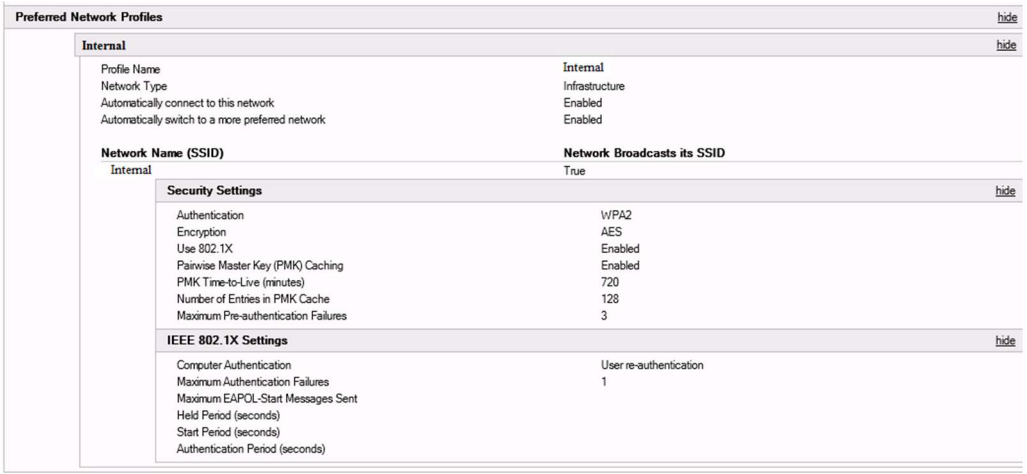
Skupiny	Šifrování	Typ ověřování	Skupinové Šifrovaní	Ověření
Interní	AES ccm	WPA PSK/WPA2 PSK	AES ccm	Radius
Externí	AES ccm	WPA EAP/WPA2 EAP		Heslem

Zdroj: vlastní



Obrázek 19 – Způsob připojení klientů do bezdrátové sítě.

Zdroj: vlastní



Obrázek 20 – Politika pro připojení interních zařízení.

Zdroj: vlastní

6.2 Nastavení sítě

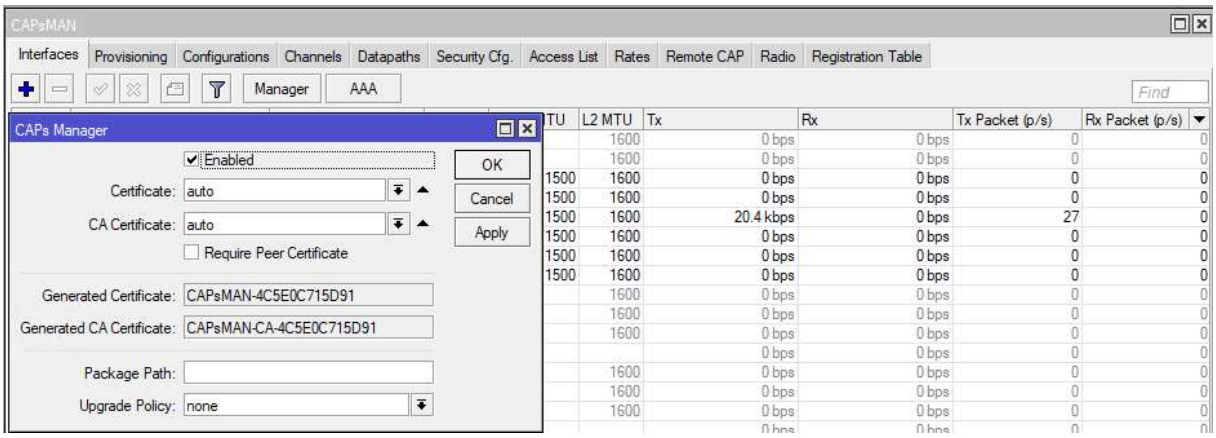
Nejdříve je potřeba provést základní konfiguraci každého zařízení a portu na přepínači (switch) do kterého je zařízení připojeno. Dalším krokem je spárovaní zařízení s hlavním zařízením AP15, z kterého je následně nastavena celá konfigurace bezdrátové sítě. Základní konfigurace zařízení je uvedena v příloze A. Konfiguraci CAPsMANa je možné provést i přes terminál viz příloha B.

Tabulka 6 – Rozvržení adresace zařízení

Identifikační název zařízení	IP adresa	Maska podsítě
AP15	192.168.30.155	255.255.255.0
AP14	192.168.30.154	255.255.255.0
AP13	192.168.30.153	255.255.255.0
AP12	192.168.30.152	255.255.255.0
AP11	192.168.30.151	255.255.255.0
AP10	192.168.30.150	255.255.255.0
Radius server	192.168.12.46	255.255.255.0
Active Directory	192.168.12.70	255.255.255.0

