Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Analýza přístupů a řešení problematiky roamingu ve Wi-Fi sítích v prostředí Cisco a Ruckus

Bakalářská práce

Autor: Jiří Mareš
Studijní obor: Aplikovaná informatika (AI3-K)

Vedoucí práce: Mgr. Josef Horálek Ph.D.

Hradec Králové duben 2018

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

_____

V Hradci Králové dne 17.4.2018 Jiří Mareš

Poděkování:

Děkuji vedoucímu bakalářské práce Mgr. Josefu Horálkovi Ph.D. za odborné vedení, věcné připomínky, pomoc a rady při zpracování této práce.

Anotace

Název: Analýza přístupů a řešení problematiky roamingu ve Wi-Fi sítích v prostředí Cisco a Ruckus

Cílem práce je představit principy a navrhnout technické řešení roamingu Wi-Fi sítí s využitím technologií Cisco. Autor práce představí důvody využívání a principy roamingu Wi-Fi sítí s důrazem na technické řešení dané problematiky. V teoretické části je představen roaming ve Wi-Fi sítích z pohledu klientského zařízení i WLC kontroleru a jsou přestaveny standardy IEEE802.11k, IEEE802.11r a IEEE802.11v. V další části je pak představen vliv roamingu na datový tok v LAN síti. V praktické části autor představí modelové řešení, provede jeho realizaci a provede měření základních parametrů síťového provozu za využití kontrolerů WLC2504, ZoneDirector 1106 a v prostředí bez jejich využití. Na daných topologiích je testován roaming klienta, především rychlost roamingu, místa roamingu a datové toky v LAN síti. Práce předpokládá základní znalosti LAN a WLAN sítí jako je OSI model, datové toky na 1, 2, 3 a 4 vrstvě, VLAN a TAG, IP adresace, TCP a UDP protokoly a znalost Wi-Fi standardů IEEE802.11a, IEEE802.11b, IEEE802.11g, IEEE802.11n a IEEE802.11ac.

Annotation

Title: Analysis of approaches and solutions to the problems of roaming in WiFi networks in an environment of Cisco and Ruckus

This bachelor thesis deal is to introduce principles and design a technical solution for roaming Wi-Fi networks using Cisco technologies. The author of the thesis will present the reasons for using and principles of roaming Wi-Fi networks with an emphasis on the technical solution of the given issue. The theoretical part introduces roaming in Wi-Fi networks from the perspective of client and WLC controller, and introduces the standards IEEE802.11k, IEEE802.11r, and IEEE802.11v. The next section introduces the influence of roaming on the data stream in the LAN. In the practical part, the author introduces the model solution, performs its implementation and performs the measurement of the basic parameters of the network traffic using the WLC2504, ZoneDirector 1106 controllers and in the environment without their use. The roaming client is tested on topologies, especially roaming, roaming and LAN streaming. The work involves basic knowledge of LAN and WLAN networks such as OSI model, 1, 2, 3 and 4 layer data flows, VLAN and TAG, IP addressing, TCP and UDP protocols, and knowledge of IEEE802.11a, IEEE802.11b, IEEE802.11g, IEEE802.11n, and IEEE802.11ac..

Obsah

1 Úvod 1

2 Cíl práce 2

3 Metodika zpracování 3

4 Teoretická část 4

4.1 L2 roaming ve Wi-Fi sítích – asociace a reasociace kleinta 4

4.1.1 Chování klientského zařízení při Wi-Fi roamingu 6

4.1.2 Chování WLC při Wi-Fi roamingu 11

4.1.3 Standardy IEEE802.11 pro Wi-Fi roaming 12

4.1.4 Shrnutí 15

4.2 L2 roaming ve Wi-Fi sítích – z pohledu toku dat sítí 16

4.2.1 Změny toku dat v síti při roamingu klienta 16

4.2.2 Způsoby řízení Wi-Fi sítě a jejich vliv na roaming a tok dat sítí 18

4.2.3 Shrnutí 23

5 Praktická část 24

5.1 Měření a data 24

5.1.1 Wi-Fi síť řízená kontrolerem s kombinovaným provozem 24

5.1.2 Použitý hardware WLAN bezdrátové sítě a jeho nastavení 28

5.1.3 Použitý software 36

5.2 Analýza naměřených hodnot 39

5.2.1 Výsledky Měření kvality signálu – pokrytí v pásmu 5GHz 40

5.2.2 Výsledky měření rychlosti roamingu – rychlosti přenosu a výpadků 42

5.2.3 Určení přesné polohy kde dochází k reasociaci Wi-Fi klienta 46

5.2.4 Analýza datových toků v síti 47

6 Shrnutí výsledků 51

7 Závěry a doporučení 52

8 Seznam použitých pojmů a zkratek 54
9 Seznam použité literatury 59
10 Přílohy 64
10.1 Výpisy konfigurací 64
10.1.1 Wi-Fi přístupový bod: Cisco Aironet SAP1142i „A“ 64
10.1.2 Kontroler: Cisco AIR-CT2504-K9 66
10.1.3 Kontroler: Ruckus ZoneDirector 1106 77
10.2 Výstupy měření 86
10.2.1 Výstupy měření programem Ping Plotter 86
10.2.2 Výstupy měření programem iPerf 94

Seznam obrázků

Obrázek 1 - Wi-Fi roaming (4) 4
Obrázek 2 - active, passive scan (14) 6
Obrázek 3 - Active Scan (3 str. 144) 7
Obrázek 4 - probe (16) 7
Obrázek 5 - probe (16) 8
Obrázek 6 - probe (16) 8
Obrázek 7 - přechod k jinému AP (17) 10
Obrázek 8 - Ralink (19) 11
Obrázek 9 - Intel (19) 11
Obrázek 10 - Netgear (20) 11
Obrázek 11 - deasociace (16) 11
Obrázek 12 - schéma sítě (23) 16
Obrázek 13 - schéma sítě (23) 17
Obrázek 14 - schéma sítě (23) 17
Obrázek 15 - autonomní AP (25) 19
Obrázek 16 – kontroler řídící AP (ne provoz) (25) 20
Obrázek 17 - kontroler s AP i provozem (25) 21
Obrázek 18 - kontroler s kombinovaným provozem (25) 22
Obrázek 19 - topologie sítě LAN (23) 27
Obrázek 20 - topologie sítě se samostatnými AP (23) 29
Obrázek 21 - Cisco Aironet 1142i – antény (37) 30
Obrázek 22 - Cisco Aironet 1142i - mainboard (37) 30
Obrázek 23 - topologie sítě s kontrolerem Cisco 2504 (23) 31
Obrázek 24 - schéma komunikace WLC a LAP 32
Obrázek 25 - topologie sítě s kontrolerem Ruckus ZoneDirector 1106 (23) 33
Obrázek 26 - ZoneFlex7372 (43) 34
Obrázek 27 - rozmístění Wi-Fi AP (23) 39
Obrázek 28 – tabulka pokrytí signálem v pásmu 5GHz rozdělena pro jednotlivé scénáře a umístění přístupových bodů 41

Seznam tabulek

Tabulka 1 - Wi-Fi standardy (10) 5
Tabulka 2 - toky dat WLAN a LAN sítí 23
Tabulka 3 - Výsledky Měření kvality signálu – pokrytí v pásmu 5GHz 41
Tabulka 4 - Výsledky měření času odezvy jednotlivých ICMP PING a ztracené packety 43
Tabulka 5 - Výsledky měření datových toků mezi Wi-Fi klientem a LAN sítí 45
Tabulka 6 - Výsledky měření určení přesné polohy kde dochází k reasociaci Wi-Fi klienta 47
Tabulka 7 - Porovnání datových toků v síti během jednotlivých scénářů 50

1 Úvod

Wi-Fi je dnes běžná součást života a díky mobilním telefonům, tabletům a dalším chytrým zařízením se tato technologie těší velkému rozmachu. Z hlediska počtu připojených koncových klientů tak již dříve dominantní kabelové připojení je čím dál více vytlačováno a nahrazováno právě bezdrátovým připojením Wi-Fi (1). K tomu dopomáhá i stále se zvyšující rychlost, jakou jsou schopni se klienti připojovat k Wi-Fi infrastruktuře. Tato rychlost v současné době může blížit 3,5Gbit/s.

Zvyšující se počet klientských zařízení připojených do Wi-Fi sítě s sebou nese některé specifické požadavky na konfiguraci, nastavení a řízení sítě. A nejedná se jen o bezpečnost, jak by se mohlo zdát na první pohled. To aby klientský komfort ve Wi-Fi síti byl srovnatelný s tím, na jaký jsou uživatelé zvyklí z kabelového připojení, je nutné ve Wi-Fi síti věnovat pozornost Wi-Fi roamningu.

2 Cíl práce

Cílem této práce je porovnat podporu Wi-Fi roamingu ze strany dvou předních výrobců Wi-Fi technologií a zároveň zmapovat chování WLAN sítě v různých scénářích. V teoretické části práce rozebírá principy roamingu, chování jak klienta, tak sítě, jednotlivé standardy a možná omezení v jednotlivých designech WLAN sítí. V praktické části práce jsou porovnány tři nejčastější modely návrhů WLAN sítí. V prvním případě se jedná o WLAN síť využívající autonomní Wi-Fi přístupové body. Ve druhém případě se jedná o WLAN síť řízenou kontrolerem s tunelováním datového provozu. Ve třetím případě se jedná o WLAN síť řízenou kontrolerem pouze s řízením AP (bez tunelování datového provozu). V prvních dvou případech je využita technologie výrobce Cisco, ve třetím případě technologie od výrobce Ruckus. V obou případech jsou jak WLAN, tak LAN prvky počítačové sítě konfigurovány dle doporučení výrobce. U všech třech případů jsou hodnoceny jak samotný roaming, tak i chování dat v síti. Výsledky jak roamingu, tak i toku dat jsou nakonec zhodnoceny z hlediska vhodnosti nasazení.

3 Metodika zpracování

Bakalářská práce vychází z analýzy odborné literatury, dále pak z technických dat a doporučení výrobců. Téma Wi-Fi roamingu není v česky psané odborné literatuře příliš rozšířené, proto většina uvedených zdrojů odkazuje na anglicky psanou odbornou literaturu, či články. Ani odborná literatura v anglickém jazyce však nenabízí ucelenou knihu, či samostatné pojednání na toto téma. Bylo tedy nutné vycházet z dílčích kapitol věnovaných tématu roamingu a z materiálů jednotlivých výrobců.

Teoretická část se tak zabývá rozborem stávajícího stavu roamingu, jeho podpory ze strany výrobců a standardů IEEE (česky „Institut pro elektrotechnické a elektronické inženýrství“) (2) vypracovaných pro usnadnění Wi-Fi roamingu.

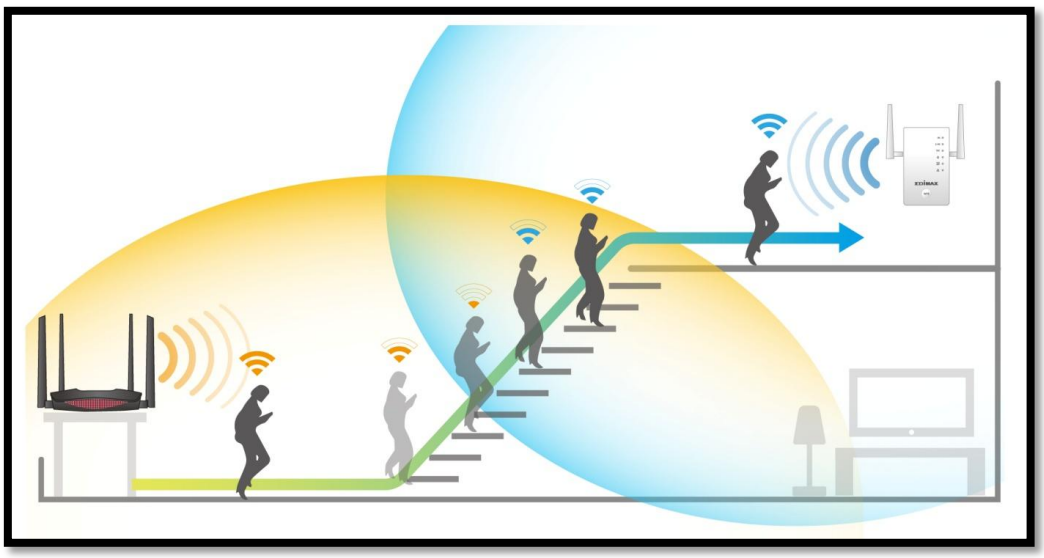
V praktické části je ověřena podpora Wi-Fi roamingu od předních výrobců Wi-Fi, firem Cisco a Ruckus. W-Fi přístupové body jsou pro měření zapojeny do LAN sítě se shodnou topologií. Lan síť je pak nastavena dle doporučení výrobce pro nejlepší funkci Wi-Fi roamingu. Během měření byla sbírána data pro porovnání řešení od obou výrobců.

Závěrečná část práce porovnává data z měření. Porovnána je samotná podpora roamingu, rychlost roamingu i vhodnost jednotlivých doporučených nastavení pro různá využití sítě.

4 Teoretická část

4.1 L2 roaming ve Wi-Fi sítích – asociace a reasociace kleinta

Wi-Fi roaming je proces, kdy klienti přecházejí z jednoho Wi-Fi vysílače na druhý Wi-Fi vysílač (dále již jen AP ze zkratky „Access Point“ označující Wi-Fi vysílače). Děje se tak buď z důvodu pohybu klienta, nebo kvůli potřebám optimalizovat zátěž v síti. Jde tedy o to zajistit, aby se klient včas přepojil z jednoho AP na jiné v co nejrychlejším čase a s co nejmenšími zásahy do existujícího spojení (3).



Obrázek 1 - Wi-Fi roaming (4)

Podobný scénář je řešen i na jiných sítích s pohybujícími se klienty, např. na sítích mobilních telefonů GSM, ale na Wi-Fi je situace přeci jen poněkud jiná. Sítě pro mobilní telefony GSM byly již od počátku zamýšleny jako rozsáhlé sítě s větším množstvím pohybujících se klientů a proto byl i přechod klientů mezi vysílači již od počátku zakomponován jako důležitá součást standardu a protokolů. GSM síť má tak přehled o připojených klientech a sama řídí se kterým vysílačem BTS bude telefon komunikovat a kam bude přepojen dále. (5)

U Wi-Fi je situace jiná. Sítě Wi-Fi nebyly z počátku zamýšleny jako prostředek pro připojení pohybujících se klientů, ale spíše jen jaké odložení drátů v sítě ethernet. Až později, s příchodem rozsáhlejších sítí a hlavně rozšířením

zařízení používajících Wi-Fi vznikla potřeba řešit ve Wi-Wi síti i problematiku Roamingu.

Roaming jako takový tedy není součástí Wi-Fi standardů tak jak je známe jako IEEE 802.11a/b/g/n nebo ac (6). S řešením roamingu se začalo až teprve nedávno a tak standardy IEEE 802.11k, IEEE 802.11r přišly až v roce 2008 a standard IEEE 802.11v v roce 2011 (7) (8) (9). Ani tyto standardy však nedokáží roaming řešit z pohledu sítě, pouze pomáhají klientovi se odpojit a opět připojit ve správný okamžik.

Tabulka 1 - Wi-Fi standardy (10)

Rok uvedení	**Standard IEEEE**	**Technologie**	**Frekvence**	**Přenosové rychlosti Mbps**
1997	802.11 Prime	FHSS	2,4GHz	1, 2
1999	802.11a	OFDM	5GHz	6, 9, 12, 18, 24, 36, 48, 54
1999	802.11b	HR-DSSS	2,4GHz	1, 2, 5.5, 11
2003	802.11g	ERP-OFDM		6, 9, 12, 18, 24, 36, 48, 54
		ERP-DSSS		1, 2, 5.5, 11
2009	802.11n	SU-MIMO	2,4GHz	MCS
			5GHz	MCS
2013	802.11ac	MU-MIMO	5GHz	

Ve Wi-Fi sítích tak předání klienta mezi jednotlivými AP není v pravomoci sítě, ale je plně v kompetenci klienta. Samotná Wi-Fi síť, nebo chcete-li Wi-Fi infrastruktura může jen poskytnout klientovi informace usnadňující přesun, ale odpojení a opětovné připojení musí provést klient sám. Je to tedy opačný přístup oproti sítím GSM, kde je vše řízeno sítí a klient sám nemá možnost přesun nijak ovlivnit (11).

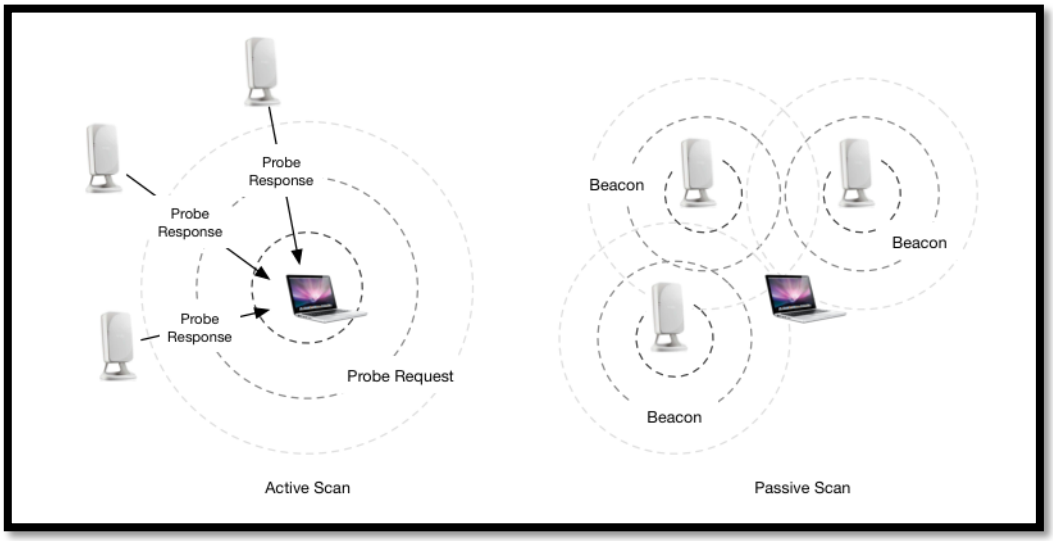
Z toho, že za asociaci a tedy i přesun mezi jednotlivými AP je zodpovědný klient, sice na jednu stranu pro klienta vyplývají výhod z možnosti přesnějšího nastavení, kdy a jak se připojovat, či odpojovat od Wi-Fi sítě, na druhou možnost to dost komplikuje nastavení Wi-Fi sítě samotné. Wi-Fi síť se tak musí vypořádat s poskytnutím dostatečné kvality signálu zařízením, jejichž připojování a odpojování nemá pod svou kontrolou. Je tedy vždy na konkrétním zařízení jak se s přesunem z AP na AP vypořádá (12).

4.1.1 Chování klientského zařízení při Wi-Fi roamingu

Aby mohl mít klient spravovat své připojení k jednotlivým AP, musí si vytvářet a udržovat databázi jednotlivých AP ve svém okolí. Z této databáze pak Klient čerpá i při roamingu. Proces zjištění AP v okolí je poměrně jednoduchým proces, který si zajišťuje klient někdy bez kooperace s Wi-Fi sítí (málo obvyklé), nebo ve spolupráci (toto řešení je běžně používáno) (3 str. 165).

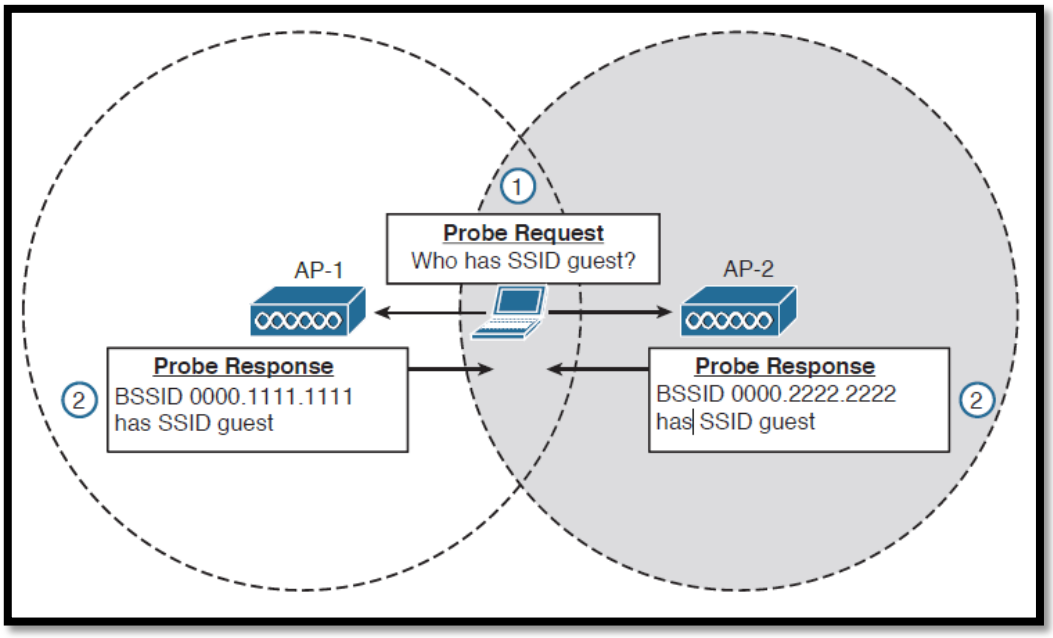
4.1.1.1 Proces zjištění AP v okolí klienta

Kontrolu zda je klient v dosahu nějaké Wi-Fi sítě může klient provádět dvojím způsobem (13 stránky 134-137). Jednak pasivním skenováním, tj. klient prochází jednotlivé kanály Wi-Fi a naslouchá, nebo aktivní skenování, při kterém se klient na hledání aktivně podílí. Tento způsob výrazně převažuje. (11)



Obrázek 2 - active, passive scan (14)

Zjištění AP v okolí při využití „Active scanning“ probíhá v několika krocích (15) (13 stránky 135-137). Stejně jako při pasivním skenování i při aktivním skenování klient prochází všechny dostupné Wi-Fi kanály, ale namísto aby na každém kanálu jen naslouchal, sám vyšle „Probe Request“ rámec s dotazem, které sítě jsou na tomto kanálu dostupné.



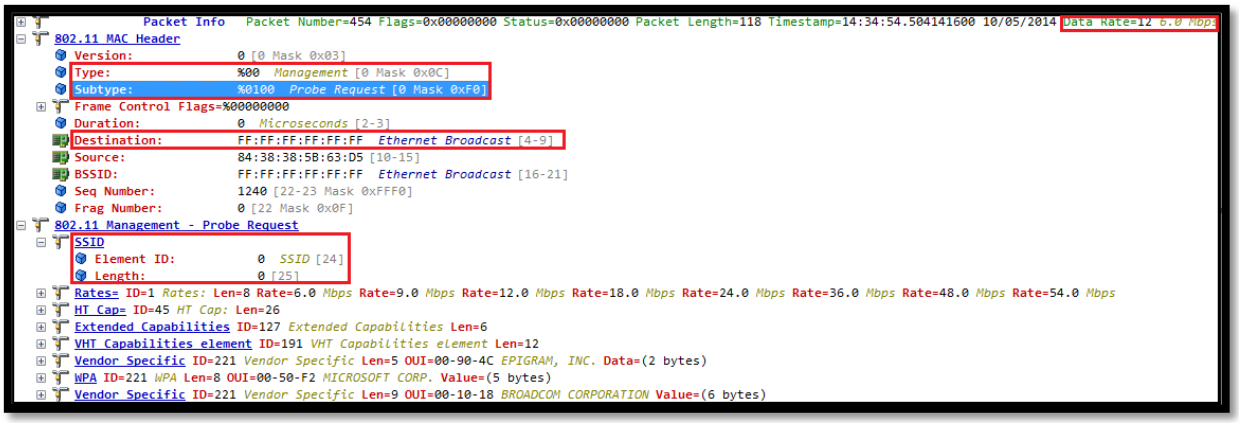
Obrázek 3 - Active Scan (3 str. 144)

„Probe Request“ (3 str. 140) je odeslán na broadcastovou adresu (ff:ff:ff:ff:ff:ff) a po jeho odslání se spouští odpočet „ProbeTimer“ během kterého klient čeká na odpovědi. Pokud odpověď během této doby nepřijde, klient přeladí na další kanál a vysílání opakuje.

