UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

# Problematika VLANs Controlleru

Tomáš Svoboda

Bakalářská práce
2013

**Univerzita Pardubice**
**Fakulta elektrotechniky a informatiky**
Akademický rok: **2012/2013**

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Tomáš Svoboda** |
| Osobní číslo: | **I11194** |
| Studijní program: | **B2646 Informační technologie** |
| Studijní obor: | **Informační technologie** |
| Název tématu: | **Problematika VLANs Controlleru** |
| Zadávající katedra: | **Katedra informačních technologií** |

Zásady pro vypracování:

Autor práce představí problematiku využití a konfigurace VLANs Controlleru v bezdrátových sítích. Autor představí základní přístupy k návrhu a realizaci bezdrátových sítí na principu Eduroam. Důraz bude kladen na funkce a využití VLANs controlleru. V praktické části se autor pokusí simulovat funkci bezdrátové sítě typu Eduroam s využitím VLANs controlleru v laboratorních podmínkách.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

**SMITH, Jeff. Controller-based wireless LAN fundamentals. Indianapolis, Ind.: Cisco Press, c2011, xvi, 294 p. ISBN 978-158-7058-257.**
**BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.**

Vedoucí bakalářské práce: **Mgr. Josef Horálek**
Katedra softwarových technologií

Datum zadání bakalářské práce: **21. prosince 2012**
Termín odevzdání bakalářské práce: **10. května 2013**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 29. března 2013

**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 8. 4. 2013 Tomáš Svoboda

**Poděkování**

Na tomto místě bych rád poděkoval Mgr. Josefu Horálkovi za cenné rady, které jsem využil při zpracování bakalářské práce a Ing. Soně Neradové za umožnění přístupu do síťových laboratoří. Dále bych rád poděkoval rodičům a všem, kteří mě během studia podporovali.

**Anotace**

Tato práce představuje problematiku využití a konfigurace VLANs Controlleru v bezdrátových sítích. Důraz je kladen na funkce a využití VLANs Controlleru. Další částí je navržení bezdrátové sítě na principu sítě Eduroam.

Vlastní návrh je realizován pomocí FreeRADIUS serveru, VLANs Controlleru a přístupových bodů od firmy Cisco.

**Klíčová slova**

autentizace, bezdrátové sítě, Eduroam, RADIUS server, FreeRADIUS, VLANs Controller

**Title**

VLANs Controller

**Annotation**

This thesis introduces the possibilities of using and configuration of VLANS Controller in wireless networks. The emphasis is on functions and use of VLANS Controller. Another part is to design wireless network on principle of Eduroam network.

Design itself is realized using the FreeRADIUS server, VLANs Controller and access points from the Cisco company.

**Keywords**

autentization, wireless networks, Eduroam, RADIUS server, FreeRADIUS, VLANs Controller

# Obsah

## Seznam zkratek

| | |
|---|---|
| AP | Access Point |
| CAPWAP | Control And Provisioning of Wireless Access Points |
| DHCP | Dynamic Host Configuration Protocol |
| EoIP | Ethernet over IP |
| LWAP | Lightweight Access Point |
| MAC | Media Access Control |
| MD5 | Message-Digest Algorithm |
| VLAN | Virtual LAN |
| RADIUS | Remote Authentication Dial In User Service |
| VoIP | Voice over Internet Protocol |
| VPN | Virtual Private Network |
| WLAN | Wireless LAN |
| WLC | Wireless LAN Controller |

## Seznam obrázků



## Seznam tabulek

# Úvod

Cílem práce je popsat využití a konfiguraci VLANs Controlleru v bezdrátových sítích. První část práce obsahuje úvod do VLAN sítí, bezpečnosti a obecný princip fungování VLANs Controlleru. Dále je popsán princip sítí typu Eduroam a možnosti využití VLANs Controlleru v sítích tohoto typu.

Druhá část práce se zabývá praktickým návrhem a realizací bezdrátové sítě s využitím VLANs Controlleru na principu sítě typu Eduroam. Síť je zabezpečena pomocí autentizace uživatelů na RADIUS serveru. Mezi uživatelem a RADIUS serverem je dále vytvořeno důvěryhodné spojení, kvůli vyšší bezpečnosti a zamezení neoprávněnému přístupu do sítě.

# 1 Funkce a využití VLANs Controlleru

VLANs Controllery jsou zařízení sloužící k centrálnímu řízení a správě bezdrátových sítí. Oproti síťové infrastruktuře, založené na správě každého přístupového bodu jako samostatné jednotky, přináší řadu výhod. Tato práce se zabývá VLANs Controllery firmy Cisco, které se označují jako Wireless LAN Controllers (WLC).

Mezi nejdůležitější aspekty pro použití centralizované správy patří používání jednotných bezpečnostních pravidel v rámci celé sítě, možnost regulace výkonu přístupových bodů, provádění konfiguračních změn z jednoho místa v síti a zajištění roamingu pro uživatele. Tyto možnosti jsou detailněji popsány v následujících kapitolách.

Použití WLC však nepřináší pouze výhody. Zásadní nevýhodou jeho použití je fakt, že se stává se kritickým místem celé sítě. V případě výpadku WLC by se síť stala nepoužitelnou. Je proto vhodné nepoužívat pouze jediný, ale několik WLC. Pokud dojde k výpadku jednoho WLC, zbývající slouží jako záložní. Dalším důležitým faktorem pro nasazení více WLC je omezený počet AP, které může WLC obsloužit.

## 1.1 VLAN sítě

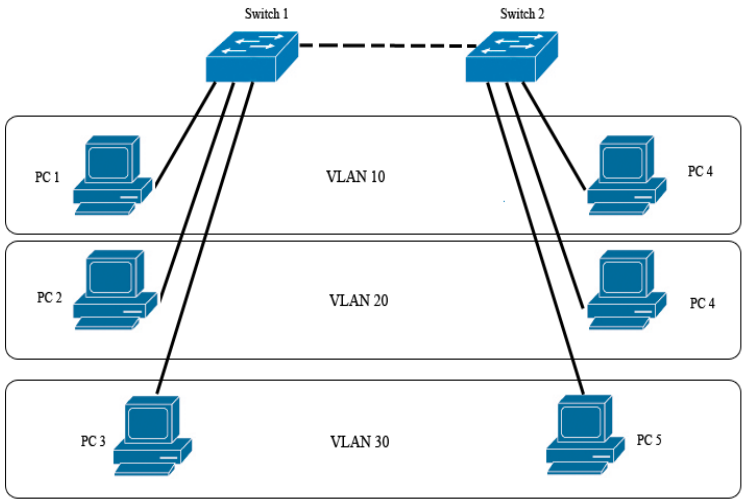
V současné době, při budování stále rozsáhlejších počítačových sítí, je kladen velký důraz na efektivní využití výkonu celé sítě. U malých sítí toto nepředstavuje, vzhledem k menšímu počtu připojených uživatelských stanic a náročnosti na správu, zásadní problém.

Při výstavbě sítě většího rozsahu, případně rozšířením stávající sítě o další pracovní stanice nebo aktivní prvky (switche, routery) může dojít k neefektivnímu využívání výkonu sítě. Na vině je především špatný návrh sítě. Zejména snižování skutečné přenosové rychlosti představuje problém, protože se zvyšujícím se počtem pracovních stanic dochází k rozšiřování broadcastové domény a posílání velkého množství broadcastových informací. Velké množství broadcastových informací snižuje efektivitu celé LAN, protože informace jsou posílány i stanicím, které je nepotřebují [20].

Dalším problémem je využívání síťových prostředků. Příkladem může být síť ve firmě, která má několik oddělení. Každé oddělení může využívat jiné síťové prostředky, které ale zároveň nemusí nebo nesmí být využívány stanicemi v rámci jiného oddělení. Ve firmě je umístěn tiskový server, ke kterému mají mít přístup zaměstnanci z finančního oddělení, ale pro ostatní oddělení je nedostupný. Pro povolení, či zamítnutí přístupu k serveru, musí správce sítě provést konfigurační úpravy na každé uživatelské stanici. Stanice se tak stává závislou na svém fyzickém umístění. Pokud se její umístění změní (stanice se přesune z jednoho oddělení do druhého), je nutné změnit její konfiguraci pro správné fungování v rámci oddělení, protože jiné oddělení může využívat jiné síťové prostředky.

Výše uvedené problémy řeší sítě typu VLAN. VLAN jsou nezávislé, logické sítě v rámci jednoho nebo více fyzických zařízení, pracujících na druhé vrstvě ISO-OSI modelu (switch). V rámci jednoho switche je možné dosáhnout stejného efektu, jako v případě

použití jednoho switche pro jednu síť a druhého pro druhou síť. Pomocí VLAN lze logicky segmentovat síť na základě vybraných parametrů, jako je například organizační struktura podniku, pobočky podniku, případně podle jiných zvolených kritérií. Každá VLAN zároveň představuje jednu broadcastovou doménu. Tím dochází k redukci zatížení sítě posíláním broadcastových informací, které jsou posílány pouze v rámci VLAN. Stanice jsou nezávislé na svém fyzickém umístění v síti.




**Obrázek 1 – VLAN sítě**

S VLAN sítěmi se zachází stejně, jako se sítěmi typu LAN. Každá VLAN je jednoznačně identifikována pomocí čísla, většinou označovaného jako VLAN ID. Standardní rozsah VLAN ID je od 1 do 1005, přičemž 1002 až 1005 jsou určeny pro Token Ring a FDDI VLAN. Volitelně lze VLAN přidělit jméno, především pro lepší orientaci. VLAN se dělí na pět základních typů:

- datová,
- hlasová,
- defaultní,
- řídící,
- a nativní.

Datová VLAN je určená pro přenos uživatelských dat mezi stanicemi. Nepřenáší žádná data určená pro správu sítě.

Hlasová VLAN je využívána především při nasazení IP telefonie. Umístěním provozu do samostatné VLAN je zajištěna dostatečná šířka pásma a tím i kvalita přenášených hovorů.

Defaultní VLAN je součástí každého switche, který podporuje VLAN. Nelze ji vypnout ani vymazat. Switche firmy Cisco používají jako defaultní VLAN 1. Do této VLAN jsou po zapnutí přiřazeny všechny porty switche.

Řídící VLAN je jakákoliv VLAN, která má přiřazenu IP adresu a masku sítě. Pomocí této VLAN lze konfigurovat switch. Řídící VLAN se stává po zapnutí switche VLAN 1. Toto řešení je z důvodu bezpečnosti nevyhovující, protože umožňuje neautorizovaný přístup ke switchi. Pro zvýšení bezpečnosti je vhodné vytvořit samostatnou řídící VLAN. Do nativní VLAN je zařazována všechna komunikace z trunk portů, které jsou detailněji popsány v kapitole 1.1.2. Rámce, které nenesou žádné označení, jsou také umístěny do nativní VLAN [27].

Pro zvýšení bezpečnosti a přehlednosti je nutné používat pro každou VLAN jiný subnet IP adres, stejně jako v případě klasických LAN sítí.

### 1.1.1 Zařazení komunikace do VLAN

Porty, které se využívají pro komunikaci ve VLAN se označují jako přístupové porty (access porty). Pro komunikaci v rámci VLAN sítě musí být porty zařazeny do příslušné VLAN.

Pro zařazení portů do VLAN se používají následující metody zařazení:

- podle portu,
- podle protokolu nebo adresy podsítě,
- a podle MAC adresy.

Při zařazení podle portu je port switche ručně nakonfigurován do příslušné VLAN. Zařízení připojené k tomuto portu je automaticky přidáno do dané VLAN. Jedná se o nejpracnější, ale široce používané řešení. Jednou z nevýhod tohoto řešení je případná rekonfigurace portu, v případě zařazení stanice do jiné VLAN. Vytvoření VLAN s přiřazením portu může vypadat následujícím způsobem:

```
S1>enable
S1#conf t
S1(config)#vlan 10
S1(config-vlan)#name Studenti
S1(config-vlan)#exit
S1(config)#interface fastEthernet 0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#no shutdown
```

Zařazení podle protokolu využívá informací síťové vrstvy. Stanice lze do VLAN zařazovat podle typu síťového protokolu a případně podle IP adresy podsítě. Zjišťování informací ze třetí vrstvy se stává zároveň velkou nevýhodou, protože k získání těchto informací potřebuje switch určitý čas. Tím dochází ke zpomalování předávání rámců mezi switchi. V porovnání se zařazením podle portu ale přináší velkou výhodu. Není nutná rekonfigurace portu v případě, že se stanice změní své umístění.

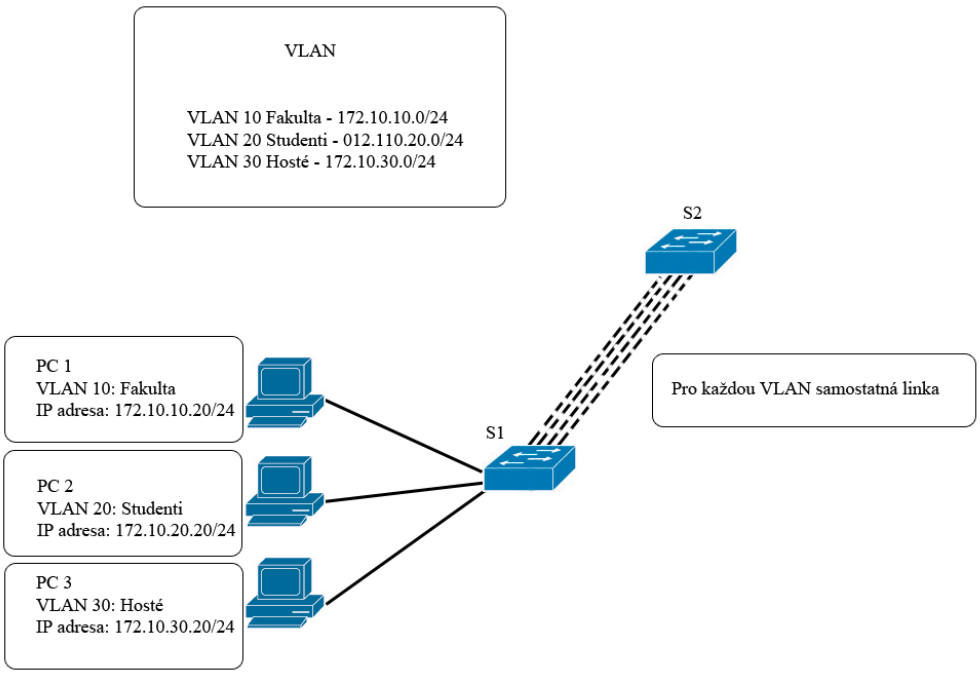
Při zařazování podle MAC adresy si každý switch udržuje v paměti tabulku MAC adres připojených zařízení zároveň s informací, do které VLAN dané zařízení patří. Zásadní

výhodou je možnost připojování zařízení do libovolného portu switche, který zajistí automatické zařazení do požadované VLAN. Pro rozsáhlé sítě není toto řešení vhodné z důvodu manuálního nastavení tabulky MAC adres s příslušnými VLAN [16].

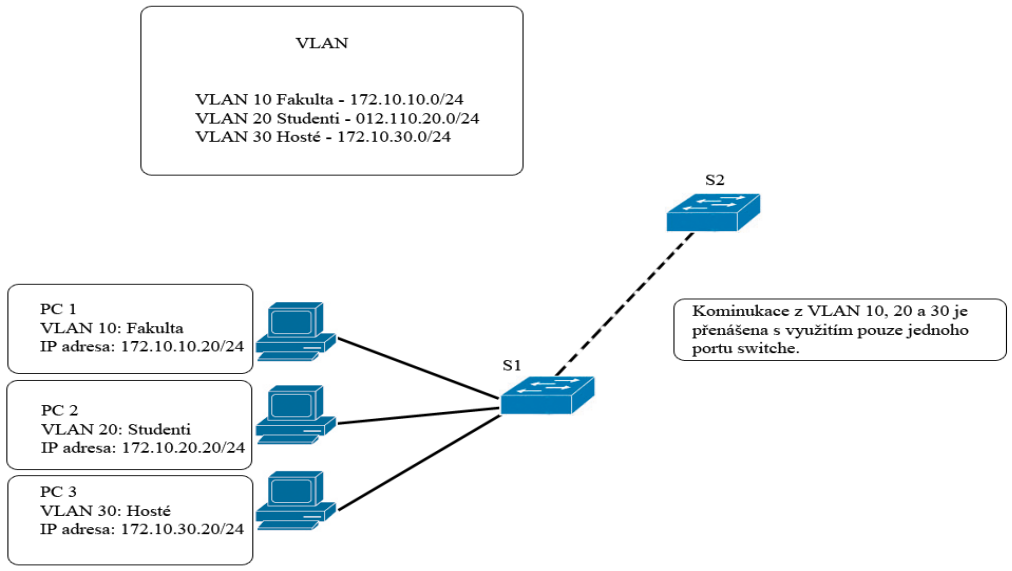
### 1.1.2 VLAN trunk

V počítačových sítích nebývá VLAN součástí pouze jednoho switche, ale celé sítě. Protože se VLAN chová jako nezávislá síť, je při propojení switchů zapotřebí pro každou VLAN samostatná linka, jak je patrné z Obrázek 2 obrázku. Vzhledem k omezenému počtu portů, kterými switche disponují, je při použití velkého množství VLAN sítí tato varianta nepřijatelná.