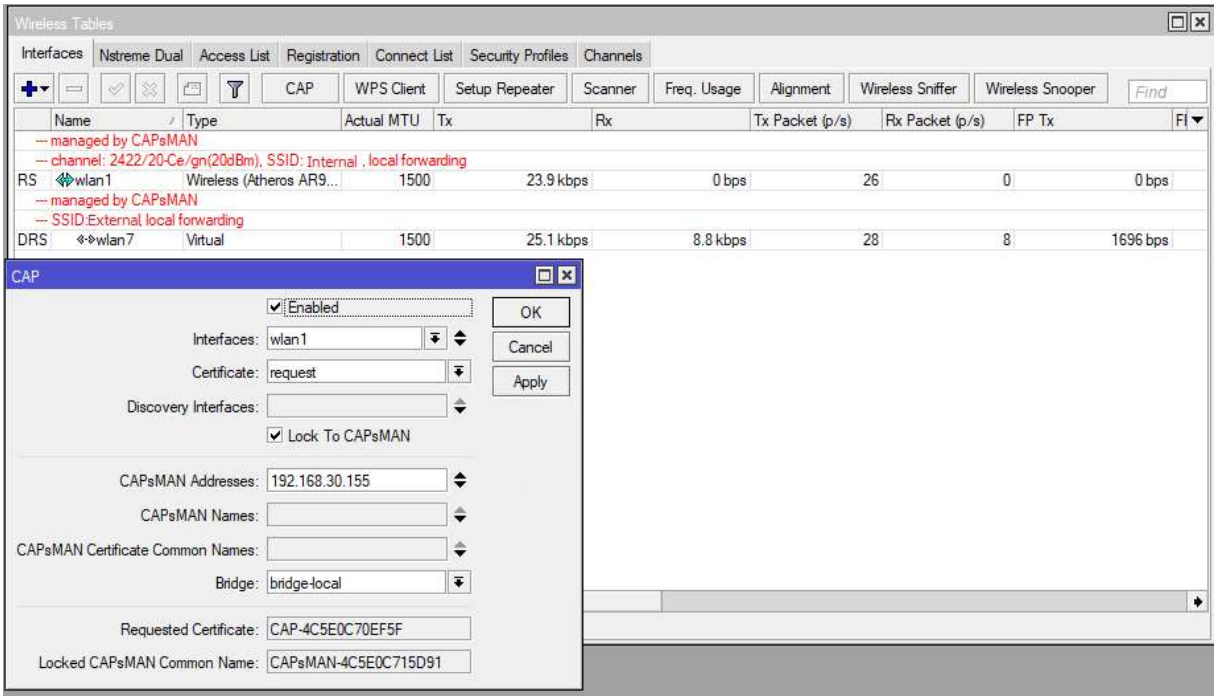
Zdroj: vlastní

1. Základní konfigurace zařízení:
   - Vypnutí výchozího DHCP serveru.
   - Nastavení identity zařízení (AP10, AP11, AP12, AP13, AP14 a AP15).
   - Natavení DNS.
   - Nastavení IP adresy a výchozí brány.
2. Konfigurace portu na přepínači switch.
3. Konfigurace modulu CAPsMAN.
   - Vygenerování certifikátu v modulu CAPsMAN viz Obrázek 21.
   - Na bezdrátovém rozhrání nastavit připojení k hlavnímu zařízení a po načtení certifikátu zaškrtnout uzamčení k hlavnímu zařízení viz Obrázek 22.
   - Nastavit zabezpečení, komunikační kanály, datovou cestu a konfiguraci Wi-Fi viz Obrázek 24 až 27.
   - Nastavení připojených zařízení v modulu CAPsMAN viz Obrázek 28.
4. Nastavení Radius serveru viz Obrázek 23.
5. Konfigurace Radius serveru.



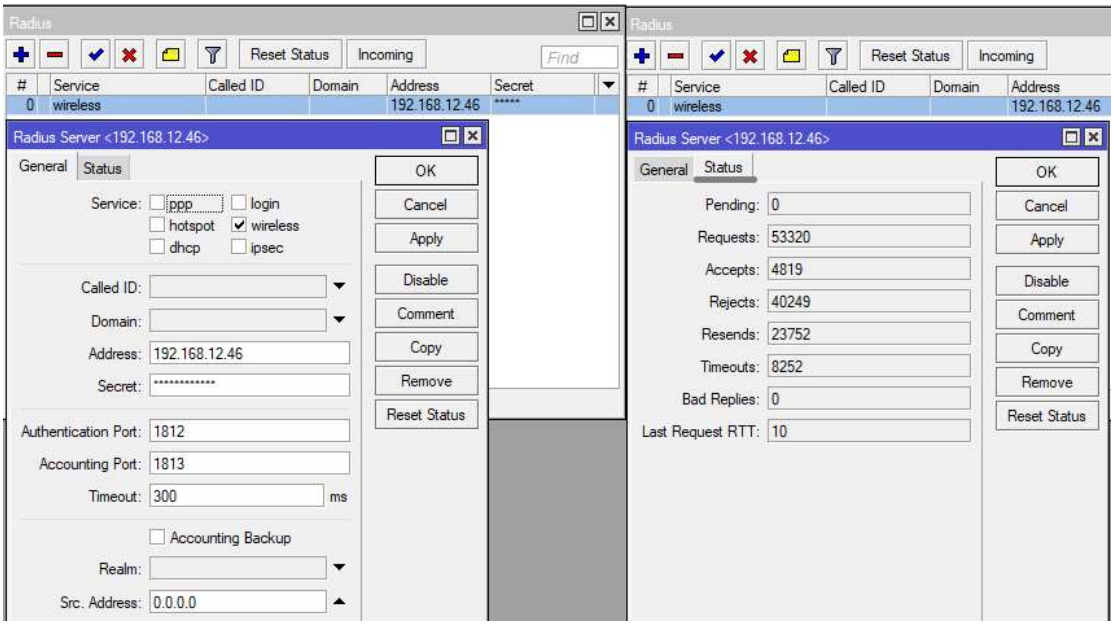
Obrázek 21 – Vygenerování certifikátu na AP15

Zdroj: vlastní



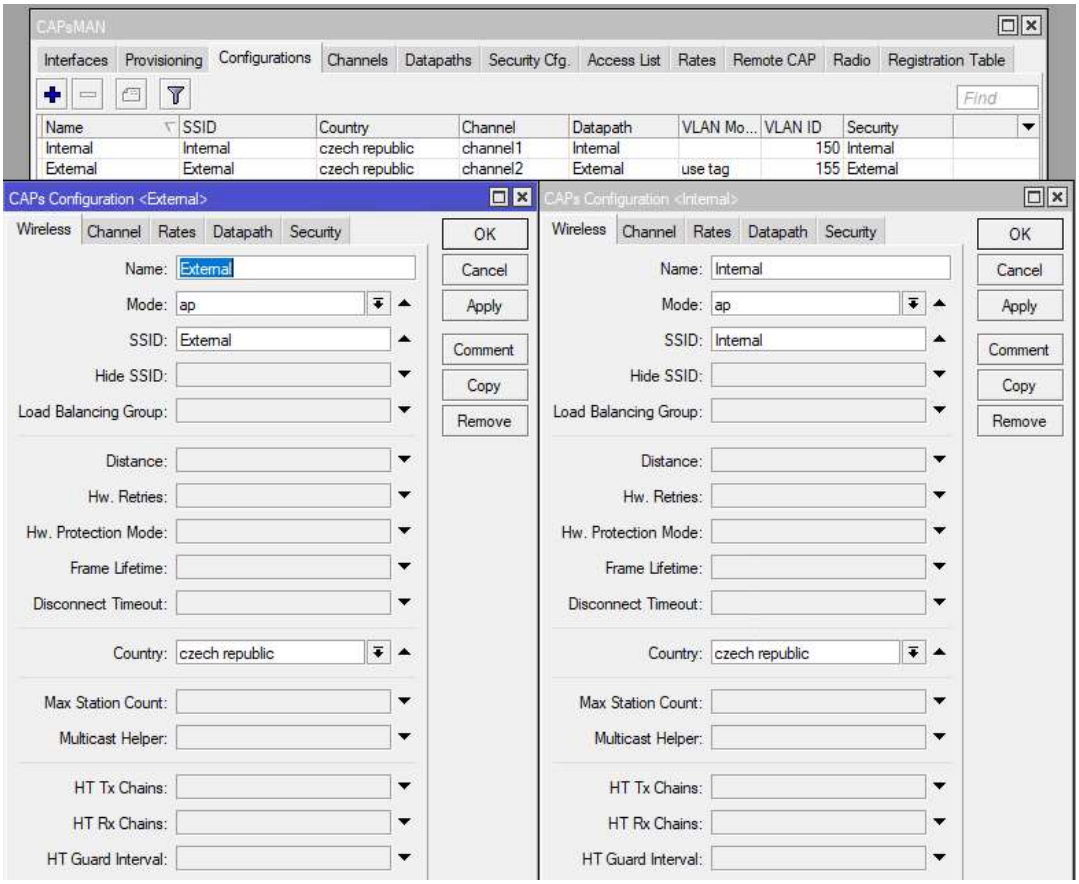
Obrázek 22 – Spárovaní zařízení a následné uzamčení k AP15