Pac...	Transmitter	Receiver	Flags	Ch...	Signal	Data ...	Size	Protocol	Size Bar
240	B8:38:61:99:1A:AF	Ethernet Broadcast	*	149	54%	24.0	259	802.11 Beacon	802.11 Beacon
241	B8:38:61:99:1A:AF	84:38:38:5B:63:D5	#+	149	57%	24.0	24	802.11 BAR	802.11 BAR
242	84:38:38:5B:63:D5	Ethernet Broadcast	*	149	51%	6.0	122	802.11 Probe Req	802.11 Probe Req
243	B8:38:61:99:1A:AF	84:38:38:5B:63:D5	*+	149	54%	24.0	253	802.11 Probe Rsp	802.11 Probe Rsp
244		B8:38:61:99:1A:AF	#	149	50%	24.0	14	802.11 Ack	
245		84:38:38:5B:63:D5	#	149	49%	6.0	14	802.11 CTS	
246	B8:38:61:99:1A:AE	Ethernet Broadcast	*P	149	54%	24.0	294	802.11 Beacon	802.11 Beacon
247	84:38:38:5B:63:D5	B8:38:61:99:1A:AF	*	149	50%	24.0	45	802.11 Auth	802.11 Auth
248		84:38:38:5B:63:D5	#	149	55%	24.0	14	802.11 Ack	
249	B8:38:61:99:1A:AF	84:38:38:5B:63:D5	*	149	57%	24.0	34	802.11 Auth	802.11 Auth
250		B8:38:61:99:1A:AF	#	149	48%	24.0	14	802.11 Ack	
251	84:38:38:5B:63:D5	B8:38:61:99:1A:AF	*	149	50%	24.0	176	802.11 Assoc Req	802.11 Assoc Req
252		84:38:38:5B:63:D5	#	149	55%	24.0	14	802.11 Ack	
253	B8:38:61:99:1A:AF	84:38:38:5B:63:D5	*	149	57%	24.0	200	802.11 Assoc Rsp	802.11 Assoc Rsp
254		B8:38:61:99:1A:AF	#	149	47%	24.0	14	802.11 Ack	
255	84:38:38:5B:63:D5	B8:38:61:99:1A:AF	C	149	50%	24.0	30	802.11 Null Data	802.11 Data
256		84:38:38:5B:63:D5	#	149	55%	24.0	14	802.11 Ack	
257	B8:38:61:99:1A:AF	Ethernet Broadcast	*	149	55%	24.0	259	802.11 Beacon	802.11 Beacon

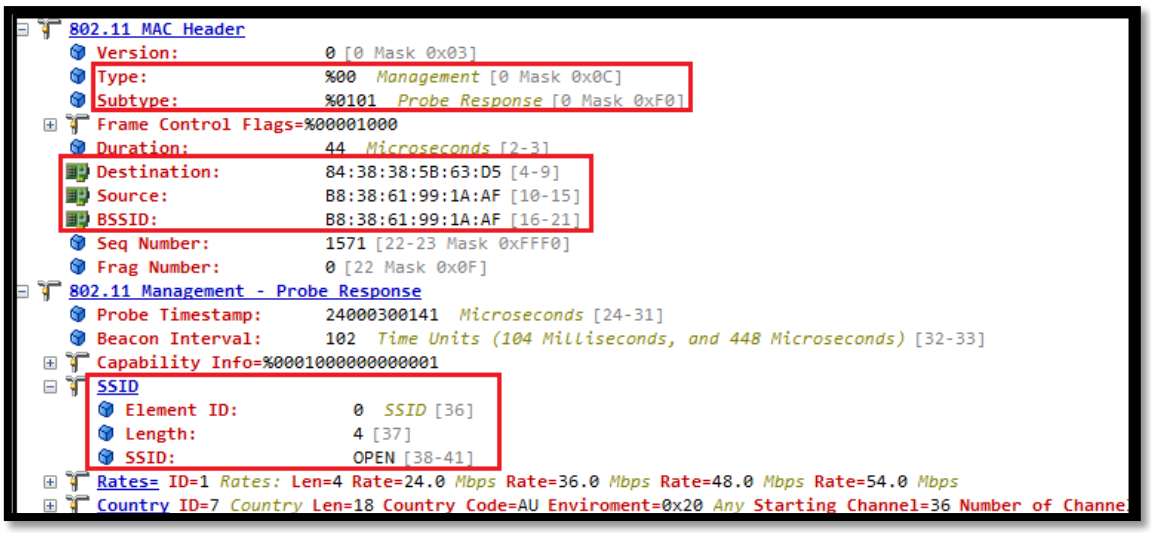
Obrázek 4 - probe (16)

Pokud se podíváme na „Probe Request“ zjistíme, že jeho součástí je i název SSID. V případě, jako je zjištění AP v okolí, klient využívá „Probe Request“ k prvotnímu zjištění Wi-Fi sítí v okolí vloží do této hodnoty 0 (tedy ff:ff:ff:ff:ff:ff – tato hodnota bývá někdy označována jako „Wildcard SSID“ nebo „Null Probe Request“). Položka SSID tak v rámci nezůstává nikdy prázdná. Komunikace je značena jako režijní.



Obrázek 5 - probe (16)

V rámeci „Probe Request“ můžeme nalézt i další informace, které klient propaguje do svého okolí. Typicky se jedná o informace, které protokoly IEEE 802.11 klient podporuje (13 stránky 136-137). Na tuto zprávu zareagují veškerá Wi-Fi AP a odešlou své informace v rámci „Probe Response“. Opět se jedná o režijní komunikaci (značenou jako „Management“), je zde již MAC adresa konkrétního rádia, kterým AP odpovídá, vyplněné SSID, podporované rychlosti a další parametry.



Obrázek 6 - probe (16)

Klient si následně seznam všech AP, ze kterých dostal odpověď, uloží do tabulky. Výpis tohoto seznamu je následně prezentován uživateli nejčastěji jako seznam dostupných Wi-Fi sítí. Nicméně tento výpis nemusí být vždy úplný. Pokud se totiž v seznamu AP najdou AP, které mají všechny parametry shodné, systém zobrazí do

výpisu uživateli jen to s nejsilnějším signálem. V tabulce si však systém uchovává veškerá AP a to až do dalšího cyklu „Probe“.

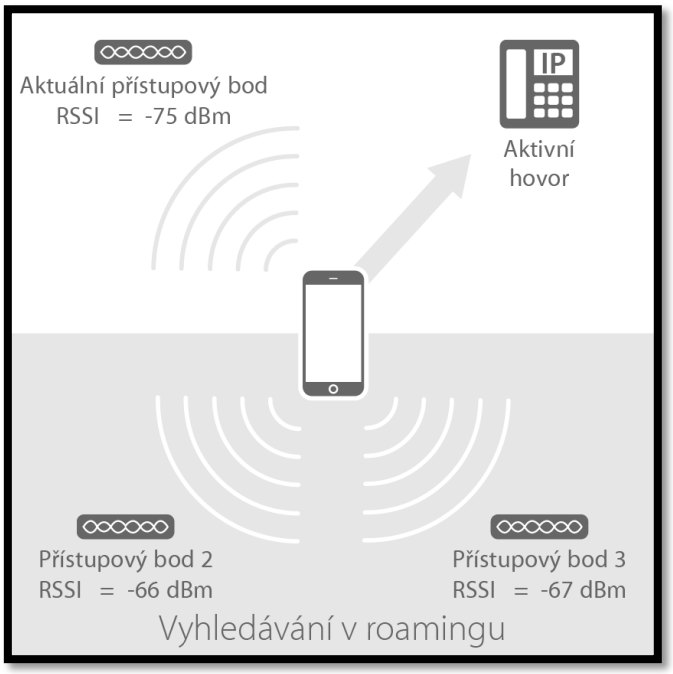
4.1.1.2 Přechod klienta k jinému AP

Klient přistupuje k Wi-Fi roamingu zpravidla tak, že v pravidelných intervalech aktualizuje seznam okolních AP (včetně jejich kvality) a pokud kvalita připojení k aktuálnímu AP poklesne pod určitou mez, připojí se k nejlepšímu AP na seznamu, které má shodné má shodné SSID. Poměrně často bývá spouštěčem roamingu také rozdíl kvality signálu mezi aktuálním a nejlepším AP na seznamu. Samotné nastavení mezí, kdy k roamingu dojde, závisí na konkrétním nastavení ovladače Wi-Fi karty. Proces roamingu na straně klienta počítá minimálně s třemi proměnnými (17). Jsou to:

1. **interval snímání AP v síti**
    - Tato hodnota znamená, jak moc často klient opakuje „Probe“ (3 str. 140) a aktualizuje tak tabulku AP.
    - Častější snímání vede na jednu stranu k aktuálnějším informacím, na druhou stranu pak zařízení stojí více režijního provozu.
    - Toto nastavení má vliv na rychlost Wi-Fi (více režijních rámců nutně krátí datový provoz) a také na spotřebu („zbytečný“ režijní provoz je nutné odbavovat i v jinak nečinném stavu a to spotřebovává systémové prostředky a nepřímo tak i baterii u zařízení napájených z baterie)
2. **prahová hodnota signálu pro hledání kandidáta**
    - zde hraje roli hlavně úroveň signálu. S klesající úrovní signálu vzrůstá režijní provoz zabraňujícím chybám.
    - Přibližně od úrovně -71dBm dochází ke snižování rychlosti a pod úrovní signálu -94dBm se spojení již neudrží
3. **minimální rozdíl síly signálu**
    - Zde rozumíme rozdíl signálu mezi nejlepším a nejhorším AP na seznamu klienta
    - Nízká hodnota sice může zaručit, že klient se bude snažit vždy přejít na AP s momentálně nejlepším signálem, nicméně ten může i kolísat.

V takovém případě nízká hodnota může vést k tzv. flapování mezi AP, tedy neustálému přeskakování mezi AP s velmi podobnou úrovní signálu.

- Naopak vysoká hodnota může vést k tomu, že se klient drží AP se špatným signálem, přestože je k dispozici AP s lepším signálem a díky tomu i větší rychlostí přenosu dat.

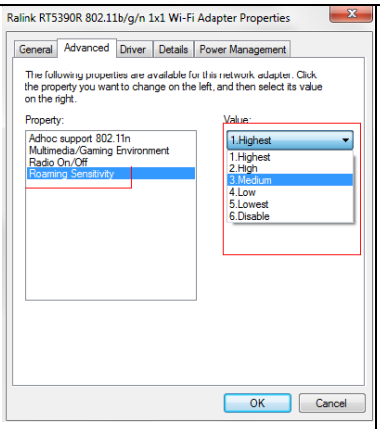


Obrázek 7 - přechod k jinému AP (17)

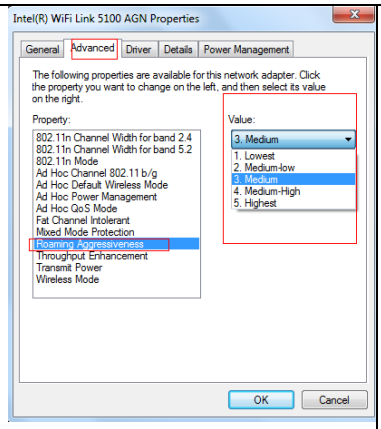
Pokud bychom uvažovali nejběžněji používané hodnoty, vypadal by příklad tato (17):

1. Každých 120s vyhledej okolní AP.
2. Pokud síla signálu poklesne pod -75dBm najdi lepší AP
3. Pokud má nejlepší kandidát na seznamu signál lepší alespoň o 8dBm (zde -67dBm) proveď přepojení.

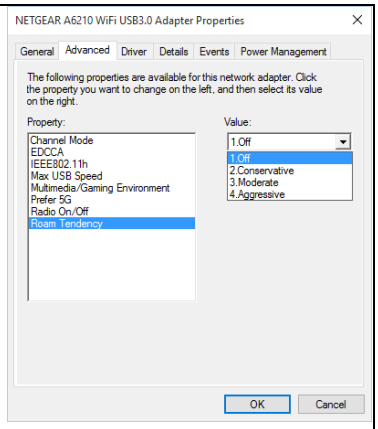
Výše uvedené parametry můžeme ovlivnit právě nastavení Wi-Fi karty. Nastavení mívá nejčastěji podobu parametru „roaming aggressivites“ u chipsetů Intel (18) nebo “Roam decision” (síla signálu) a “Roam tendency” (rozdíl síly signálu) pro chipsety Broadcom.



Obrázek 8 - Ralink (19)



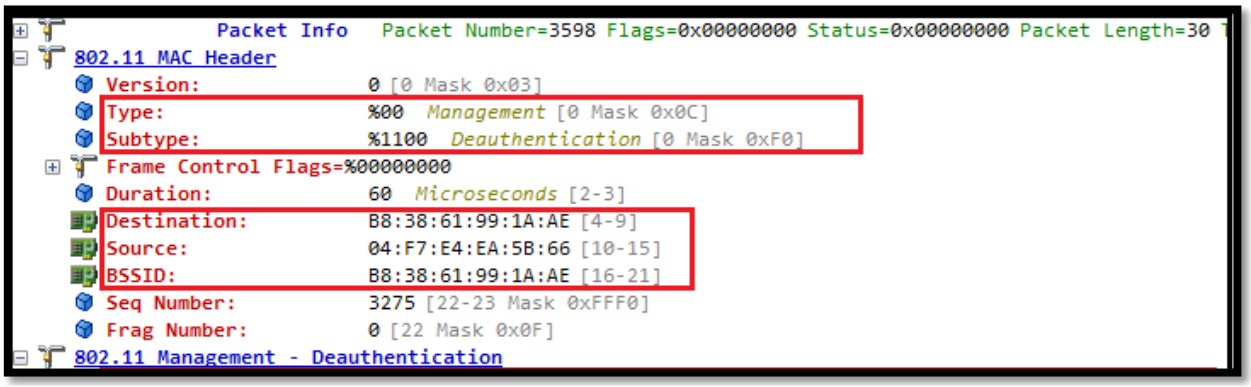
Obrázek 9 - Intel (19)



Obrázek 10 - Netgear (20)

4.1.2 Chování WLC při Wi-Fi roamingu

Co se týče sítí s Wi-Fi kontrolery, zde přichází do úvahy druhá možnost řízení roamingu a to je vynucení roamingu sítí. Jde o to, že kontroler, který řídí AP v síti má z jednotlivých AP jak informace o aktivních spojeních, tak o proběhnutých „Probe“. Díky tomu má možnost zjistit, že klient se již nachází v dosahu jiného AP s lepším signálem a násilně donutit klienta k roamingu. K tomu dochází nejčastěji tak, že Wi-Fi kontroler, který má informace o síle signálu, donutí klienta k opětovné asociaci tím, že mu zašle rámec „Dissassoc“ a tím jeho stávající spojení ukončí. Klient je pak nucen zahájit asociaci znovu, tentokráte však s AP, které má nejlepší signál.



Obrázek 11 - deasociace (16)

Takovéto chování však není doporučováno, neboť kontroler většinou nemá přesné informace o datových tocích s klientem a tedy neví přesně, jakou komunikaci

odpojením přeruší a také nemá žádnou možnost jak vyzvat donutit klienta k opětovnému připojení.

4.1.3 Standardy IEEE802.11 pro Wi-Fi roaming

Z důvodu optimalizace přechodu a možnosti nabídnout v komunikaci Klient – WLC Kontroler možnost lepší koordinace vzniklo postupně několik IEEE802.11 rozšiřujících standardů, které pomáhají optimalizovat přechod klienta mezi jednotlivými AP.
Standardy IEEE 802.11k, IEEE 802.11r a IEEE 802.11v také napomáhají k tomu, že celý proces odpojení a znovu připojení klienta je výrazně rychlejší.

4.1.3.1 IEEE 802.11k

Standard IEEE 802.11k je standard ustanovený v roce 2008 společně se standardem IEEE 802.11r. Oba standardy byly navrženy, aby umožnily zlepšení reasociací klientů v sítích WLAN (7).

Standard IEEE 802.11k je distribuován WLAN sítí a data z něho jsou přijímána klientem. Přijetí dat není vyžadováno, a pokud k výměně dat nedojde, na výsledek roamingu to nebude mít zásadní vliv (tj. klient bez podpory IEEE 802.11k provede roaming standardním způsobem jako by v síti IEEE 802.11k implementován nebyl).

Standard IEEE 802.11k zkracuje čas potřebný k roamingu tím, že umožňuje klientovi rychleji určit, na které AP by měl provést roaming a jak. WLAN síť klientovi prostřednictvím AP, s nímž je klient v současné době připojen, poskytne informace o sousedních AP a jejich vysílacích kanálech. Tímto způsobem, má klient připravený k roamingu, lepší představu o tom, na jaká AP v okolí se může znovu asociovat (3 str. 165).

Zjednodušeně si lze komunikaci představit asi takto (21 stránky 11-14):

1. AP detekuje, že se chce klient odpojit
2. AP informuje klienta, že je WLAN síť připravena znovu jej asociovat na jiném AP
3. Klient potvrdí přijetí informace a vyžádá si seznam blízkých AP

4. AP odešle klientovi seznam AP
5. Klient provede asociaci na nejlepší AP ze seznamu.

4.1.3.2 IEEE 802.11r

Standard IEEE 802.11r byl ustanoven v roce 208 společně jako doplněk standardů IEEE 802.11k a IEEE802.11r. Oproti standardu IEEE 802.11k, či IEEE 802.11v nepředává jen informace o stavu sítě, ale s klientem aktivně komunikuje a vyžaduje jeho spolupráci (8).

Standard IEEE 802.11r je zaměřen na urychlení samotné reasociace. K tomu dochází využitím funkce FT (Fast Basic Service Set Transition), která urychlí ověřování a to jak s předsdílenými klíči PSK, tak i s radius ověřováním 802.1X.

Pro běžnou asociaci klientů na AP v IEEE 802.11 je typické zaslání 4 zpráv. To je poměrně rychlá komunikace nepředstavující velkou zátěž. Nicméně situace s příchodem standardů IEEE 802.11i (podpora šifrování WPA) a ověřováním 802.1X (Ověřování pomocí Radius) a 802.11e (Media Access Control – zjednodušeně podpora QoS) počet těchto zpráv dramaticky vzrostl. A to do takové úrovně, že může trvat i několik sekund.

Protokol 802.11i (WPA) specifikuje, že pro autentizaci je klient povinen si znovu vyjednat svůj klíč s Radius serverm po každém přechodu (handoff). Tuto časově náročnou aktivitu lze nicméně urychlit, pokud část klíčů, generovaná na straně systému bude již spočítána předem a připravena v cache paměti. A právě provedení přípravy klíčů a nastavení QoS provádí protokol 802.11r na AP a tím zkracuje dobu potřebnou k reasociaci až pod 50ms a minimalizuje tím výpadek datového provozu na úroveň, která je již použitelná i pro přenos hlasu (21 stránky 3-9).

Nesprávná implantace 802.11r v minulosti vedla v na podzim roku 2017 k prolomení bezpečnosti WPA2 známé jako „KRACK“. V současné době je již tato chyba u většiny výrobců opravena tak, aby předpřipravené klíče nebyly klientovi odesílány pouze na základě shody MAC adres klienta (22).

4.1.3.3 IEEE 802.11v

Standard IEEE 802.11v je standard ustanovený v roce 2011 jako doplnění a rozšíření standardů IEEE 802.11k a IEEE802.11r. K výše uvedeným standardům přidává lepší lokalizaci klienta, předání dat o fyzické vrstvě a možnost úspory baterie klienta. V současnosti tak tyto tři standardy řeší kompletní dostupnou podporu roamingu klientů ve Wi-Fi sítích (9).

Standard IEEE 802.11v je podobně jako IEEE 802.11k distribuován WLAN sítí a data z něho jsou přijímána klientem. Přijetí dat není vyžadováno, a pokud k výměně dat nedojde, na výsledek roamingu to nebude mít zásadní vliv (tj. klient bez podpory IEEE 802.11k provede roaming standartním způsobem jako by v síti IEEE 802.11v implementován nebyl).

Standard IEEE 802.11v poskytuje klientovi rozšířené informace informace o fyzické vrstvě a MAC adresách AP a to včetně jejich vytíženosti. Standard přináší RTLS (Real Time Location Services), která umožňuje administrátorům sítě lepší lokalizaci klientů v síti. S tím je samozřejmě spojen i roaming, neboť WLAN jsou tak k dispozici přesnější data o poloze klienta.

Další prvek, který IEEE802.11v přináší je Wake-On-WLAN. Tato funkce umožňuje klientům výrazně zeslabit výkon vysílače a tím prodloužit životnost baterie. Na funkčnost roamingu Wake-On-WLAN vliv nemá (3 str. 141).

Pro funkčnost roamingových standardů je nutná podpora jak na straně AP (případně WLC) tak na straně klienta, kde ji zajišťuje OS s podporou ovladače Wi-Fi karty. Nelze tedy jen na základě použitého OS, konkrétní Wi-Fi karty, či typu AP říci, že podpora roaming standardů bude fungovat.

Pokud síť i klient dokáží využít 802.11k/r/v zkrátí se tak doba potřebná k roamingu i na několik milisekund. Což je zvláště žádoucí pro potřeby datových přenosů citlivých na výpadky jako jsou VoIP, či voice a video obecně.

4.1.4 Shrnutí

V následujícím shrnutí jsou uvedeny hlavní body kapitoly:

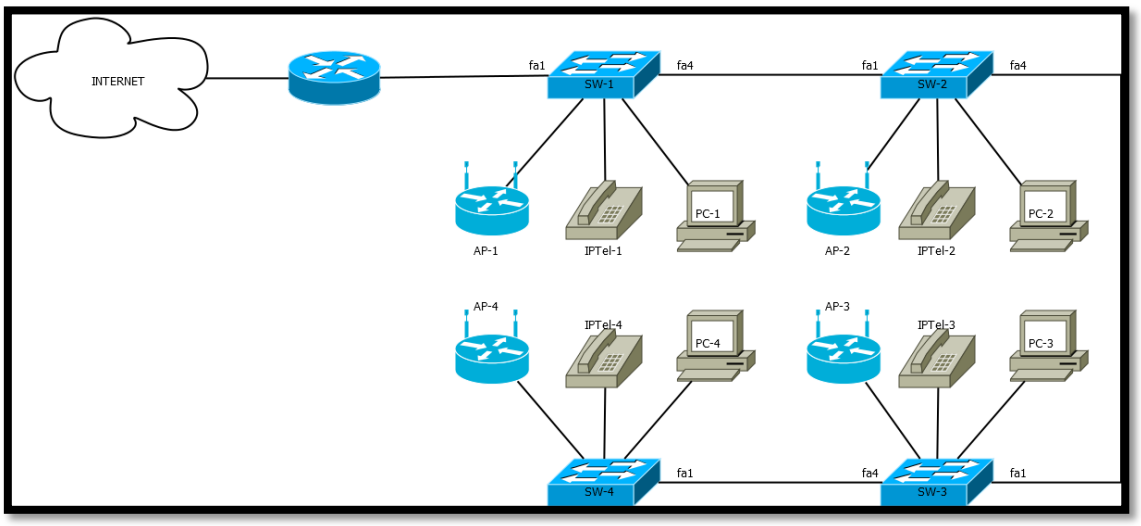
- Ve Wi-Fi sítích je za přechod od jednoho Wi-Fi přístupového bodu k druhému plně zodpovědný klient.
- Ochotu klienta k roamingu lze ovlivnit nastavením parametrů WLAN karty
- WLAN kontroler může klienta donutit k roamingu jednostranným odpojením od sítě
- standardy IEEE802.11k, IEEE802.11r a IEEE802.11v mohou klientovi poskytnout dodatečné informaci o struktuře WLAN sítě, jejím vytížení a urychlit proces autorizace.

4.2 L2 roaming ve Wi-Fi sítích – z pohledu toku dat sítí

Problematika odpojování a opětovné připojování klientů však není jediným problémem se kterým je třeba se v rámci Wi-Fi roamingu vypořádat. Dalším důležitým bodem řešení roamingu je řešení toku dat sítí. Tento bod bývá v implementacích často opomíjen a právě i z tohoto důvodu bych se na něj chtěl v této práci soustředit.

4.2.1 Změny toku dat v síti při roamingu klienta

Podívejme se na datové toky na jednoduchém modelu sítě. Zde uvedený model sítě se skládá ze 4 PC, 4 IP telefonů, 4 Wi-Fi přístupových bodů, 4 přepínačů (switchů) a jednosho směrovače (routeru) připojeného do internetu.