Řešení spočívá v propojení switchů pomocí jedné linky, jejíž porty jsou nastaveny v trunk režimu. Nastavení portu do režimu trunk je zapotřebí provést na všech zařízeních, které jsou pomocí trunku propojeny. Trunk porty podporují nativní VLAN. Tím získáváme velkou výhodu v podobě kompatibility s LAN sítěmi. V LAN sítích nedochází k označování rámců. Všechny rámce, které přichází z LAN sítě, jsou umístěny do nativní VLAN.




**Obrázek 2 – VLAN bez použití trunku**

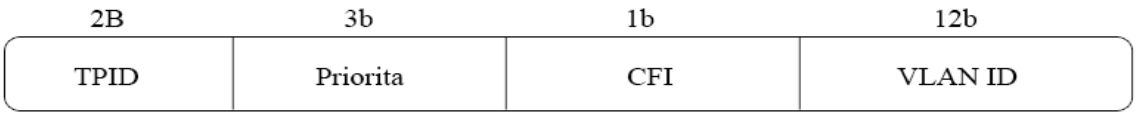



**Obrázek 3 – VLAN s použitím trunku**

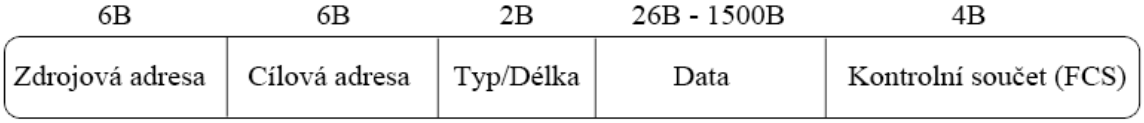
### 1.1.3 Označování rámců – 802.1q

Použitím trunk spojů nedochází ke zbytečnému plýtvání volnými porty. Vzhledem k tomu, že data z více VLAN jsou přenášena pouze po jediném fyzickém spoji, je pro zajištění správné komunikace třeba rozlišit, která data přísluší které VLAN. K tomu se využívá protokol 802.1q, který zajišťuje označování rámců.

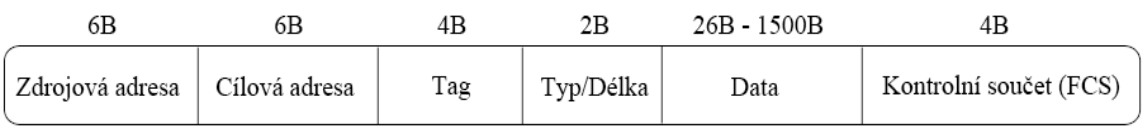
802.1q rozšiřuje originální rámec o 4B tag. První 2B nesou informaci o tom, že se jedná o 802.1q protokol. Dále je obsažena priorita rámce, CFI definuje přenos bitů a VLAN ID jednoznačně identifikuje číslo VLAN, které je rámec určen. Přidáním tagu do původního rámce dochází k jeho změně, proto je nutné přepočítat i kontrolní součet [2],[9].




**Obrázek 4 – Formát 802.1q tagu**

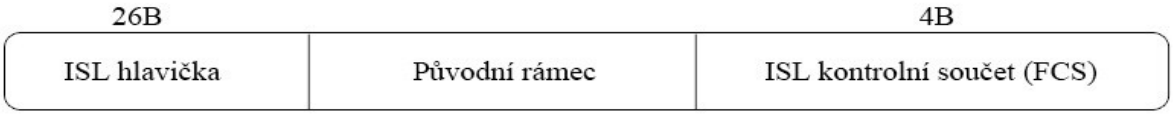



**Obrázek 5 – Originální Ethernetový rámec**




**Obrázek 6 – Rámec označený pomocí 802.1q**

Protokol 802.1q není jediným používaným řešením pro označování rámců. Před jeho standardizací byl používán protokol ISL, který je Cisco proprietární. Funguje tedy pouze na zařízeních od této firmy.



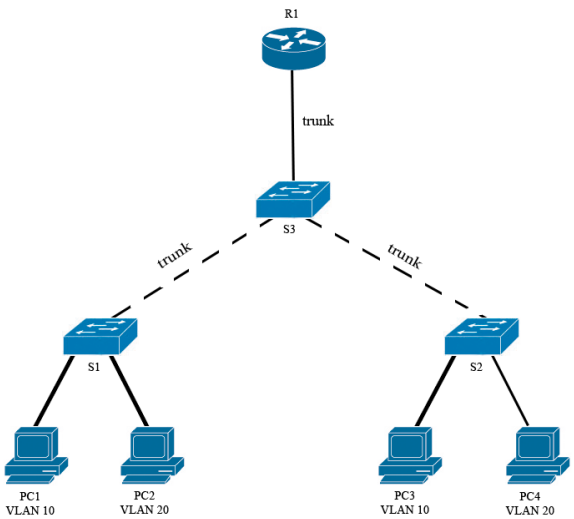

**Obrázek 7 – Formát ISL rámce**

Původní rámec je zapouzdřen do ISL rámce, pomocí přidání ISL hlavičky a kontrolního součtu. VLAN ID je obsaženo v ISL hlavičce spolu s mnoha dalšími informacemi jako je cílová adresa rámce, typ rámce a další. Zásadní nevýhodou je nárůst velikosti rámce o 30B. Dnes se tento protokol používá v minimálním rozsahu.

### 1.1.4 Komunikace mezi VLAN

Ke komunikaci v rámci VLAN plně dostačují switche, protože se VLAN chová jako oddělená a nezávislá síť. Nicméně v praxi spolu uživatelé musí komunikovat v rámci celé sítě, napříč jednotlivými VLAN. K tomu je zapotřebí zařízení, které funguje jako router. Nejčastěji se využívá právě router. Lze využít i switche, které podporují směrování na třetí vrstvě ISO-OSI modelu. Tyto switche se označují jako L3 switche.

Routery samozřejmě disponují velmi malým množstvím portů, což vede ke vzniku stejného problému jako u switchů, v případě použití jednoho portu pro jednu VLAN síť. Řešení se opět nabízí s použitím trunk spoje a vedení komunikace pouze jednou fyzickou linkou. Rozhraní, které router využívá pro komunikaci je logicky děleno na podrozhraní, jejichž počet je stejný jako počet VLAN sítí. Cisco routery využívají pro rozlišování komunikace, stejně jako switche, protokol 802.1q.




**Obrázek 8 – Topologie sítě s využitím routování mezi VLAN**

Pro komunikaci mezi VLAN stačí pouze použít jednotlivá podrozhraní na routeru. Následně určit, jaký typ se používá pro označování rámců a nastavit IP adresu, která se stává výchozí bránou pro stanice v dané VLAN. Po zapnutí rozhraní dojde automaticky k zapnutí všech podrozhraní. Následující příklad ilustruje konfiguraci routování mezi VLAN sítěmi [5].

```
R1>enable
R1#conf t
R1(config)#interface fastEthernet 0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)# ip address 172.16.10.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface fastEthernet 0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)# ip address 172.16.20.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface fastEthernet 0/0
R1(config-if)#no shutdown
```

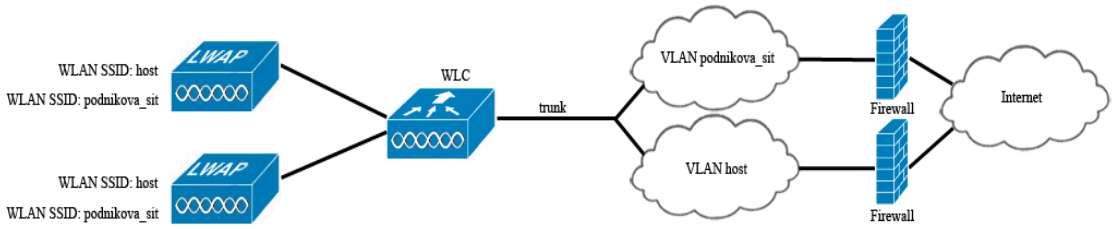
## 1.2 Správa VLAN pomocí WLC

Princip VLAN sítí popsaný v předchozí kapitole představuje efektivní způsob pro návrh a údržbu sítě typu LAN v pevných sítích. Dnes se vedle klasických pevných sítí používají také bezdrátové sítě, ve kterých jsou, při použití centralizované správy, VLAN sítě stejně efektivně spravovány pomocí WLC.

Součástí každého WLC jsou statická a dynamická rozhraní. Všechna rozhraní musí být zařazena do nějaké VLAN a mít přiřazenu IP adresu. Ve výchozím stavu, pokud nejsou použity VLAN, jsou všechny rozhraní zařazeny do VLAN 0. Je tedy používán stejný postup jako v případě konfigurace VLAN na klasickém switchi, pouze s jiným VLAN ID.

Dynamická rozhraní umožňují směrování různých bezdrátových sítí do různých VLAN. Pro každou VLAN je vytvořena nezávislá bezdrátová síť s unikátním SSID. Provoz z bezdrátové sítě je pak směrován do příslušné VLANy.

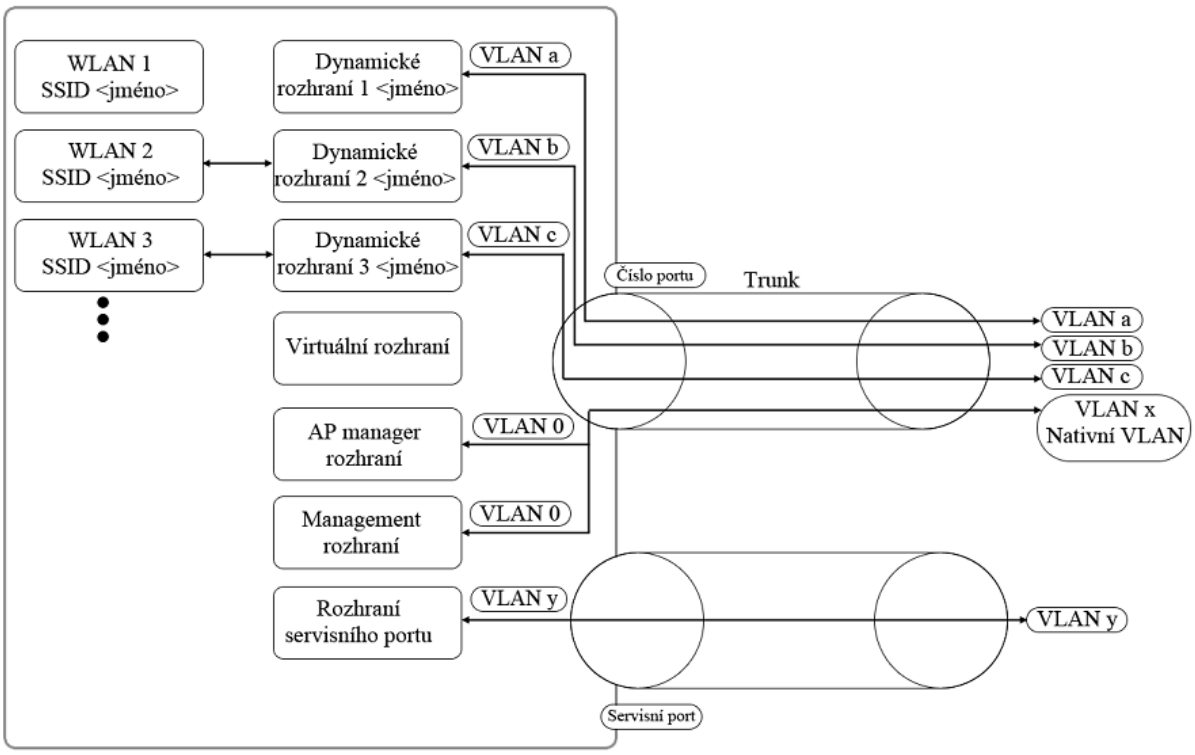
Tento přístup uplatňují zejména firmy a instituce, které chtějí neoprávněným osobám zabránit v přístupu do vnitropodnikové sítě, ale zároveň jim umožnit například přístup k internetu. Pro tuto potřebu stačí vytvořit VLAN síť, nezávislou na podnikové síti, která má přístup do internetu a připojit ji k WLC. Dále vytvořit bezdrátovou síť s příslušným SSID a nastavit její směrování do příslušné VLAN [3].




**Obrázek 9 – Oddělené WLAN sítě**

Konfigurace dynamických rozhraní je plně v režii správce sítě. V počátečním stavu není nakonfigurováno žádné dynamické rozhraní. Dynamická rozhraní tedy nelze použít pro management WLC a správu přístupových bodů. Z tohoto důvodu na WLC existují dvě pevná statická rozhraní. AP-manager a management.

Rozhraní AP-manager slouží pro komunikaci WLC s přístupovými body. Pro konfiguraci WLC je určeno management rozhraní. Obě rozhraní jsou ve výchozím stavu ve stejné VLAN a musí mít tedy nastavenu IP adresy ze stejného subnetu. Nastavení IP adresy na management rozhraní přináší pro správce sítě obrovskou výhodu v možnosti následné konfigurace WLC s použitím webového rozhraní, které je přehlednější, než konfigurace v příkazové řádce. K WLC se dále lze připojit pomocí Telnetu, SSH, případně pomocí servisního portu.




**Obrázek 10 – Architektura WLC**

## 1.3 Přístupové body bezdrátové sítě

Bezdrátové sítě, které nepoužívají centralizované řešení, využívají autonomní AP. Autonomní AP poskytují všechny služby nutné pro fungování sítě. Při použití centralizovaného řešení není jejich nasazení vhodné, protože celá síť je řízena z WLC.

WLC nepracují s klasickými autonomními AP, ale s AP, které firma Cisco označuje LWAP. LWAP jsou upraveny pro používání v centralizovaném řešení. Jejich operační systém je nahrazen speciální verzí, upravenou pro komunikaci s WLC. LWAP se stává pouze prostředníkem mezi připojovanými klienty a WLC [10].

LWAP má odpovědnost především za ukládání paketů do vyrovnávací paměti, jejich přeposílání a informování WLC o žádostech klientů, kteří se chtějí k dané síti připojit. Konfigurace firmware, řízení bezpečnosti a distribuční služby jsou řízeny z WLC.

Důležitou vlastností LWAP je možnost řízení jejich výkonu. WLC může efektivně regulovat výkon jednotlivých LWAP a tím zajistit hladké fungování celé sítě.

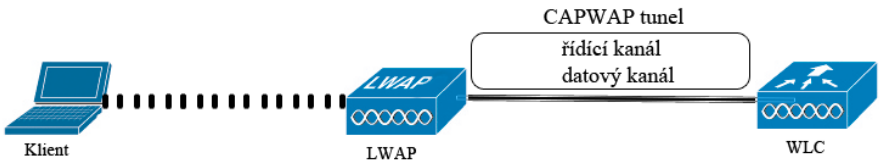
## 1.4 Protokol CAPWAP

Komunikace mezi LWAP a WLC je zajištěna protokolem CAPWAP. CAPWAP protokol byl standardizován organizací IETF. Je definován v RFC 5415 a vychází z protokolu LWAPP. Dle [4] jsou součástí protokolu dva kanály, řídící a datový.

Řídícím kanálem komunikuje WLC s LWAP a je využíván při navázání spojení mezi LWAP a WLC. Řídící kanál je z důvodu bezpečnosti zašifrován pomocí protokolu DTLS, který vychází z protokolu TLS. DTLS zabezpečuje spojení pomocí handshakingu, který jako bezpečnostní mechanismus využívá certifikáty, případně PSK (předsdílená fráze) [24].