Zdroj: vlastní



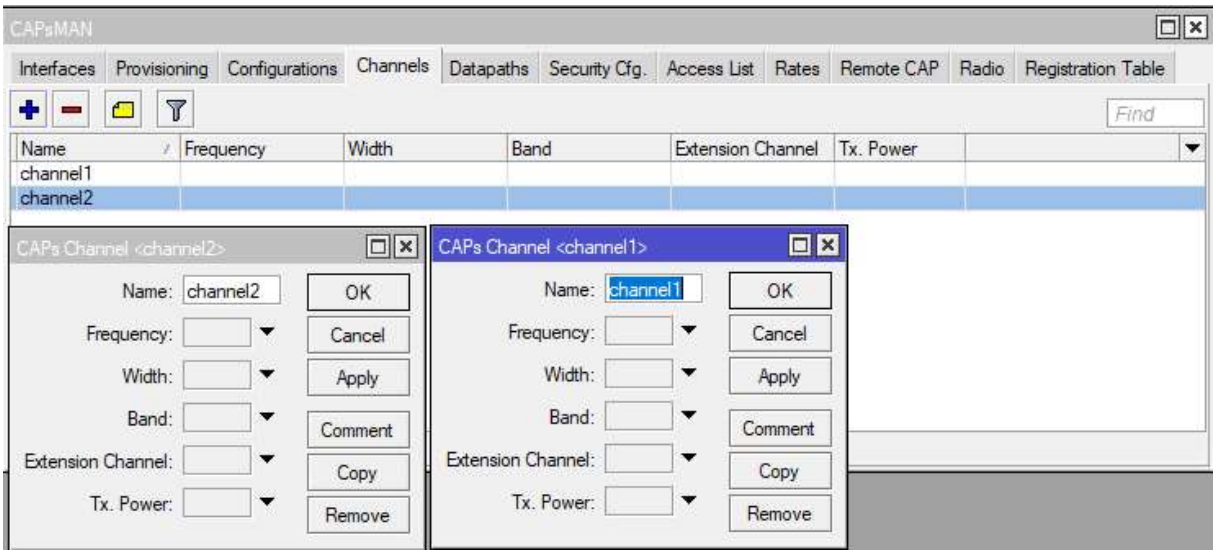
Obrázek 23 – Nastavení Radius serveru a ukázka statistiky na zařízení AP15

Zdroj: vlastní



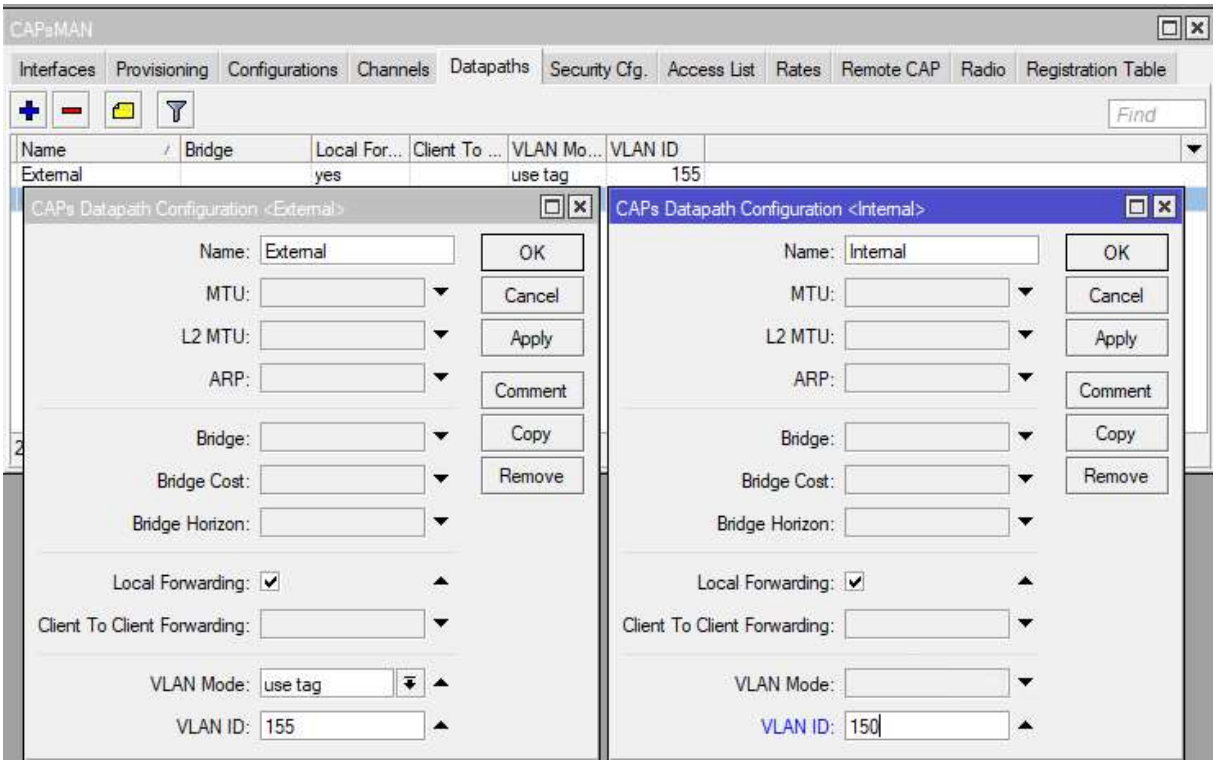
Obrázek 24 – Nastavení SSID Wi-Fi.