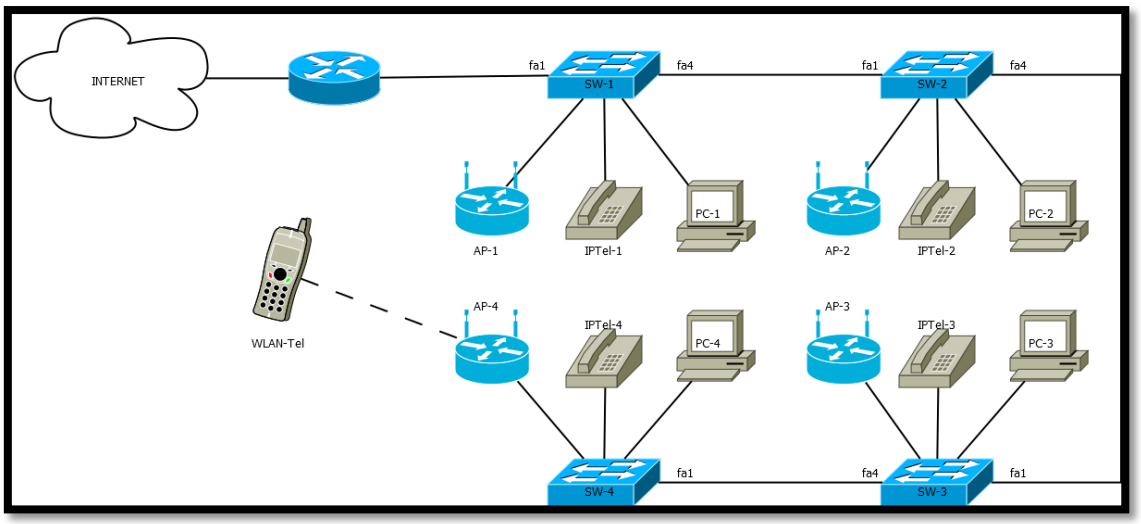
Obrázek 12 - schéma sítě (23)

Pokud se zaměříme pouze klientská PC, pak nás asi nijak nepřekvapí, jak datové toky v takové síti probíhají. Bude to vždy z PC do nejbližšího switche SW a ze switche, pak portem fa1 do dalšího switche, nakonec do routeru a do internetu. V takovémto zapojení je cesta paketů pevně daná. Pakety vždy dorazí v do routeru v pořadí, v jakém je PC odešle do sítě.

Pokud přidáme IP telefony a správně dopolníme konfigurace switchů o značkování a prioritizaci packetů QoS, máme tu již složtější situaci. Ale i v takovém případě, by packety dorazily na switch vždy v očekávaném pořadí. Jediné co by se mohlo stát, že packety z IPtelefonů za určitých okolností předběhnou packety z PC. Na pořadí v jakém packety z konkrétního zařízení dorazí na router, to však nebude

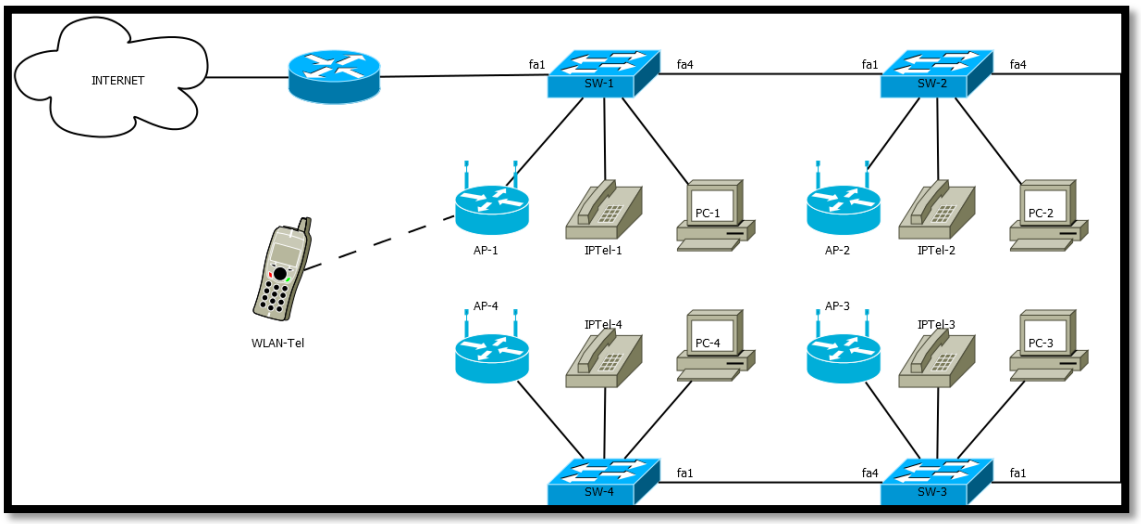
mít vliv. Jinak řečeno packety z IPTel-4 dorazí na roter ve stejném pořadí jak je IPTel-4 odeslal, bez ohledu na to zda na switchi „předbehnou“ packety z PC-4. A i packety z PC-4 dorazí na router ve shodném pořadí, jak byly odeslány, bez ohledu na to zda byly předběhnuty pakety s vyšší prioritou.

Jiná situace však nastává u Wi-Fi. Zde je příklad telefonu, připojeného na Wi-Fi a uskutečňujícího hlasový hovor. Data z tohoto telefonu jsou cestou **WLAN-Tel -> AP-4 -> SW-4 -> SW-3 -> SW-2 -> SW-1 -> router**. Do routeru dorazí ve shodném pořadí, v jakém byla odeslána z telefonu.



Obrázek 13 - schéma sítě (23)

Pokud však WLAN-Tel telefon přejde od AP-4 k AP-1 cesta odesílaných packetů se náhle zkrátí na pouhé **WLAN-Tel -> AP-4 -> SW-1 -> router**.



Obrázek 14 - schéma sítě (23)

Může tak dojít k tomu, že data, která byla odeslána dříve, dorazí do cíle později než data, která byla odeslána až po nich. V běžném datovém provozu takovéto nedodržení pořadí nepředstavuje až takový problém. Data (pokud využívají TCP) mohou být sestavena znovu ve správném pořadí. U přenosu hlasu je však situace poněkud jiná. Na rozdíl od dat je přenos hlasu vysoce citlivý jak na zpoždění, tak hlavně na pořadí jednotlivých paketů, zároveň však využívá pro transport UDP protokol, který neumožňuje opravit pořadí (24).

4.2.2 Způsoby řízení Wi-Fi sítě a jejich vliv na roaming a tok dat sítí

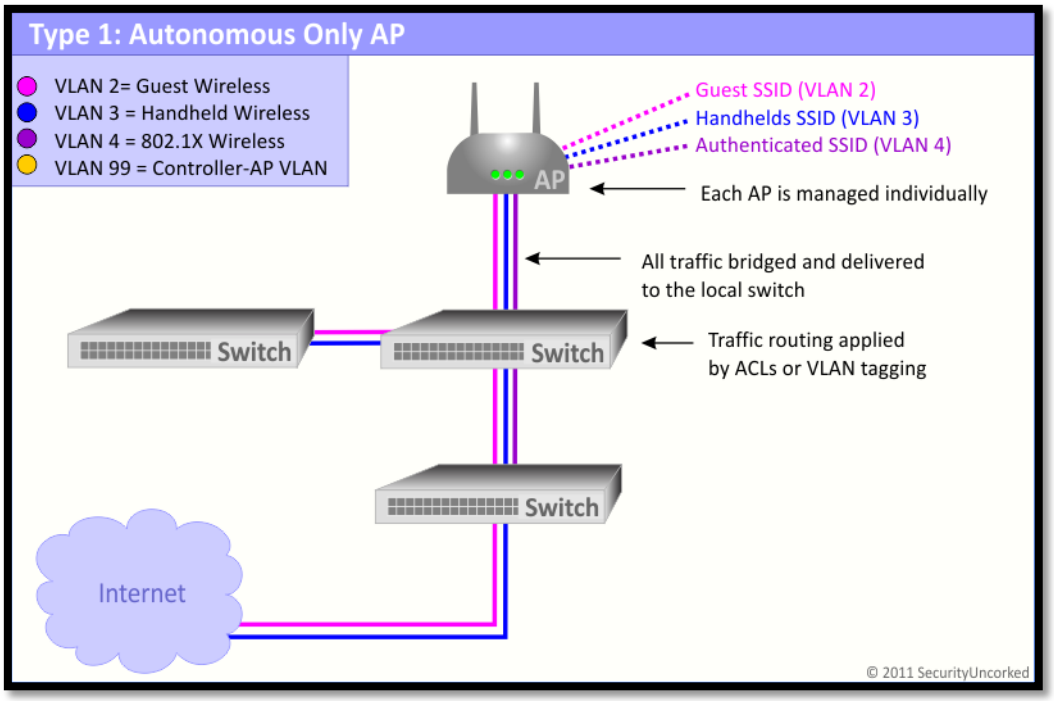
Z pohledu řízení AP a tím pádem i řízení roamingu, včetně řízení datových toků v síti můžeme nalézt čtyři různé scénáře (25):

- Wi-Fi síť využívající autonomní AP
- Wi-Fi síť řízená kontrolerem pouze s řízením AP
- Wi-Fi síť řízená kontrolerem s tunelováním datového provozu
- Wi-Fi síť řízená kontrolerem s kombinovaným provozem

Zde jsou jednotlivé scénáře popsány podrobněji.

4.2.2.1 Wi-Fi síť využívající autonomní AP

Je sítí s plně autonomními AP bez Wi-Fi kontroleru. Je to nejstarší způsob řešení, který se uplatňuje i dnes, převážně v malých sítích, kde není třeba Wi-Fi roaming příliš řešit. AP v tomto systému nazýváme „stand-alone“ a jsou to autonomní AP vybavená všemi funkcemi nutnými pro asociaci, zabezpečení a samostatný provoz. Pro AP je možné přidat SSID do konkrétní VLAN pomocí webového rozhraní, či příkazové řádky (dle typu AP). Každé AP má své vlastní řízení a je nutné nastavovat konfiguraci SSID, zabezpečení a pravidel firewallu na každém AP samostatně, samozřejmě s ohledem na vysílací výkon a kanály využívané ostatními autonomními AP (26).



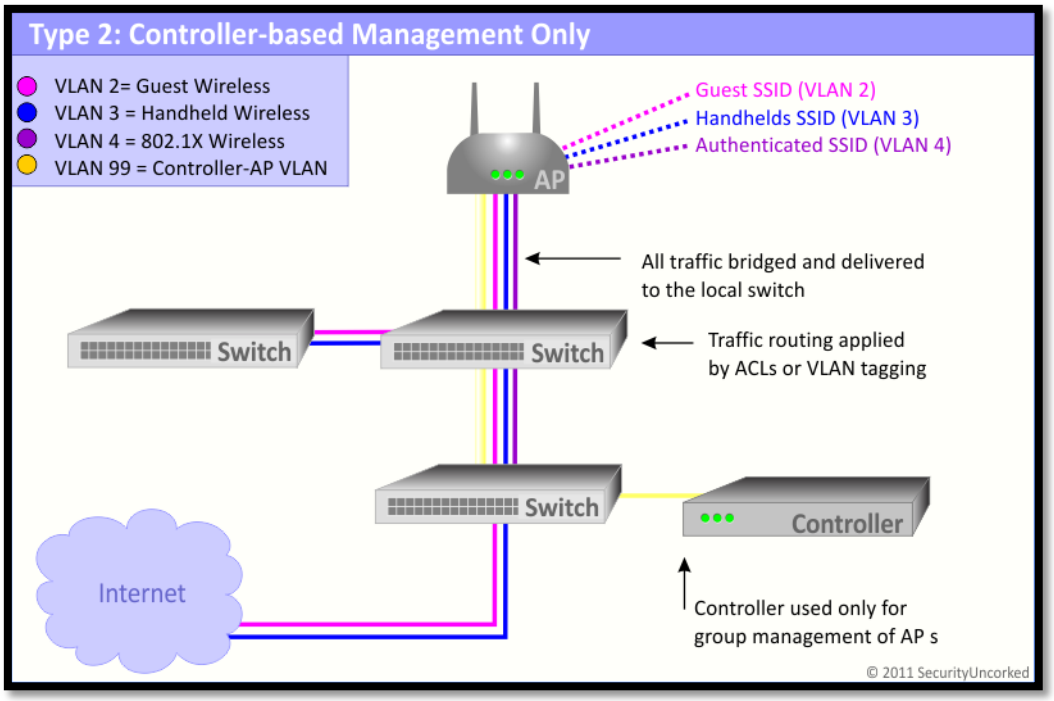
Obrázek 15 - autonomní AP (25)

Wi-Fi Roaming na takovéto síti není nijak řízen, je zcela na klientovi jak se asociuje k novému AP. Standardy IEEE 802.11k/r/v v této síti nejsou využívány, neboť každé AP zajišťuje pouze svůj vlastní provoz včetně asociace. Data od klientů do této sítě přichází podobně jako by přicházely z jiného přepínače, či směrovače, kdy každé SSID odpovídá jedné VLAN. Případné zabezpečení izolace klientů, taktéž optimalizace průchodů packetů sítí je nutno řešit na přepínačích, či směrovačích sítě (27 str. 162).

Takováto architektura vyniká jednoduchostí a cenou. Pro absenci centrálního řízení však není vhodná pro rozsáhlejší instalace, nebo instalace kde je třeba řešit rychlejší reasociaci Wi-Fi klientů při roamingu.

4.2.2.2 Wi-Fi síť řízená kontrolerem pouze s řízením AP

Je sítí s AP řízenými Wi-Fi kontrolerem, který za jednotlivé AP řeší vhodné nastavení vysílacích kanálů, nastavení vysílacího výkonu, řeší i asociaci klientů, včetně nastavení bezpečnosti a rozložení zátěže. Samotná AP pak pouze přenáší datový provoz do VLAN na základě konfigurace, kterou jim poskytne Wi-Fi kontroler (28 stránky 301-305).



Obrázek 16 – kontroler řídící AP (ne provoz) (25)

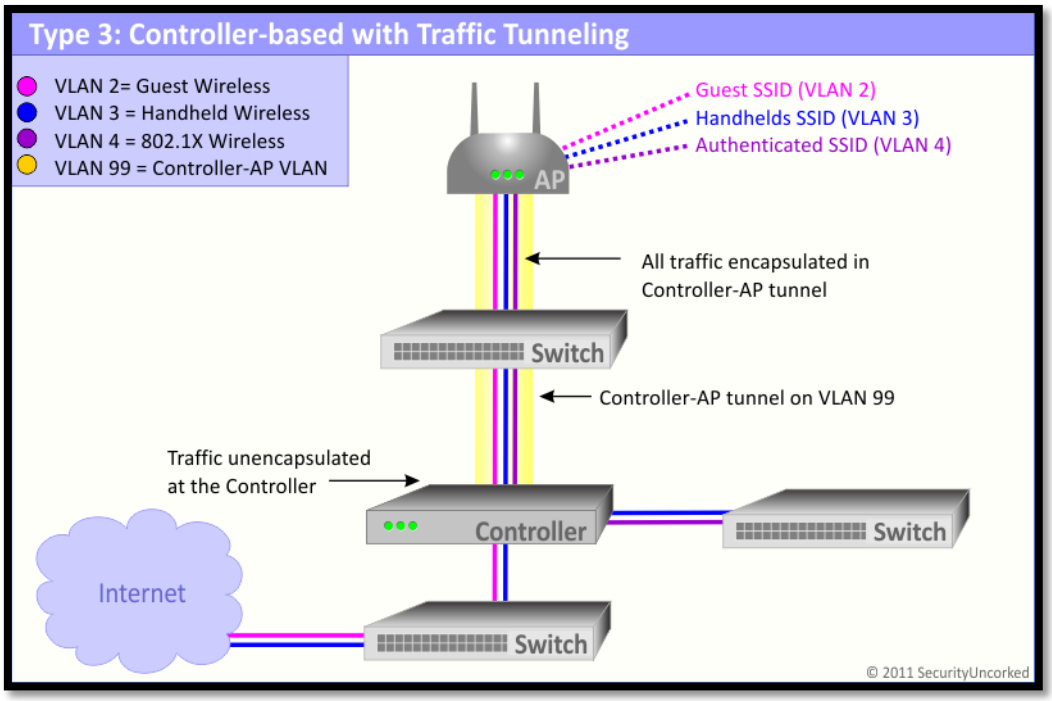
Wi-Fi roaming v takovéto síti je řízen kontrolerem jako centrálním prvkem sítě. Standardy IEEE 802.11k/r/v v takovéto síti mohou být využívány, neboť kontroler má k dispozici informace o klientech z jednotlivých AP. Data od klientů do této sítě však stále přicházejí podobně, jako by přicházely z jiného přepínače, či směrovače, kdy každé SSID odpovídá jedné VLAN. Případné zabezpečení izolace klientů, taktéž optimalizace průchodů packetů sítí je nutno řešit na přepínačích, či směrovačích sítě. Této architektury využívají např.: Cisco Mobilty Express, Aruba instant, Ruckus ZoneDirector, či Unifi, nebo Mikrotik Capsman.

Takováto architektura neklade velké nároky na HW Wi-Fi kontroleru, který tak někdy může být i součástí AP. Síť však stále nedokáže zajistit správné pořadí packetů a není proto vhodná pro nasazení pro služby jako VoIP, či voice a video obecně.

4.2.2.3 Wi-Fi síť řízená kontrolerem s tunelováním datového provozu

Je nejstarším způsobem používaným v sítích řízenými Wi-Fi kontrolerem. Wi-Fi kontroler zde nejen řeší za jednotlivá AP vhodné nastavení vysílacích kanálů, nastavení vysílacího výkonu, asociaci klientů, nastavení bezpečnosti a rozložení zátěže, ale přebírá i samotný datový provoz. Kontroler s jednotlivými AP udržuje

komunikaci pomocí zabezpečených CAPWAP tunelů. Do tunelů je směřována nejen režijní komunikace Wi-Fi sítě zahrnující nastavení AP, počty klientů, předávání asociací klientů, ale i samotný datový provoz, který klient se sítí vytváří (28 str. 21).



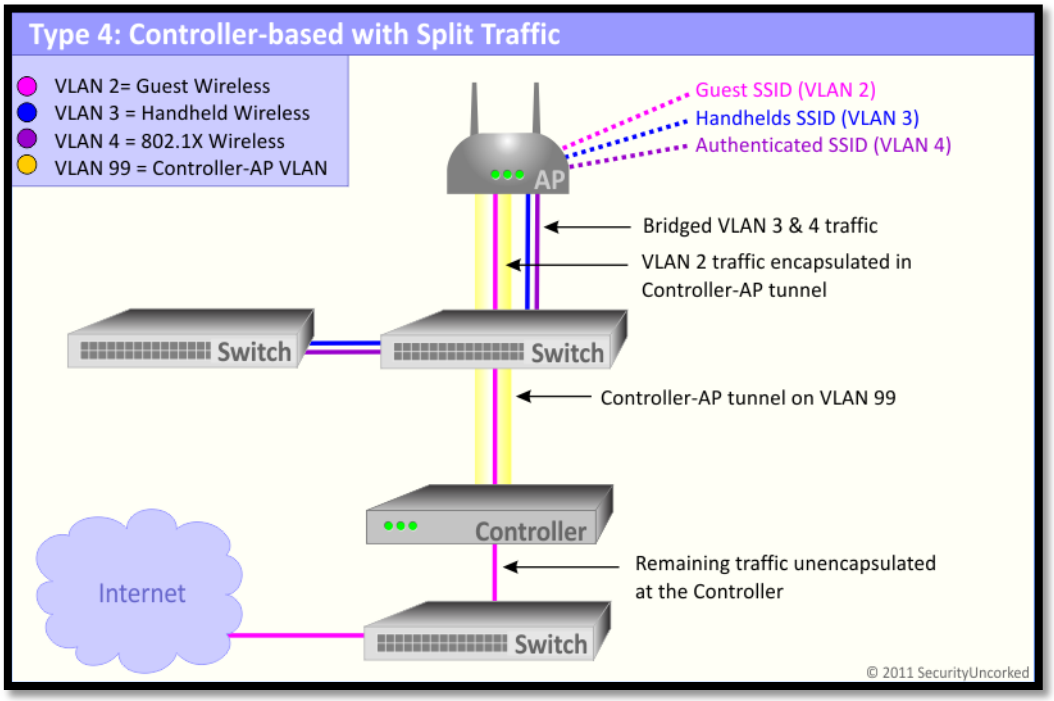
Obrázek 17 - kontroler s AP i provozem (25)

Wi-Fi roaming v takovéto síti je řízen kontrolerem jako centrálním prvkem sítě. Standardy IEEE 802.11k/r/v v takovéto síti mohou být využívány, neboť kontroler má k dispozici informace o klientech z jednotlivých AP. Veškerá data od klientů v této síti pak putují do kontroleru, který je rozdělí do jednotlivých VLAN. Případné zabezpečení izolace klientů, jakož i správné pořadí packetů zde řídí kontroler, který je centrálním prvkem nejen řízení, ale i datového provozu sítě. Této architektury využívají např.: Cisco WLC, Aruba Mobility Controler, Ruckus ZoneDirector.

Takováto architektura klade velké nároky na HW Wi-Fi kontroleru, který tak je tak vždy samostatným zařízením v síti. Tím, že veškerý Wi-Fi datový provoz je zpracováván kontrolerem musí mít kontroler k dispozici dostatečný výpočetní výkon pro balení a vybalování datového provozu z VLAN do CAPWAP tunelů a naopak. Navíc vzniká nutnost dostatečně rychlého připojení kontroleru do sítě.

4.2.2.4 Wi-Fi síť řízená kontrolerem s kombinovaným provozem

Je sítí s AP řízenými Wi-Fi kontrolerem, který za jednotlivé AP řeší vhodné nastavení vysílacích kanálů, nastavení vysílací ho výkonu, řeší i asociaci klientů a nastavení bezpečnosti a rozložení zátěže. Samotná AP pak pouze přenáší datový provoz do VLAN, nebo jej směřují do CPAWAP tunelu na základě konfigurace, kterou jim poskytne Wi-Fi kontroler.



Obrázek 18 - kontroler s kombinovaným provozem (25)

Wi-Fi roaming v takovéto síti je řízen kontrolerem jako centrálním prvkem sítě. Standardy 802.11k/r/v v takovéto síti mohou být využívány, neboť kontroler má k dispozici informace o klientech z jednotlivých AP. Data pak putují buď přímo do sítě, nebo do kontroleru na základě konfigurace jednotlivých WLAN. Může tak být využita jak přenosová rychlost sítě včetně využití QoS, bezpečnosti, či směrování, tak centrální řízení a řazení dat Wi-Fi kontrolerem. Této architektury využívají např.: Aruba Mobility Controler, Ruckus ZoneDirector, Cisco WLC/FlexConnect.

Takováto architektura klade vyšší nároky na přípravu a konfiguraci jednotlivých WLAN, zaručuje však nejlepší možné využití prostředků přepínačů a směrovačů, při současném udržení vysoké kvality VoIP a obecně voice služeb.

4.2.3 Shrnutí

Následující tabulka shrnuje a srovnává možné toky dat WLAN a LAN sítí:

Tabulka 2 - toky dat WLAN a LAN sítí

	Wi-Fi síť využívající autonomní AP	**Wi-Fi síť řízená kontrolerem pouze s řízením AP**	**Wi-Fi síť řízená kontrolerem s tunelováním datového provozu**	**Wi-Fi síť řízená kontrolerem s kombinovaným provozem**
Umožňuje řízení roamingu	**NE**	**ANO**	**ANO**	**ANO**
Umožňuje podporu IEEE802.11k/r/v	**NE**	**ANO**	**ANO**	**ANO**
Zapouzdřuje provoz	**NE**	**NE**	**ANO**	**Částečně***
Vhodná pro datový provoz	**ANO**	**ANO**	**Částečně****	**ANO**
Vhodná pro hlas a video	**NE**	**NE**	**ANO**	**ANO**
Náročnost konfigurace	**Střední*****	**Střední*****	**Snadná**	**Náročná*****

* Zapouzdření se týká pouze vybraných BSSID.

** Veškerá data musí putovat LAN sítí do kontroleru a následně zpět do LAN sítě. Hrozí vznik úzkého hrdla.

*** Na portech přepínačů, ke kterým jsou připojeny přístupové body, musí být konfigurovány VLAN a bezpečnost pro každý port zvlášť.

5 Praktická část

5.1 Měření a data

Pro praktické ověření vlivu jednotlivých faktorů na rychlost roamingu klienta a tok dat sítí byly zvoleny tři scénáře, ve kterých byl testován vliv protokolů IEEE 802.11 k/r/v a na rychlost roamingu a tedy především reasociace klienta, dále podpora roamingu ze strany výrobců WLC (zde se jedná především o nastavení vynucování reasociace) a také měření toku dat sítí při různých scénářích.

5.1.1 Wi-Fi síť řízená kontrolerem s kombinovaným provozem

Jako prostředí pro scénáře byl zvolen rodinný dům osazen třemi Wi-Fi přístupovými body. Přístupové body Wi-Fi byly rozmístěny tak aby pokryly celý prostor sílou signálu -65dB jak v pásmu 2,4GHz, tak v pásmu 5GHz. Takováto síla signálu zajistí stabilní přenos dat bez nutnosti nadměrně zatěžovat provoz režijními a opravnými packety. Zároveň byly zajištěny dostatečné překryvy signálů jednotlivých přístupových bodů. Při umístění byla zohledněna doporučení výrobců (3 stránky 153-182) (29) (30).

Kompletní mapu pokrytí prostoru signálem je dispozici v příloze, která obsahuje celkovou heatmapu pokrytí pro každý ze tří použitých scénářů.