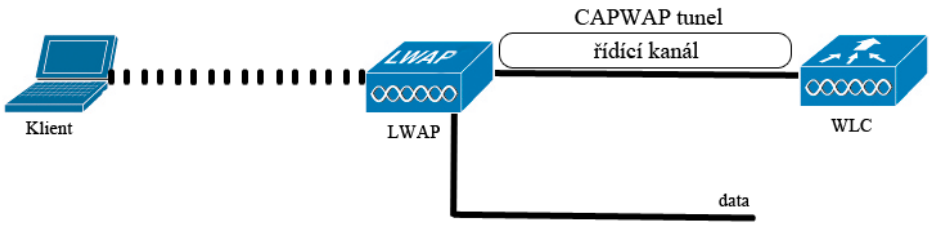
### 1.4.1 Řízení přístupu k médiu

Jednou z klíčových vlastností CAPWAP protokolu jsou politiky řízení přístupu k médiu. Politiky split MAC a local MAC definují, které funkce jsou zachovány na LWAP a které zajišťuje WLC. WLC používá defaultně politiku split MAC. Všechna data a řídící zprávy jsou zapouzdřovány pomocí CAPWAP protokolu a prochází přes WLC dále do sítě. Data určená pro připojené klienty jsou na WLC zapouzdřena a posílána klientům přes LWAP [25].




**Obrázek 11 – Split MAC politika**

U politiky local MAC je část prostředků pro řízení vrácena zpět LWAP. Přenos dat se výrazně liší od politiky split MAC. Data mohou být mezi LWAP a WLC přenášena CAPWAP tunelem jako rámce 802.3. Tato možnost však není na zařízeních firmy Cisco podporována. Další možností je odesílání dat dále do sítě přímo z LWAP. Mezi WLC a LWAP jsou posílány pouze řídící zprávy. Tato možnost je výhodná v případě malé rychlosti sítě mezi LWAP a WLC, protože posíláním dat by docházelo ke značnému zpomalení celého provozu v síti. Celková správa sítě, především z pohledu zajištění mobility, se stává komplikovanější, než u split MAC politiky.




**Obrázek 12 – Local MAC politika**

### 1.4.2 Připojení přístupových bodů k WLC

Aby byl LWAP schopen v dané síti komunikovat s WLC, musí mít přidělenu IP adresu. Může ji získat prostřednictvím DHCP serveru nebo statickým nastavením. Pro asociaci s WLC využívá LWAP zprávy typu discovery request. Zprávu discovery request zasílá LWAP jednomu nebo více WLC. WLC odpovídá zprávou discovery response.

| IP hlavička | UDP hlavička | CAPWAP hlavička | Kontrolní hlavička | Atributy zprávy |
|---|---|---|---|---|

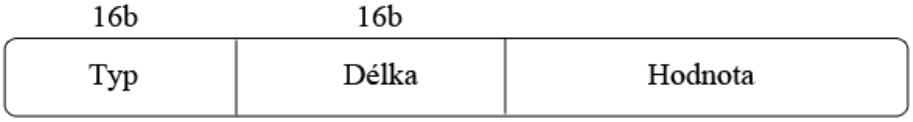
**Obrázek 13 – Formát CAPWAP zpráv discovery response a discovery request**

IP hlavička obsahuje IP adresy odesílatele a příjemce zprávy. Zdrojové a cílové porty jsou součástí UDP hlavičky. CAPWAP hlavička obsahuje informace o typu přenášených dat, příjemci dat a případné fragmentaci paketu [4].

| 8b | 5b | 5b | 5b | 1b | 1b | 1b | 1b | 1b | 1b | 3b |
|---|---|---|---|---|---|---|---|---|---|---|
| CAPWAP preambule | HLEN | RID | WBID | T | F | L | W | M | K | Příznaky |
| Fragment ID | | | Fragment offset | | | | | | | Rsvd |
| MAC adresa LWAP (volitelně) | | | | | | | | | | |
| Specifické informace (volitelně) | | | | | | | | | | |
| Datový rámec | | | | | | | | | | |

**Obrázek 14 – Formát CAPWAP hlavičky**

Protože použití UDP protokolu jako transportního mechanismu nezaručuje doručení odpovědi, případně může dojít k jejímu vícenásobnému doručení, obsahuje kontrolní hlavička číslo sekvence, pomocí které se dotazy a odpovědi párují. Kontrolní hlavička také určuje typ zprávy. Atributy zprávy obsahují informaci o typu dat, jejich délce a data samotná [4].




**Obrázek 15 – Formát atributu zprávy discovery request a discovery response**

Při zasílání zprávy discovery request však vzniká problém s určením cílové IP adresy WLC. LWAP, po připojení do sítě, adresu WLC nezná. Pro zjištění adresy WLC používá LWAP čtyři různé způsoby a to [25]:

- zaslání zprávy na broadcastovou adresu,
- lokálně uloženým seznamem IP adres WLC, ke kterým byl v minulosti připojen,
- získáním IP adresy ze serveru DHCP,
- nebo získáním IP adresy se serveru DNS.

Zasláním zprávy na broadcastovou adresu se zajistí, že všechna WLC, nacházející se v dané síti tuto zprávu obdrží a mohou odpovědět zprávou discovery response.

Další z možností je získání adresy ze seznamu uložených IP adres. Záznamy IP adres WLC, ke kterým byl LWAP v minulosti připojen, má uloženy v NVRAM paměti.

Získání adresy pomocí DHCP serveru je náročnější, než posílání broadcastové adresy. DHCP server musí podporovat možnost 43. Většina IP adres přidělena zařízením v počítačových sítích je dnes přidělována právě z DHCP serveru. Z toho důvodu je konfigurace podpory možnosti 43 snadným řešením k získání adres WLC. Seznam adres WLC nalezne LWAP v paketu DHCPOFER, který obdrží od DHCP serveru.

Poslední možností je získání adresy WLC z DNS serveru. K použití tohoto řešení je však nutné mít v síti umístěn DNS server. Doména má tvar CISCO-CAPWAPCONTROLLER.domena. Domena je doménové jméno, které je třeba přeložit na příslušnou IP adresu. Doménové jméno získá LWAP od DHCP serveru, společně s IP adresou DNS serveru, který má pro překlad použít. Tato možnost je, oproti získání adresy přímo z DHCP serveru, náročnější na implementaci, vzhledem k nutnosti konfigurace DNS serveru. Pro sítě malého a středního rozsahu není z tohoto důvodu příliš vhodná.

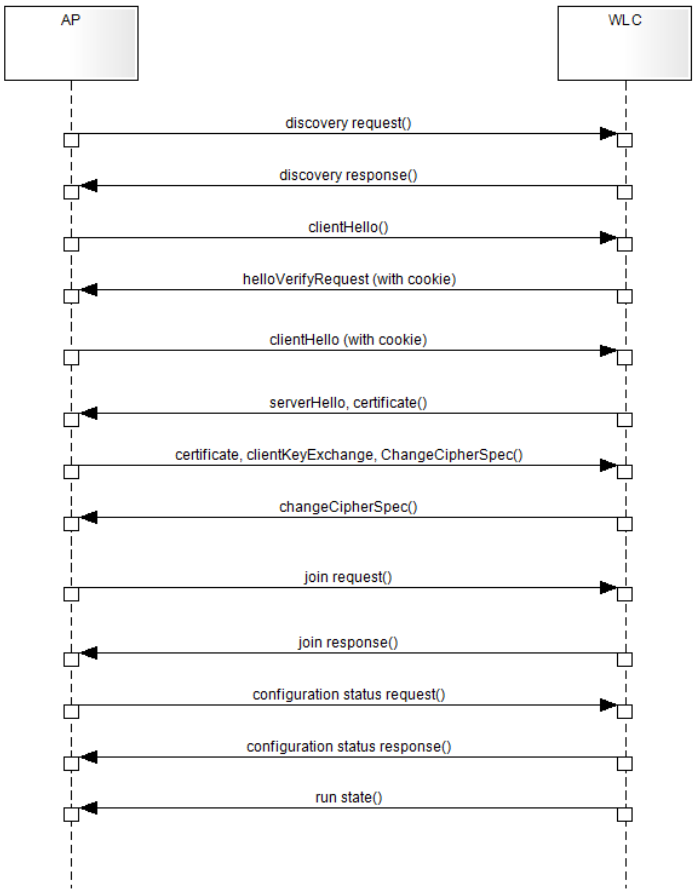
Výše popsaný proces se opakuje tak dlouho, dokud není schopen LWAP vyhledat alespoň jeden WLC, ke kterému se připojí.

LWAP je asociováno vždy pouze s jedním WLC. V případě obdržení více zpráv typu discovery response se musí rozhodnout, ke kterému WLC se připojí. K tomu používá několik metod výběru. Každé LWAP může mít nastavenu adresu primárního, sekundárního a terciálního WLC.

LWAP preferuje připojení na primární WLC. V případě neúspěchu se pokusí připojit na sekundární, popř. terciální WLC. V případě, že tyto adresy nastaveny nejsou, se LWAP pokusí připojit na WLC, který je nakonfigurovaný jako tzv. master.

I tento postup však může selhat. Potom se LWAP připojí k WLC, který má nejmenší vytíženost (nejméně připojených LWAP).

Po výběru nejvhodnějšího WLC je navázáno spojení mezi LWAP a WLC. Po vytvoření důvěryhodného spojení pomocí DTLS požádá LWAP o připojení k příslušnému WLC. Postup připojení LWAP k WLC je znázorněn na následujícím obrázku.




**Obrázek 16 – Handshaking a připojení k WLC**

Fáze připojení LWAP k WLC dle [4],[12],[24]:

1. Odesláním zprávy discovery request LWAP zjišťuje, zda jsou v síti dostupné WLC.
2. Dostupné WLC odpoví LWAP zprávou discovery response. LWAP si následně vybere, ke kterému WLC se připojí.
3. LWAP zašle WLC zprávu clientHello, která obsahuje seznam všech podporovaných kryptografických metod a náhodnou hodnotu, která je později použita jako základ pro vytvoření šifrovaného DTLS tunelu.
4. WLC zašle LWAP zprávu helloVerifyRequest spolu s využitím bezestavových cookie, které jsou generovány za pomocí hodnot, obdržených ve zprávě clientHello.

5. LWAP zopakuje požadavek clientHello s přidáním bezestavových cookie. WLC ověří příchozí cookie a pokračuje v handshakingu pouze tehdy, pokud je cookie platné. Tento mechanismus je využíván pro zamezení DoS útoků.

6. WLC vybere vhodnou metodu pro šifrování a společně s certifikátem ji, prostřednictvím zpráv serverHello a certificate zašle LWAP.

7. Klient přijme certifikát od WLC a spolu s ním získá informace, jaká metoda šifrování se bude používat. Po ověření certifikátu zašle LWAP zprávu ChangeCipherSpec, která oznamuje WLC, že všechna následující komunikace bude zašifrována sjednanou šifrou.

8. WLC odpoví zprávou ChangeCipherSpec. Od této chvíle je veškerá komunikace, mezi LWAP a WLC, v obou směrech šifrována.

9. Zprávou join request požádá LWAP o připojení k WLC. Zprávou join response WLC toto připojení povolí.

10. Prostřednictvím configuration status request a configuration status response LWAP informuje WLC o své aktuální konfiguraci a případně obdrží aktualizace.

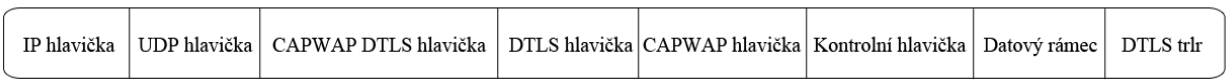
### 1.4.3 Přenos dat

K přenosu uživatelských dat mezi WLC a LWAP slouží datový kanál. Z důvodu bezpečnosti je vhodné ho zabezpečit, stejně jako řídící kanál, pomocí DTLS. Datové a zprávy jsou posílány ve formě UDP datagramů s využitím portu 5247 na WLC. Port na LWAP je libovolný [4].

Struktura CAPWAP paketu bez použití DTLS obsahuje, stejně jako u řídících zpráv, IP hlavičku s IP adresou odesílatele a příjemce, UDP hlavičku s čísly portů a CAPWAP hlavičku pro případnou fragmentaci.


**Obrázek 17 – Formát paketu bez použití DTLS**

Při použití zabezpečení datového kanálu pomocí DTLS se struktura paketu výrazně změní. Paket obsahuje navíc CAPWAP DTLS hlavičku, která identifikuje, že je chráněn pomocí DTLS. DTLS hlavička obsahuje informace o šifrování dat a ověřování. DTLS trailer (trlr) poskytuje ochranu zabezpečení zpráv.




**Obrázek 18 – Formát paketu s použitím DTLS**

## 1.5 Klienti v bezdrátové síti

Klienti, kteří se připojují do bezdrátové sítě, musí být jednoznačně identifikováni pomocí IP adresy. Každý klient má v rámci sítě unikátní IP adresu. Adresy mohou být klientům nastaveny staticky nebo dynamicky prostřednictvím DHCP serveru. Statické nastavení IP adres je vhodné především sítích malého rozsahu. V rozsáhlejších bezdrátových sítích, do kterých se připojuje velké množství klientů, je statické nastavování adres velice nepraktické. Nutnost udržovat informace o klientech, jejich IP adresách a zajistit aby nedošlo k přidělení stejné adresy více klientům je velice neefektivní a ve velkých sítích prakticky nemožné.

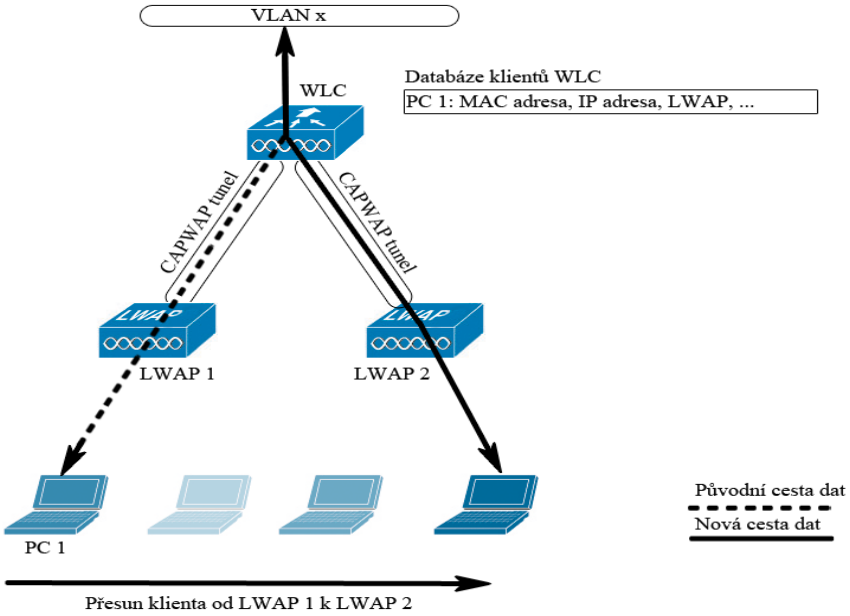
Přidělováním adres prostřednictvím DHCP serveru je zajištěna unikátnost IP adresy pro každého klienta. DHCP server si vede informace o zapůjčených adresách a době jejich platnosti. WLC disponuje interním DHCP serverem. Lze nastavit rozsah přidělovaných IP adres, masku sítě a dobu, po kterou je IP adresa zapůjčena klientovi. Tento DHCP server je možné použít pouze tam, kde všechna připojená LWAP leží ve stejném subnetu IP adres. Je ideálním řešením v sítích středního rozsahu s maximálně deseti LWAP, kde není k dispozici externí DHCP server [7].

Nejlepším řešením je použití externího DHCP serveru. Pokud WLC spravuje více bezdrátových sítí, každé síti je možné nastavit jiný rozsah a subnet přidělovaných IP adres. Při použití interního DHCP serveru nelze tohoto dosáhnout [8].