Zdroj: vlastní



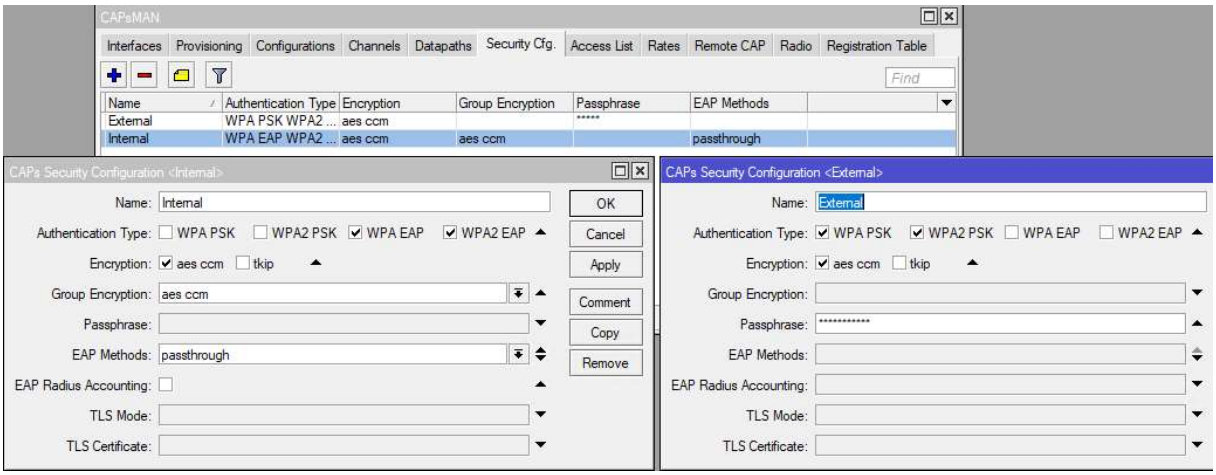
Obrázek 25 – Nastavení kanálu.

Zdroj: vlastní



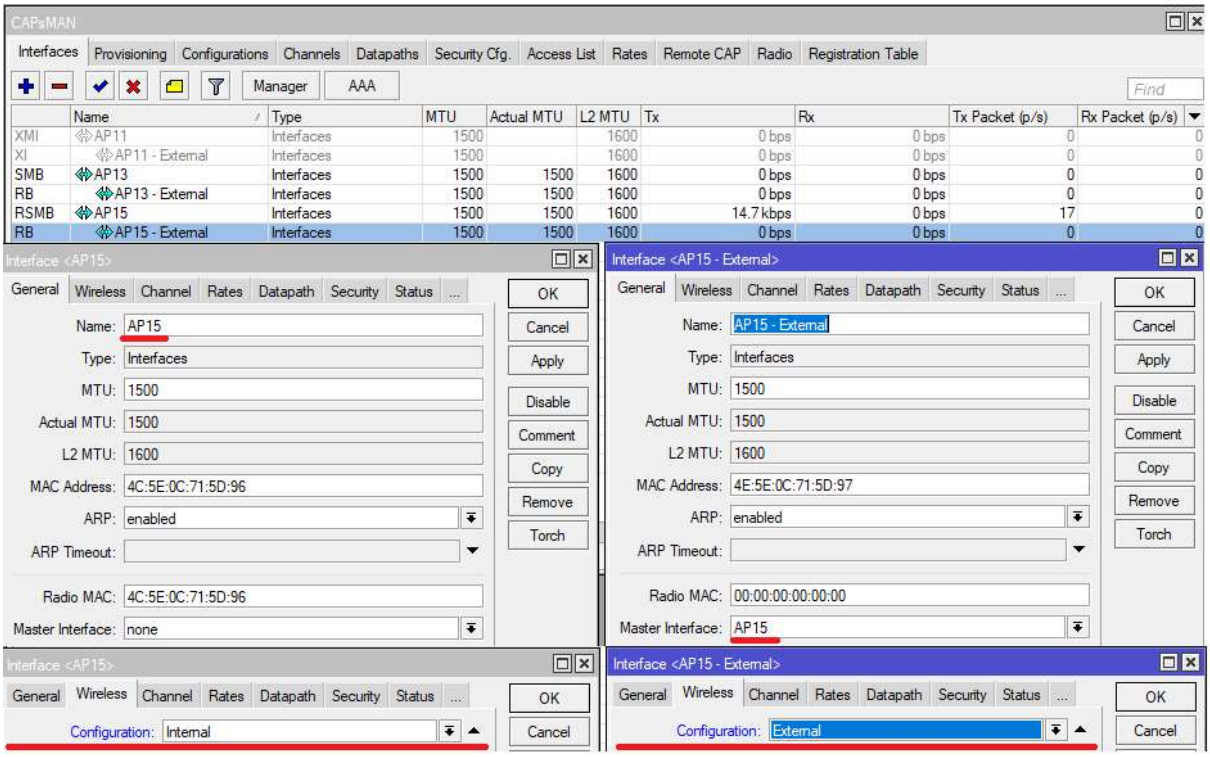
Obrázek 26 – Nastavení datových cest.

Zdroj: vlastní



Obrázek 27 – Nastavení zabezpečení.

Zdroj: vlastní



Obrázek 28 – Nastavení připojených zařízení.

Zdroj: vlastní

6.3 Nastavení Radius serveru

Radius server byl vybrán pro operační systém Linux s projektem FreeRadius, který patří mezi nejrozšířenější pro tyto distribuce. FreeRadius je jednoduchý na konfiguraci i na instalaci. Prvním krok bylo nainstalovat Linux server, který byl následně zaregistrován v doméně. Samba byla již nainstalována, a postup přenastavení je následovný:

1. Úprava souboru Samby: smb.conf viz Příloha C
2. Úprava souboru Kerberos: krb5.conf viz Příloha D
3. Úprava souboru nsswitch.conf viz Příloha E
4. Restart Linux serveru
5. Instalace FreeRadius společně s Openssl
    a. Stáhnout poslední verzi Openssl, rozbalit a nainstalovat pomocí příkazů:

```
tar –zxvf openssl-0.9.7f.tar

Nainstalovat do: /usr/local/openssl/
./config --prefix=/usr/local/openssl shared

make
make install
```

    b. Stáhnout poslední verzi FreeRadiusu a naistalovat pomocí příkazů:

```
make
make install
```

6. Úprava souboru ntlm_auth viz Příloha F
7. Úprava souboru clients.conf viz Příloha G
8. Úprava souboru mschap viz Příloha H
9. Úprava souboru eap.conf viz Příloha CH
10. Úprava souboru inner-tunnel viz Příloha I

Zdroj: zpracováno dle (RANDRIAMAMPIONONA,2016)

7 ZPRÁVY MEZI RADIUS SERVEREM A KLIENTY

Pro popis zpráv je nejdříve důležité zmapovat, jak vůbec odposlechnout zprávy zasílané mezi klientem a Radius serverem. Odposlech komunikace na Radius serveru nebyl zcela úspěšný. Na Radius serveru je totiž možné odposlechnout pouze komunikaci mezi přístupovým bodem a serverem nikoli celou komunikaci. Aby bylo možné popsat komunikaci mezi Radius serverem a klientem je zapotřebí zastavit ověřování klientů. Nastavit přesměrovaní vedené komunikaci do textového souboru a po připojení jednoho ze zařízení opět ověřovaní zapnout.