Jednotlivé scénáře pak představují měření dle zadání práce. Jedná se tedy o měření možností roamingu v sítích Wi-Fi nastavených podle „best practice“ jednotlivých výrobců (21) (29) (30) (31) (32) (33) (34) (35) (36). Jedná se tedy především o měření přechodu mezi jednotlivými přístupovými body v těchto prostředích:

A. Síť se samostatnými Wi-Fi přístupovými body, bez centrálního řízení.

- Tato síť reprezentuje scénář většiny domácností (či malých firem) vybavených více než jedním Wi-Fi přístupovým bodem, avšak bez centrálního řízení. Jednotlivé Wi-Fi přístupové body tak o sobě nevědí, nesdílí informace o vysílané síti ani o připojených klientech.
- Výhody této architektury plynou především z její jednoduchosti a cenové nenáročnosti. Díky absenci řídícího prvku je snížený počet tzv „single point of failure (31)“ které představují riziko zastavení celého systému – v našem případě Wi-Fi sítě.

- Nevýhody jsou pak reprezentovány zejména nutností konfigurace každého prvku samostatně, nemožnost sdílení informací o výkonu, asociacích, vytíženosti, rušení nebo např. o existujících klientech (32).

B. Síť s využitím Wi-Fi kontroleru Cisco WLC2504

- Tato síť reprezentuje typický scénář sítě s centrálním řízením, kdy jednotlivé přístupové body jsou řízeny centrálním prvkem, který spravuje jak asociace klientů, řízení výkonu, ale i celý datový provoz Wi-Fi sítě.
- Výhody toho řízení jsou především v kompletním a úplném přehledu o Wi-Fi síti a to jak o konfiguraci přístupových bodů, tak o toku dat sítí. Jednotné řízení tak umožňuje síť nastavit prakticky okamžitě bez nutnosti konfigurace portů switchů a přesto s využitím služeb jako jsou např. QoS (33).
- Nevýhodu představuje zařazení tzv „single point of failure (31)“ do sítě, kdy výpadek kontroleru má za následek nefunkčnost celé Wi-Fi sítě. Dalším probléme je zdvojení provozu sítě na interface, kterým je kontroler připojen do sítě. K tomuto dochází v důsledku využití tunelovaného provozu. Data pro Wi-Fi tak musí nejprve do kontroleru (první průchod), kde jsou zabalena do tunelovaného provozu a odeslána na příslušné AP (druhý průchod). Pro připojení kontroleru se tak doporučuje využít více fyzických interface, nebo kontroler připojit rychlejším logickým portem např. s využitím tzv. eterchannel (33).

C. Síť s využitím Wi-Fi kontroleru Ruckus ZoneDirector 1106

- Tato síť reprezentuje řízení sítě kontrolerem, avšak bez tunelování datového provozu. Kontroler tak pouze řídí Wi-Fi přístupové body, asociaci klientů, řízení výkonu, či rozložení zátěže, nijak však nezasahuje do vlastního průchodu dat sítí.
- Výhodou tohoto řešení je snížená náročnost na výkon kontroleru (nemusí tak balit celý Wi-Fi provoz do tunelů a posílat jej na jednotlivá AP), možnost optimalizovat průchod tad sítí na základě pravidel a tříd QoS již existujících na switchích. Při výpadku kontroleru pak typicky nedochází k vypnutí celé Wi-Fi sítě, ale pouze k omezení funkčnosti (omezení se týka funkcí které ma

na starosti kontroler, typicky tedy asociace nových klientů, přeladění radií a reakce na změny v rádiovém provozu atd. – přenos dat u stávajících klientů zůstává většinou bez dopadu)

5.1.1.1 Měřené hodnoty

Cílem měření je zjistit, ve kterém ze scénářů bude Wi-Fi roaming fungovat nejlépe, tj. tak aby přechod klienta z jednoho přístupového bodu na druhý byl co nejplynulejší. Měření se tedy zaměřuje na dvě hodnoty. Jsou to:

A. **Měření rychlosti reasociace**. Zde je měřen ICMP PING klienta v 0,5sec intervalech a současně případné výpadky packetů. Jako nejlepší výsledky, jsou hodnoceny ty, u kterých došlo k nejmenším (pokud možno neměřitelným) výpadkům či zpomalení ICMP PINGů.
B. **Měření datového toku.** Zde je měřena rychlost datového toku mezi klientem a serverem připojeným kabelovým Cat5e připojením v síti. Měření datového toku je prováděno v obou směrech v protokolech TCP i UDP. Jako nejlepší výsledky, jsou hodnoceny ty, u kterých došlo k nejmenšímu poklesu rychlosti datového toku.
C. **Měření místa roamingu.** Zde je měřeno kde přesně k reasociaci klienta dochází. Jako nejlepší výsledky jsou hodnoceny ty, kdy klient zůstává na nejlepším možném signálu.

5.1.1.2 Wi-Fi klient a síťový server

Pro měření byl použit Wi-Fi kliet na straně bezdrátového provozu a server s kabelovým připojením v síti. Přičemž klient se pohybuje mezi jednotlivými přístupovými body a server je na pevném místě v síti. Klient kontroluje, zda je pro něho server dostupný pomocí ISMP PINGu a zároveň klient a server odesílají a přijímají TCP a UDP data. Pro Wi-Fi klienta a server v síti byl použitý následující hardware:

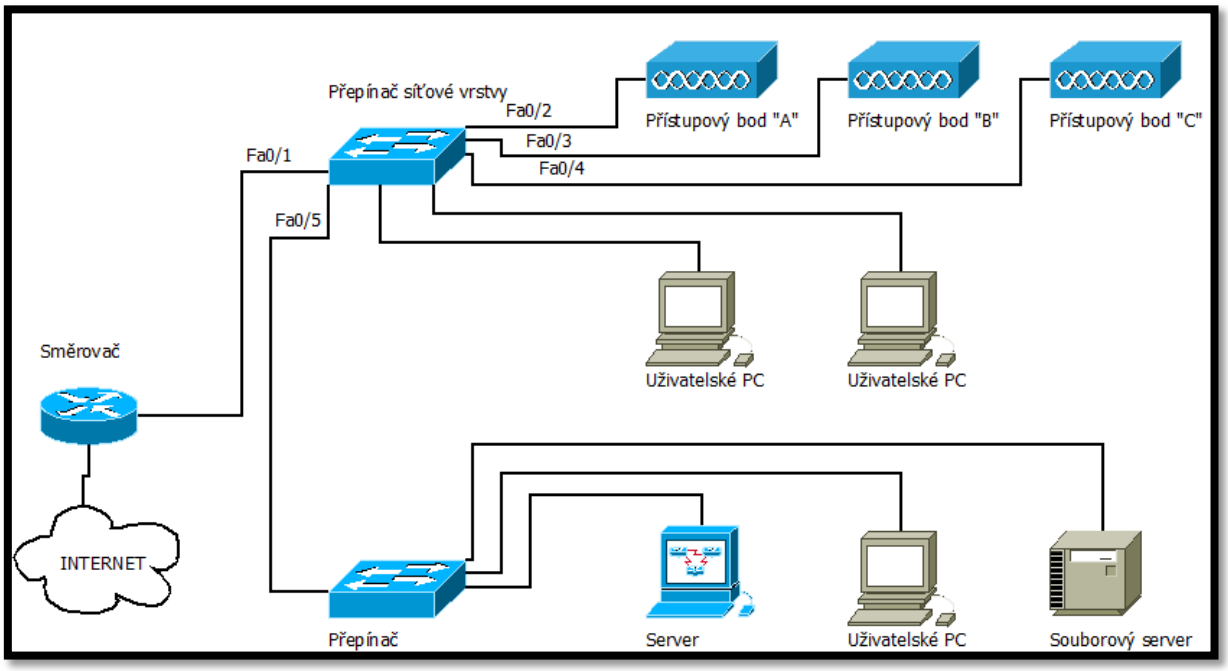
- **Wi-Fi klient.** Byl vyžit notebook Lenovo Yoga s operačním systémem Windows 10 Professional, vybaven síťovou kartou Intel Dual Band Wireless-AC 7260 s aktuálními ovladači verze 17.15.0.5.

- **Server v síti.** Byl využit PC s operačním systémem „Windows 10 Professional 64bit“, vybaven síťovou kartou „NVIDIA nForce Networking Controler“ s ovladači verze 7.3.1.7336.

Na klientu ani na serveru nejsou aktivní žádné další programy či služby využívající síť. Oba počítače pracují s posledními aktualizacemi Windows.

5.1.1.3 Topologie LAN sítě a síťový hardware

Pro měření Wi-Fi roamingu všech scénářů byla použita shodná LAN síť menšího rozsahu, tak aby co nejvíce odpovídala domácí síti, či síti v malé firmě. LAN Síť tak obsahuje směrovač, řiditelný přepínač, přepínač, server, souborový server a několika uživatelskými PC. Prvky sítě jsou zapojeny podle následující topologie:



Obrázek 19 - topologie sítě LAN (23)

Jednotlivé prvky v LAN síti jsou tyto:

- **Směrovač**. Jako směrovač sítě je využit router Cisco 881 s Cisco IOS Software verze 12.4(24)T3 release (fc2)
- **Přepínač síťové vrstvy**. Jako páteřní switch v síti je použit switch Cisco Catalyst WS-C3560-8PC. Přepínač slouží zároveň k připojení a napájení Wi-Fi přístupových bodů dle standardu 802.11af (PoE) (34).

- **Přepínač**. Jako koncový switch je v síti požit switch Cisco SG100-16 (35).
- **Server**. Byl využit PC s operačním systémem „Windows 10 Professional 64bit“, vybaven síťovou kartou „NVIDIA nForce Networking Controler“ s ovladači verze 7.3.1.7336. Server v síti udržuje TCP AUD komunikaci s Wi-Fi klientem a slouží k testu dostupnosti.
- **Souborový server**. Souborový server je zastoupen NAS zařízením Zyxel IX2. (Toto zařízení do měření a tesů nijak nezasahuje).
- **Uživatelská PC**. Jednotlivé další počítače v síti jsou představovány PC s operačním systémem Windows 10. (Tato zařízení do měření a tesů nijak nezasahují).

LAN síť je statická a mezi jednotlivými měřeními ani mezi jednotlivými scénáři nebyla síť nijak měněna. Výjimku tvoří připojení prvků WLAN do LAN sítě. Souborový server a uživatelská PC do datových toků mezi Wi-Fi klientem a serverem nijak nezasahují. V nákresu sítě jsou tato zařízení označena jako šedá. Wi-Fi přístupové body jsou během měření napájeny z řízeného přepínače dle standardu 802.11af (PoE).

5.1.2 Použitý hardware WLAN bezdrátové sítě a jeho nastavení

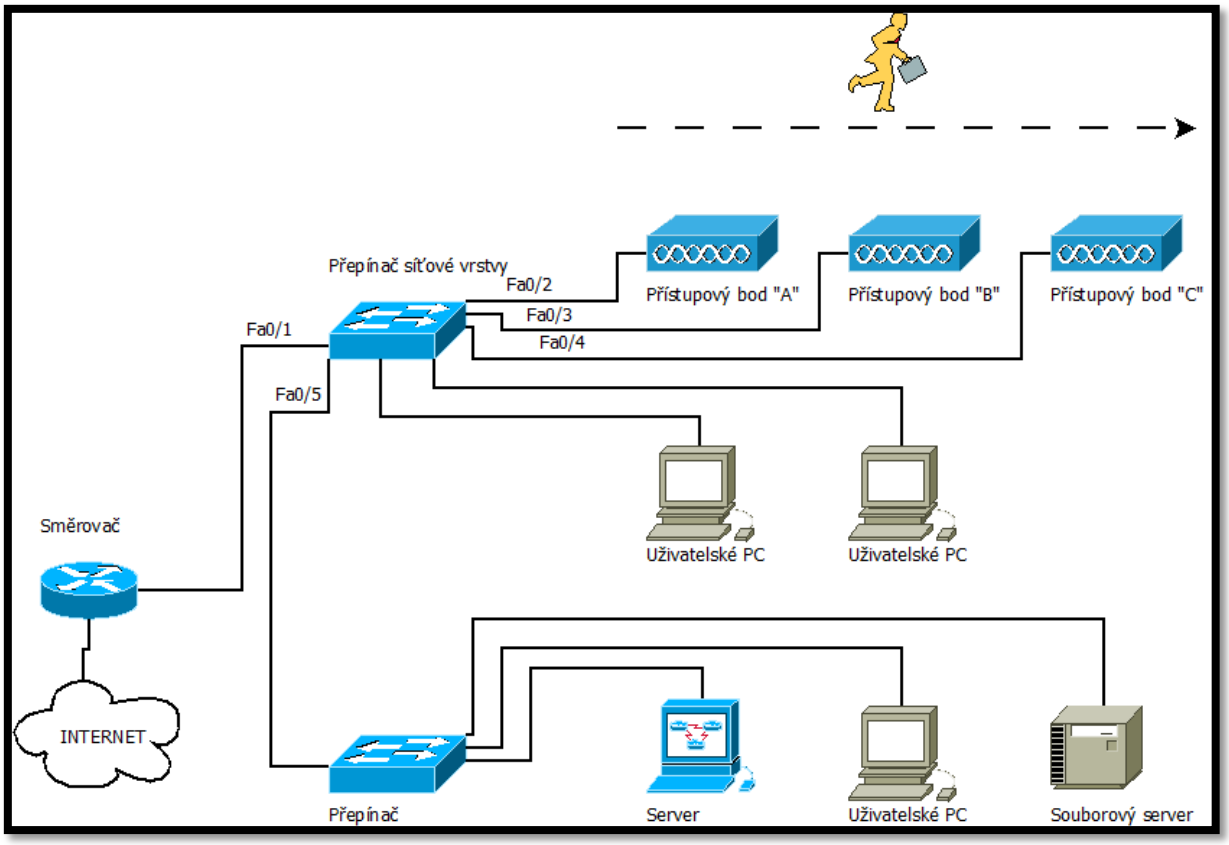
Jako použitý hardware bezdrátové sítě WLAN je označen takový hardware, který přímo souvisí s chodem bezdrátové sítě. Tedy jednotlivé Wi-Fi přístupové body, případně kontrolery, pokud jejich nasazení scénář vyžadoval. Prvky WLAN bezdrátové sítě byly přidány do LAN sítě a připojeny do portů řiditelného přepínače (páteřní switch).

Nastavení a konfigurace jednotlivých prvků WLAN byly provedeny vždy podle doporučení výrobce pro co nejlepší chod sítě, případně pro optimalizaci Wi-Fi roamingu (21) (29) (30) (31) (32) (33) (34) (35) (36).

Použitý hardware WLAN sítí rozdělený dle využití v jednotlivých scénářích:

5.1.2.1 Síť se samostatnými Wi-Fi přístupovými body, bez centrálního řízení

Síť vychází ze scénáře „Síť se samostatnými Wi-Fi přístupovými body, bez centrálního řízení“ a její topologie je navržena takto:



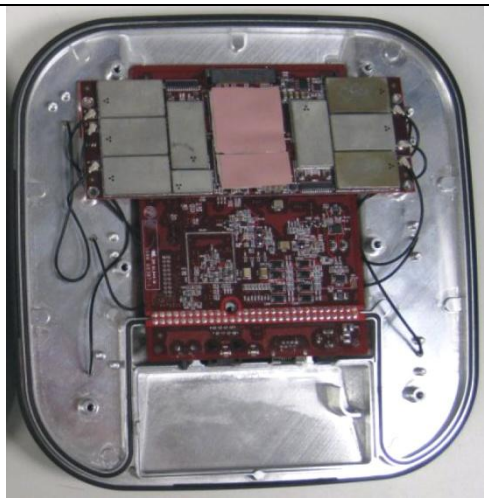
Obrázek 20 - topologie sítě se samostatnými AP (23)

Pro síť s využitím plného tunelovaného provozu (řízení i dat) byl zvolen tento hardware:

- **Wi-Fi přístupový bod: Cisco Aironet SAP1142i**

  Wi-Fi přístupový bod Cisco řady 1140 představuje jednoduchý Wi-Fi přístupový bod pracující v pásmech popsaných standardy 802.11a/g/n. Cisco Aironet 1142i umožňuje pracovat jak s 20MHz, tak i s 40MHz kanály (v měření jsou vždy použity pouze 20MHz kanály), disponuje dvěma anténami na straně vysílače, třemi anténami na straně přijímače a umožňuje zpracovávat dva datové kanály (2x3:2 MIMO). Umožňuje připojení klienta maximální rychlostí 300 Mbps (36).

Obrázek 21 - Cisco Aironet 1142i – antény (37)



Obrázek 22 - Cisco Aironet 1142i - mainboard (37)

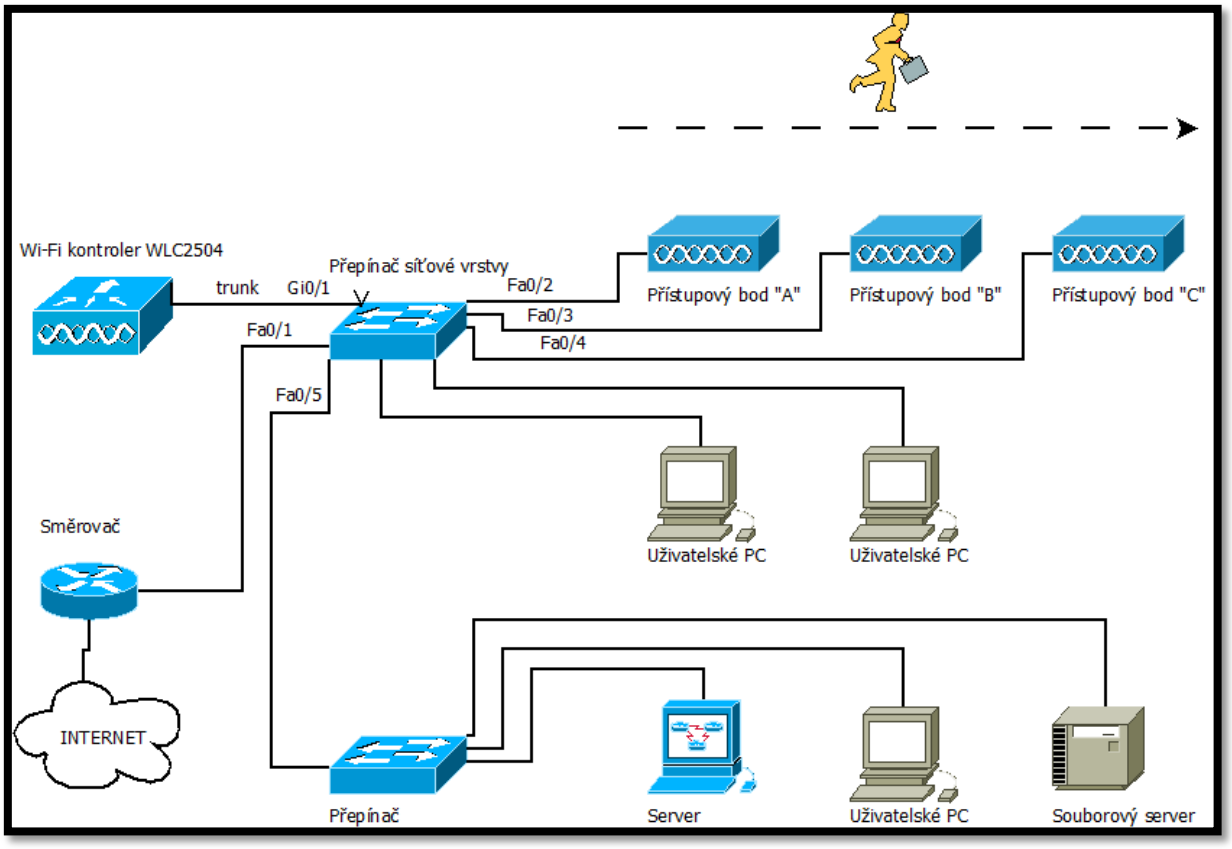
Wi-Fi přístupový bod Cisco Aironet 1142i pro účely měření pracuje s verzí firmware 15.3.3-JD13. Je nakonfigurováno vysílání pouze jedno BSSID pojmenovaného „TEST-Cisco-SAP1142i“ se zabezpečením WPA2-PSK Wi-Fi přístupové body mají oproti továrnímu nastavení upravena tato nastavení:

- Výběr kanálů v pásmu 2,4GHz omezen na výběr z kanálů 1,6 a 11
- AP mají nastaveno vypnutí rádií, pokud ztratí link na ethernetovém portu

Konfigurace přístupových bodů vychází z dokumentu „Cisco IOS Configuration Guide for Autonomous Cisco Aironet Access Points“ (27) a její kompletní výpis je k dispozici uveden v oddíle přílohy.

5.1.2.2 Síť s využitím Wi-Fi kontroleru Cisco WLC2504

Síť vychází ze scénáře „Síť s využitím Wi-Fi kontroleru Cisco WLC2504“ a její topologie je navržena takto:



Obrázek 23 - topologie sítě s kontrolerem Cisco 2504 (23)

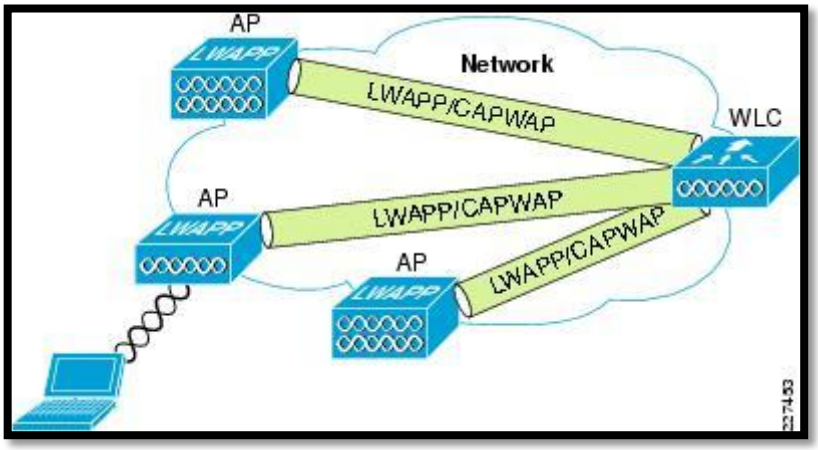
Pro síť s využitím plného tunelovaného provozu (řízení i dat) byl zvolen tento hardware:

- **Kontroler: AIR-CT2504-K9 – Cisco 2500 Series Wireless LAN Controller**

  Tento typ kontroleru je určen pro malé a střední podniky nebo pobočky. Pracuje se standardy 802.11n a 802.11ac. Jedná se o základní verzi kontrolerového řešení od společnosti Cisco. Kontroler řady 2500 umožňuje hlobkovou inspekci paketů pro klasifikaci splikac a propojení s kvalitou služeb QoS a tím umožňuje upřednostňovat kritické aplikace v síti. Kontroler Cisco 2504 může řídit síť až se 75 přístupovými body Cisco Aironet s připojeným až 1000 klientů. Umožnuje dále vytváření „Mobility Group“ tedy sdružování více kontrolerů Cisco do jedné skupiny tak, aby si předávaly informace o klientech a RF provozu. Z hlediska bezpečnosti splňují kontrolery řady 2500 certifikace PCI (architektura vhodná pro platební karty) a jsou tedy vhodné pro transakční datové aplikace (38).

- **Wi-Fi přístupový bod: Cisco Aironet LAP1142i**

  Z hlediska použitého hardware se jedná o shodný přístupový bod jako Cisco Aironet SAP1142i (36). Oba přístupové body se liší pouze použitým software. Cisco LAP1142i tak nevyužívá vlastní logiku k asociaci klientů, oproti tomu vytváří tunelovaný provoz s kontrolerem (39).