### 1.5.1 Mobilita klientů – roaming

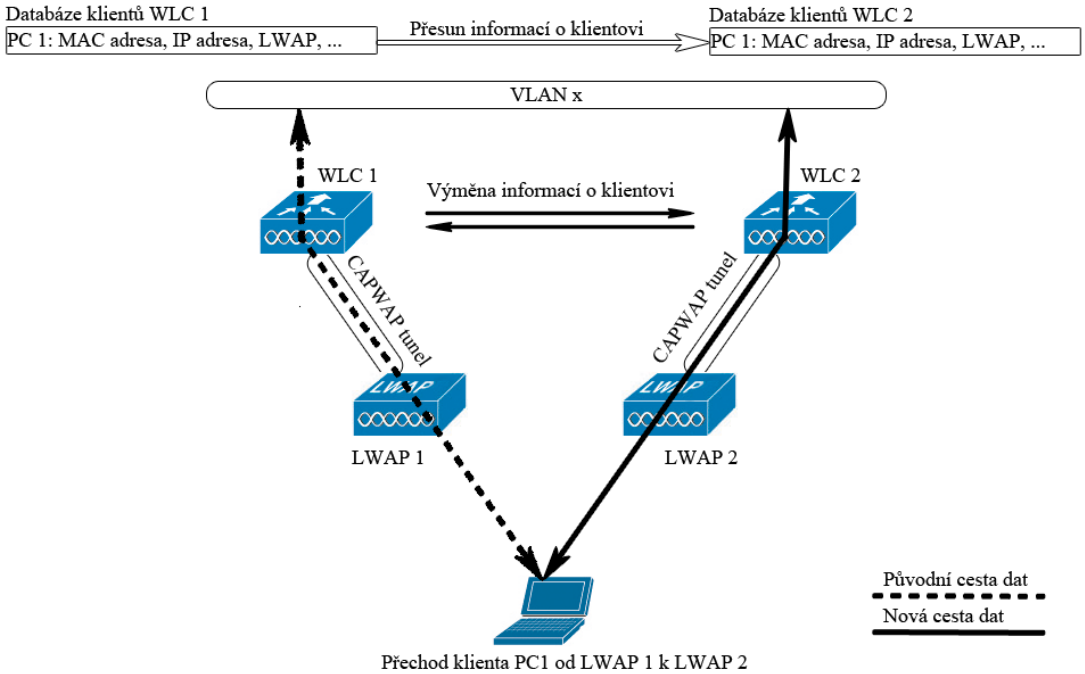
Roaming je označení pro zajištění mobility klientů v bezdrátových sítích. Jedná se o zajištění plynulého přechodu klienta od jednoho přístupového bodu k jinému, bez ztráty připojení. Po připojení klienta k LWAP dochází na WLC k vytvoření záznamu o klientovi a uložení tohoto záznamu do databáze. Součástí záznamu je IP adresa a MAC adresa klienta, informace o typu používaného zabezpečení, kvalitě služeb (QoS), WLAN síti a LWAP, ke kterému je klient připojen. Tento záznam WLC následně využívá pro jednoznačnou identifikaci klienta při přeposílání jemu určených dat.

Roaming je realizován na druhé nebo třetí vrstvě ISO-OSI modelu. Pokud se klient přesune do místa se slabou sílou signálu, začne automaticky vyhledávat LWAP, které vysílá silnější signál. Následně klient vybere nejvhodnější LWAP, připojí se a případně opětovně autentizuje. Jestliže se klient přesouvá mezi LWAP, které jsou připojeny ke stejnému WLC, jedná se o intracontroller roaming. Záznam o klientovi je aktualizován o informace o novém LWAP, ke kterému se klient připojil. Protože se klient pohybuje v rámci jedné podsítě, není třeba změna IP adresy [6].



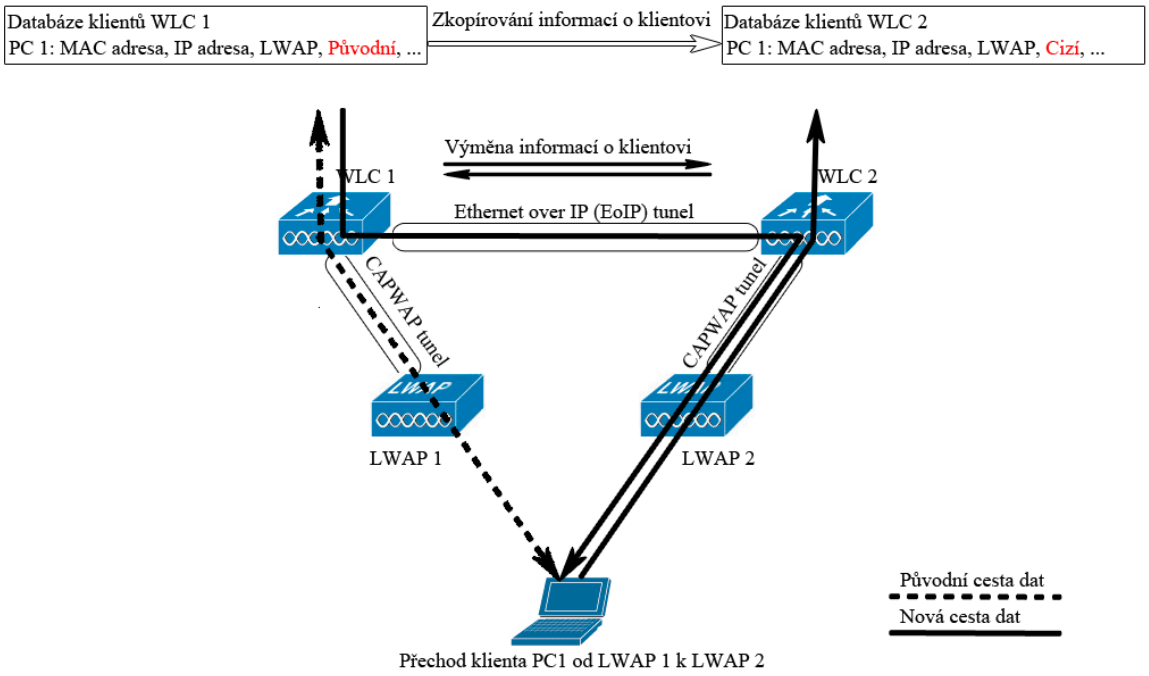

**Obrázek 19 – Intracontroller roaming**

Jestliže se klient přesune k jinému LWAP, které je navíc připojeno k jinému WLC, je proces předání informací složitější, než v případě intracontroller roamingu. Proces předání uživatele je závislý na tom, zda se oba WLC nachází ve stejném subnetu IP adres. Pokud jsou oba WLC ve stejném subnetu, požádá WLC 2 o informace o klientovi WLC 1. Záznam obsahující tyto informace je přesunut na WLC 2 a je aktualizován o informace o novém LWAP. Jedná se o takzvaný intercontroller roaming, jak je patrné z následujícího obrázku.



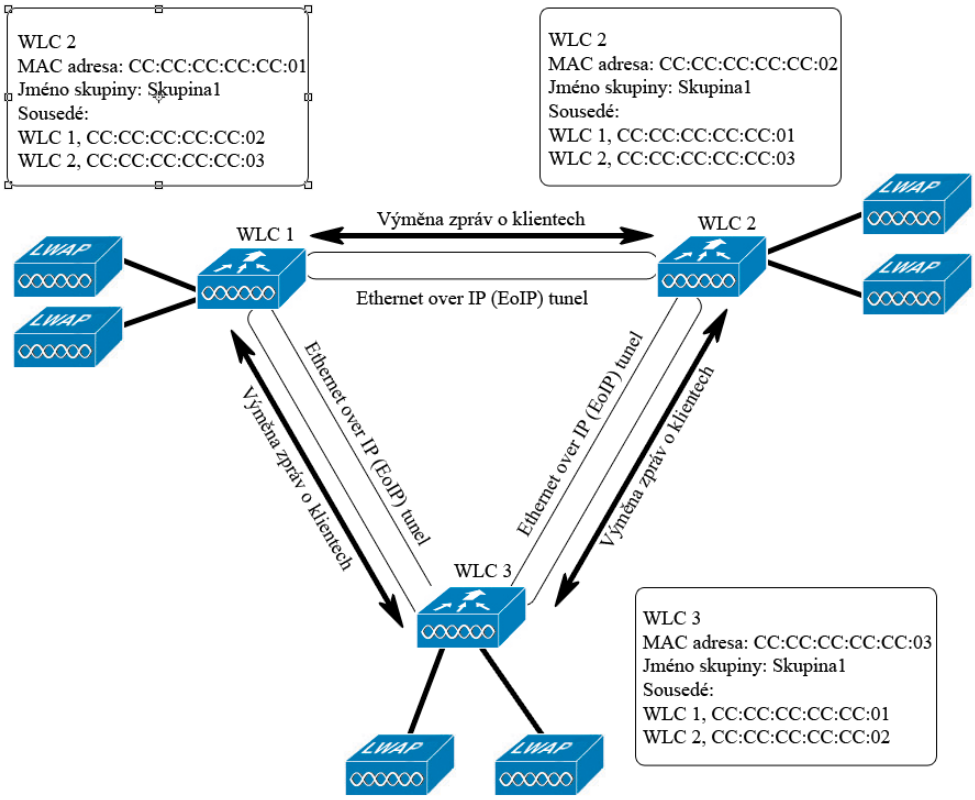

**Obrázek 20 – Intercontroller roaming**

Jestliže WLC 2 neleží ve stejném subnetu IP adres jako WLC 1, je postup předání klienta podobný jako při intercontroller roamingu. Nedochází ale k přesunu záznamu o klientovi na WLC 2. WLC 1 si pouze označí klientův záznam jako původní. Záznam o klientovi je následně zkopírován na WLC 2, kde je označen jako cizí. Odchozí data jsou posílána jinou cestou, než data příchozí. Odchozí data jsou odesílána přímo přes WLC 2. Příchozí data jsou přeposílána prostřednictvím EoIP tunelu z WLC 1 na WLC 2, který je přeposílá dále klientovi. Hovoříme o takzvaném intersubnet roamingu.




**Obrázek 21 – Intersubnet roaming**

Roaming klientů je dále možné omezit pouze na určitou skupinu WLC, což přispívá k větší kontrole mobility klientů. WLC lze segmentovat do pojmenovaných skupin, ve kterých dochází k výměně informací a stavů klientů. V jedné skupině může být až 24 WLC. Každý WLC obsahuje záznam určující jeho příslušnost ke skupině a dále záznamy o ostatních WLC, kteří jsou členy dané skupiny. Pokud klient přejde pod správu jiného WLC, odešle toto WLC unicastovou zprávu všem ostatním, kteří jsou členy dané skupiny. Všechna potřebná data o klientovi poskytne původní WLC, ke kterému byl klient připojen [6].




**Obrázek 22 – Segmentace WLC do skupin**

Roaming mezi jednotlivými skupinami WLC je možný pouze tehdy, pokud mají WLC jedné skupiny ve svých seznamech nastaveny příslušná jména a identifikaci WLC z jiných skupin, se kterými chtějí sdílet informace.

## 1.6 Bezpečnost bezdrátové sítě

Zajištění bezpečnosti představuje dnes jednu z priorit při návrhu počítačových sítí. Dříve se bezpečnosti nevěnovala taková pozornost, protože počítače byly obsluhovány pouze vyškolenými pracovníky. To se ale s postupným rozšířením internetu a používáním počítačů běžnými uživateli změnilo. Potřeba chránit připojení k síti a předejít tak jeho možnému zneužití se stala prioritou.

Základem bezpečnosti je určit, kteří uživatelé mají oprávnění přístupu do sítě a jim přístup povolit. Uživatelům, kteří toto právo nemají, je třeba v přístupu do sítě zabránit. Nezabezpečené bezdrátové sítě představují pro útočníky snadný způsob pro jejich zneužití. Útočník může snadno a nepozorovaně využívat připojení ke svým účelům, případně se i vydávat za někoho, kým ve skutečnosti není a tím získat přístup k citlivým informacím.

V případě decentralizované správy je nastavení bezpečnostních pravidel velice obtížné. Každému AP je třeba individuálně nastavit, jaká bezpečnostní pravidla má používat. To může vést, při větším množství AP, k nestejně definovaným bezpečnostním pravidlům pro celou síť a k případnému přístupu neoprávněných uživatelů.

Při použití centralizovaného řešení, s využitím WLC, je nastavení zabezpečení prováděno pouze na jednom místě a stejná bezpečnostní pravidla jsou uplatňována v rámci celé sítě. Zajištění jednotné bezpečnosti je jednou z hlavních funkcí WLC a častým důvodem pro použití centralizovaného řešení. Bezpečnost je na WLC zajišťována na druhé nebo třetí vrstvě ISO-OSI modelu.

Na třetí vrstvě je nejčastější zajištění zabezpečení pomocí webové autentizace, případně pomocí VPN tunelování. Tyto metody jsou detailně popsány v kapitole 2.

Na druhé vrstvě se nejčastěji používá ověřování uživatelů prostřednictvím RADIUS serveru za použití standardu 802.1X a EAP.

### 1.6.1 802.1x a EAP

802.1x je standard, který byl původně určen pro drátové sítě, dnes se využívá především v bezdrátových sítích. 802.1x vychází z protokolu PPP (Point-to-Point), který se používá pro spojení ve WAN sítích. Protokol PPP používá ve své základní implementaci dvě metody ověřování – PAP a CHAP. Obě tyto metody jsou založeny na autentizaci pomocí kombinace uživatelského jména a hesla. PAP nepoužívá při přenosu těchto údajů žádnou formu šifrování. Může dojít k jejich odposlechu a následnému zneužití [19].

CHAP je založen na metodě vzájemné autentizace klienta a serveru. Klient a server sdílí stejný šifrovací klíč. Server nejprve vygeneruje náhodný řetězec, který zašle klientovi. Ten přidá k přijatému řetězci heslo, pomocí hashovací funkce MD5 vytvoří tzv. hash a odešle tuto zprávu zpět na server. Server vytvoří hash původní zprávy odeslané klientovi a následně ji porovná s obdrženou zprávou od klienta. Pokud se zprávy shodují, je autentizace úspěšná. Server musí znát nejen nešifrované heslo klienta, ale i původní vygenerovaný řetězec.

Další metodou, která vychází z CHAP a byla vyvinuta firmou Microsoft, je MS-CHAP. MS-CHAP používá jako hashovací funkci MD4. Tato metoda nepotřebuje k úspěšnému ověření heslo v nezašifrované podobě, ale pouze jeho hash vytvořený MD4 funkcí. Ověřovací proces je pak stejný jako u metody CHAP.

V současnosti je používána především novější varianta MS-CHAPv2, která používá obousměrnou autentizaci a MD4 hashovací funkci. Server nejprve zašle klientovi náhodně vygenerovaný řetězec znaků spolu s identifikátorem relace. Klient po přijetí zprávy také vygeneruje náhodný řetězec znaků a odpoví serveru zprávou, která obsahuje uživatelské jméno klienta, hash přijatého řetězce, vygenerovaný řetězec klienta, hash hesla a identifikátor relace. Server porovná obdrženou zprávu s odeslanou zprávou a zašle klientovi zprávu obsahující údaje o úspěšném, či neúspěšném ověření spolu s odpovědí obsahující vygenerovaný řetězec serveru a klienta, heslo a šifrovanou odpověď klienta. Klient na jejím základě autentizuje server a zamítne, či povolí připojení [18][21].

Postupem času se však začaly ukazovat nevýhody výše zmíněných metod. Především zabezpečení je založeno na jednoduché autentizaci, která je navíc prováděna ihned po

navázání spojení a využívá pouze kombinace uživatelského jména a hesla. Proto byl vytvořen protokol EAP (Extensible Authentication Protocol), který doplnil protokol PPP o další autentizační mechanismy. Pro autentizaci prostřednictvím EAP se používají nejen hesla, ale také certifikáty, tokeny a další. EAP nezajišťuje samotnou autentizaci, ale je pouze transportním mechanismem pro 802.1x [1].

802.1x je založen na třech komponentech – klient, autentizátor a autentizační server. Klient je zařízení, které žádá o přístup do sítě a musí být ověřena jeho totožnost. Aby mohl klient používat autentizaci prostřednictvím 802.1x a EAP, musí mít nainstalován speciální program (supplicant). Tento program je dnes běžně implementován v operačních systémech Windows. Podporu 802.1x v OS Linux zajišťuje například program WPA supplicant [15].