Přesměrování do textového souboru lze provést následovně:

```
root@lamp ~# /etc/init.d/freeradius stop
[ ok ] Stopping FreeRADIUS daemon: freeradius.

root@lamp ~# /usr/sbin/freeradius -X > /tmp/freeradius.txt

root@lamp ~# /etc/init.d/freeradius start
[ ok ] Starting FreeRADIUS daemon: freeradius.
```

Do textového souboru freeradius nebude přesměrována jen komunikace mezi klienty a Radius serverem, ale i celé nastavení Radius serveru s hesly, proto dejte pozor, kam bude soubor uložen. Ověření jednoho uživatele bude zabírat v souboru zhruba 600 řádků. Komunikaci je nutné nechal proběhnout celou, dokud nebude klient úspěšně ověřen a nebudou tím nasbíraný všechny potřebné informace. Informace získáte postupně jednotlivými zprávami mezi klientem a serverem (Access-Request a Access-Challenge) v případě, že by Radius server neobdržel všechny potřebné informace, skončí komunikace zprávou přístup odmítnut (Access-Reject).

Příklad úspěšného ověření klienta naleznete v příloze J, ve zprávě jsou zvýrazněny důležité informace. Přiložená zprava obsahuje potvrzení všech zpráv dříve vyměněných mezi serverem a klientem s potvrzením přístupu do interní sítě (Access-Accept).

7.1 Komunikace mezi Radius serverem a klienty

1. Supplican zašle žádost o přihlášení do sítě (EAPOL Start).
2. Bezdrátové zařízení odpoví zasláním požadavku o ověření klienta (EAP Request identity)
3. Supplican odpoví bezdrátovému zařízení zasláním informací o své totožnosti (EAP Response identity). Bezdrátové zařízení zprávu upraví do Radius protokolu a zašle na Radiu server (Radius Access-Request).

```
rad_recv: Access-Request packet from host
192.168.30.155 port 59499, id=12, length=190
```

4. Autentizační server zašle na bezdrátové zařízení výzvu pro změnu protokolu EAP na PEAP. Ve zprávě je také obsažena žádost o navázání TLS tunelu. (Radius Access-Challenge). Bezdrátové zařízení upraví zprávu z protokolu Radius do protokolu EAP a přepošle na klienta.

```
[eap] processing type peap
[peap] processing EAP-TLS
```

5. Pomocí ClientHello a ServerHello zpráv se server s klientem domluví na verzi TLS a na šifrovací, popřípadě kompresní metodě. Server následně zašle svůj certifikát a klíč. Klient zašle veřejný klíč a server odpoví zprávou ServerHelloDone, která signalizuje dohodu na použitých mechanizmech. Klient dále odešle informační zprávu pro server ChangeCipherSpec, která říká Radius serveru, že všechna následná data budou šifrována. Server mu stejnou zprávou se zašifrovaným obsahem Finished odpoví. Následná komunikace je šifrována.

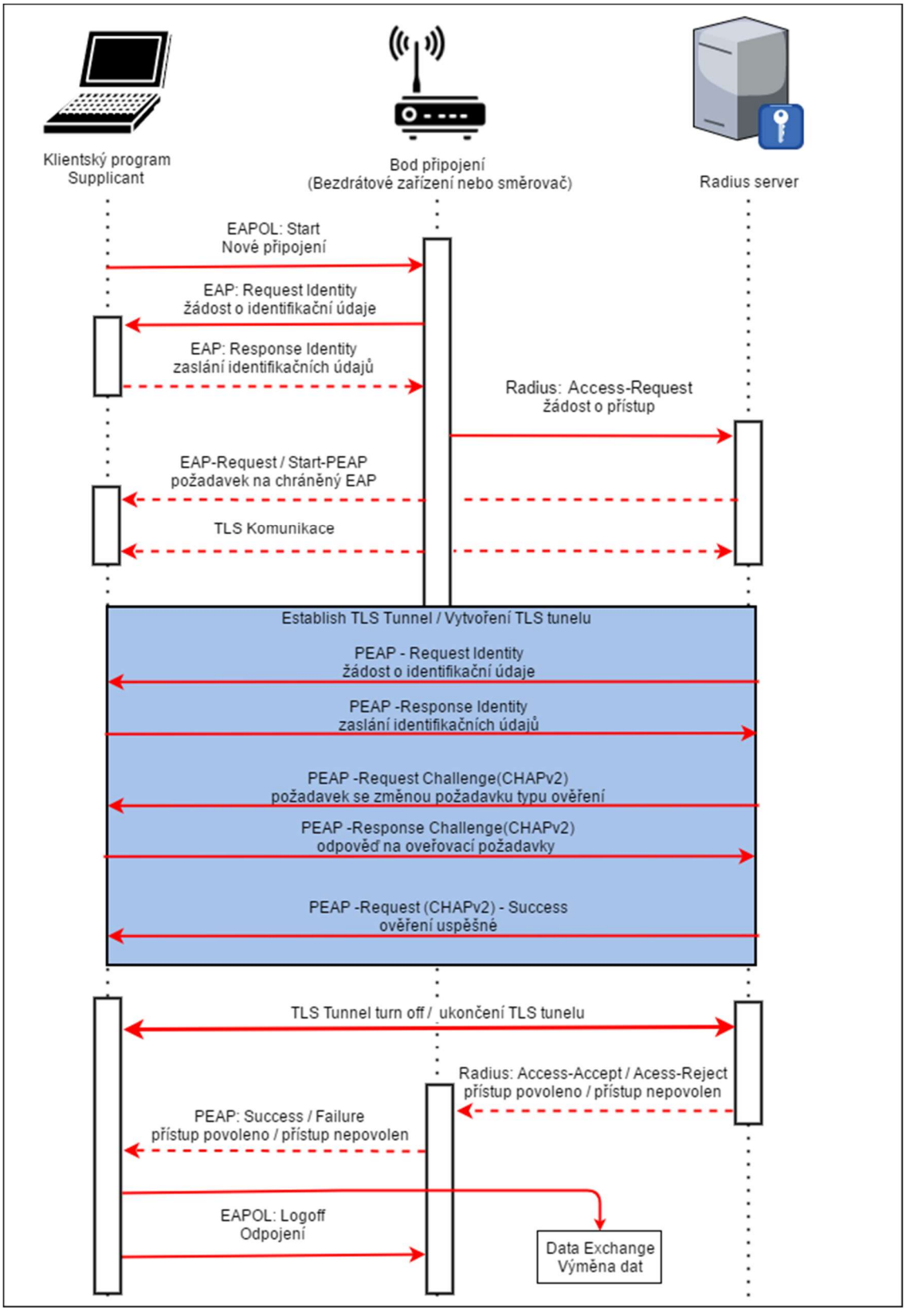
```
[peap] <<< TLS 1.0 Handshake [length 0099], ClientHello
[peap]     TLS_accept: SSLv3 read client hello A
[peap] >>> TLS 1.0 Handshake [length 0039], ServerHello
[peap]     TLS_accept: SSLv3 write server hello A
[peap] >>> TLS 1.0 Handshake [length 02c2], Certificate
[peap]     TLS_accept: SSLv3 write certificate A
[peap] >>> TLS 1.0 Handshake [length 014b], ServerKeyExchange
[peap]     TLS_accept: SSLv3 write key exchange A
[peap] >>> TLS 1.0 Handshake [length 0004], ServerHelloDone
[peap] <<< TLS 1.0 Handshake [length 0046], ClientKeyExchange
[peap]     TLS_accept: SSLv3 read client key exchange A
[peap]     TLS_accept: SSLv3 read certificate verify A
[peap] <<< TLS 1.0 ChangeCipherSpec [length 0001]
[peap] <<< TLS 1.0 Handshake [length 0010], Finished
[peap]     TLS_accept: SSLv3 read finished A
[peap] >>> TLS 1.0 ChangeCipherSpec [length 0001]
[peap]     TLS_accept: SSLv3 write change cipher spec A
[peap] >>> TLS 1.0 Handshake [length 0010], Finished
```