Obrázek 24 - schéma komunikace WLC a LAP

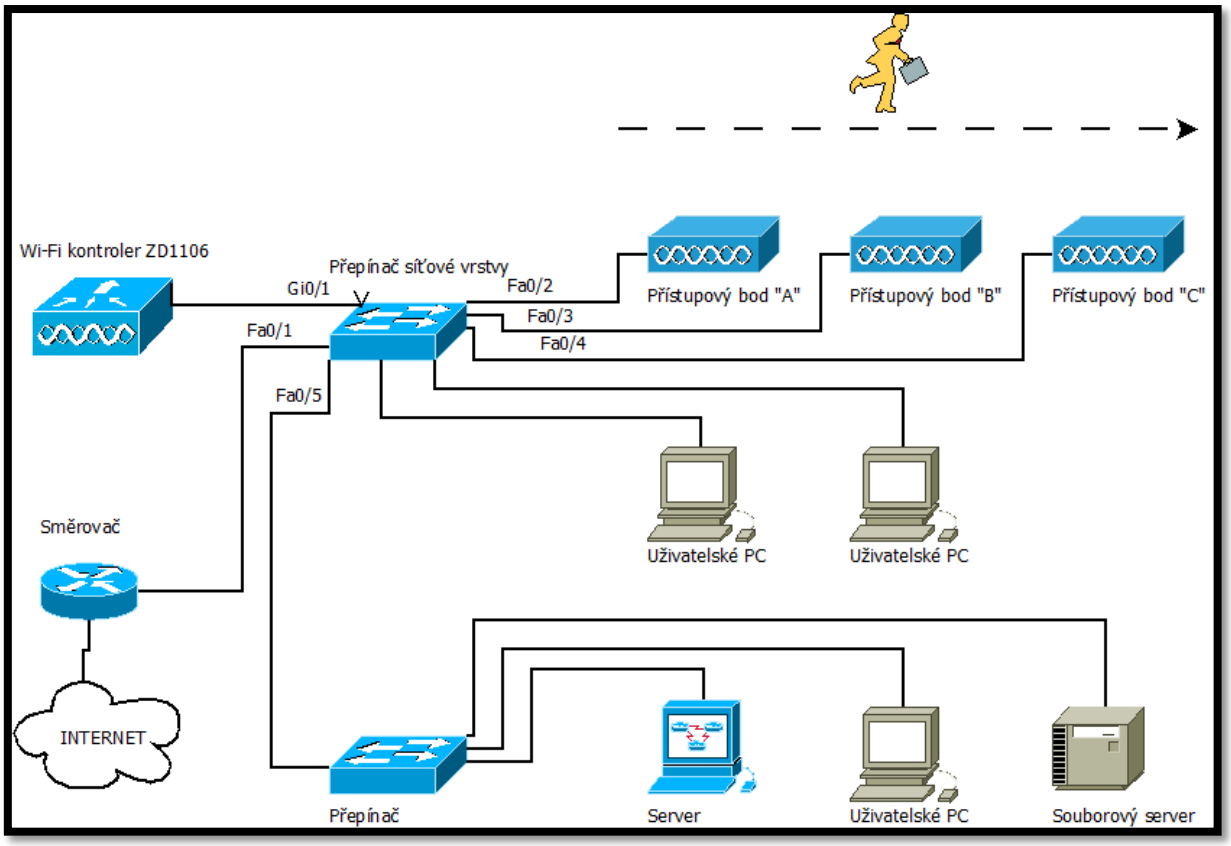
Kontroler Cisco 2504 pro účely měření pracuje s verzí firmware 8.3.133.0. Je nakonfigurováno vysílání pouze jedno BSSID pojmenovaného „TEST-Cisco-WLC2504“ se zabezpečením WPA2-PSK. Kontroler má oproti továrnímu nastavení upravena tato nastavení:

- WLANs > Edit > Advanced > 11k: Neighbor List ENABLE
- WLANs > Edit > Security > Layer2 > Fast trensmition ADAPTIVE
- WIRELESS > 802.11a/n/ac > Network > General: RSSI Threshold -65
- WIRELESS > 802.11a/n/ac > Client Roaming:
  - Minimim RSSI -59
  - Scan Treshold -45
  - Transition Time 1
- WIRELESS > Advanced > Optimized Roaming > 802.11a:
  - Enable
  - Interval 5
  - Data Rate Treshold 54mbps

Konfigurace kontroleru Cisco 2504 vychází z dokumentu „Enterprise Best Practices for iOS devices and Mac computers on Cisco Wireless LAN“ (40), „802.11r, 802.11k, and 802.11w Deployment Guide“ (21), „Wireless LAN Controller (WLC) Design“ (39), „Enterprise Mobility 8.5 Deployment Guide“ (33). Úplný výpis konfigurace je uveden v oddíle přílohy.

5.1.2.3 Síť s využitím Wi-Fi kontroleru Ruckus ZoneDirector 1106

Síť vychází ze scénáře „Síť s využitím Wi-Fi kontroleru Ruckus ZoneDirector 1106“ a její topologie je navržena takto:



Obrázek 25 - topologie sítě s kontrolerem Ruckus ZoneDirector 1106 (23)

Pro síť s využitím bez tunelování datového provozu, ale s řízením přístupových bodů kontrolerm byl zvolen tento hardware:

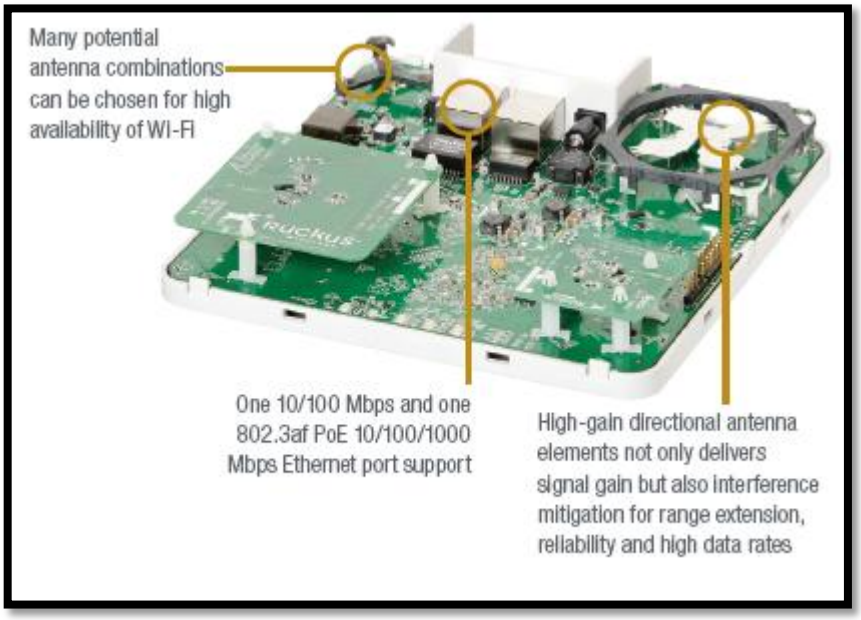
- **Kontroler: Ruckus ZoneDirector 1106**

  Ruckus ZoneDirector řada Wi-Fi kontrolerů od společnosti Ruckus. Kontrolery ZoneDirectory vynikají jednoduchostí obsluhy i snadností prvotní instalace. Je určen pro malé a střední podniky, kterým nabízí

pokročilé funkce centralizované správy Wi-Fi bez složité administrace. Kontroler umí pracovat se všemi Wi-Fi přístupovými doby Ruckus ZoneFlex (v závislosti na použitém fw) a oproti kontrolerům vyžších řad je tak omezen pouze svým výpočetním výkonem. Kontroler podporuje až 128 WLAN, Smart Mesh, QoS s WLAN prioritizací a má přednastavený captive portál pro využití s hostovskou WLAN. Kontroler využívá technologii BeamFlex a technologii SmartRoam. (41) Technologie SmartRoam by měla napomoci hladšímu přechodu klietů z jednoho AP na druhé díky sledování signálu klientů (42).

- **Wi-Fi přístupový bod: ZoneFlex 7372 Access Point**

  Wi-Fi přístupový bod Ruckus ZoneFlex 7372 je Wi-Fi přístupový bod střední třídy. Pracující v pásmech popsaných standardy 802.11a/g/n. Umožňuje pracovat jak s 20MHz, tak i s 40MHz kanály (v měření jsou vždy použity pouze 20MHz kanály), disponuje dvěma anténami na straně vysílače, dvěma anténami na straně přijímače a umožňuje zpracovávat dva datové kanály (2x2:2 MIMO). Umožňuje připojení klienta maximální rychlostí 300 Mbps. Wi-Fi přístupový bod: ZoneFlex 7372 využívá technologii BeamFlex, která umožňuje směrovat signál k uživateli pomocí soustavy směrových antén (43).



Obrázek 26 - ZoneFlex7372 (43)

Kontroler Ruckus ZoneDirector 1106 pro účely měření pracuje s verzí firmware 9.10.2.0 buid 53. Je nakonfigurováno vysílání pouze jedno BSSID pojmenovaného „TEST-Ruckus-ZD1106“ se zabezpečením WPA2-PSK. Kontroler má oproti továrnímu nastavení upravena tato nastavení:

- Configure > WLAN > Fast BSS Transmition > enable
- Configure > WLAN > Radio Resource Managment > enable

Konfigurace kontroleru Ruckus ZoneDirector 1106 vychází z dokumentů „Ruckus Wireless ZoneDirector Quick Setup Guide“ (44) a „Ruckus Wireless™ ZoneDirector™ Release 9.10 User Guide“ (45)a „Ruckus Konwledge - When should I use SmartRoam?“ (42). Úplný výpis konfigurace je uveden v oddíle přílohy.

5.1.3 Použitý software

Pro měření signálu i vlastního roamingu byly použity různé produkty ve freeware licencích, nebo ve formě demoverzí zdarma. Využití software je možno rozdělit do dvou fází:

5.1.3.1 Měření kvality signálu – pokrytí

Pro měření rozložení signálu byly použity programy:

- **Airmagnet Survey Pro** (produkt společnosti Netscout)

  Jedná se o komerční program „Airmagnet Survey Pro“ společnosti Netscout, které je předním vývojářem software pro Wi-fi měření a Hetmaping. Společnost Netscout paří společně se společností Ekahau mezi nejlepší vývojáře software pro měření Wi-Fi signálu a je výrobci doporučována jako vhodný software pro nezávislé měření signálu (46 str. 4).

  Airmagnet Survey Pro verze 8.7 umožňuje při měření definování stěn v plánu, nebo nastavení škály signálu.

- **InSSIDer** (produkt společnosti Metageek)

  Program InSSIDer představuje nejpoužívanější software na měření signálu pro operační systém Windows. Je doporučován i v ofociálních příručkách výrobců hardware jako referenční software. (46 str. 19)

  Verze programu verze 4.2.2. umožňuje v krátkých intervalech sledovat vysílací výkon dostupných přístupových bodů, včetně jejich MAC adres.

  Z měření pak byly zpracovány reporty na pokrytí signálem pro BSSID, tak i pro pokrytí signálem jednotlivých Wi-Fi přístupových bodů. Takovéto reporty umožňují lépe určit hranici dosahu signálu jednotlivých Wi-Fi přístupových bodů.

5.1.3.2 Měření rychlosti roamingu – rychlosti přenosu a výpadků

Pro měření rozložení signálu byly použity programy:

- **PingPlotter for Windows** (produkt společnosti PingPlotter)

  Pro měření byl využit program PingPlotter for Windows ve verzi 5.5.9 release 2018-02-27 ve zkušební, časově omezené, verzi. Program

umožňuje v nastavitelných intervalech zasílat ICMP PING na zařízení v síti. PingPlotter pak následně graficky znázorňuje výsledky (případně umožňuje jejich export do *.csv souboru). Kromě času odpovědí na jednotlivé ISM PING packety zobrazuje také ztracené packety a vypočítává průměrný čas opovědi (47). Pro účely testu byl software instalován na mobilního klienta a hodnota intervalů pingu byla nastavena na nejnižší možnou mez, tedy 0,5sec. tedy 500ms (pokud byl měřená reasociace klienta mezi Wi-Fi prístupovými body kratší, považujeme ji pro účely měření za neměřitelnou). Zaznamenávány jsou pak časy odezvy jednotlivých ICMP PING a ztracené packety.

- **iPerf** (open-source software)

  Program iPerf (48) je při měření využit pro analýzu datových toků mezi Wi-Fi klientem a LAN sítí. Program běží na dvou místech, na serveru a klientovi. Mezi nimi pak generuje TCP provoz. Výsledky prezentuje výpisem (nebo graficky, pokud je využita nadstavba jPerf). V rámci měření je software nasazen na Wi-Fi klientovi a Serveru v LAN síti. V průběhu testu je sledován TCP provoz od klienta na server (49). Měření slouží jako doplněk informací o dostupnosti zjišťovaných pomocí programu „PingPlotter for Windows“ a pomáhá odhalit výpadky, které by jinak, při samotném měření ICMP PING s frekvencí 500ms mohly zůstat skryty.

- **> netsh wlan show interfaces** (CommandLine Windows společnosti Microsoft)

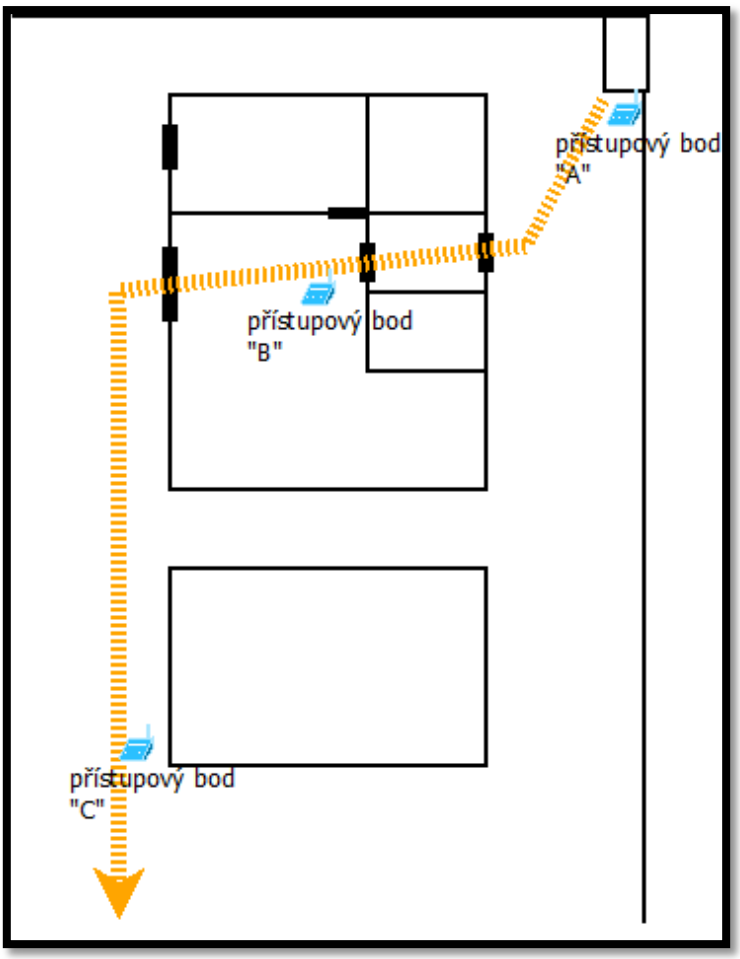
  Jako určení přesné polohy kde dochází k reasociaci Wi-Fi klienta byl použit příkaz „netsh wlan show interfaces“. Tento příkazý zobrazuje základní informace o Wi-Fi připojení. Pro účely měření jsou důležité zejména: MAC adresu Wi-Fi přístupového bodu, ke kterému je klient asociován, číslo Wi-Fi kanálu a síla signálu (50). Jelikož jsou údaje vyčítány přímo ze Wi-Fi síťové karty, která je zjišťuje během režijního „probe“ provozu, nemá zobrazování těchto informací negativní vliv ani na ICPM PING ani na Zátěžový test provozu. Příkaz je zpracováván

v dávkovém *.bat souboru, jež jej spouští každé 2sec. Výstup souboru slouží k určení polohy, kde došlo k reasociaci klienta.

Kombinací výstupů PingPlotter for Windows a iperf tak byl získán přehled o výpadcích, či poklesu datových toků do sítě během roamingu v jednotlivých scénářích. Výpis „netsh wlan show interfaces“ pak umožnil sledovat Wi-Fi přístupový bod, ke kterému je klient momentálně asociován. Kompletní výstupy programu iperf naleznete v sekci přílohy.

5.2 Analýza naměřených hodnot

Měření bylo rozděleno do dvou částí. V první se jednalo o měření kvality signálu, tedy pokrytí v druhé pak samotný roaming. Rozmístění Wi-Fi přístupových bodů i směr pohybu klienta je vyznačen na obrázku níže.



Obrázek 27 - rozmístění Wi-Fi AP (23)

Všechna měření probíhala na stejném místě a za stejných podmínek. Klient se vždy pohyboval stejným směrem, tj. od přístupového bodu „A“, k přístupovému bodu „B“ a „C“, kde bylo vždy měření ukončeno. Také rozestavení Wi-Fi přístupových bodů bylo u všech měření shodné. Měření roamingu probíhalo vždy v pěti opakováních jak pro ICMP PING tak pro přenos dat.

Samotné výsledky měření jsou pak prezentovány referenčním výsledkem, případně obrázkem a krátkým popisem v jednotlivých sekcích:

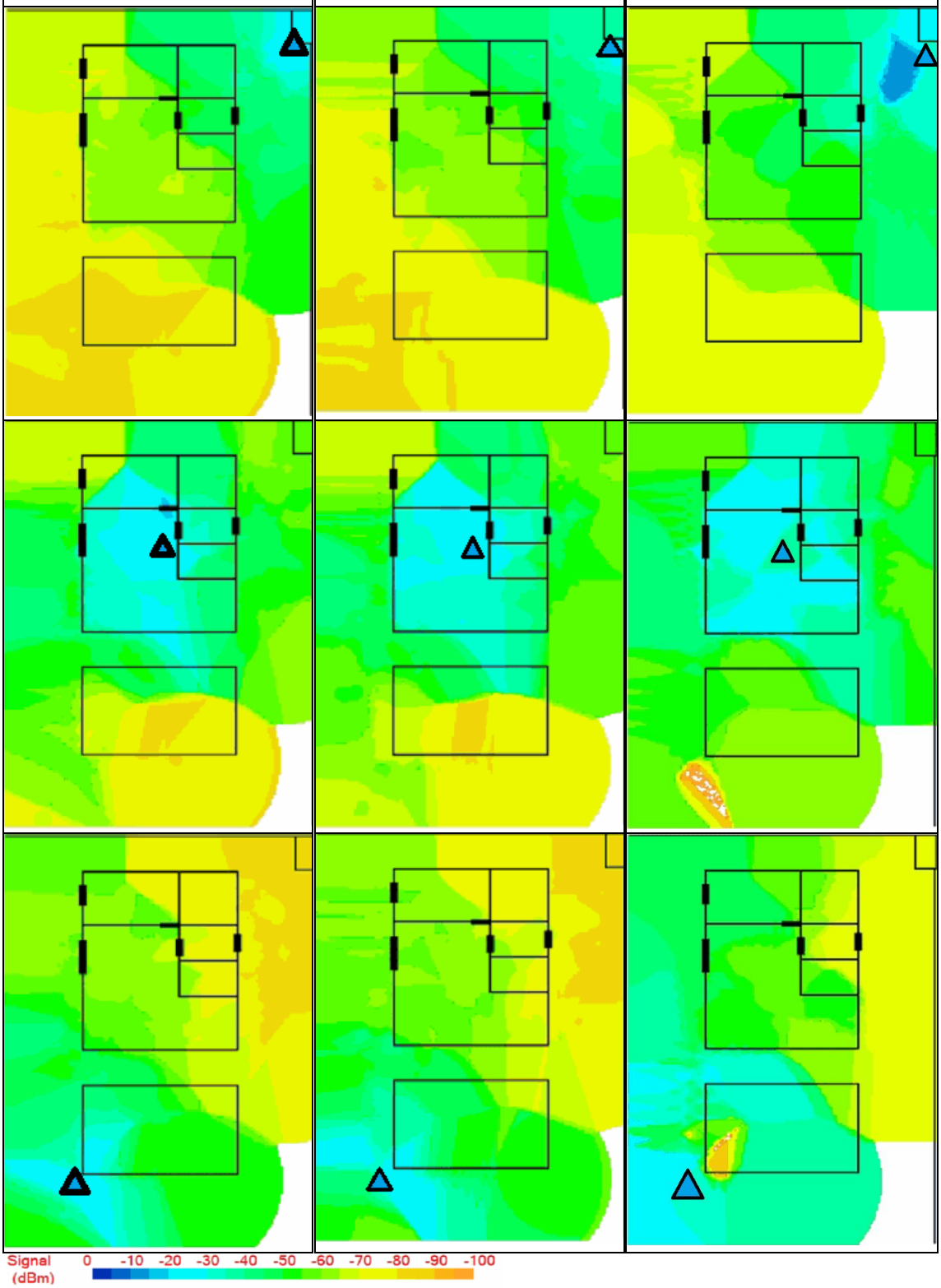
- Výsledky Měření kvality signálu – pokrytí v pásmu 5GHz

- Výsledky měření rychlosti roamingu – rychlosti přenosu a výpadků
  - časy odezvy jednotlivých ICMP PING a ztracené packety
  - analýza datových toků mezi Wi-Fi klientem a LAN sítí
- určení přesné polohy kde dochází k reasociaci Wi-Fi klienta
- Analýza datových toků v síti

5.2.1 Výsledky Měření kvality signálu – pokrytí v pásmu 5GHz

Analýza pokrytí v pásmu 5GHz zachycuje rozšíření signálu testovanou oblastí. Mezi prvními dvěmi scénáři není vidět příliš patrný rozdíl. Výsledky se liší až při třetím scénáři. Tyto odchylky jsou způsobeny použitím jiných Wi-Fi přístupových bodů. Zatím co v prvních dvou scénářích se jedná o shodné přístupové body Cisco aironet 1142i, lišícími se pouze po stránce software a řízení, ve třetím scénáři byly vyžity přístupové body Rucku ZoneFlex 7372. I když jsou přístupové body Cisco Aironet 1142i a Ruckus ZoneFlex 7372 podobné výkonově, cenově i dobou uvedení, přeci jen se liší konstrukcí. Nejvíce pak konstrukcí antén. Zatím co přístupové body Cisco Aironet 1142i využívají klasických dipólových antén (36), přístupové body Rucku ZoneFlex 7372 využívají směrové antény s technologií BeamFlex (43). Rozdíl je pak nejvíce patrný na mapě pokrytí jednotlivými přístupovými body. Přístupové body Rucku ZoneFlex 7372 pokrývají větší část prostoru silnějším signálem.

Tabulka 3 - Výsledky Měření kvality signálu – pokrytí v pásmu 5GHz

Síť se samostatnými Wi-Fi přístupovými body, bez centrálního řízení	Síť s využitím Wi-Fi kontroleru Cisco WLC2504	Síť s využitím Wi-Fi kontroleru Ruckus ZoneDirector 1106
		

Obrázek 28 – tabulka pokrytí signálem v pásmu 5GHz rozdělena pro jednotlivé scénáře a umístění přístupových bodů

5.2.2 Výsledky měření rychlosti roamingu – rychlosti přenosu a výpadků

Měření rychlosti roamingu nejvíce odhalilo rozdíly v řízení. Zde je již patrný rozdíl mezi všemi scénáři a to i přesto, že přístupové body použité v prvním a druhém scénáři jsou po technické stránce shodné a liší se jen použitým software a způsobem řízení. Jednotlivé části měření jsou rozebrány níže.

5.2.2.1 časy odezvy jednotlivých ICMP PING a ztracené packety

Časy odezvy na packety ICMP PING společně s analýzou ztracených packetů tvoří první část měření rychlosti roamingu. Měří se zde čas mezi odesláním ICMP packetu od klienta na server do návratu odpovědi od serveru zpět na klienta. Rychlost je měřena v milisekundách. Měřený úsek představuje přibližně jednu minutu, po kterou se klient pohyboval od po trase měření od pobud A k bodu B a následně k bodu C.

Z měření prvního scénáře (Síť se samostatnými Wi-Fi přístupovými body, bez centrálního řízení) je jasně patrné, že během roamingu došlo ke zpomalení a následné ztrátě packetů a to během obou roamingů. Při roamingu mezi přístupovými body „A“ a „B“ je patrné zpoždění ICMP PING 90ms následované výpadkem, při roamingu mezi přístupovými body „B“ a „C“ je patrné zpoždění 160ms následované výpadkem.

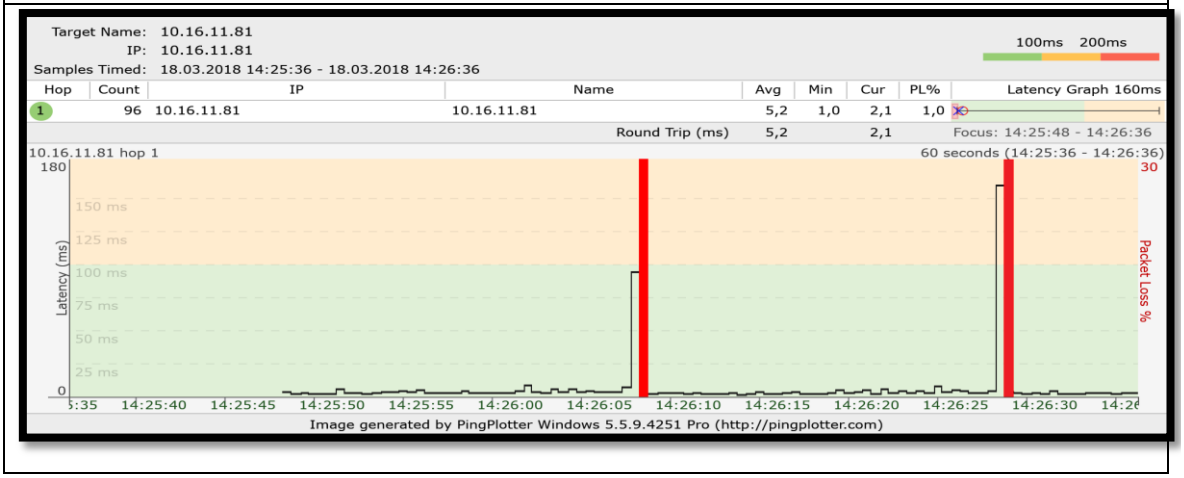
U druhého scénáře (Síť s využitím Wi-Fi kontroleru Cisco WLC2504) pak je vidět, že i zde k výpadku došlo, avšak již se tak nedělo při každém z provedených pokusů, ale pouze při přechodu klienta mezi přístupovými body „B“ a „C“. Při roamingu mezi přístupovými body „A“ a „B“ docházelo pouze ke zpoždění, jak je patrné z výpisu.