Autentizátor představuje prostředníka mezi klientem a autentizačním serverem. Typicky se jedná o AP nebo router. V případě použití centralizovaného řešení je v roli autentizátora WLC.

Autentizační server je zařízení, provádějící samotnou autentizaci uživatele. Nejčastěji se používá RADIUS server. Ten může společně s informací o ověření předat autentizátorovi další informace o klientovi. Autentizátor může například přiřadit klienta do určité VLAN, případně mu nastavit jiná pravidla či omezení.

Pro zajištění autentizace pomocí 802.1X a EAP je nutné, aby klient, autentizátor a autentizační server podporovaly 802.1X a EAP. Dnes jsou 802.1X a EAP definovanými standardy, takže jejich podpora je zajištěna na téměř všech zařízeních.

Při komunikaci mezi klientem a autentizátorem jsou EAP zprávy zapouzdřeny a přenášeny pomocí ethernetových rámců. Ty jsou v literatuře označovány jako EAPOL (EAP over LAN). Mezi autentizátorem a autentizačním serverem jsou EAP zprávy zapouzdřeny a komunikace je předávána prostřednictvím zpráv protokolu RADIUS.

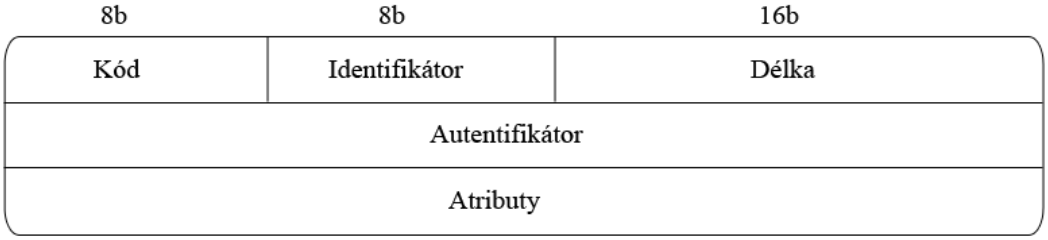
Standard 802.1x přinesl do bezdrátových sítí nejen možnost bezpečné autentizace uživatelů, ale také výraznou změnu v zabezpečení šifrování komunikace prostřednictvím WEP. Při použití klasického WEP šifrování sdílí všechny stanice stejný šifrovací klíč. Tento klíč je možné odhalit pouhým sledováním provozu na síti. Z toho důvodu není vhodné WEP používat. 802.1x umožňuje dynamickou obnovu WEP klíčů. WEP klíč tedy není sdílený všemi klienty, ale každý klient má svůj vlastní. Lze nastavit dobu platnosti klíče. Po uplynutí této doby dochází k automatickému vygenerování nového klíče. Dynamická obnova WEP klíčů nezaručuje úplnou odolnost vůči útokům, ale zabraňuje odhalení provozu v celé síti. Pokud se útočníkovi podaří klientův WEP klíč rozluštit, neodhalí komunikaci v celé síti, ale pouze komunikaci klienta [17].

### 1.6.2 Protokol RADIUS

RADIUS je AAA (autorizace, autentizace, accounting) protokol, který umožnuje ověřování a sběr informací o uživatelích. Pro autentizaci a autorizaci je jako transportní

protokol používán UDP s cílovým portem 1812. Accounting využívá také UDP protokol s cílovým portem 1813. RADIUS funguje na principu klient – server.

Prostřednictvím RADIUS protokolu autentizátor zasílá autentizačnímu serveru informace, na základě kterých autentizační server povolí, či zamítne klientovi do sítě přístup. Protokol RADIUS používá pro komunikaci mezi klientem a serverem šest základních druhů zpráv [23].




**Obrázek 23 – Formát zprávy protokolu RADIUS**

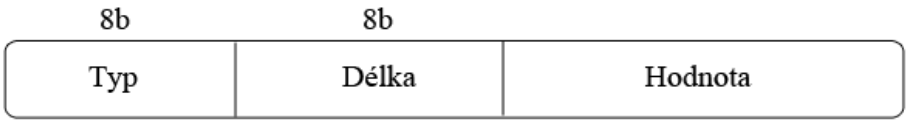
Pole kód obsahuje specifické číslo, které určuje, o jaký typ zprávy se jedná:

1. Access Request – kód 1. Tato zpráva obsahuje požadavek pro autentizační server pro ověření uživatele.
2. Access Accept – kód 2. Tato zpráva je zaslána autentizátorovi, stejně jako Access Reject, ale v případě úspěšné autentizace klienta. Autentizátor při jejím obdržení povolí klientovi přístup do sítě.
3. Access Reject – kód 3. Tato zpráva je zaslána autentizátorovi, při neúspěšné autentizaci klienta. Autentizátor nepovolí klientovi přístup do sítě.
4. Accounting Request – s kódem 4. Autentizátor prostřednictvím této zprávy žádá autentizační server o accounting.
5. Accounting Response – kód 5. Touto zprávou potvrzuje autentizační server autentizátorovi žádost o accounting.
6. Access Challenge – kód 11. Touto zprávou požaduje autentizační server po klientovi zadání hesla.

Protože RADIUS protokol využívá UDP, který je bezestavový a nezaručuje doručení odpovědi, případně se může odpověď doručit vícekrát, je nezbytné určit, která odpověď přísluší kterému dotazu. Toto párování zajišťuje pole identifikátor.

Komunikace mezi autentizačním serverem a autentizátorem musí být zabezpečena, aby nemohlo dojít k podvržení autentizačního serveru a tím umožněn přístup neoprávněným uživatelům. Autentizátor si musí být jistý, že odpovědi pochází od nepodvrženého autentizačního serveru. Autentizační server vloží do odpovědi na dotaz řetězec, který je umístěn v poli autentifikátor a kterým je odpověď autorizována. Autorizace je založena na principu sdíleného tajemství, které zná pouze autentizační server a autentizátor.

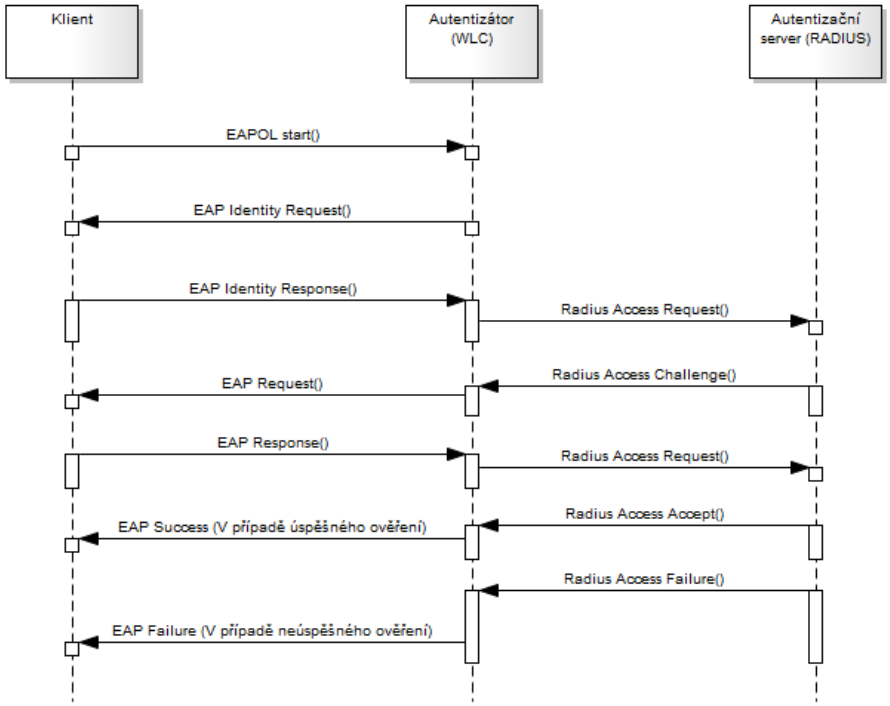
Pole délka udává celkovou velikost zprávy. Poslední položkou jsou atributy, které obsahují data pro autentizační server. Těchto atributů existuje celá řada a jejich detailní popis je uveden na [22].




**Obrázek 24 – Formát atributu protokolu RADIUS**

### 1.6.3 Autentizace klientů

Po připojení klienta k autentizátoru je síťový provoz na portu, ke kterému se klient připojuje, zablokován. Přes port prochází pouze zprávy protokolu 802.1x a port se nachází v neautorizovaném stavu. V případě úspěšného ověření klienta dojde k přepnutí portu do autorizovaného stavu a je povolen síťový provoz.




**Obrázek 25 – Autentizace klienta**

Postup autentizace:

1. Klient naváže spojení s autentizátorem odesláním rámce EAPOL Start. Autentizátor se přijetím tohoto rámce dozví, že se chce klient připojit do sítě.

2. Autentizátor zašle klientovi rámec EAP Identity Request, ve kterém žádá klienta o autentizaci.

3. Klient odpoví zprávou EAP Identity Response, ve kterém poskytne požadované údaje. Například, ke které síti se chce připojit.

4. Autentizátor tuto zprávu přijme. Vybalí jí z EAPOL rámce, zapouzdří jí do zprávy typu Radius Access Request a přepošle autentizačnímu serveru.

5. Autentizační server odpoví klientovi prostřednictvím autentizátoru zprávou typu EAP Request, s pomocí které si od klienta vyžádá autentizační údaje. Na autentizátoru opět dochází k přebalení zprávy.

6. Klient tyto údaje poskytne autentizátoru prostřednictvím zprávy EAP Response. Autentizátor zprávu zapouzdří do zprávy Radius Access Challenge a přepošle autentizačnímu serveru.

7. Autentizační server, v případě úspěšného ověření, pošle autentizátoru zprávu typu Radius Access Accept. Autentizátor zašle klientovi zprávu EAP Success a povolí síťový provoz na portu, přes který je klient připojen. V případě neúspěšného ověření, autentizátor zašle klientovi zprávu EAP Failure a síťový provoz na portu, přes který je klient připojen, zůstává zakázán.

Poskytování údajů mezi 4. a 6. bodem je závislé na použité variantě EAP. Výše popsaný postup popisuje obecně princip fungování autentizace klienta.

### 1.6.4 Varianty EAP

Protokol EAP podporuje velké množství metod autentizace. Mezi nejznámější patří LEAP, TLS, MD5, PEAP a TTLS. Využití v bezdrátových sítích mají zejména metody TLS, TTLS, LEAP a PEAP. Každá metoda používá zabezpečovací mechanismus, založený na jiných principech. Pro použití je nutné, aby zařízení, mezi kterými probíhá vzájemná autentizace, používaly stejnou autentizační metodu [28].

- MD5 využívá pro autentizaci kombinaci uživatelského jména a hesla, která je šifrována pomocí MD5. Zabezpečení pomocí této metody není vhodné, protože nedokáže čelit slovníkovým útokům. Podporuje pouze jednocestné ověřování. To znamená, že AP dokáže ověřit klienta, ale klient nemá možnost ověření AP, ke kterému je připojen. MD5 také neumožňuje dynamické generování WEP klíčů. Tato metoda není v současné době, vzhledem ke své zranitelnosti, příliš používána.

- LEAP (Lightweight Extensible Authentication Protocol) je metoda vyvinuta firmou Cisco. Podporuje vzájemnou autentizaci a dynamickou obnovu WEP klíčů. Jedná se o proprietární metodu, která nebyla ve své době podporována ostatními výrobci.

- TLS (Transport Layer Security) využívá pro autentizaci certifikáty podepsané certifikační autoritou. Autentizační server a klient mají instalovány certifikáty, pomocí kterých dochází ke vzájemné autentizaci. I klient má tedy ověřenu síť, do které se připojuje. Komunikace je chráněna TLS tunelem, který znemožňuje odposlech. TLS poskytuje dynamickou obnovu WEP klíčů. Nevýhoda použití této

metody spočívá v nutnosti přidělování a zajištění správy klientských certifikátů. Přesto představuje, díky své bezpečnosti, vhodnou formu zabezpečení.

- TTLS (Tunneled Transport Layer Security) je rozšířením TLS. Podobně jako TLS využívá certifikátů. Certifikát je třeba pouze pro ověření autentizačního serveru. Klient se autentizuje pomocí hesla. Použití TTLS je proti TLS výrazně jednodušší, protože se certifikáty používají pouze na straně serveru a není nutná správa klientských certifikátů, jako v případě TLS.

- PEAP (Protected EAP) využívá rozdílných metod autentizace serveru a klienta. Nejdříve dochází k autentizaci serveru, který je autentizován stejně, jako při použití metody TTLS, tedy pomocí certifikátu. Následně dochází k autentizaci klienta. Protože je komunikační kanál chráněn pomocí TLS tunelu, je možné použít, pro autentizaci klienta, například MS-CHAPv2.

# 2 Sítě typu Eduroam

Centrální řízení pomocí WLC se používá nejen k lepším konfiguračním možnostem pro správu celé sítě. V akademickém prostředí lze tímto způsobem připojit celou bezdrátovou síť k celosvětové síti Eduroam. V současné době je k síti Eduroam připojena většina českých vysokých škol a státních organizací. Na stejném principu fungují všechny sítě typu Eduroam [14].

Síť Eduroam je založena na principu roamingu, to znamená využívání jednoho uživatelského účtu, pomocí kterého může uživatel využívat připojení k síti u jakéhokoliv člena projektu Eduroam. Tato idea vznikla v rámci organizace Terena Mobility TF v roce 2003. Na pilotním testování se podílelo pět institucí z Holandska, Finska, Řecka, Velké Británie a Portugalska. Později se začali zapojovat další organizace nejen z Evropy, ale z celého světa. Eduroam má velice dobře popsanou dokumentaci, určenou jak pro koncové uživatele, tak pro správce sítě. Dokumentace obsahuje nejen postupy, jak se připojit k síti Eduroam jako koncový uživatel, ale popisuje i postup připojení separátně vytvořené bezdrátové sítě do sítě Eduroam. Všechny potřebné informace jsou dostupné na [13].

## 2.1 Uživatelé

Uživatelé se připojují k síti Eduroam pomocí kombinace uživatelského jména a hesla. Uživatelské jméno se skládá ze jména uživatele a identifikace jeho domovské organizace (realmu). Uživatelské jméno má tvar jmeno@realm.

## 2.2 Autentizace uživatelů

Základem zabezpečení sítě Eduroam je AAA infrastruktura. Tato infrastruktura má za cíl zabezpečit přístup oprávněným uživatelům. Neoprávnění uživatelé do sítě přístup mít nemohou. Zabezpečení sítě Eduroam je založeno na standardu 802.1x s využitím EAP a autentizací uživatele na RADIUS serveru, tedy na stejném principu, jaký byl popsán v kapitole 1.6. Nejvíce používané varianty EAP v síti Eduroam jsou PEAP s MS-CHAPv2, TTLS a TLS, jejichž princip byl popsán v kapitole 1.6.4. Pro uživatele, kteří se nemohou připojit pomocí 802.1x, se dále nabízí možnost připojení pomocí webového formuláře nebo VPN.

### 2.2.1 Hierarchická struktura RADIUS serverů

Síť Eduroam je celosvětově rozšířená a není proto, z praktických důvodů a především z hlediska efektivity, možné realizovat autentizaci všech uživatelů pouze na jediném RADIUS serveru. Autentizace v síti Eduroam je proto založena na hierarchické struktuře RADIUS serverů, která se skládá ze třech základních úrovní. Lokální RADIUS server, národní RADIUS server a top-level RADIUS sever.