6. Radius Server si znovu s klientem vymění zprávy s ověřením identity v šifrovaném tunelu (PEAP Request identity a PEAP Response identity).
7. Autentizační server ještě zažádá o změnu ověření přes MS-CHAPv2(Radius Access-Challenge)

   Klient Radius serveru odpoví přihlašovacími údaji v požadovaném formátu. Pokud jsou údaje správné, TLS tunel bude uzavřen

8. Radius server zašle bezdrátovému zařízení zprávu o povolení přístupu (Radius Access-Accept). Bezdrátové zařízení přeloží zprávu z Radius protokolu do protokolu PEAP a povolí klientovy přístup do sítě.

```
Sending Access-Accept of id 18 to 192.168.30.173 port 59499
```



Obrázek 29 – Komunikace mezi Radius serverem a klienty.

Zdroj: vlastní

8 ZÁVĚR

Začátek práce se věnuje bezpečnosti sítě, bezpečnostním zásadám a základním ISO standardům. Dále práce vysvětluje AAA technologie s protokoly Radius a TACACS+. U protokolu Radius objasňuje typy zpráv, které Radius server používá pro komunikaci s bezdrátovými zařízeními. Následující kapitola je věnována zabezpečení bezdrátových sítí s popisem jednotlivých typů zabezpečení. V kapitole je také čtenář obeznámen s autentizačním protokolem EAP a typy šifrování komunikace. Dále se práce věnuje problematice zařízeních Mikrotik jejich nastavení a implementaci do firemního prostředí. Zvolená zařízení jsou podrobně charakterizována v následující kapitole. Práce se dále zabývá návrhem infrastruktury sítě. Věnuje se také podrobnému popisu zpráv mezi Radius serverem a klienty. Získaná komunikace mezi Radius Serverem a klienty je podrobně popsána a pro lepší představu bylo vytvořeno schéma síťové komunikace.

Cílem práce bylo navrhnout infrastrukturu sítě, která je rozdělena do dvou nezávislých bezdrátových sítí. První bezdrátová sít slouží interním zařízením mezi, které patří notebooky, monitorovací a zobrazovací stanice a také pracovní stanice, které nemají možnost připojení do ethernetu. Zařízení jsou ověřována pomocí uživatelských účtu přes Radius server. Tyto uživatelské účty jsou spravovány pomocí AD. Druhá bezdrátová síť sloužila pro připojení externích zaměstnanců a mobilních telefonů. Při připojení do této sítě získávali přístup pouze k internetu. Samotná sít byla bezpečně oddělena, aby nezasahovala do komunikace vnitřní sítě pomocí VLAN. Následně byla popsána komunikace mezi klienty a Radius serverem. Získané poznatky mohou čtenářovi pomoci s výstavbu nové firemní infrastruktury bezdrátové sítě nebo modernizaci stávající bezdrátové sítě. Získané teoretické a praktické zkušenosti jsem využil následně při implementaci bezdrátové sítě do firemního prostředí.

9 POUŽITÁ LITERATURA

BARRETO, Jose. What's new in SMB 3.1.1 in the Windows Server 2016 Technical Preview 2. Blogs.technet.microsoft.com [online]. 2015 [cit. 2017-04-29]. Dostupné z: https://blogs.technet.microsoft.com/josebda/2015/05/05/whats-new-in-smb-3-1-1-in-the-windows-server-2016-technical-preview-2/

EDUROAM. Eduroam v rámci české NREN. Eduroam.cz [online]. 2016 [cit. 2017-04-29]. Dostupné z: https://www.eduroam.cz/cs/spravce/uvod

FIEDLER, Petr a Zdeněk BRADÁČ. Zabezpečení bezdrátových sítí WiFi (IEEE 802.11b, g). Automa.cz [online]. 2004 [cit. 2017-04-29]. Dostupné z: http://automa.cz/cz/casopis-clanky/zabezpeceni-bezdratovych-siti-wifi-ieee-802-11b-g-2004_10_32563_1627/

HOLEČEK, Petr. Jak hacknout WiFi s WEP, aneb nepoužívejte WEP. *Www.ryu.cz* [online]. 2013 [cit. 2017-04-29]. Dostupné z: https://www.ryu.cz/bezpecnost/jak-hacknout-wifi-s-wep-aneb-nepouzivejte-wep/

IMB. Šifrovací šifry a režimy. Ibm.com [online]. 2013 [cit. 2017-04-29]. Dostupné z: https://www.ibm.com/support/knowledgecenter/cs/SSGU8G_12.1.0/com.ibm.sec.doc/ids_en_010.htm

MICROSOFT. Extensible Authentication Protocol (EAP). Tools.ietf.org [online]. 2004 [cit. 2017-04-29]. Dostupné z: https://tools.ietf.org/html/rfc3748

MIKROTIK k. Manual: CAPsMAN. Wiki.mikrotik.com [online]. 2017 [cit. 2017-04-26]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:CAPsMAN

MIKROTIK. Manual: Initial Configuration. Wiki.mikrotik.com [online]. 2011 [cit. 2017-04-26]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Initial_Configuration

MIKROTIK. Manual: Upgrading. Wiki.mikrotik.com [online]. 2017 [cit. 2017-04-26]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Upgrading

MIKROTIK. Mikrotik: About us. *Mikrotik.com* [online]. Latvian, 2016 [cit. 2017-04-26]. Dostupné z: https://mikrotik.com/aboutus

RANDRIAMAMPIONONA, José. Guide/FreeRADIUS Active Directory Integration HOWTO: Introduction. *Wiki.freeradius.org* [online]. 2016 [cit. 2017-04-27]. Dostupné z: http://wiki.freeradius.org/guide/freeradius-active-directory-integration-howto#introduction_mods-available-mschap

ROUTERBOARD. RB951G-2HnD. In: *Routerboard.com* [online].2016 [cit. 2017-04-27]. Dostupné z: https://img.routerboard.com/mimg/903_m.png

ROUTERBOARD. RBcAP-2n. In: *Routerboard.com* [online]. 2016 [cit. 2017-04-27]. Dostupné z: https://img.routerboard.com/mimg/997_hi_res.png

THOMAS, Thomas M. Zabezpečení počítačových sítí bez předchozích znalostí. Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0417-6.