Třetí scénář (Síť s využitím Wi-Fi kontroleru Ruckus ZoneDirector 1106) ukazuje, že i zde dochází ke zpomalení, je však nejkratší ze všech scénářů a ke strátě packetů nedošlo vůbec. I zde je patrné, že roaming mezi přístupovými body „B“ a „C“ je delší, než mezi přístupovými body „A“ a „B“.

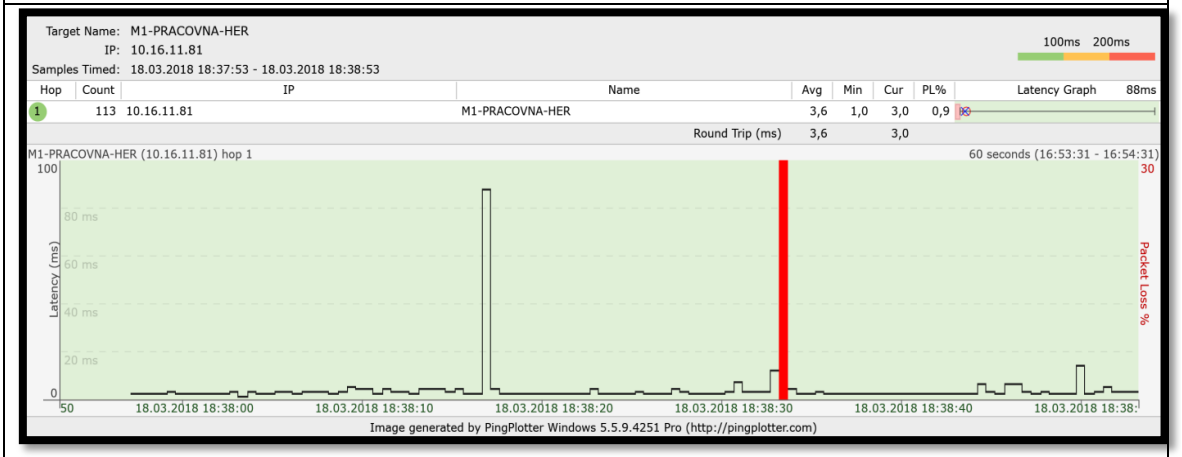
Výsledky měření jsou prezentovány v tabulce, kde jednotlivé řádky představují jednotlivé scénáře.

Tabulka 4 - Výsledky měření času odezvy jednotlivých ICMP PING a ztracené packety

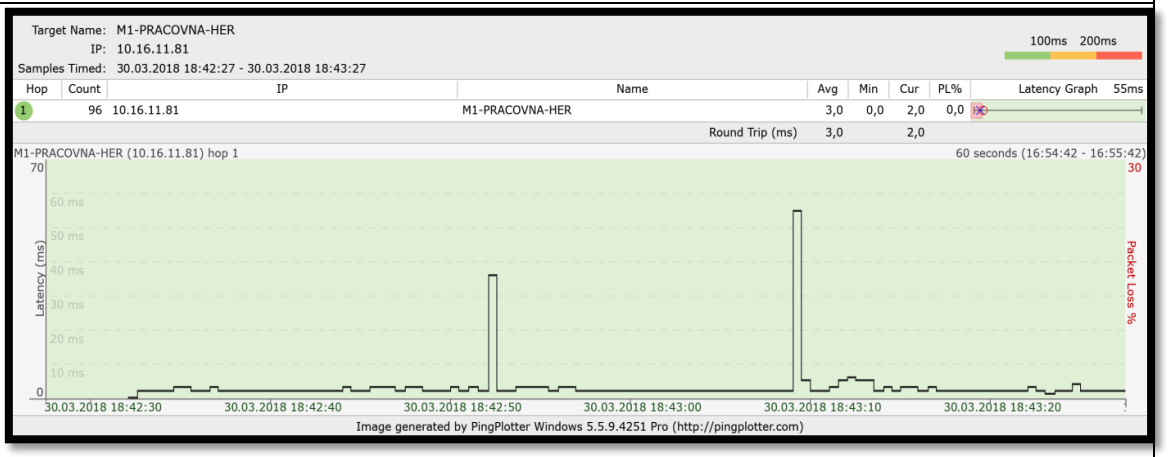
Síť se samostatnými Wi-Fi přístupovými body, bez centrálního řízení



Síť s využitím Wi-Fi kontroleru Cisco WLC2504



Síť s využitím Wi-Fi kontroleru Ruckus ZoneDirector 1106



5.2.2.2 analýza datových toků mezi Wi-Fi klientem a LAN sítí

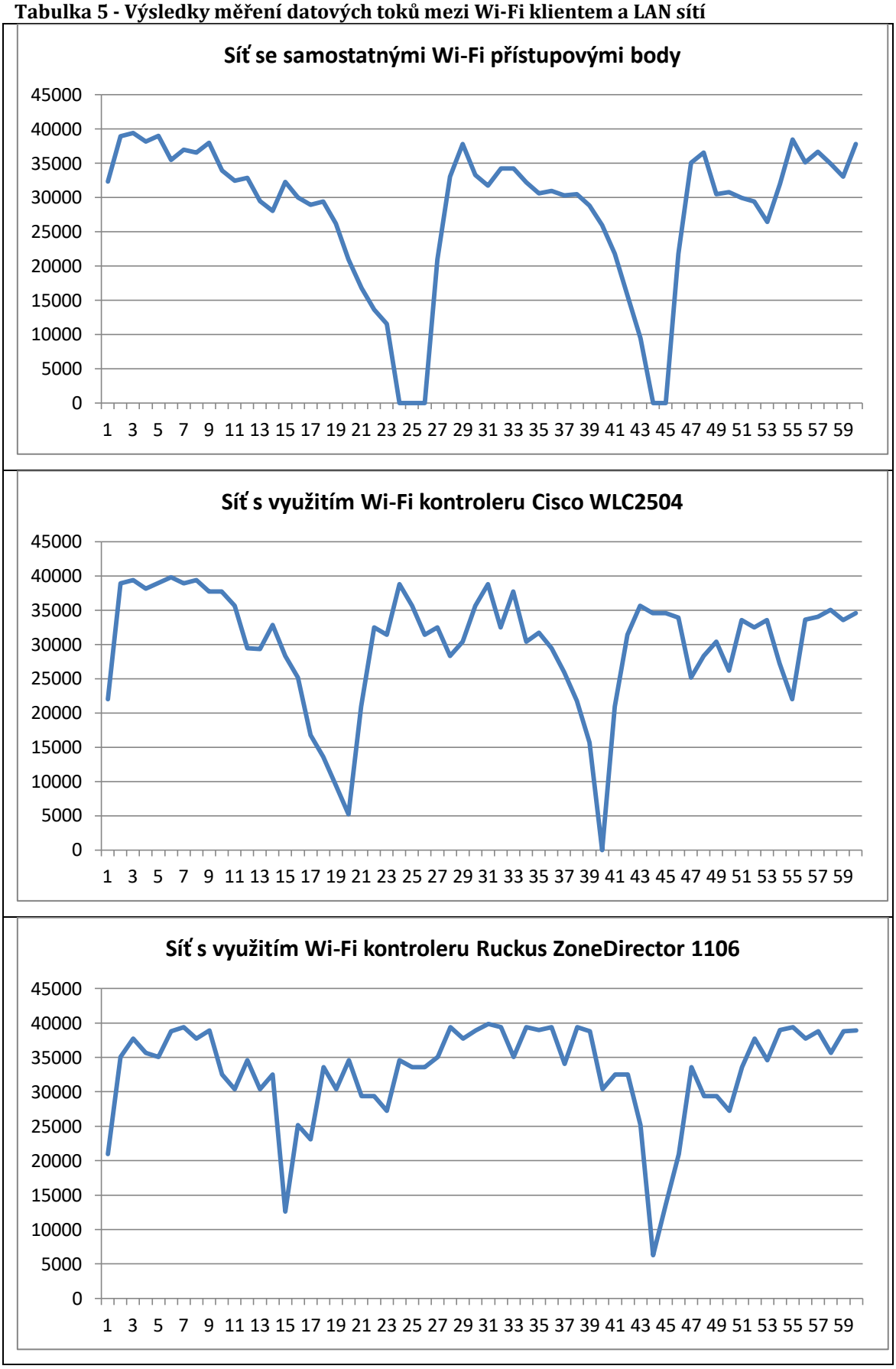
Analýza datových toků sítí byla provedena měření datového toku TCP opět mezi klientem a serverem. K měření byl využit program „iperf“ a výstupy z něho jsou prezentovány pomocí grafů.

Z měření je opět patrné, že první scénář (Síť se samostatnými Wi-Fi přístupovými body, bez centrálního řízení) nenabízí rychlé přepojení klienta a opakují se tak výpadky, které byly patrné již v měření odezvy ICMP PING. Také je patrné snižování přenesených dat mezi klientem a serverem, které ukazuje na slábnoucí kvalitu připojení klienta k přístupovému bodu. Toto zpomalování přenosu pak vyvrcholí ztrátou spojení a připojení k dalšímu přístupovému bodu.

Druhý scénář (Síť s využitím Wi-Fi kontroleru Cisco WLC2504) oproti tomu vykazuje při měření datových toků stabilnější spojení. Reasociace klienta k novému přístupovému bodu je i v tomto měření patrná, avšak, není provázena úplnou ztrátou spojení a nepředchází jí zpomalení toku dat až na úroveň výpadku. Je tedy patrné, že klient se rozhodl k reasociaci ne na základě ztráty spojení, ale už dříve, jakmile zaregistroval zpomalení a dostal se do dosahu přístupového bodu nabízejícího lepší kvalitu připojení.

Třetí scénář (Síť s využitím Wi-Fi kontroleru Ruckus ZoneDirector 1106) ukazuje nejstabilnější spojení. K poklesu datového toku sice dochází, je však nejmenší ze všech testovaných scénářů. I zde dochází k reasociaci na základě lepší kvality připojení, ne až na základě ztráty připojení (jak je patrné v prvním scénáři). Reasociace je však provádena v jiný čas, což souvisí s jinou úrovní pokrytí signálem.

Tabulka 5 - Výsledky měření datových toků mezi Wi-Fi klientem a LAN sítí



5.2.3 Určení přesné polohy kde dochází k reasociaci Wi-Fi klienta

Určení místa kde probíhala reasociace klienta doplňuje informace o rychlostech reasociace klienta. To kde klient reasociaci zahájil, vypovídá o kvalitě roamingu.

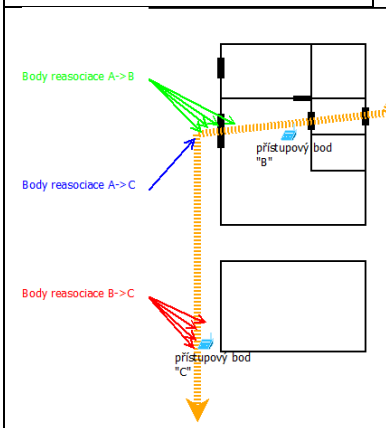
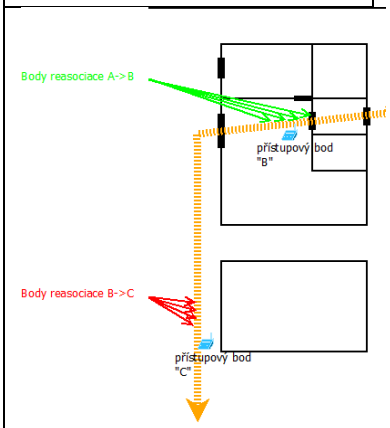
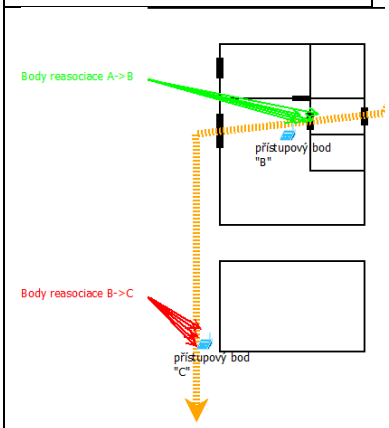
V případě prvního scénáře (Síť se samostatnými Wi-Fi přístupovými body, bez centrálního řízení) je patrné, že reasociaci klient zahájil až na hranici signálu -67dbm, tedy ve chvíli, když již signál poklesnul.

Oproti tomu ve druhém scénáři (Síť s využitím Wi-Fi kontroleru Cisco WLC2504) byla reasociace zahájena dříve. To umožnilo klientovi vyhnout se zpomalení v důsledku snížení přenosové rychlosti. Dále díky podpoře protokolů IEEE802.11k a IEEE802.11v tak síť s kontrolerem klientovi ušetří čas nutný pro aktivní skenování a vyhledání kanálů na kterých se nachází další přístupové body sítě.

V případě třetího scénáře (Síť s využitím Wi-Fi kontroleru Ruckus ZoneDirector 1106) se ukazuje, že k reasociaci klienta mezi přístupovými body „A“ a „B“ dochází dříve a k reasociaci klienta mezi přístupovými body „B“ a „C“ dochází později než v obou předchozích scénářích. Klient v tomto případě také využívá podporu protokolů IEEE802.11k a IEEE802.11v a roaming proto zahajuje dříve, než dojde k výpadkům spojení. Zároveň je, však díky použití odlišné konstrukce antén v přístupových bodech je rozložení signálu jiné, než v prvním a druhém scénáři.

Výsledky měření jsou prezentovány v tabulce, kde jednotlivé sloupce představují jednotlivé scénáře.

Tabulka 6 - Výsledky měření určení přesné polohy kde dochází k reasociaci Wi-Fi klienta

Síť se samostatnými Wi-Fi přístupovými body, bez centrálního řízení	Síť s využitím Wi-Fi kontroleru Cisco WLC2504	Síť s využitím Wi-Fi kontroleru Ruckus ZoneDirector 1106
		

5.2.4 Analýza datových toků v síti

Analýza datových toků v síti umožňuje určit kudy jednotlivé packety v případě jednotlivých scénářů putují. Pro analýzu slouží výpisy z páteřního switche (Cisco Catalyst WS-C3560-8PC) tak informační výpisy „log“ jednotlivých přístupových bodů a kontrolerů použitých v jednotlivých scénářích.

5.2.4.1 Síť se samostatnými Wi-Fi přístupovými body, bez centrálního řízení

Jak je patrné z výpisu páteřního switche hodnota RXBS v řádku FastEthernet0/2 je prakticky shodná s hodnotou TXBS v řádku FastEthernet0/5. A také naopak hodnota TXBS v řádku FastEthernet0/5 je prakticky shodná s hodnotou RXBS v řádku FastEthernet0/2.

To jasně ukazuje, že datová výměna probíhala přímo mezi klientem a serverem.

```
m-sw01#show interfaces summary

*: interface is up
IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
TRTL: throttle count
```

```
 Interface          IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
-----------------------------------------------------------------------
* Vlan1              0    0   0    0  2000   3  4000   2   0
* FastEthernet0/1      0    0   0    0  2000   2  9000   7   0
* FastEthernet0/2      0    0   0    0 1664000 298 2298000 235   0
  FastEthernet0/3      0    0   0    0    0   0    0   0   0
  FastEthernet0/4      0    0   0    0    0   0    0   0   0
* FastEthernet0/5      0    0   0    0 2288000 226 1665000 297   0
* FastEthernet0/6      0    0   0    0  2000   1  5000   4   0
  FastEthernet0/7      0    0   0    0    0   0    0   0   0
  FastEthernet0/8      0    0   0    0    0   0    0   0   0
* GigabitEthernet0/1    0    0   0    0    0   0  9000   9   0
```

Při roamingu také dochází k změně datových toků, které páteřní switch vyhodnocuje jako nestandardní chování a upozorňuje na něj výpisem:

```
5w6d: %SW_MATM-4-MACFLAP_NOTIF: Host ac7b.a136.6550 in vlan 1 is flapping between port Fa0/2 and port Fa0/3
```

Tento výpis upozorňuje na to, že klient, jehož MAC adresa byla za portem Fa0/2 (a tedy připojena na přístupový bod „A“) náhle posílá data zpoza portu Fa0/3 (a tedy zpoza přístupového portu „B“).

Samotné Wi-Fi přístupové body Cisco Aironet 1142i ve verzi firmware jsou schopny detekovat pohyb klienta a přestože jsou konfigurovány samostatně, pak pomocí CDP protokolu tyto informace sdílí. Jak nám ukazuje výpis logu:

100	Mar 1 00:40:22.036	Information	Interface Dot11Radio1, Deauthenticating Station ac7b.a136.6550 Reason: Sending station has left the BSS
101	Mar 1 00:40:22.036	Information	Station ac7b.a136.6550 Roamed to 64d8.148b.1450
102	Mar 1 00:21:47.075	Information	Interface Dot11Radio1, Station TEST-Cisco-SAP1 ac7b.a136.6550 Associated KEY_MGMT[WPAv2 PSK]

Tento výpis ukazuje prvotní asociaci klienta (řádek 102), následuje informace o roamingu (řádek 101), okamžitě následována informací o disociaci (řádek 100).

5.2.4.2 Síť s využitím Wi-Fi kontroleru Cisco WLC2504

Jak je patrné z výpisu páteřního switche hodnota RXBS v řádku FastEthernet0/2 je jen mírně vyšší oproti hodnotě TXBS v řádku FastEthernet0/5. A také naopak hodnota RXBS v řádku FastEthernet0/2 je mírně vyšší v porovnání s hodnotou TXBS v řádku FastEthernet0/5. Toto navýšení reprezentuje řídící

provoz probíhající mezi přístupovým bodem a Wi-Fi kontrolerem. Zároveň však je patrné zdvojení provozu na portu kontroleru GigabitEthernet0/1 a to v obou směrech.

```
m-sw01#show interfaces summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface            IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
------------------------------------------------------------------------
* Vlan1                0    0    0    0    0    0    0    0    0
* FastEthernet0/1      0    0    0    0 2000    3 2000    2    0
* FastEthernet0/2      0    0    0    0 1883000  302 2195000  229    0
  FastEthernet0/3      0    0    0    0    0    0    0    0    0
  FastEthernet0/4      0    0    0    0    0    0    0    0    0
* FastEthernet0/5      0    0    0    0 2114000  228 1710000  303    0
* FastEthernet0/6      0    0    0    0    0    0    0    0    0
  FastEthernet0/7      0    0    0    0    0    0    0    0    0
  FastEthernet0/8      0    0    0    0    0    0    0    0    0
* GigabitEthernet0/1   0    0    0    0 3938000  529 4003000  537    0
```

5.2.4.3 Síť s využitím Wi-Fi kontroleru Ruckus ZoneDirector 1106

V případě třetího scénáře se ukazuje, že datová výměna probíhala přímo mezi klientem a serverem, avšak je patrný i řídící provoz Wi-Fi sítě mezi přístupovým bodem a Wi-Fi kontrolerem. Datový tok mezi klientem a serverem je patrný z výpisu páteřního switche, kde hodnota RXBS v řádku FastEthernet0/2 je opět jen mírně větší oproti hodnotě TXBS v řádku FastEthernet0/5. A také naopak hodnota TXBS v řádku FastEthernet0/5 je mírně nižší oproti hodnotě RXBS v řádku FastEthernet0/2. Řídící provoz mezi přístupovým bodem a Wi-Fi kontrolerem pak vidíme na řádku GigabitEthernet0/1, který zároveň prakticky odpovídá rozdílu mezi datovými toky řádků FastEthernet0/2 a FastEthernet0/5.

```
m-sw01#show interfaces summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
```

```
TXBS: tx rate (bits/sec)        TXPS: tx rate (pkts/sec)
TRTL: throttle count

 Interface          IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
------------------------------------------------------------------
* Vlan1              0    0   0    0    0    0    0    0    0
* FastEthernet0/1        0    0   0    0 2000    3 2000    3    0
* FastEthernet0/2        0    0   0    0 1714000 308 2198000 245    0
  FastEthernet0/3        0    0   0    0    0    0    0    0    0
  FastEthernet0/4        0    0   0    0    0    0    0    0    0
* FastEthernet0/5        0    0   0    0 2118000 226 1610000 287    0
* FastEthernet0/6        0    0   0    0 2000    1 5000    4    0
  FastEthernet0/7        0    0   0    0    0    0    0    0    0
  FastEthernet0/8        0    0   0    0    0    0    0    0    0
* GigabitEthernet0/1     0    0   0    0   72000   19 102000   22    0
```

Při roamingu také dochází k změně datových toků, které páteřní switch vyhodnocuje jako nestandardní chování a upozorňuje na něj výpisem:

```
5w6d: %SW_MATM-4-MACFLAP_NOTIF: Host ac7b.a136.6550 in vlan 1 is flapping between port Fa0/2 and port Fa0/3
```

Tento výpis upozorňuje na to, že klient, jehož MAC adresa byla za portem Fa0/2 (a tedy připojena na přístupový bod „A“) náhle posílá data zpoza portu Fa0/3 (a tedy zpoza přístupového portu „B“).

5.2.4.4 Shrnutí

Celková Analýza datových toků v síti během jednotlivých scénářů je pak shrnuta v následující tabulce:

Tabulka 7 - Porovnání datových toků v síti během jednotlivých scénářů

	Síť se samostatnými Wi-Fi přístupovými body, bez centrálního řízení	**Síť s využitím Wi-Fi kontroleru Cisco WLC2504**	**Síť s využitím Wi-Fi kontroleru Ruckus ZoneDirector 1106**
Zdvojení provozu v LAN síti	**NE**	**ANO**	**NE**
Detekuje LAN roaming jako chybu	**ANO**	**NE**	**ANO**
Detekuje WLAN řešení roaming jako chybu	**NE**	**NE**	**NE**

6 Shrnutí výsledků

Hodnocení kvality Roamingu jasně ukazuje na vzrůstající význam této problematiky. Ve všech scénářích se projevil nějaký způsob výrobce, jak s roamingem klienta pomoci. A to dokonce i ve scénáři bez centrálního řízení, kde jednotlivé přístupové body detekovaly přechodu klienta a ve výpisech jej správně označovali nejen jako disociaci, ale jako roaming na další přístupový bod. Faktem však zůstává, že ve scénáři bez centrálního řízení klient přešel na další přístupový bod, až pokud signál z aktivního přístupového bodu kles pod únosnou mez a nikdy dříve. V jednom z případě měření byl dokonce přístupový bod „B“ zcela vynechán, díky tomu, že klient se tak dlouho držel bodu „A“, až nakonec přešel přímo na bod „C“. S nasazením centrálního řízení a kontroleru Cisco WLC2504 tyto problémy odpadly a zvýšily se možnosti nastavení roamingu a reasociace klienta a to nejen pro celou síť, ale i pro případná jednotlivá BSSID. Kontroler tak umožňuje zohlednit různé potřeby klientů, podle toho zda využívají hlasové, či datové služby. Kontrolerové řešení od společnosti Ruckus pak nabízí specifické možnosti díky kombinaci technologií „SmartRoam“ a „BeamFlex“, které umožňují ponechat aktivního klienta delší dobu na lepším signálu, pomocí směrování signálu soustavou směrových antén. Zároveň scénář s Wi-Fi kontrolerm a přístupovými body Ruckus vykazolal nejmenší zpoždění při testu datového přenosu. Také náročnost nastavení v tomto případě byla oproti řešení od Cisco nízká. Ukazuje se, že podpora roamingu se dnes již stává součástí vybavení nejen centrálně řízených Wi-Fi sítí, ale že ji někteří výrobci implementují i do samostatných přístupových bodů. Pokud však má být roaming v síti řízen podle potřeb datové provozu, je stále kontroler nezbytným řešením. Zde je však nutné řešit i vhodné využití tunelování provozu, které je sice velmi doporučované v sítích s podporou hlasu, ale také výrazně zvyšuje datový provoz. Jako optimální se tak jeví využít tunelování provozu pouze pro voice, či videohovory a ostatní datový provoz ponechat přímo v konkrétní VLAN bez zapouzdření. Pro správnou funkci roamovacích protokolů IEEE 802.11 k/r/v je však také nutná podpora v klientských zařízeních. Zde hlavně přední výrobci podporu do svých zařízení již doplňují.