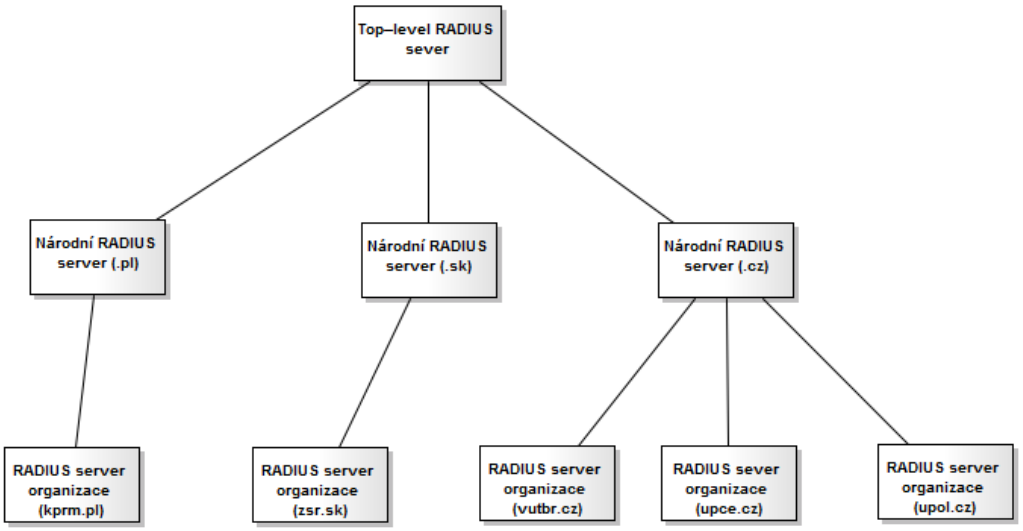
Každá organizace připojená do sítě Eduroam má svůj lokální RADIUS server, který zajišťuje ověření uživatelů, kteří mají tuto organizaci jako domovskou. Uživatelské účty mohou být vedeny přímo na RADIUS serveru, v podobě textového souboru nebo uloženy

v databázi, na kterou je možné RADIUS server napojit. Vedení účtů v databázi má výhody především při velkém počtu uživatelů.

Lokální RADIUS servery jsou dále připojeny na národní RADIUS server, který zajišťuje předávání požadavků mezi organizacemi, v rámci dané země. Nejvýše v hierarchii jsou umístěny top-level RADIUS servery, které zajištují předávání požadavků mezi národními RADIUS servery. Evropské top-level RADIUS servery jsou umístěny v Holandsku a Německu. Asie a oblast Pacifiku mají top-level RADIUS servery umístěny v Austrálii a Hong Kongu.

Pro směrování požadavků mezi RADIUS servery jsou využívány realmy, které jednoznačně identifikují uživatelovu domovskou organizaci. Tyto realmy mají rovněž hierarchickou strukturu, podobnou struktuře DNS serverů. Příkladem jména uživatele, který má jako domovskou organizaci Univerzitu Pardubice může být username@upce.cz. Realm v tomto případě jednoznačně identifikuje organizaci a zemi, ze které uživatel pochází. Uživatel je z České republiky a jeho domovskou organizací je Univerzita Pardubice.

Uživatel, který se připojí do sítě v domovské organizaci, je ověřen lokálním RADIUS serverem. V případě, že se uživatel připojuje do sítě mimo svou domovskou organizaci, dochází pomocí struktury RADIUS serverů k předání autentizačních údajů na RADIUS server uživatelovi domovské organizace, který zajistí ověření a zašle zpět informaci, zda uživatel má právo se připojit do sítě.

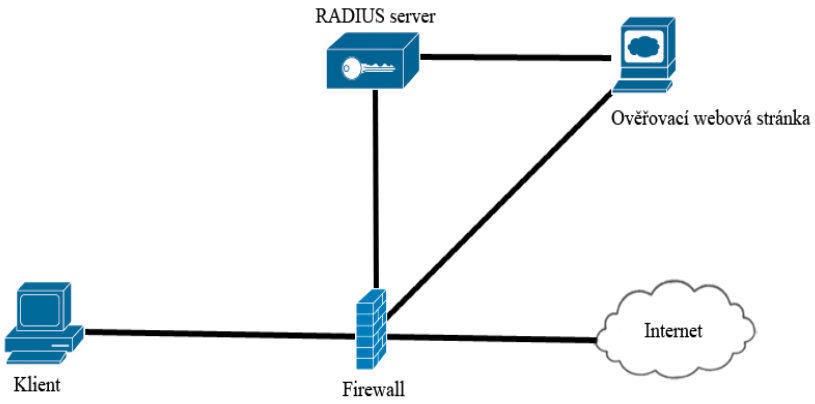



**Obrázek 26 – Hierarchická struktura RADIUS serverů**

### 2.2.2 Autentizace pomocí webového formuláře

Autentizace pomocí webového formuláře představuje alternativu k protokolu 802.1x. Provoz je v první fázi chráněn firewallem, který zamezuje přístupu do sítě. Uživateli je povolen přístup pouze na webovou stránku zajišťující autentizaci. Po zadání přístupových

údajů je ověřena identita uživatele. V případě úspěšného ověření firewall povolí síťový provoz. Autentizace nevyžaduje na straně klienta žádný speciální program jako v případě 802.1x.




**Obrázek 27 – Autentizace na bázi webového formuláře**

### 2.2.3 Autentizace pomocí VPN

VPN autentizace je v dnešní době využívána jako spolehlivý prostředek k připojení uživatele, který se nachází mimo lokální síť. V síti Eduroam představuje další způsob pro ověření identity. Síť, do které se uživatel pokouší připojit, je chráněna firewallem, stejně jako v případě autentizace webovým formulářem. Uživatel se připojí na VPN koncentrátor své domácí sítě, který v případě úspěšné autentizace zašle firewallu žádost o povolení komunikace. Firewall povolí komunikaci a uživatel je připojen do sítě.

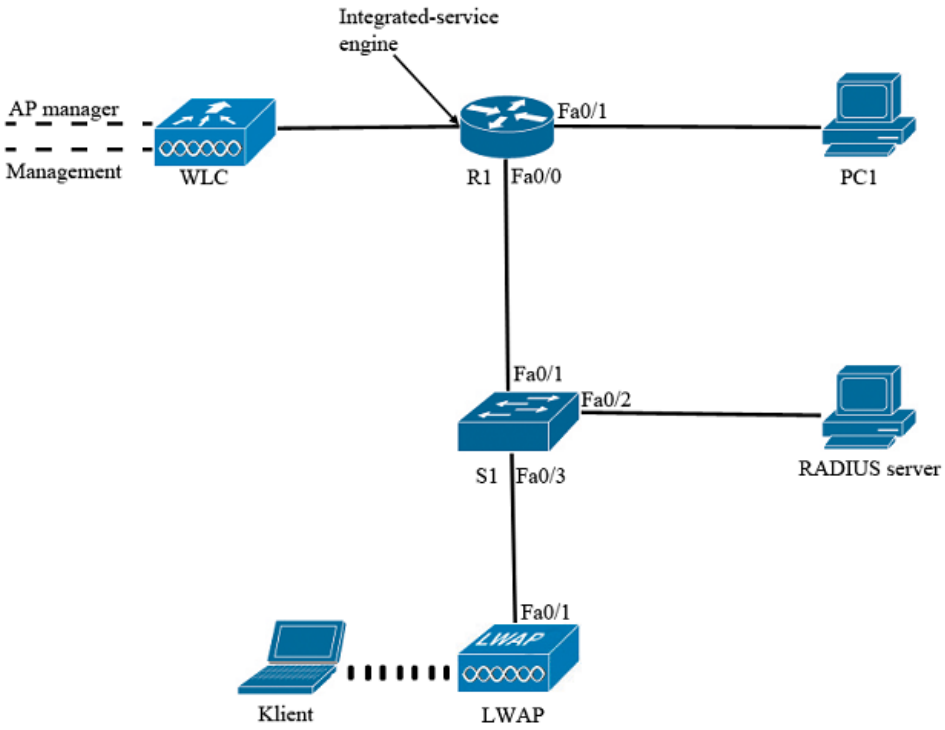
# 3 Návrh a praktická realizace bezdrátové sítě

Cílem praktické části práce je vytvoření bezdrátové sítě, která bude centrálně řízena WLC. Ověřování klientů a správu uživatelů bude zajišťovat RADIUS server, s využitím ověřování PEAP spolu s MS-CHAPv2, tedy kombinací uživatelského jména a hesla. Uživateli bude povolen přístup do sítě pouze tehdy, pokud dojde k jeho úspěšné autentizaci na RADIUS serveru. Pro ověření pravosti RADIUS serveru bude klient využívat certifikát, podepsaný soukromou certifikační autoritou.

## 3.1 Topologie sítě

Centrálním prvkem navržené sítě je WLC. V návrhu je využit WLC ve formě zásuvného modulu typu nme-air-wlc8-k9 a nikoliv WLC jako samostatné zařízení. WLC modul je přístupný stejným způsobem jako všechna další rozhraní routeru. Dalším klíčovým prvkem je Cisco router řady 2811, který je možné si přizpůsobit pomocí množství zásuvných modulů. Router je zároveň nastaven jako DHCP server a poskytuje IP adresy nejen připojeným klientům, ale i LWAP. Současně s přidělením IP adresy LWAP poskytne také informaci o IP adrese, případně adresách WLC, které LWAP použije pro následnou asociaci s WLC.

WLC šíří jednu bezdrátovou síť s SSID wlan10. Úspěšné připojení klienta k této síti je závislé na kladném vyřízení požadavku o přidělení IP adresy, vlastnictví příslušného certifikátu pro ověření pravosti RADIUS serveru a následné úspěšné autentizaci vůči RADIUS serveru.




**Obrázek 28 – Topologie sítě**

**Tabulka 1 – Adresní plán**

| Zařízení | Rozhraní | IP adresa | Maska sítě | Výchozí brána |
|---|---|---|---|---|
| PC1 | Síťová karta | 172.16.20.10 | 255.255.255.0 | 172.16.20.1 |
| R1 | Fa0/1 | 172.16.20.1 | 255.255.255.0 | N/A |
| | Fa0/0 | 192.168.100.1 | 255.255.255.0 | N/A |
| | Integrated-service Engine | 192.168.50.254 | 255.255.255.0 | N/A |
| RADIUS server | Eth0 | 192.168.100.2 | 255.255.255.0 | 192.168.100.1 |
| WLC | Management | 192.168.50.1 | 255.255.255.0 | 192.168.50.254 |
| | AP-Manager | 192.168.50.2 | 255.255.255.0 | 192.168.50.254 |
| | Virtual gateway | 2.2.2.2 | N/A | N/A |
| | vlan10 | 192.168.10.254 | 255.255.255.0 | 192.168.10.1 |

## 3.2 FreeRADIUS

Při výběru vhodného RADIUS serveru se nabízí různá řešení v závislosti na použitém operačním systému, počtu uživatelů, případně dalších zvolených kritérií.

Při výběru operačního systému je hlavním požadavkem administrátora především stabilita a možnosti konfigurace. Z tohoto důvodu byl v návrhu upřednostněn operační systém GNU/LINUX, který je nejen stabilní, ale oproti Microsoft Windows a Mac OS X nabízí větší možnosti konfigurace. Distribuce GNU/LINUX jsou zdarma a obsahují z velké většiny pouze svobodný software, takže je lze dále upravovat a šířit. Použití Microsoft Windows, případně MAC OS X je dražší, protože se jedná o operační systémy, které nejsou zdarma. MAC OS X je navíc závislý na zařízeních firmy Apple a tím se pro tento návrh sítě stává také nepoužitelným.

GNU/LINUX nabízí několik distribucí. Mezi nejznámější patří Debian, Fedora, Ubuntu, Arch Linux, Mandriva a mnohé další. Volba konkrétní distribuce je plně v režii správce sítě. V návrhu byla použita distribuce Ubuntu verze 10.04, se kterou má autor této práce největší zkušenosti.

Pro GNU/LINUX existuje několik variant RADIUS serverů, které jsou zdarma a liší se pouze konfiguračními možnostmi a podporovanými metodami autentizace. Nejznámějším je FreeRADIUS, který se vyznačuje velmi dobře zpracovanou dokumentaci nejen na oficiálních internetových stránkách, ale především v konfiguračních souborech, které obsahují konkrétní příklady nastavení parametrů pro fungování serveru. Z tohoto důvodu byl vybrán právě FreeRADIUS. Instalace a spuštění FreeRADIUS serveru je uvedena v příloze A.

Dalšími variantami RADIUS serveru pro GNU/LINUX jsou například GNU RADIUS a OpenRADIUS. Mezi alternativy FreeRADIUS serveru pro Microsoft Windows patří TekRADIUS, případně Windows Server.

### 3.2.1 Generování certifikátů

Při vytváření zabezpečeného spojení mezi klientem a RADIUS serverem se k identifikaci serveru používá digitální certifikát. Certifikát je elektronicky podepsaný veřejný šifrovací klíč, který obsahuje identifikační údaje majitele certifikátu. Certifikáty jsou vydávány certifikační autoritou, která zaručuje pravost údajů obsažených v certifikátu. Certifikační autoritou se může stát i sám tvůrce certifikátu vydáním soukromého certifikátu. Klienti ale nemají v tomto případě možnost ověření pravosti certifikační autority, je tedy zcela na nich, zda certifikátu důvěřují [17].

V návrhu sítě využívá klient, pro ověření pravosti RADIUS serveru, soukromého certifikátu, který byl vygenerován v operačním systému GNU/LINUX pomocí OpenSSL.

Postup generování certifikátu:

1. Vytvoření soukromého šifrovacího klíče. Soubor mykey.pem obsahuje šifrovací soukromý klíč. V průběhu generování je třeba vyplnit údaje, ze kterých je nejdůležitější heslo soukromého klíče. Vyplněné údaje jsou součástí přílohy B.

   ```
   openssl req -new -nodes -keyout mykey.pem -out server.csr
   ```

2. Vytvoření šifrovacího klíče pro server. Klíč je vygenerován za pomoci soukromého šifrovacího klíče. Výsledkem je soubor serverkey.key

   ```
   openssl rsa -in mykey.pem -out serverkey.key
   ```

3. Vytvoření soukromého certifikátu s platností 720 dní

   ```
   openssl x509 -in server.csr -out servercert.cert -req -signkey
   serverkey.key -days 720
   ```

4. Vytvoření certifikátu pro klienta

   ```
   openssl x509 -in servercert.cert -out servercert.crt -outform DER
   ```

Pro klienta je důležitý soubor servercert.crt, který si přidá mezi důvěryhodné certifikační autority. Soubory servercert.cert a serverkey.key využívá FreeRADIUS pro navázání a šifrování komunikace.

### 3.2.2 Konfigurační soubory

Nastavení parametrů FreeRADIUS je uloženo v konfiguračních souborech. V distribuci Ubuntu 10.04 jsou tyto soubory umístěny ve složce */etc/freeradius*. Nejdůležitějšími soubory jsou *eap.conf, proxy.conf, users* a *clients.conf*.

Součástí souboru *eap.conf* je použitá metoda EAP. V tomto návrhu se jedná o metodu PEAP společně s MS-CHAPv2. Protože MS-CHAPv2 využívá zabezpečeného TSL kanálu, je součástí souboru je také heslo soukromého klíče, cesta k šifrovacímu klíči a serverovému klíči. Po úpravách tedy vypadá soubor následovně:

```
eap { default_eap_type = peap
tls {
certdir = ${confdir}/certs
cadir = ${confdir}/certs
private_key_password = heslo
private_key_file = ${certdir}/serverkey.key
certificate_file = ${certdir}/servercert.cert
}
peap { default_eap_type = mschapv2 }
}
```

Zbylý obsah souboru je možné vymazat, případně zakomentovat přidáním symbolu # před každý řádek.

V souboru *proxy.conf* lze omezit počet připojení a počet požadavků, které jsou předány v rámci jednoho připojení. Dále se zde definuje způsob zpracování a předávání požadavků mezi RADIUS servery, což je typické pro sítě typu Eduroam. Návrh sítě v této práci definuje pouze lokální RADIUS server, takže předávání požadavků není třeba konfigurovat. Požadavky bez realmu (*NULL*), ostatní požadavky (*DEFAULT*) a požadavky s realmem „upce_bp.cz“ bude zpracovávat lokální RADIUS server. Všechny ostatní požadavky budou odmítnuty. Upravený soubor *proxy.conf* vypadá následovně:

```
proxy server { default_fallback = no }
realm LOCAL {}
realm NULL {}
realm upce_bp.cz {}
```

Informace o uživatelích jsou uloženy v souboru *users*. Součástí souboru je uživatelské jméno a heslo, které RADIUS server používá při autentizaci uživatele. Dále je možné využít volitelných informací, jejichž součástí být přidělovaná IP adresa a maska sítě. Správa uživatelů pomocí souboru *users* není vhodná při vysokém počtu uživatelských účtů, proto je vhodné použít databázové řešení. Použití databázového řešení překračuje rozsah této práce.