TRAPANI, Gina. How to Crack a Wi-Fi Network's WEP Password with BackTrack. Lifehacker.com [online]. 2011 [cit. 2017-04-29]. Dostupné z: http://lifehacker.com/5305094/how-to-crack-a-wi-fi-networks-wep-password-with-backtrack

VANHOE, Mathy a Frank PIESSENS. RC4 NOMORE. Rc4nomore.com [online]. 2011 [cit. 2017-04-29]. Dostupné z: http://www.rc4nomore.com/

WILLENS, LIVINGSTON, RUBENS, MERIT a SIMPSON. Remote Authentication Dial In User Service (RADIUS). Freeradius.org [online]. 2000 [cit. 2017-04-29]. Dostupné z: https://freeradius.org/rfc/rfc2865.html

10 PŘÍLOHY

Příloha A – *Základní konfigurace zařízení AP15*

```
/ip address
add address=192.168.30.155/24 comment="default configuration"
interface=ether2-master-local network=192.168.30.0

/ip dns
set allow-remote-requests=yes servers=192.168.12.70

/ip firewall nat
add action=masquerade chain=srcnat comment="default configuration"
disabled=yes out-interface=ether1-slave-local to-addresses=0.0.0.0

/ip route
add check-gateway=ping distance=1 gateway=192.168.30.254
```

Příloha B – *Nastavení modulu CAPsMAN na zařízení AP15*

```
/caps-man channel
add name=channel1
add name=channel2

/caps-man datapath
add local-forwarding=yes name=External vlan-id=155 vlan-mode=use-tag
add local-forwarding=yes name=Internal vlan-id=150

/caps-man security
add authentication-types=wpa-psk,wpa2-psk encryption=aes-ccm
name=External passphrase=Heslo
add authentication-types=wpa-eap,wpa2-eap eap-methods=passthrough
encryption=aes-ccm group-encryption=aes-ccm name=Internal

/caps-man configuration
add channel=channel2 country="czech republic" datapath=External
datapath.vlan-id=155 datapath.vlan-mode=use-tag mode=ap name=External
security=External ssid=Externa
add channel=channel1 country="czech republic" datapath=Internal mode=ap
name=Internal security=Internal security.eap-radius-accounting=no ssid=
Internal
```

Příloha C – *Úpravy v konfiguračním souboru: smb.conf*

```
#======================= Global Settings =====================
[global]
## Browsing/Identification ###
# Change this to the workgroup/NT-domain name your Samba server will
part of
#   workgroup = WORKGROUP
   workgroup = skola-upce
# server string is the equivalent of the NT Description field
   server string = %h server
#======================= Share Definitions =====================
winbind use default domain = no
#winbind use default domain = yes
#password server = skola-upce.com
password server = dc1.skola-upce.com
realm = skola-upce.com
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
```

Příloha D – *Úpravy v konfiguračním souboru: krb5.conf*

```
[libdefaults]
      default_realm = SKOLA-UPCE.COM

# The following krb5.conf variables are only for MIT Kerberos.
      krb4_config = /etc/krb.conf
      krb4_realms = /etc/krb.realms
      kdc_timesync = 1
      ccache_type = 4
      forwardable = true
      proxiable = true

# The following libdefaults parameters are only for Heimdal Kerberos.
      v4_instance_resolve = false
      v4_name_convert = {
            host = {
                  rcmd = host
                  ftp = ftp
            }
            plain = {
                  something = something-else
            }
      }
      fcc-mit-ticketflags = true

[realms]
        SKOLA-UPCE.COM = {
        kdc = SKOLA-UPCE.COM
        }

[domain_realm]

[login]
      krb4_convert = true
      krb4_get_tickets = false
```

Příloha E – *Úpravy v konfiguračním souboru: nsswitch.conf*

```
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed,
try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat winbind
group:          compat winbind
shadow:         compat winbind

hosts:          files dns
networks:       files

protocols:      db files winbind
services:       db files winbind
ethers:         db files
rpc:            db files

netgroup:       nis
```

Příloha F – *Radius server úprava souboru: ntlm_auth*

```
exec ntlm_auth {
      wait = yes
#     program = "/path/to/ntlm_auth --request-nt-key --domain=MYDOMAIN
--username=%{mschap:User-Name} --password=%{User-Password}"
      program = "/usr/bin/ntlm_auth --request-nt-key --domain=skola-
upce.com --username=%{mschap:User-Name} --password=%{User-Password}"
}
```

Příloha G – *Radius server úprava souboru: Clients.conf*

```
client 192.168.30.155 {
      secret            = rad98574635rws
      shortname         = AP15
}
```

Příloha H – *Radius server úprava souboru: mschap*

```
mschap {
      with_ntdomain_hack = yes
      ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --
username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}} --
challenge=%{%{mschap:Challenge}:-00} --nt-response=%{%{mschap:NT-
Response}:-00}"
access_attr = "dialupAccess"
}
```

Příloha CH – *Radius server úprava souboru: eap.conf*

```
eap {
            default_eap_type = peap
            timer_expire     = 60
            ignore_unknown_eap_types = no
            max_sessions = 4096
            peap {
            default_eap_type = mschapv2
            copy_request_to_tunnel = no
            use_tunneled_reply = no
}
tls {
            random_file = /dev/urandom
}
```