7 Závěry a doporučení

Cílem této bakalářské práce bylo představit principy a navrhnout technické řešení roamingu Wi-Fi sítí s využitím technologií u dvou předních výrobců Wi-Fi infrastruktury, zhodnotit podporu roamingu a zároveň porovnat vliv architektury sítě a datového toku v síti na kvalitu roamingu. Teoretická část práce se tak přímo se věnovala představení principů fungování Wi-Fi roamingu, které byly následně využity, či přímo testovány v praktické části práce a nezabývala základy funkcí Wi-Fi sití.

Teoretická část tak pojednává v první části o vlastním roamingu klienta a jeho možnostech roaming ovlivňovat. Dále pak o možnostech WLC kontrolerů ovlivňovat roaming a v neposlední řadě o standardech IEEE802.11, které se roamingu týkají. Této problematice se také věnuje i část měření a testů praktické části práce a to konkrétně testy zaměřené a rychlost roamingu a polohu klienta během roamingu. Druhá část teoretické části se pak společně s praktickými testy datových toků v síti zaměřují na Wi-Fi roaming z pohledu datových toků v LAN síti a doporučovanou architekturou u jednotlivých výrobců.

Výsledky testů provedených a prezentovaných v praktické části práce pak jasně ukazují na výhody použití centrálního řízení Wi-Fi sitě WLAC kontrolerem. Obě kontrolerová řešení vynikala nad řešení se samostatně řízenými přístupovými body. A to jak v rychlosti roamingu, tak v omezení výpadků, či lepší volbě místa roamingu klienta. Měření datových toků pak ukazuje na možný vznik úzkého hrdla v LAN síti pokud WLC kontroler využívá zapouzdření datového provozu (v testech reprezentován scénářem s využitím WLC kontroleru Cisco). Takovéto řešení pak sice přináší nejlepší ochranu pořadí packetů, ale za cenu zdvojení provozu v místě napojení kontroleru. Oproti tomu řešení zcela bez kontroleru zatěžuje LAN síť sice nejméně, avšak na druhé straně nenabízí vůbec žádnou ochranu packetů, ani podporu roamingu a packety po roamingu, byly v síti dokonce označovány jako částečně chybné. Ani poslední řešení v podobě scénáře s využitím WLC kontrolru Ruckus nenabízelo optimální řešení. Zde sice nedocházelo ke zdvojení provozu na straně kontroleru, roaming fungoval, avšak nepokrýval možnost ochrany pořadí packetů.

Při hodnocení výsledků obou kontrolerů se tak dostáváme do nelehké situace, kdy každé řešení nabízí určitá pozitiva i omezení. Kontroler Ruckus ZD1106 společně s přístupovými body Ruckus ZF7372 nabídl nejlepší výsledky, co se týče rychlosti roamingu, avšak také žádnou ochranu dat po tom co se data dostala z přístupového bodu na switch. Oproti tomu řešení Cisco s kontrolerem WLAC2504 a s přístupovými body Cisco LAP1142 nedosahovalo takových výsledků v rychlosti roamingu jako Ruckus, avšak díky využiti CAPWAP tunelů ochraňuje packety do LAN sítě je kontroler zasílá vždy ve stavu a pořadí v jakém je získal od bezdrátového klienta.

Výsledky tak upozorňují na to, že je třeba věnovat zvýšenou pozornost problematice roamingu a datových toků už v návrhu WLAN/LAN sítě. Tedy především správně analyzovat jednotlivé datové toky a vhodně je rozdělit je do samostatných VLAN s vhodně řešeným nastavením QoS a zapouzdřenín, či naopak nezapouzdřením WLAN provozu. Pokud bychom se totiž spolehli jen na jedno řešení, mohlo by se stát, že bude omezena propustnost sítě, nebo síť nebude schopna zajistit požadovanou kvalitu hlasových, či video služeb. Ideálním řešením se tak jeví kombinovat výhody obou testovaných kontrolorových řešení a do WLAN sítě s kombinovaným provozem. Tedy sítě, které je řízena WLAN kontrolerem a zapouzdřuje datový tok citlivý na zpoždění, či poškození, ale zároveň nechává bez zapouzdření běžný datový tok, kterému tak poskytuje veškerou volnou kapacitu LAN sítě. Kontrolery obou výrobců takovéto nastavení umožňují, liší se jen ve způsobech implementace. Zatím co kontroler Ruckus ZoneDirector nabízí pro toto řešení jednoduché zapnutí, tak u kontorleru Cisco WLC2504 se setkáváme s komplexnějším přístupem v možnostech nastavení.

8 Seznam použitých pojmů a zkratek

- adresa MAC
    - Hardwarová adresa vrstvy datových spojů, kterou musí mít definovánu každý port a každé zařízení, připojené do segmentu sítě LAN. Ostatní zařízení v síti pak podle těchto adres vyhledávají přesné umístění logických adres. Adresy MAC mají délku 6 bajtů a jejich podobu řídí institut IEEE; její součástí je zpravidla vypálená adresa BIA lokálního rozhraní LAN. Nazývá se také hardwarová adresa, fyzická adresa, vypálená adresa nebo adresa vrstvy MAC (vrstvy řízení přístupu k médiu).

- BSSID (SSID)
    - Identifikátor bezdrátové sítě Wi-Fi. Přístupový bod (AP, access point) vysílá periodicky svůj identifikátor v takzvaném majákovém rámci (beacon frame) a klienti si tak mohou snadno vybrat, ke které bezdrátové síti se připojí.

- IEEE (Institute of Electrical and Electronics Engineers)
    - Profesní organizace, mezi jejíž aktivity patří mimo jiné definice standardů (norem) v řadě oborů výpočetní techniky a elektroniky, včetně komunikací a počítačových sítí. Standardy IEEE pro sítě LAN dnes ve světě mezi těmito sítěmi převládají. Celá řada protokolů se běžně označuje jen referenčním číslem příslušné normy IEEE.

- IGMP (Internet Group Management Protocol)
    - Protokol, ve kterém hostitelé sítě IP oznamují své členství ve vícesměrových skupinách přilehlým vícesměrovým směrovačům.

- lokální síť (Local Area Network, LAN)
    - V širším slova smyslu je to libovolná síť, která propojuje dva nebo více počítačů a s nimi souvisejících zařízení v relativně omezeném prostoru (do několika kilometrů). Jsou to zpravidla sítě s vysokou přenosovou rychlostí a malou četností chyb a pracují nejčastěji uvnitř firem. Fyzické kabely a elektrické signály pro fyzickou a linkovou vrstvu z referenčního modelu OSI jsou definovány ve standardech sítí LAN. Příkladem nejčastěji používaných technologií sítí LAN jsou standardy Ethernet, FDDI a Token Ring.

- paket
    - V datové komunikaci se takto označuje základní logická jednotka přenášených informací. Paket se skládá z určitého portu datových bajtů, které jsou obaleny neboli zapouzdřeny do hlaviček a/nebo zápatí, jež obsahují informace o původu paketu, o jeho cíli apod. Různé protokoly zapojené do vysílání pak přidávají svoje vlastní vrstvy informací hlaviček, které poté interpretuje odpovídající protokol v přijímajícím zařízení.

- protokol
    - V počítačové síti se takto označuje specifikace množiny pravidel pro určitý typ komunikace. Pojem se někdy používá také pro software, který je implementací protokolu.

- přepínač (switch)
    - V počítačových sítích je to zařízení, které je odpovědné za různé funkce jako filtrování, plošné rozesílání (záplava) a odesílání rámců. Při odesílání se rozhoduje podle cílové adresy jednotlivých rámců. Přepínač pracuje na vrstvě datových spojů referenčního modelu OSI.

- Přístupový bod (AP)
    - Zařízení, ke kterému se klienti připojují. Klienti spolu nekomunikují přímo, ale prostřednictvím přístupového bodu, takže mohou být jednodušší a nemusejí být ve vzájemném rádiovém spojení. Centralizovaný způsob komunikace též umožňuje použití směrových antén, které zvyšují dosah rádiového signálu. Tento typ spořádání nazýváme infrastrukturní síť. Opakem jsou ad-hoc sítě, kde jsou dva nebo více klientů ve vzájemném přímém rádiovém spojení (bez existence rostředníka). Přístupový bod je obvykle realizován malým jednoúčelovým zařízením (viz obrázek), ale s potřebnou softwarovou výbavou se jím může stát i jakýkoliv počítač s bezdrátovým Wi-Fi zařízením. Některá z těchto jednoúčelových zařízení využívají jako základ operační systém Linux.

- rámec (frame)
    - Logická jednotka informací, odesílaná do přenosového média vrstvou datových spojů. Pojem často označuje hlavičku a zápatí, které obklopují data obsažená v jednotce a které slouží pro synchronizaci a řízení chyb.

- reakční doba (latence)
    - V širším slova smyslu je to doba, kterou zabere paketu cesta z jednoho místa na druhé. Ve speciálních souvislostech sítí se jedná buďto o prodlevu mezi provedením požadavku o přístup k síti a okamžikem, kdy je danému mechanismu přiděleno oprávnění vysílat, nebo o prodlevu mezi okamžikem, kdy zařízení přijme datový rámec, a okamžikem, kdy tento rámec přepošle dále do cílového portu.

- síťová vrstva
    - V referenčním modelu sítí OSI je to vrstva 3; je v ní implementováno směrování, a vrstva tak umožňuje výběr spojení a tras mezi dvěma koncovými systémy. Viz též aplikační vrstva, vrstva datových spojů, fyzická vrstva, prezentační vrstva, relační vrstva, transportní vrstva.

- směrovač (router)
    - Softwarové nebo hardwarové zařízení síťové vrstvy, které pomocí jedné nebo více metrik rozhoduje o nejlepší cestě pro přenos daného síťového provozu. Při desílání paketů mezi sítěmi se směrovače řídí podle informací v síťové vrstvě. Historicky se toto zařízení někdy nazývalo brána (gateway).

- šifrování (encryption)
    - Převod informací do nečitelné podoby, v níž jsou tak chráněné před neuvedeným přístupem. Každé schéma šifrování používá nějaký známý algoritmus, jehož účinky musí na přijímající straně „obrátit“ algoritmus opačného směru, a to v procesu nazývaném dešifrování.

- TCP (Transmission Control Protocol)
    - Protokol pro řízení přenosu. Spojovaný protokol transportní (přenosové) vrstvy referenčního modelu OSI, který poskytuje spolehlivé doručení dat.

- trunková linka
    - „Kmenová“ linka mezi přepínači a od některých serverů k přepínačům. Trunkové linky přenášejí provoz mnoha sítí VLAN. Přístupové linky připojují oproti tomu hostitelská zařízení k přepínači a přenášejí informace jen od té sítě VLAN, jejímž členem dané zařízení je.

- tunelování
    - Metoda, která překonává omezení různých protokolů. K tomu obaluje (zapouzdřuje) pakety jednoho protokolu do rámců jiného protokolu a takto zapouzdřený paket přenáší přes síť, která podporuje obalový protokol.

- UDP (User Datagram Protocol)
    - Nespojovaný protokol transportní (přenosové) vrstvy ze sady protokolů TCP/IP, který umožňuje jednoduché vyměňování datagramů bez potvrzování a bez záruky skutečného doručení, takže počítá s tím, že potřebné zpracování chyb a opakované vysílání zajišťují jiné protokoly. Protokol UDP je definován v dokumentu RFC 768.

- VLAN (Virtuální LAN)
    - Skupina zařízení v jedné nebo více logicky segmentovaných (oddělených) sítích LAN, kterou konfigurujeme pomocí softwaru pro správu. Zařízení tak mohou spolu komunikovat stejně, jako by byla přímo připojena ke stejnému fyzickému médiu, přestože jsou fyzicky rozmístěna na několika různých segmentech sítě LAN. Virtuální sítě VLAN nejsou postavené na fyzickém, ale na logickém propojení zařízení, a proto jsou mimořádně flexibilní.

- VLAN ID
    - Identifikátor sítě VLAN, někdy označovaný jako „barva VLAN“. Zapisuje se do rámce a v něm přijímajícímu přepínači oznamuje, do jaké VLAN daný rámec náleží.

- WLAN
    - Bezdrátová lokální síť je bezdrátová počítačová síť, která spojuje dvě nebo více zařízení pomocí bezdrátové distribuční metody (často rozprostřené spektrum nebo OFDM rádio) v omezeném prostoru, jako je doma, ve škole, počítačové laboratoři nebo kancelářské budově.

- vnitřní síť
    - V mechanismu NAT se za vnitřní síť označuje množina sítí, které podléhají překladu; vnější síť pak tvoří všechny ostatní adresy, tedy obvykle adresy umístěné ve veřejném Internetu.

- Wi-Fi (nebo také Wi-fi, WiFi, Wifi, wi-fi, wifi)
    - Označení pro několik standardů IEEE 802.11 popisujících bezdrátovou komunikaci v počítačových sítích (též Wireless LAN, WLAN). Tato technologie využívá tak zvaného „bezlicenčního frekvenčního pásma“,.

- zpoždění (delay)
    - Časový rozdíl mezi okamžikem, kdy odesílatel zahájí transakci, a okamžikem přijetí první odpovědi. Stejným pojmem se označuje také čas potřebný k přemístění paketu ze zdroje do cíle po zadané trase.

9 Seznam použité literatury

1. **Cisco.** Cisco Visual Networking Index: Forecast and Methodology, 2016–2021. Cisco White Paper. [Online] červen 2017. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf. C11-481360-01.

2. **IEEE.** Institute of Electrical and Electronics Engineers. [Online] www.ieee.org.

3. **Hucaby, David.** CCNA Wirelwss 200-355 Oficisal Cert Guide. Indianapolis : Cisco Press, 2016. 987-1-58714-457-8.

4. **Edimax.** AC1200 Dual-Band Home Roaming Wi-Fi Upgrade Extender. Home Wi-Fi System. [Online] [obrázek], 2017. http://www.edimax.com/edimax/merchandise/merchandise_detail/data/edimax/global/whole_home_wifi_system_ac1200_dual-band/re11s/.

5. **Eberspächer, Jörg.** Chapter 6. Roaming and Handover. [autor knihy] Hans-Jörg Vögel, Christian Bettstetter, Christian Hartmann Jörg Eberspächer. GSM - Architecture, Protocols and Services, Third Edition. místo neznámé : Online ISBN: 9780470741719, 2008.

6. **alliance, Wi-Fi.** How does a client roam? WiFi alliance - Knowledge center. [Online] 2018. https://www.wi-fi.org/knowledge-center/faq/how-does-a-client-roam.

7. **IEEE-Standards-Association.** IEEE 802.11k-2008. IEEE STANDARD. [Online] 2018. http://standards.ieee.org/findstds/standard/802.11k-2008.html.

8. —. IEEE 802.11r-2008. IEEE STANDARD. [Online] 2018. http://standards.ieee.org/findstds/standard/802.11r-2008.html.

9. —. IEEE Std 802.11v-2011. IEEE STANDARD. [Online] 2018. http://standards.ieee.org/findstds/standard/802.11v-2011.html.

10. **Nayanajith, Rasika.** mrn-cciew. CWAP – 802.11 Overview. [Online] [obrázek], září 2014. https://mrncciew.com/2014/09/23/cwap-802-11-overview/.

11. **Cisco.** 802.11 Fundamentals - Cisco. Cisco Connected Mobile Experiences (CMX) CVD. [Online] 4. září 2014. https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/CMX/CMX_802Fund.pdf.

12. **Ruckus.** Roaming with standalone APs. Ruckus Knowledge. [Online] 11. leden 2014. https://support.ruckuswireless.com/answers/000001616.

13. **Carroll, Brandon James.** Bezdrátové sítě Cisco. Brno : Computer Press a.s., 2011. 978-80-251-2884-8.

14. **Granados, Adrian.** Understanding the Scan Modes in WiFi Explorer Pro. [Online] [obrázek], 11. březen 2017. https://www.adriangranados.com/blog/understanding-scan-modes-wifiexplorerpro.

15. **Wu Q., Lin H., Liang J.** Advances in Wireless Sensor Networks. Theoretical Analysis of WiFi Location Fingerprint Samplig Period. místo neznámé : Springer, Berlin, Heidelberg, 2015.

16. **Nayanajith, Rasika.** mrn-cciew. CWAP 802.11- Probe Request/Response. [Online] [obrázek], říjen 2014. https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/.

17. Support Apple. Bezdrátový roaming pro firmy. [Online] Apple, 19. 2 2018. https://support.apple.com/cs-cz/HT203068.

18. **Intel.** Wi-Fi Roaming Aggressiveness. Intel Support. [Online] 15. Listopad 2017. https://www.intel.com/content/www/us/en/support/articles/000005546/network-and-i-o/wireless-networking.html.

19. **tp-link.** What can I do if my client can't roam between my wireless router and TP-Link AP & Range Extender product? tp-link support. [Online] [obrázek], 4. leden 2014. https://www.tp-link.com/us/faq-592.html.

20. **NETGEAR.** A6210 advanced features of firmware v1.0.0.32. NETGEAR Support. [Online] [obrázek], 28. listopad 2016. https://kb.netgear.com/30056/A6210-advanced-features-of-firmware-v1-0-0-32.

21. **Cisco.** 802.11r, 802.11k, and 802.11w Deployment Guide, Cisco IOS-XE Release. Cisco Technical References. [Online] 25. 1 2014. https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33.pdf.

22. Key Reinstallation Attacks. [Online] 2017. https://www.krackattacks.com/.

23. **Autor.** Schámatické zapojení sítě. [Online] [obrázek].

24. **Cisco.** Understanding Delay in Packet Voice Networks. Cisco White Paper. [Online] Cisco Public, 2. únor 2006. https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/5125-delay-details.html.

25. The 4 Wireless Controller Architectures You Need to Know. securityuncorked.com. [Online] 31. 1 2012. http://securityuncorked.com/2011/11/the-4-wireless-controller-architectures-you-need-to-know/.

26. **Cisco.** Cisco Aironet Series 1700/2700/3700 Access Points Deployment Guide. Cisco technical References. [Online] 3. listopad 2014. https://www.cisco.com/c/en/us/td/docs/wireless/technology/apdeploy/8-0/Cisco_Aironet_3700AP.html.

27. —. Cisco IOS Configuration Guide for Autonomous. Cisco Configuration Guides. [Online] 2 2018. https://www.cisco.com/c/en/us/td/docs/wireless/access_point/15-3-3/configuration/guide/cg15-3-3.pdf.

28. —. Enterprise Mobility 8.1 Design Guide. [Online] 17. 11 2017. https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide.pdf.

29. **Kim, Patrick Croak and Young.** Site Survey Guidelines for WLAN Deployment. Cisco TAC Engineers. [Online] 10. 4 2013. https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.pdf. 116057.

30. **Ruckus.** AP Deployment Guide Best Practices Design Guide. [Online] 6. 3 2018. https://ruckus-support.s3.amazonaws.com/private/documents/1345/AP%20Best%20Practices%20Deployment%20Guide.pdf?AWSAccessKeyId=AKIAJM3QLNNKLOV235TQ&Expires=1520876567&Signature=ifk00l2ZplOmcGkDMhjky0EUzDI%3D.

31. BusinessDictionary - single point of failure. BusinessDictionary. [Online] [Citace: 12. 3 2018.] http://www.businessdictionary.com/definition/single-point-of-failure.html.

32. **Cisco.** The Benefits of Centralization in Wireless LANs via the Cisco Unified Wireless Network . Cisco White Paper. [Online] 2006. https://www.cisco.com/web/AP/wireless/pdf/Benefits_of_centralizedWLan.pdf.

33. —. Enterprise Mobility 8.5 Deployment Guide. Cisco white Paper. [Online] 5. 12 2017. https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-

5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide.pdf.

34. —. Cisco Catalyst 3560 Series Switches Data Sheet. Data Sheets. [Online] 5. 8 2014. https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3560-series-switches/product_data_sheet09186a00801f3d7d.pdf.

35. —. Cisco 100 Series Unmanaged Switches Cisco Small Business Data Sheet. Data Sheets. [Online] 7. 8 2012. https://www.cisco.com/c/en/us/products/collateral/switches/small-business-100-series-unmanaged-switches/datasheet_C78-582017.pdf.

36. Cisco Aironet 1140 Series Access Point. Data Sheet. [Online] 16. 11 2015. https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1130-ag-series/datasheet_c78-502793.pdf.

37. **Hardware, Tom's.** Test Gear: Cisco Aironet 1142 And Aruba AP125. Review. [Online] [obrázek], 17. 8 2009. http://www.tomshardware.com/reviews/beamforming-wifi-ruckus,2390-9.html.

38. **Cisco.** Cisco 2500 Series Wireless Controllers. Data Sheet. [Online] 13. 2 2017. https://www.cisco.com/c/en/us/products/collateral/wireless/2500-series-wireless-controllers/data_sheet_c78-645111.pdf.

39. —. Wireless LAN Controller (WLC) Design and Features FAQ. FAQ. [Online] Cisco, 2. 4 2015. https://www.cisco.com/c/en/us/support/docs/wireless/wireless-lan-controller-software/118833-wlc-design-ftrs-faq.pdf.

40. Enterprise Best Practices for iOS devices and Mac computers on Cisco Wireless LAN. White Paper. [Online] 1 2018. https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/8-6/Enterprise_Best_Practices_for_iOS_devices_and_Mac_computers_on_Cisco_Wireless_LAN.pdf.

41. **Ruckus.** ZoneDirector™ 1100. data sheet. [Online] http://www.settelecom.nl/bost/pdf/ds-zonedirector-1100.pdf.

42. —. When should I use SmartRoam? Konwledge. [Online] 13. 3 2018. https://support.ruckuswireless.com/answers/000002277.

43. —. ZoneFlex™ 7372. data sheet. [Online] http://a030f85c1e25003d7609-b98377aee968aad08453374eb1df3398.r40.cf2.rackcdn.com/datasheets/ds-zoneflex-7372.pdf.

44. —. Ruckus Wireless ZoneDirector Quick Setup Guide. Technical Documents. [Online] 6. 3 2018. https://ruckus-support.s3.amazonaws.com/private/documents/296/800-70433-001_-_ZD_QSG_%28QSG_format%29_-_Rev_B_-_20130301.pdf?AWSAccessKeyId=AKIAJM3QLNNKLOV235TQ&Expires=1521059232&Signature=mykH%2BVQ%2BcWBnvRGyNM27TOMqrv4%3D.

45. —. Ruckus Wireless™ ZoneDirector™ Release 9.10 User Guide. Technical Documents. [Online] 6. 3 2018. https://ruckus-support.s3.amazonaws.com/private/documents/676/ZoneDirector%209.10%20User%20Guide%20-%20Rev%20B%20-%2020150320.pdf?AWSAccessKeyId=AKIAJM3QLNNKLOV235TQ&Expires=1521059412&Signature=adL9lxle4U1WdDGx6F2ReXQcFNA%3D.

46. **Cisco.** Site Survey Guidelines for WLAN Deployment. TechNotes. [Online] 10. 4 2013. https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.pdf.

47. PingPlotter Version 5 Manual. How It works. [Online] 2017. https://www.pingplotter.com/files/pdf/pingplotter_v5manual.pdf.

48. **iperf.** iperf3: A TCP, UDP, and SCTP network bandwidth measurement tool. GitHub. [Online] 8 2017. https://github.com/esnet/iperf.

49. **Štrauch, Adam.** Iperf: měření rychlosti spojení. Root.cz. [Online] 27. 7 2012. https://www.root.cz/clanky/iperf-mereni-rychlosti-spojeni/.

50. **Microsoft.** Analyze the wireless network report. Microsoft Support. [Online] Microsoft, 5. 10 2016. https://support.microsoft.com/en-us/help/4000462/windows-10-analyzing-wireless-network-report.

51. **TamoSoft.** TamoSoft® Throughput Test. Products. [Online] TamoSoft. https://www.tamos.com/products/throughput-test/.