Pro potřeby návrhu jsou v souboru *users* evidovány informace o uživateli user. Soubor *users* má následující strukturu:

```
"user" Cleartext-Password:="user"
Reply-Message:="Hello"
```

Poslední z důležitých konfiguračních souborů *clients.conf* obsahuje informace o připojených klientech, v tomto případě WLC, kteří směřují požadavky na RADIUS server. Struktura souboru *clients.conf* vypadá následovně:

```
client 192.168.50.1 {
secret = password
shortname = AP
}
```

## 3.3 Konfigurace routeru

Před samotnou konfigurací routeru je vhodné smazat starou konfiguraci:

1. Vstup do privilegovaného režimu.

```
enable
```

2. Vymazání staré konfigurace.

```
erase startup-config
```

3. Restart routeru.

```
reload
```

Po restartu routeru do továrního nastavení se mohou začít konfigurovat příslušné parametry. Podrobná konfigurace routeru je uvedena v příloze C.

1. Nastavení zabezpečení routeru. Přístup přes konzoli a virtuální terminály je chráněn heslem. Stejně tak přístup do privilegovaného režimu routeru.

```
line console 0
password cisco
login
enable secret class
line vty 0 4
password cisco
login
```

2. Nastavení IP adresy na rozhraní FastEthernet 0/0.

```
interface Fa0/0
ip address 192.168.100.1 255.255.255.0
no shutdown
```

3. Nastavení IP adresy na rozhraní FastEthernet 0/1.

```
interface Fa0/1
ip address 172.16.20.1 255.255.255.0
no shutdown
```

4. Router přiděluje dynamicky IP adresy pomocí DHCP, nesmí však přidělit svojí vlastní IP adresu a adresu RADIUS serveru. Dochází tedy k vyhrazení určitého rozsahu adres, které nebudou dynamicky přidělovány.

```
ip dhcp excluded-address 192.168.100.1 192.168.100.10
```

5. Vytvoření DHCP poolu pro přidělování IP adres LWAP. Zde je třeba dobře nastavit volbu 43, pomocí které, jak bylo řečeno v teoretické části, obdrží LWAP adresu WLC. Tato volba se zapisuje ve formátu typ + délka + hodnota. Typ má vždy hexadecimální hodnotu 0xf1. Pole délka udává počet WLC umístěných v síti * 4 a pole hodnota je příslušná IP adresa WLC. Tyto pole jsou udávány také v hexadecimálním tvaru.

```
ip dhcp pool lwap
network 192.168.100.0 255.255.255.0
default-router 192.168.100.1
option 60 ascii "AP"
option 43 hex f104c0a83201
```

6. Vytvoření DHCP poolu pro přidělování IP adres klientům bezdrátové sítě s SSID wlan10.

```
ip dhcp pool vlan10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
```

7. Nastavení IP adresy na rozhraní integrated-service Engine 1/0 (WLC)

```
interface integrated-service Engine 1/0
ip address 192.168.50.254 255.255.255.0
no shutdown
exit
```

## 3.4 Konfigurace VLANs Controlleru (WLC)

Protože je WLC součástí routeru, je zapotřebí při jeho konfiguraci nejprve otevřít session na daný port.

```
service-module integrated-service Engine 1/0 session
```

V případě, že nebyl WLC nikdy předtím konfigurován, dochází ke spuštění průvodce konfigurací WLC, ve kterém se musí vyplnit všechny požadované informace. Podrobná konfigurace je uvedena v příloze D.

1. V prvním kroku se průvodce dotazuje na název systému

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
WLAN Controller:#Controller
```

2. Nastavení přihlašovacích údajů pro administraci WLC (maximálně 24 ASCII znaků).

```
Enter Administrative User Name (24 characters max):ccna
Enter Administrative Password (24 characters max):ccna
Re-enter Administrative Password: ccna
```

3. Nastavení IP adresy, masky sítě a výchozí brány pro management rozhraní. Dále povolení, či zakázání podpory VLAN. V případě nepodporování VLAN je tento identifikátor nastaven na 0.

```
Management Interface IP Address:192.168.50.1
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.50.254
Management Interface VLAN Identifier (0 = untagged):0
Management Interface Port Num [1]:1
```

4. Nastavení adresy DHCP serveru, který bude klientům přidělovat IP adresy. V návrhu je použit DHCP sever na routeru, tato adresa bude tedy totožná s adresou management rozhraní na WLC.

```
Management Interface DHCP Server IP Address:192.168.50.1
```

5. Nastavení IP adresy, masky sítě a výchozí brány pro AP-manager rozhraní.

```
AP Manager Interface IP Address:192.168.50.2
AP-Manager is on Management subnet, using same values
```

6. Nastavení adresy DHCP serveru, který bude přidělovat IP adresy LWAP. Opět je využíván DHCP konfigurovaný na routeru. IP adresa bude tedy stejná, jako v případě DHCP na management rozhraní.

```
AP Manager Interface DHCP Server:192.168.50.1
```

7. Nastavení adresy pro virtuální bránu. Virtuální brána je používána pro zabezpečení na 3. vrstvě. Toto zabezpečení není v návrhu použito, adresa tedy může mít jakýkoli tvar.

```
Virtual Gateway IP Address:1.1.1.1
```

8. Nastavení jména skupiny WLC. WLC ve stejné skupině si mohou navzájem vyměňovat informace o svých připojených klientech, jak je popsáno v kapitole 1.5.1.

```
Mobility/RF Group Name:MG
```

9. Nastavení jména výchozí bezdrátové sítě.

```
Network Name (SSID):bp-ssid
```

10. Klienti musí požádat o IP adresu DHCP server. Není žádoucí povolit zadávání statických IP adres.

```
Allow Static IP Addresses [YES][no]:no
```

11. V dalším kroku se průvodce táže, zda se používá zabezpečení pomocí RADIUS serveru. Návrh počítá s existencí RADIUS serveru jako klíčového prvku pro zabezpečení celé sítě, proto v této fázi dochází k zadaní IP adresy, masky sítě a hesla pro komunikaci s RADIUS serverem.

```
Configure a RADIUS Server now? [YES][no]: yes
Enter the RADIUS server address: 192.168.100.2
Enter the RADIUS server port[1812]:
Enter the RADIUS server secret: password
```

12. Zadání kódu země.

```
Enter Country Code (enter 'help' for a list of countries) [US]: CZ
```

13. Povolení či zakázání podpory pro 802.11b, 802.11a, 802.11g.

```
Enable 802.11b Network [YES][no]: no
Enable 802.11a Network [YES][no]: no
Enable 802.11g Network [YES][no]: yes
```

14. Konfigurace Radio Resource Management.

```
Enable Auto-RF [YES][no]:no
```

15. Konfigurace NTP serveru. V této fázi je nutné nastavit čas a datum na přibližně správnou hodnotu. V případě nesprávné konfigurace se nebudou LWAP schopny připojit k WLC.

```
Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: 03/12/13
Enter the time in HH:MM:SS format: 08:30:00
```

16. Uložení nastavení a restart WLC.

```
Configuration correct? If yes, system will save it and reset.
[yes][NO]:yes
```

Po uložení konfigurace dojde k restartu WLC a následném zastavení na následujícím příkazu požadujícím zadání uživatelského jména a hesla.

```
User:ccna
Password:****
(Cisco Controller) >
```

Pro každou bezdrátovou síť, kterou WLC spravuje, je třeba vytvořit dynamické rozhraní a tuto síť s příslušným rozhraním spárovat.

1. Vytvoření dynamického rozhraní vlan10 pro VLAN 10.

```
(Cisco Controller) >config interface create vlan10 10
```

2. Nastavení IP adresy, masky sítě a výchozí brány pro rozhraní vlan10.

```
(Cisco Controller) >config interface address vlan10 192.168.10.254
255.255.255.0 192.168.10.1
```

3. Vytvoření WLAN sítě s SSID wlan10.

```
(Cisco Controller) >config wlan create 10 wlan10
```

4. Spárování VLAN rozhraní s vytvořenou WLAN.

```
(Cisco Controller) >config wlan interface 10 vlan10
```

5. Nastavení IP adresy DHCP serveru, který poskytuje IP adresy klientům.

```
(Cisco Controller) >config interface dhcp dynamic-interface vlan10
primary 192.168.10.1
```

6. Nastavení zabezpečení WLAN pomocí protokolu 802.1x. Defaultní zabezpečení vytvořené sítě je WPA. Před samotnou změnou zabezpečení je nutné vypnout

rozhraní bezdrátové sítě, následně odstranit defaultní zabezpečení a nastavit nové. Nakonec rozhraní opět zapnout.

```
(Cisco Controller) >config wlan disable 10
(Cisco Controller) >config wlan security wpa disable 10
(Cisco Controller) >config wlan security 802.1X enable 10
(Cisco Controller) >config wlan enable 10
```

7. Posledním krokem je nastavení WLC do režimu master, jak je popsáno v kapitole 1.4.2.

```
(Cisco Controller) >config network master-base enable
```

Pro ověření správnosti nastavení se může použít příkaz ping. Pomocí příkazu ping lze ověřit nejen dostupnost rozhraní na routeru, případně WLC, ale také dostupnost RADIUS serveru.

```
R1#ping 192.168.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1#ping 192.168.50.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1#ping 192.168.100.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

## 3.5 Konfigurace klienta

Pokud se chce klient připojit k bezdrátové síti, musí nejprve nainstalovat vygenerovaný certifikát mezi důvěryhodné kořenové certifikační autority. Tento postup je detailněji popsán v příloze E. Následně vybere klient příslušnou síť, ke které se chce připojit a je vyzván k zadání přihlašovacího jména a hesla. V tomto případě jsou jméno a heslo totožné (user, user). WLC přepošle tyto údaje RADIUS serveru, který je porovná s údaji uloženými v souboru users, kde najde shodu a umožní tak klientovi přístup do sítě. Spolu s tím dojde k přidělení IP adresy z DHCP serveru.

# Závěr

Cílem práce bylo popsat důležité funkce WLC a možnosti jeho využití v bezdrátových sítích. Dále prakticky realizovat bezdrátovou síť s využitím WLC a centrální autentizace uživatelů na RADIUS serveru.

Práce je logicky dělena na dvě části. První část je věnována možnostem využití a funkcím WLC, který je využíván jako centrální prvek pro řízení bezdrátové sítě. Nejdůležitějšími funkcemi WLC jsou podpora VLAN sítí, podpora roamingu a široké možnosti podporovaných metod zabezpečení bezdrátové sítě, z nichž byla v této práci využita metoda 802.1x ve spolupráci s RADIUS serverem. Dále je v práci detailněji popsána síť Eduroam. Na stejném principu fungují všechny sítě tohoto typu. Akademická síť Eduroam je však nejrozšířenější, proto byl princip vysvětlen právě na této síti.

Ve druhé části práce byla navržena bezdrátová síť, na principu sítě Eduroam, za použití RADIUS serveru jako centrálního autentizačního mechanismu. Pro účely návrhu byl vybrán FreeRADIUS, který je určen pro operační systém GNU/LINUX a vyznačuje se velmi dobře zpracovanou dokumentací. Centrálním řídícím prvkem sítě je WLC modul. Tento řídí všechna připojená LWAP, zároveň s tím zajišťuje uplatnění jednotných bezpečnostních pravidel pro celou síť.

Jak již bylo uvedeno v praktické části práce, důležitým krokem je správné nastavení datumu a času při konfiguraci WLC. Pokud jsou tyto hodnoty nastaveny špatně, nedojde k asociaci LWAP s WLC.

Při konfiguraci DHCP serveru na routeru je nutné věnovat pozornost volbě 43, která oznamuje LWAP IP adresu WLC. Pro různé řady LWAP se tato možnost zadává trochu jiným způsobem. Před konfigurací DHCP serveru je žádoucí podívat se do dokumentace k danému LWAP, jakým způsobem je vhodné konfigurovat příslušnou volbu.

Návrh sítě byl úspěšně realizován a otestován v síťové laboratoři NET101 FEI UPCE.

## Literatura


[1] BÁČA, Vladimír. *Bezdrátová technologie wi-fi* [online]. Brno, 2007 [cit. 2013-01-05]. Dostupné z WWW: <http://autnt.fme.vutbr.cz/szz/2007/BP_Baca.pdf>. Bakalářská práce. Vysoké učení technické v Brně. Vedoucí práce Ing. Tomáš Marada, Ph.D.

[2] BOUŠKA, Petr. VLAN - Virtual Local Area Network. *Samuraj-cz.com* [online]. 2007 [cit. 2012-11-11]. Dostupné z WWW: <http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/>.

[3] BOUŠKA, Petr. Cisco WCS, WLC - Wireless Guest Access. *Samuraj-cz.com* [online]. 2008 [cit. 2012-11-11]. Dostupné z WWW: <http://www.samuraj-cz.com/clanek/cisco-wcs-wlc-wireless-guest-access/>.

[4] CALHOUN, P., M. MONTEMURRO a D. STANLEY. *Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification* [online]. 2009 [cit. 2012-12-09]. Dostupné z WWW: <https://tools.ietf.org/rfc/rfc5415.txt>

[5] CISCO. Configuring InterVLAN Routing and ISL/802.1Q Trunking on a Catalyst 2900XL/3500XL/2950 Switch Using an External Router. [online]. 2005 [cit. 2012-12-15]. Dostupné z WWW: <http://www.cisco.com/en/US/tech/tk389/tk815/technologies_configuration_example09186a00800949fd.shtml>

[6] CISCO. Chapter 11 - Configuring Mobility Groups. [online]. 2012 [cit. 2013-01-06]. Dostupné z WWW: <http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/c40mobil.html>

[7] CISCO. DHCP with the WLC [online]. 2009 [cit. 2012-12-08]. Dostupné z WWW: <http://www.cisco.com/en/US/products/ps6366/products_tech_note09186a0080af5d13.shtml#Internal-DHCP>

[8] CISCO. Guest WLAN and Internal WLAN using WLCs Configuration Example. [online]. 2009 [cit. 2012-12-08]. Dostupné z WWW: <http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008070ba8f.shtml#configs>

[9] CISCO. Inter-Switch Link and IEEE 802.1Q Frame Format [online]. © 2006 [cit. 2012-11-18]. Dostupné z WWW: <http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094665.shtml>.

[10] CISCO. Lightweight Access Point FAQ. [online]. 2010 [cit. 2013-03-10]. Dostupné z WWW: <http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00806a4da3.shtml>

[11] CISCO. VLANs on Wireless LAN Controllers Configuration *Example* [online]. 2011 [cit. 2012-11-11]. Dostupné z WWW: <http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00805e7a24.shtml>.

[12] CRANKSHAFT PUBLISHING. CAPWAP Session Establishment/AP Joining Process (Cisco Wireless LAN Controllers) Part 2. *What-when-how: In Depth Tutorials and Information* [online]. 2012 [cit. 2012-12-15]. Dostupné z WWW: <http://what-when-how.com/deploying-and-troubleshooting-cisco-wireless-lan-controllers/overview-of-capwap-cisco-wireless-lan-controllers/>

[13] DURNFORD, Laura. 'How to....' (deploy, promote and support) eduroam. *Eduroam* [online]. 2011 [cit. 2013-03-10]. Dostupné z WWW: <https://confluence.terena.org/display/H2eduroam/%27How+to....%27+%28deploy%2C+promote+and+support%29+eduroam;jsessionid=69264C1CCA5FD432696DE4052566F8C3>

[14] EDUROAM. Cisco WLC na TUL. 1996-2012 CESNET, z. s. p. o. *Eduroam* [online]. 2007 [cit. 2012-12-15]. Dostupné z WWW: <http://eduroam.cz/cs/spravce/ap/ciscowlc>

[15] HNÍDEK, Jiří. *802.1X pro Linux: Instalace a konfigurace* [online]. 2009 [cit. 2012-11-25]. Dostupné z WWW: <http://liane.tul.cz/cz/802.1X_pro_Linux>

[16] LUHOVÝ, Karel. VLAN (2) - typologie VLAN. *Svět sítí* [online]. 2003 [cit. 2012-12-02]. Dostupné z WWW: <http://www.svetsiti.cz/clanek.asp?cid=VLAN-2-typologie-VLAN-1442003>

[17] MORAVEC, Petr. *Bezpečné autentifikované bezdrátové připojení* [online]. Pardubice, 2010 [cit. 2013-03-16]. Dostupné z WWW: <http://hdl.handle.net/10195/37588>. Bakalářská práce. Univerzita Pardubice. Vedoucí práce Mgr. Tomáš Hudec.