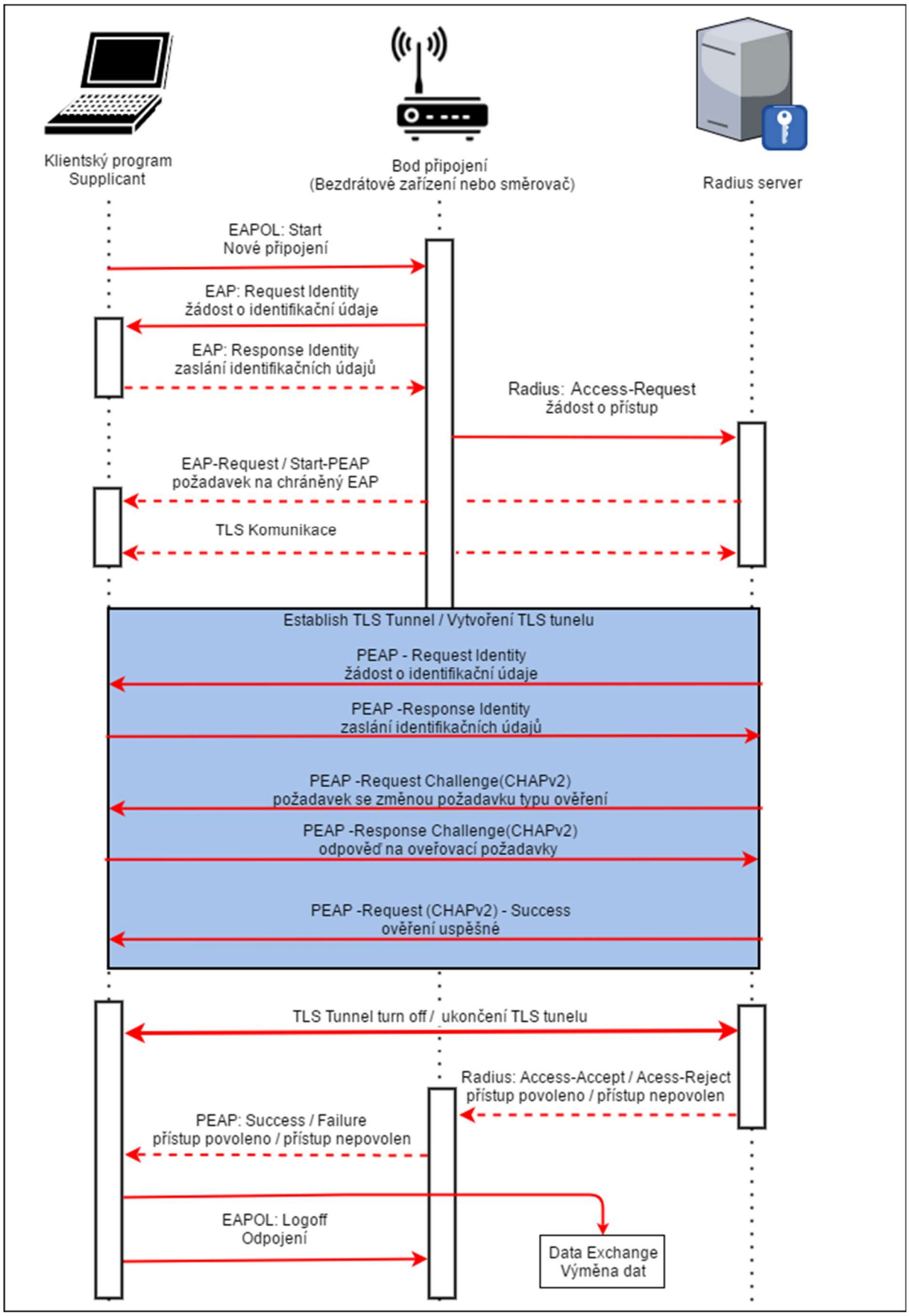
Příloha I – *Radius server úprava souboru: inner-tunnel*

```
authorize {
      chap
      mschap
      suffix
      update control {
      Proxy-To-Realm := LOCAL
      }
      eap {
            ok = return
      }
      #  Read the 'users' file
      files
      expiration
      logintime
      pap
}
```

Příloha J – *Poslední zpráva mezi klientem a Radius serverem*

```
rad_recv: Access-Request packet from host 192.168.30.155 port 59499,
id=18, length=227
      User-Name = "skola-upce\\kozeny"
      NAS-Identifier = "f09fc2331510"
      NAS-Port = 0
      Called-Station-Id = "F2-XX-C2-XX-15-10:Internal"
      Calling-Station-Id = "2C-56-DC-AB-C6-74"
      Framed-MTU = 1400
      NAS-Port-Type = Wireless-802.11
      Connect-Info = "CONNECT 0Mbps 802.11b"
      EAP-Message =0x02e6002b190017030100ea2e7c8f27622155cbad2
      State = 0x3275d5593cc4edc6f3faf534
      Message-Authenticator = 0xde0e82415e24bfe2798c886e
# Executing section authorize from file /etc/freeradius/sites-
enabled/default
+- entering group authorize {...}
++[preprocess] returns ok
++[chap] returns noop
++[mschap] returns noop
++[digest] returns noop
[suffix] No '@' in User-Name = "apag-elektronik\kozeny", looking up
realm NULL
[suffix] No such realm "NULL"
++[suffix] returns noop
[eap] EAP packet type response id 230 length 43
[eap] Continuing tunnel setup.
++[eap] returns ok
Found Auth-Type = EAP
# Executing group from file /etc/freeradius/sites-enabled/default
+- entering group authenticate {...}
[eap] Request found, released from the list
[eap] EAP/peap
[eap] processing type peap
[peap] processing EAP-TLS
[peap] eaptls_verify returned 7
[peap] Done initial handshake
[peap] eaptls_process returned 7
[peap] EAPTLS_OK
[peap] Session established.  Decoding tunneled attributes.
[peap] Peap state send tlv success
[peap] Received EAP-TLV response.
[peap] Success
[eap] Freeing handler
++[eap] returns ok
Login OK: [apag-elektronik\\kozeny] (from client AP15 port 0 cli 2C-56-
DC-AB-C6-74)
# Executing section post-auth from file /etc/freeradius/sites-
enabled/default
+- entering group post-auth {...}
++[exec] returns noop
Sending Access-Accept of id 18 to 192.168.30.155 port 59499
      MS-MPPE-Recv-Key = 0x309xxxxxxxxxxxxxxxxxxxxxxxxxxxx
      MS-MPPE-Send-Key = 0x36cxxxxxxxxxxxxxxxxxxxxxxxxxxx
      EAP-Message = 0x03e60004
      Message-Authenticator = 0x00000000000000000000000000000000
      User-Name = "apag-elektronik\\kozeny"
Finished request 29.
```

Příloha K – *Komunikace mezi Radius serverem a klienty*



Příloha L – *Přiložené CD*

Obsahující*:*

- Text práce (PDF),
- EAP protokol (JPG, PDF, XML),
- PEAP protokol (JPG, PDF, XML),
- NTLM protokol (JPG, PDF, XML),
- návrh infrastruktury (PNG),
- rozvržení sítě (PDF, XML),
- nastavení pravidla domény (PNG),
- nastaveni Mikrotik.