[18] MS-CHAP v2. MICROSOFT. *Microsoft technet* [online]. 2013 [cit. 2013-01-05]. Dostupné z WWW: <http://technet.microsoft.com/en-us/library/cc957983.aspx>

[19] ODVÁRKA, Petr. Technologie pro zlepšení bezpečnosti datových sítí - standard 802.1x (1). *Svět sítí* [online]. 2004 [cit. 2013-01-06]. Dostupné z WWW: <http://www.svetsiti.cz/clanek.asp?cid=Technologie-pro-zlepseni-bezpecnosti-datovych-siti-standard-8021x-1-922004>

[20] PETERKA, Jiří. Základy datových komunikací [online]. 1993 [cit. 2012-11-11]. Dostupné z WWW: < http://www.earchiv.cz/l224/slide.php3?l=4&me=14>.

[21] Protokol MS-CHAP v2. MICROSOFT. *Microsoft technet* [online]. 2013 [cit. 2013-01-05]. Dostupné z WWW: <http://technet.microsoft.com/cs-cz/library/cc731462(v=ws.10).aspx>

[22] RADIUS Attribute List. *The FreeRADIUS Server Project* [online]. 2012 [cit. 2013-01-05]. Dostupné z WWW: <http://freeradius.org/rfc/attributes.html>

[23] RADIUS protocol. MICROSOFT. *Windows server* [online]. 2012 [cit. 2012-12-02]. Dostupné z WWW: <http://technet.microsoft.com/en-us/library/cc781821(v=ws.10).aspx>

[24] RESCORLA, E. a N. MODADUGU. *Datagram Transport Layer Security* [online]. 2006 [cit. 2012-12-09]. Dostupné z WWW: <http://tools.ietf.org/html/rfc4347#page-4>

[25] SMITH, Jeff. Controller-based wireless LAN fundamentals. Indianapolis, Ind.: Cisco Press, c2011, xvi, 294 p. ISBN 978-158-7058-257.

[26] The Internet Engineering Task Force. [online]. 2012 [cit. 2012-11-11]. Dostupné z WWW: <http://www.ietf.org/>

[27] Types of VLAN. ORBIT-COMPUTER-SOLUTIONS.COM. *Orbit-Computer Solutions.Com: Computer Training & CCNA Networking Solutions* [online]. 2012 [cit. 2012-12-02]. Dostupné z WWW: <http://www.orbit-computer-solutions.com/Types-of-VLAN.php>

[28] Zabezpečení wifi sítí. *Soom.cz* [online]. 2008 [cit. 2013-01-05]. Dostupné z WWW: <http://www.soom.cz/index.php?name=usertexts/show&aid=652&title=Zabezpeceni-wifi-siti>

# Příloha A

Instalaci FreeRADIUS serveru je doporučeno provádět jako superuživatel root, který má všechna práva k souborům.

Přihlášení jako superuživatel root

```
sudo su
```

Instalace FreeRADIUS

```
sudo apt-get install freeradius
```

Spuštění FreeRADIUS serveru

```
sudo /etc/init.d/freeradius start
```

Zastavení FreeRADIUS serveru

```
sudo /etc/init.d/freeradius stop
```

Spuštění FreeRADIUS serveru pouze pro testovací účely

```
sudo freeradius -X
```

## Příloha B

Při generování soukromého šifrovacího klíče je nutné zadání hesla pro soukromý klíč a dalších údajů. Vydávaný certifikát je soukromý, není proto nutné vyplňovat pravdivé údaje.

```
Country Name (2 letter code) [AU]:CZ
State or Province Name (full name) [Some-State]:Czech
Locality Name (eg, city) []:Czech
Organization Name (eg, company) [Internet Widgits Pty Ltd]:student
Organizational Unit Name (eg, section) []:student
Common Name (eg, YOUR name) []:student
Email Address []:admin@email.cz
Please enter the following 'extra' attributes to be sent with your
certificate request
A challenge password []:heslo
An optional company name []:student
```

# Příloha C

Konfigurace routeru, která je použita v návrhu sítě.

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
Router#reload
Proceed with reload? [confirm]
Continue with configuration dialog? [yes/no]:no
Router>enable
Router#conf t
Router(config)#hostname R1
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable secret class
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#interface Fa0/0
R1(config-if)#ip address 192.168.100.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface Fa0/1
R1(config-if)#ip address 172.16.20.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip dhcp excluded-address 192.168.100.1 192.168.100.10
R1(config)#ip dhcp pool lwap
R1(dhcp-config)#network 192.168.100.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.100.1
R1(dhcp-config)#option 60 ascii "AP"
R1(dhcp-config)#option 43 hex f104c0a83201
R1(dhcp-config)#exit
R1(config)#ip dhcp pool vlan10
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.1
R1(config)#interface integrated-service Engine 1/0
R1(config-if)#ip address 192.168.50.254 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

# Příloha D

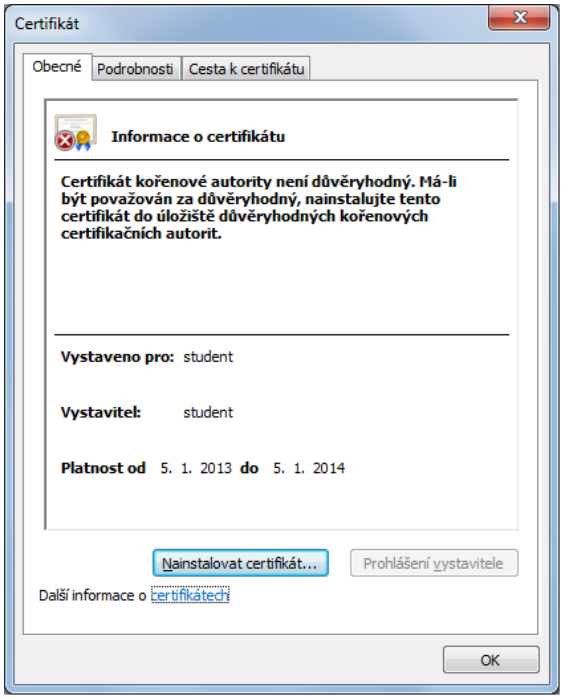
Konfigurace WLC.

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
WLAN Controller:#Controller
Enter Administrative User Name (24 characters max):ccna
Enter Administrative Password (24 characters max):ccna
Re-enter Administrative Password: ccna
Management Interface IP Address:192.168.50.1
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.50.254
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1]:
Management Interface DHCP Server IP Address:192.168.50.1
AP Manager Interface IP Address:192.168.50.2
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server:192.168.50.1
Virtual Gateway IP Address:1.1.1.1
Mobility/RF Group Name:MG
Network Name (SSID):bp-ssid
Allow Static IP Addresses [YES][no]:no
Configure a RADIUS Server now? [YES][no]: yes
Enter RADIUS server address: 192.168.100.2
Enter RADIUS server port[1812]:
Enter RADIUS server secret: password
Enter Country Code (enter 'help' for a list of countries) [US]: CZ
Enable 802.11b Network [YES][no]: no
Enable 802.11a Network [YES][no]: no
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]:no
Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: 03/12/13
Enter the time in HH:MM:SS format: 08:30:00
Configuration correct? If yes, system will save it and reset.
[yes][NO]:yes
User:ccna
Password:****
(Cisco Controller) >config interface create vlan10 10
(Cisco Controller) >config interface address vlan10 192.168.10.254
255.255.255.0 192.168.10.1
(Cisco Controller) >config wlan create 10 wlan10
(Cisco Controller) >config wlan interface 10 vlan10
(Cisco Controller) >config interface dhcp dynamic-interface vlan10
primary 192.168.10.1
(Cisco Controller) >config interface dhcp dynamic-interface vlan10
primary 192.168.10.1
(Cisco Controller) >config wlan disable 10
(Cisco Controller) >config wlan security wpa disable 10
(Cisco Controller) >config wlan security 802.1X enable 10
(Cisco Controller) >config wlan enable 10
(Cisco Controller) >config network master-base enable
```

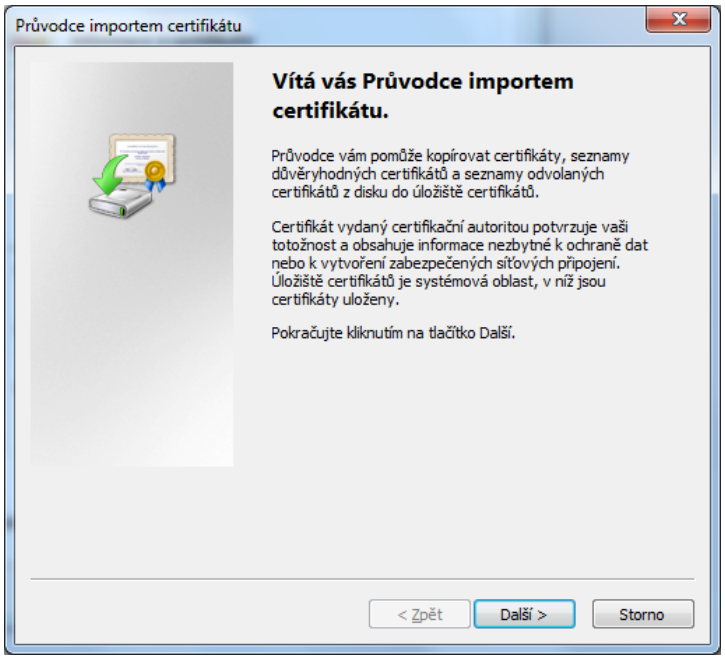
## Příloha E

Instalace vygenerovaného certifikátu mezi důvěryhodné kořenové certifikační autority.

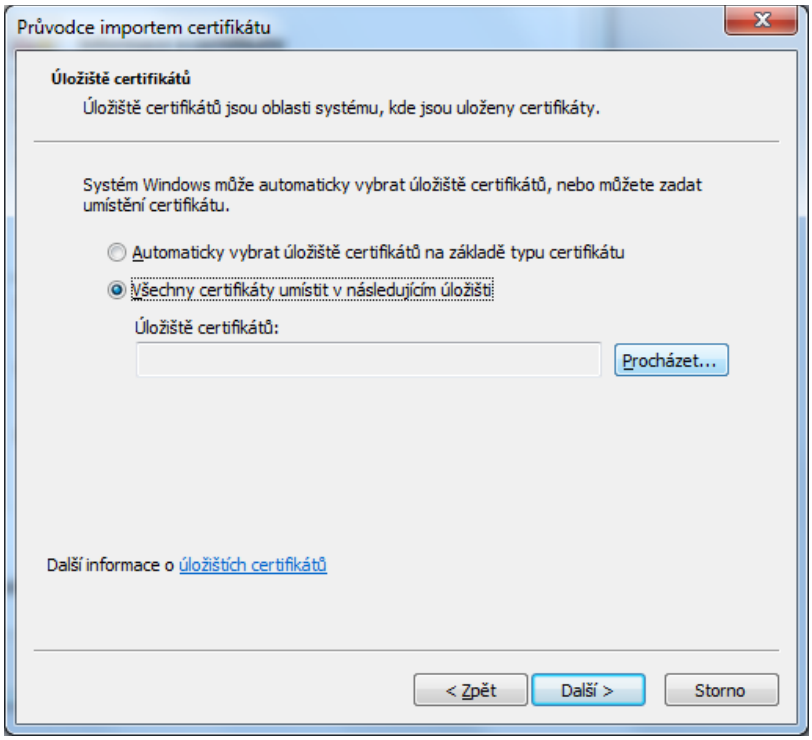
1. Dvojklikem na soubor se spustí instalace.
2. Výběr „Nainstalovat certifikát“



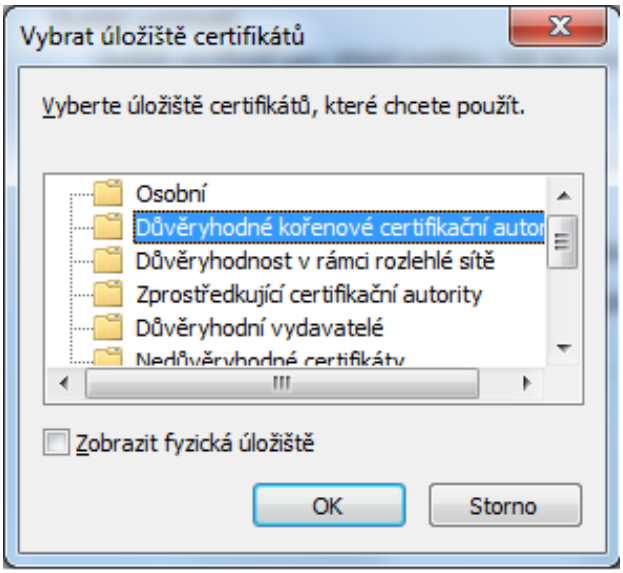

3. Spuštění průvodce instalací certifikátu.



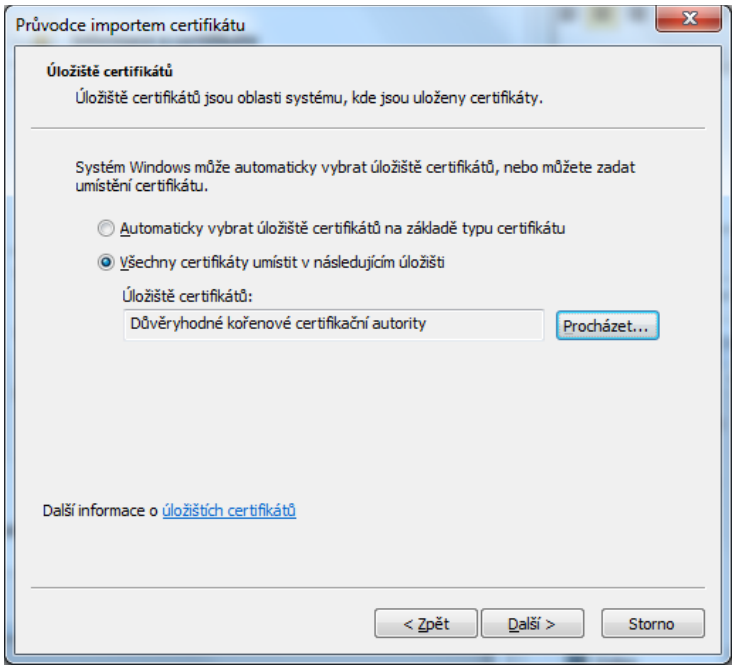
4. Volba „Všechny certifikáty“ a „Procházet…“



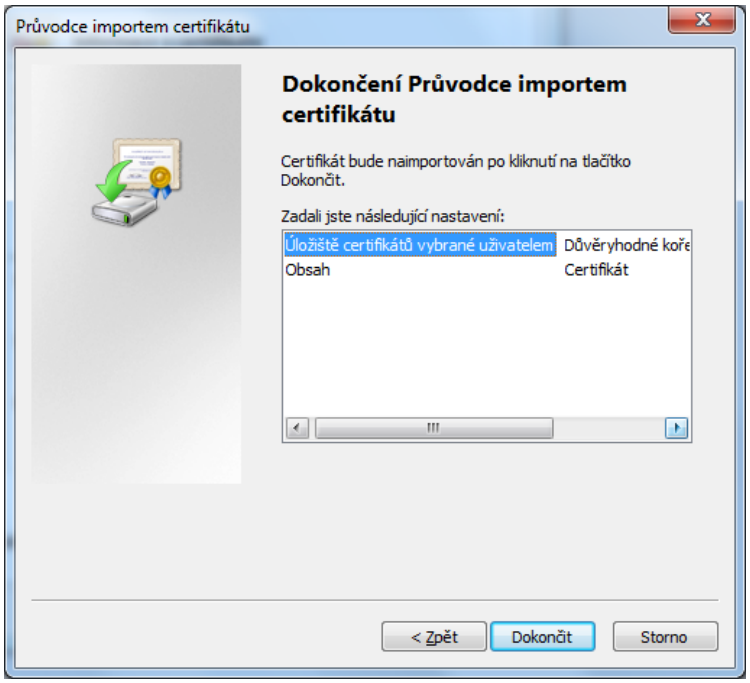

5. Volba „Důvěryhodné kořenové certifikační autority“



6. Volba „Další“




7. Volba „Dokončit“



8. Po potvrzení dalšího kroku dochází k instalaci certifikátu do uložiště certifikátů.