10 Přílohy

10.1 Výpisy konfigurací

10.1.1 Wi-Fi přístupový bod: Cisco Aironet SAP1142i „A“

```
Current configuration : 2014 bytes
!
version 15.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname TEST-Cisco-SAP1142i-A
!
!
logging rate-limit console 9
enable secret 5 $1$Cy1c$/m1vwP65UrbsEmt/MtL3B1
!
no aaa new-model
no ip source-route
no ip cef
!
!
!
!
dot11 pause-time 100
dot11 syslog
!
dot11 ssid TEST-Cisco-SAP1142i
  authentication open
  authentication key-management wpa version 2
  guest-mode
  wpa-psk ascii 7 091D1C5A4D50414553555D
!
!
!
no ipv6 cef
!
!
username Cisco password 7 123A0C041104
!
!
bridge irb
!
```

```
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid TEST-Cisco-SAP1142i
 !
 antenna gain 0
 channel least-congested 2412 2437 2462
 station-role root access-point fallback shutdown
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid TEST-Cisco-SAP1142i
 !
 antenna gain 0
 peakdetect
 no dfs band block
 channel dfs
 station-role root access-point fallback shutdown
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
```

```
 no bridge-group 1 source-learning
!
interface BVI1
 mac-address d48c.b53c.3b4d
 ip address 10.16.11.12 255.255.255.0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
!
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
 login local
 transport input all
!
end
```

10.1.2 Kontroler: Cisco AIR-CT2504-K9

```
# WLC Config Begin <Sat Mar 31 10:20:49 2018>
! Number of APs: 3
! Power Supply 1: Absent
! Power Supply 2: Absent
! PID: AIR-CT2504-K9,  SN: PSJ15320A03
! Product Version: 8.3.133.0
!
! ******************** PORT SUMMARY **********************
!
!            STP   Admin   Physical   Physical   Link   Link
! Pr  Type   Stat   Mode     Mode      Status   Status  Trap
POE
! -- ------- ---- ------- ---------- ---------- ------ ------- -
------
! 1  Normal  Forw Enable  Auto       1000 Full  Up     Enable
N/A
! 2  Normal  Disa Enable  Auto       1000 Full  Down   Enable
N/A
! 3  Normal  Disa Enable  Auto       1000 Full  Down   Enable
Enable  (Power Off)
```

```
! 4  Normal  Disa Enable  Auto       1000 Full  Down   Enable
Enable  (Power Off)
!
! ******************** CDP NEIGHBOUR SUMMARY
**********************
!
! Capability Codes: R - Router, T - Trans Bridge, B - Source
Route Bridge
!                   S - Switch, H - Host, I - IGMP, r -
Repeater,
!                   M - Remotely Managed Device
!
! Device ID        Local Intrfce     Holdtme    Capability
Platform  Port ID
! m-sw01           Gig 0/0/1         171            S I     WS-
C3560- Gig 0/1
! LAP-1142-5057.a0ca.d253
!                  Gig 0/0/1         148          T B I    AIR-
LAP11 Gig 0
! LAP-1142-d48c.b53c.3b3b
!                  Gig 0/0/1         160          T B I    AIR-
LAP11 Gig 0
! LAP-1142-d48c.b504.8c5d
!                  Gig 0/0/1         155          T B I    AIR-
LAP11 Gig 0

config msglog level verbose
config network mgmt-via-wireless enable
config network webmode enable
config network rf-network-name AP-M
config network multicast l2mcast disable management
config network multicast l2mcast disable service-port
config network multicast l2mcast disable virtual
config network telnet enable
config network master-base enable
config location expiry tags 5
config sys-nas Cisco_de:3f:04
config switchconfig strong-pwd lockout time mgmtuser 5
config switchconfig strong-pwd lockout attempts mgmtuser 3
config rf-profile channel add 36 High-Client-Density-802.11a
config rf-profile channel add 40 High-Client-Density-802.11a
config rf-profile channel add 44 High-Client-Density-802.11a
config rf-profile channel add 48 High-Client-Density-802.11a
config rf-profile channel add 52 High-Client-Density-802.11a
config rf-profile channel add 56 High-Client-Density-802.11a
config rf-profile channel add 60 High-Client-Density-802.11a
config rf-profile channel add 64 High-Client-Density-802.11a
config rf-profile channel chan-width 20 High-Client-Density-
802.11a
config rf-profile data-rates 802.11a disabled 6 High-Client-
Density-802.11a
config rf-profile data-rates 802.11a disabled 9 High-Client-
Density-802.11a
```

```
config rf-profile data-rates 802.11a mandatory 12 High-Client-
Density-802.11a
config rf-profile data-rates 802.11a supported 18 High-Client-
Density-802.11a
config rf-profile data-rates 802.11a mandatory 24 High-Client-
Density-802.11a
config rf-profile data-rates 802.11a supported 36 High-Client-
Density-802.11a
config rf-profile data-rates 802.11a supported 48 High-Client-
Density-802.11a
config rf-profile data-rates 802.11a supported 54 High-Client-
Density-802.11a
config rf-profile create 802.11a High-Client-Density-802.11a
config rf-profile tx-power-control-thresh-v1 -65 High-Client-
Density-802.11a
config rf-profile rx-sop threshold -78 High-Client-Density-
802.11a
config rf-profile tx-power-min 7 High-Client-Density-802.11a
config rf-profile channel add 1 High-Client-Density-802.11bg
config rf-profile channel add 6 High-Client-Density-802.11bg
config rf-profile channel add 11 High-Client-Density-802.11bg
config rf-profile channel chan-width 20 High-Client-Density-
802.11bg
config rf-profile data-rates 802.11b disabled 1 High-Client-
Density-802.11bg
config rf-profile data-rates 802.11b disabled 2 High-Client-
Density-802.11bg
config rf-profile data-rates 802.11b disabled 5.5 High-Client-
Density-802.11bg
config rf-profile data-rates 802.11b disabled 11 High-Client-
Density-802.11bg
config rf-profile data-rates 802.11b disabled 6 High-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 9 High-Client-
Density-802.11bg
config rf-profile data-rates 802.11b mandatory 12 High-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 18 High-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 24 High-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 36 High-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 48 High-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 54 High-Client-
Density-802.11bg
config rf-profile create 802.11b High-Client-Density-802.11bg
config rf-profile rx-sop threshold -82 High-Client-Density-
802.11bg
config rf-profile tx-power-min 7 High-Client-Density-802.11bg
config rf-profile channel add 36 Low-Client-Density-802.11a
config rf-profile channel add 40 Low-Client-Density-802.11a
```

```
config rf-profile channel add 44 Low-Client-Density-802.11a
config rf-profile channel add 48 Low-Client-Density-802.11a
config rf-profile channel add 52 Low-Client-Density-802.11a
config rf-profile channel add 56 Low-Client-Density-802.11a
config rf-profile channel add 60 Low-Client-Density-802.11a
config rf-profile channel add 64 Low-Client-Density-802.11a
config rf-profile channel chan-width 20 Low-Client-Density-
802.11a
config rf-profile data-rates 802.11a mandatory 6 Low-Client-
Density-802.11a
config rf-profile data-rates 802.11a supported 9 Low-Client-
Density-802.11a
config rf-profile data-rates 802.11a mandatory 12 Low-Client-
Density-802.11a
config rf-profile data-rates 802.11a supported 18 Low-Client-
Density-802.11a
config rf-profile data-rates 802.11a mandatory 24 Low-Client-
Density-802.11a
config rf-profile data-rates 802.11a supported 36 Low-Client-
Density-802.11a
config rf-profile data-rates 802.11a supported 48 Low-Client-
Density-802.11a
config rf-profile data-rates 802.11a supported 54 Low-Client-
Density-802.11a
config rf-profile create 802.11a Low-Client-Density-802.11a
config rf-profile tx-power-control-thresh-v1 -60 Low-Client-
Density-802.11a
config rf-profile rx-sop threshold -80 Low-Client-Density-
802.11a
config rf-profile coverage exception 2 Low-Client-Density-
802.11a
config rf-profile coverage voice -90 Low-Client-Density-802.11a
config rf-profile coverage data -90 Low-Client-Density-802.11a
config rf-profile channel add 1 Low-Client-Density-802.11bg
config rf-profile channel add 6 Low-Client-Density-802.11bg
config rf-profile channel add 11 Low-Client-Density-802.11bg
config rf-profile channel chan-width 20 Low-Client-Density-
802.11bg
config rf-profile data-rates 802.11b mandatory 1 Low-Client-
Density-802.11bg
config rf-profile data-rates 802.11b mandatory 2 Low-Client-
Density-802.11bg
config rf-profile data-rates 802.11b mandatory 5.5 Low-Client-
Density-802.11bg
config rf-profile data-rates 802.11b mandatory 11 Low-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 6 Low-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 9 Low-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 12 Low-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 18 Low-Client-
```

```
Density-802.11bg
config rf-profile data-rates 802.11b supported 24 Low-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 36 Low-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 48 Low-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 54 Low-Client-
Density-802.11bg
config rf-profile create 802.11b Low-Client-Density-802.11bg
config rf-profile tx-power-control-thresh-v1 -65 Low-Client-
Density-802.11bg
config rf-profile rx-sop threshold -85 Low-Client-Density-
802.11bg
config rf-profile coverage exception 2 Low-Client-Density-
802.11bg
config rf-profile coverage voice -90 Low-Client-Density-802.11bg
config rf-profile coverage data -90 Low-Client-Density-802.11bg
config rf-profile channel add 36 Typical-Client-Density-802.11a
config rf-profile channel add 40 Typical-Client-Density-802.11a
config rf-profile channel add 44 Typical-Client-Density-802.11a
config rf-profile channel add 48 Typical-Client-Density-802.11a
config rf-profile channel add 52 Typical-Client-Density-802.11a
config rf-profile channel add 56 Typical-Client-Density-802.11a
config rf-profile channel add 60 Typical-Client-Density-802.11a
config rf-profile channel add 64 Typical-Client-Density-802.11a
config rf-profile channel chan-width 20 Typical-Client-Density-
802.11a
config rf-profile data-rates 802.11a mandatory 6 Typical-Client-
Density-802.11a
config rf-profile data-rates 802.11a supported 9 Typical-Client-
Density-802.11a
config rf-profile data-rates 802.11a mandatory 12 Typical-
Client-Density-802.11a
config rf-profile data-rates 802.11a supported 18 Typical-
Client-Density-802.11a
config rf-profile data-rates 802.11a mandatory 24 Typical-
Client-Density-802.11a
config rf-profile data-rates 802.11a supported 36 Typical-
Client-Density-802.11a
config rf-profile data-rates 802.11a supported 48 Typical-
Client-Density-802.11a
config rf-profile data-rates 802.11a supported 54 Typical-
Client-Density-802.11a
config rf-profile create 802.11a Typical-Client-Density-802.11a
config rf-profile channel add 1 Typical-Client-Density-802.11bg
config rf-profile channel add 6 Typical-Client-Density-802.11bg
config rf-profile channel add 11 Typical-Client-Density-802.11bg
config rf-profile channel chan-width 20 Typical-Client-Density-
802.11bg
config rf-profile data-rates 802.11b disabled 1 Typical-Client-
Density-802.11bg
config rf-profile data-rates 802.11b disabled 2 Typical-Client-
```

```
Density-802.11bg
config rf-profile data-rates 802.11b disabled 5.5 Typical-
Client-Density-802.11bg
config rf-profile data-rates 802.11b disabled 11 Typical-Client-
Density-802.11bg
config rf-profile data-rates 802.11b disabled 6 Typical-Client-
Density-802.11bg
config rf-profile data-rates 802.11b supported 9 Typical-Client-
Density-802.11bg
config rf-profile data-rates 802.11b mandatory 12 Typical-
Client-Density-802.11bg
config rf-profile data-rates 802.11b supported 18 Typical-
Client-Density-802.11bg
config rf-profile data-rates 802.11b supported 24 Typical-
Client-Density-802.11bg
config rf-profile data-rates 802.11b supported 36 Typical-
Client-Density-802.11bg
config rf-profile data-rates 802.11b supported 48 Typical-
Client-Density-802.11bg
config rf-profile data-rates 802.11b supported 54 Typical-
Client-Density-802.11bg
config rf-profile create 802.11b Typical-Client-Density-802.11bg
config rf-profile channel add 1 test
config rf-profile channel add 6 test
config rf-profile channel add 11 test
config rf-profile channel chan-width 20 test
config rf-profile data-rates 802.11b disabled 1 test
config rf-profile data-rates 802.11b disabled 2 test
config rf-profile data-rates 802.11b disabled 5.5 test
config rf-profile data-rates 802.11b disabled 11 test
config rf-profile data-rates 802.11b disabled 6 test
config rf-profile data-rates 802.11b supported 9 test
config rf-profile data-rates 802.11b mandatory 12 test
config rf-profile data-rates 802.11b supported 18 test
config rf-profile data-rates 802.11b supported 24 test
config rf-profile data-rates 802.11b supported 36 test
config rf-profile data-rates 802.11b supported 48 test
config rf-profile data-rates 802.11b supported 54 test
config rf-profile create 802.11b test
config macfilter add 9c:af:ca:01:df:08 0 management
config macfilter add d0:72:dc:ac:2a:56 0 management
config 802.11a cac voice sip codec g711 sample-interval 20
config 802.11a cac voice sip bandwidth 64 sample-interval 20
config 802.11a rssi-check enable
config 802.11a l2roam rf-params custom -59 3 -54 1
config 802.11a rate disabled 6
config 802.11a rate disabled 9
config 802.11a rssi-threshold -65
config flexconnect group default-flex-group radius ap server-key
encrypt 1 9d8aae5020e74e62a8f644ffa0788bf4
a88e23907fa99e047d3d42ebf6305b4aa6c2be72
c85499cc85cbc6ae1983803f1f7f5592cde558b1278c5b03f00bca73bb2cc8
config flexconnect group default-flex-group radius ap authority
```

```
info "Cisco A_ID"
config flexconnect group default-flex-group radius ap authority
id 436973636f00000000000000000000
config flexconnect group default-flex-group add
config certificate generate webauth
config certificate generate webadmin
config license boot base
config 802.11b cac voice sip codec g711 sample-interval 20
config 802.11b cac voice sip bandwidth 64 sample-interval 20
config 802.11b 11gsupport enable
config 802.11b l2roam rf-params custom -55 3 -50 5
config mobility group domain AP-M
config logging buffered informational
config logging buffered 6
config logging syslog level informational
config logging syslog level 6
config logging traceinfo disable debugging
config netuser add encrypt username test password 1
095ac62183e923a969efc3edcc8ac30a
87c46f51ebdb7cde76aaae44d5e8c1551dcc60c8 16
27a6ab5144474cf8a093f7f3086d4f61000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000
0000 wlan 3 usertype permanent description
config radius callstationidtype ipaddr
config country CZ
config countries-list add CZ
config nmsp notification interval rssi rfid 2
config interface address management 10.16.11.10 255.255.255.0
10.16.11.1
config interface dhcp management primary 10.16.11.1 secondary
10.16.11.10
config interface dhcp management proxy-mode disable
config interface port management 1
config interface address virtual 2.2.2.3
config interface address dynamic-interface guest101 10.1.0.2
255.255.255.0 10.1.0.1
config interface vlan guest101 101
config interface dhcp dynamic-interface guest101 primary
10.1.0.1
config interface dhcp dynamic-interface guest101 proxy-mode
disable
config interface create guest101 101
config interface port guest101 2
config interface address dynamic-interface guest102 10.2.0.2
255.255.255.0 10.2.0.1
config interface vlan guest102 102
config interface dhcp dynamic-interface guest102 proxy-mode
disable
config interface create guest102 102
config interface port guest102 1
config interface address dynamic-interface guest103 10.3.0.2
255.255.255.0 10.3.0.1
config interface vlan guest103 103
```

```
config interface dhcp dynamic-interface guest103 proxy-mode
disable
config interface create guest103 103
config interface port guest103 1
config database size 2048
config mgmtuser add encrypt jiri.mares 1
4b2801496a2a216100f027da50733bca
3ae5de6dab3a8ef7eb74aaa339bd05f322c8bc7f 16
02e8f69d1dee3b73ebcddaad0b8f527300000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000 read-write
config mgmtuser telnet jiri.mares enable
config sysname Cisco_de:3f:04
config mesh convergence
config mesh ethernet-bridging vlan-transparent disable
config mdns profile service add default-mdns-profile AirTunes
config mdns profile service add default-mdns-profile Airplay
config mdns profile service add default-mdns-profile
HP_Photosmart_Printer_1
config mdns profile service add default-mdns-profile
HP_Photosmart_Printer_2
config mdns profile service add default-mdns-profile HomeSharing
config mdns profile service add default-mdns-profile Printer-IPP
config mdns profile service add default-mdns-profile Printer-
IPPS
config mdns profile service add default-mdns-profile Printer-LPD
config mdns profile service add default-mdns-profile Printer-
SOCKET
config mdns profile create default-mdns-profile
config mdns snooping enable
config mdns policy service-group user-role add default-mdns-
policy admin
config mdns policy service-group create default-mdns-policy
"Default Access Policy created by WLC"
config mdns service origin all AirTunes
config mdns service create AirTunes _raop._tcp.local. origin all
lss disable
config mdns service origin all Airplay
config mdns service create Airplay _airplay._tcp.local. origin
all lss disable
config mdns service origin all HP_Photosmart_Printer_1
config mdns service query enable HP_Photosmart_Printer_1
config mdns service create HP_Photosmart_Printer_1
_universal._sub._ipp._tcp.local. origin all lss disable query
enable
config mdns service origin all HP_Photosmart_Printer_2
config mdns service query enable HP_Photosmart_Printer_2
config mdns service create HP_Photosmart_Printer_2
_cups._sub._ipp._tcp.local. origin all lss disable query enable
config mdns service origin all HomeSharing
config mdns service query enable HomeSharing
config mdns service create HomeSharing _home-sharing._tcp.local.
origin all lss disable query enable
```

```
config mdns service origin all Printer-IPP
config mdns service create Printer-IPP _ipp._tcp.local. origin
all lss disable
config mdns service origin all Printer-IPPS
config mdns service create Printer-IPPS _ipps._tcp.local. origin
all lss disable
config mdns service origin all Printer-LPD
config mdns service create Printer-LPD _printer._tcp.local.
origin all lss disable
config mdns service origin all Printer-SOCKET
config mdns service create Printer-SOCKET _pdl-
datastream._tcp.local. origin all lss disable
config time ntp interval 3600
config time ntp server 1 46.243.51.34
config time ntp server 2 195.113.144.201
config time timezone location 14
config auth-list add mic 68:ef:bd:9b:e2:16
config auth-list add mic 68:ef:bd:9b:e1:6e
config wlan avc 1 visibility enable
config wlan wmm allow 1
config wlan avc 2 visibility enable
config wlan wmm allow 2
config wlan wmm allow 3
config wlan wmm allow 4
config wlan wmm allow 5
config wlan bss-transition disassociation-imminent oproam-timer
0 5
config wlan bss-transition enable 5
config wlan mfp client enable 1
config wlan mfp client enable 2
config wlan mfp client enable 3
config wlan peer-blocking drop 3
config wlan mfp client enable 4
config wlan mfp client enable 5
config wlan broadcast-ssid enable 1
config wlan create 1 m1 m1
config wlan exclusionlist 1 60
config wlan broadcast-ssid enable 2
config wlan create 2 guest101 m5
config wlan exclusionlist 2 60
config wlan broadcast-ssid enable 3
config wlan create 3 guest102 guest102
config wlan exclusionlist 3 60
config wlan broadcast-ssid enable 4
config wlan create 4 guest103 guest103
config wlan exclusionlist 4 60
config wlan broadcast-ssid enable 5
config wlan radio 5 802.11a-only
config wlan create 5 TEST-Cisco-WLC2504 TEST-Cisco-WLC2504
config wlan exclusionlist 5 60
config wlan dms enable 5
config wlan interface 1 management
config wlan security wpa akm psk set-key hex encrypt 1
```

```
5bf7a1bd9bd40a372638eda067d86b75
aa20647c9931aac1e442bae527418c7a81ccb6fa 48
66310d928cbc10cac678b6c337bb7be4039c193ce78b4f2f4c394e1b4bb2a516
ada8b57979972273db2d6395dd358908000000000000000000000000000000000
000000000000000000000000000000015ab97880000000000001600000000
060600010000000014e5730000000000101bd428000000000000020600000000
12c000000000000014e5730000000000 1
config wlan security wpa akm psk enable 1
config wlan security wpa akm 802.1x disable 1
config wlan security wpa enable 1
config wlan security ft over-the-ds disable 1
config wlan security web-auth server-precedence 1 local radius
ldap
config wlan interface 2 guest101
config wlan security wpa akm psk set-key hex encrypt 1
dc75530651fc43aca505dba75d2850f2
0ba9656a7f4fe497c021eb2771ffd7b676063af3 48
7850d158c684ae2597963b2e53a078b0162ac57154b51adb188a09fa72798586
006123e3d4d585ca15811d7b5e328efd000000000000000000000000000000000
000000000000000000000000000000015abaee000000000000001600000000
060600010000000014e5730000000000101bd428000000000000020600000000
12c000000000000014e5730000000000 2
config wlan security wpa akm psk enable 2
config wlan security wpa akm 802.1x disable 2
config wlan security wpa enable 2
config wlan security ft over-the-ds disable 2
config wlan security web-auth server-precedence 2 local radius
ldap
config wlan interface 3 guest102
config wlan security wpa akm 802.1x disable 3
config wlan security wpa wpa2 ciphers aes disable 3
config wlan security wpa wpa2 disable 3
config wlan security wpa disable 3
config wlan security web-passthrough email-input enable 3
config wlan security web-passthrough enable 3
config wlan security web-auth server-precedence 3 local radius
ldap
config wlan interface 4 guest103
config wlan security wpa akm 802.1x disable 4
config wlan security wpa wpa2 ciphers aes disable 4
config wlan security wpa wpa2 disable 4
config wlan security wpa disable 4
config wlan security web-auth server-precedence 4 local radius
ldap
config wlan assisted-roaming neighbor-list enable 5
config wlan interface 5 management
config wlan security wpa akm psk set-key hex encrypt 1
1f289df83cec2a861acbea4a15d70ade
2924ac774b713bb5f950c9c4a7d299ab34bbeb58 48
0e54456f3519375b470134feb0d077d8d4b7c7fc88276f3f5e390fabf6125881
9be544801cf653ca9e24a42375d8215e000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000
```

```
00000000000000000000000000000000 5
config wlan security wpa akm psk enable 5
config wlan security wpa akm 802.1x disable 5
config wlan security wpa enable 5
config wlan security ft adaptive enable 5
config wlan security web-auth server-precedence 5 local radius
ldap
config wlan apgroup add mar
config wlan apgroup qinq tagging eap-sim-aka mar enable
config wlan apgroup add mar-tes-pek
config wlan apgroup qinq tagging eap-sim-aka mar-tes-pek enable
config wlan apgroup add tes-pek
config wlan apgroup qinq tagging eap-sim-aka tes-pek enable
config wlan apgroup nasid Cisco_de:3f:04 mar
config wlan apgroup nasid Cisco_de:3f:04 mar-tes-pek
config wlan apgroup nasid Cisco_de:3f:04 tes-pek
config wlan session-timeout 1 0
config wlan session-timeout 2 1800
config wlan session-timeout 3 1800
config wlan session-timeout 4 1800
config wlan session-timeout 5 0
config wlan enable 1
config dhcp dns-servers guest102 10.2.0.2 10.2.0.1 8.8.8.8
config dhcp default-router managment 10.16.11.1
config dhcp network managment 10.16.11.0 255.255.255.0
config dhcp address-pool managment 10.16.11.200 10.16.11.250
config dhcp lease managment 600
config dhcp default-router guest102 10.2.0.1
config dhcp network guest102 10.2.0.0 255.255.255.0
config dhcp address-pool guest102 10.2.0.201 10.2.0.210
config dhcp lease guest102 86400
config dhcp create-scope managment
config dhcp create-scope guest102
config advanced 802.11b channel add 1
config advanced 802.11b channel add 6
config advanced 802.11b channel add 11
config advanced 802.11a channel add 36
config advanced 802.11a channel add 40
config advanced 802.11a channel add 44
config advanced 802.11a channel add 48
config advanced 802.11a channel add 52
config advanced 802.11a channel add 56
config advanced 802.11a channel add 60
config advanced 802.11a channel add 64
config advanced 802.11a coverage data rssi-threshold -72
config advanced 802.11a coverage voice rssi-threshold -65
config advanced 802.11a optimized-roaming interval 5
config advanced 802.11a optimized-roaming datarate 54
config advanced 802.11a optimized-roaming enable
config advanced probe limit 2 500
config rfid timeout 1200
config rfid status enable
config rfid mobility pango disable
```

```
config ap bhrate 0 all
config ap dtls-version dtls_all
config ap preferred-mode ipv4 all
config ap packet-dump capture-time 10
config ap packet-dump buffer-size 2048
config ap packet-dump truncate 0
transfer upload path /
transfer upload serverip 10.16.11.81
transfer upload datatype config
transfer upload filename config.txt
transfer download path /
transfer download serverip 10.16.11.81
transfer download filename config.txt

# WLC Config End <Sat Mar 31 10:21:00 2018>
```

10.1.3 Kontroler: Ruckus ZoneDirector 1106

```
Protocol Mode= IPv4-Only
Device IP Address:
 Mode= Manual
 IP Address= 192.168.0.2
 Netmask= 255.255.255.0
 Gateway Address= 192.168.0.1
 Primary DNS=
 Secondary DNS=

Management VLAN:
 VLAN ID= 1

Country Code:
 Code= Czech Republic

Identity:
 Name= ZoneDirector1106

Session Statistics:
 Enable= false
 Limited Unauthorized Session= true

NTP:
 Status= Enabled
 Address= ntp.ruckuswireless.com

Log:
 Status= Disabled
 Address=
```

```
 Facility=
 Priority=
 AP Facility=
 AP Priority=
 event log level= 2

Tunnel MTU:
 Tunnel MTU= 1500

Bonjour Service:
 Status= Enabled

Telnet Server:
 Status= Disabled

FTP Server:
 Status= Enabled
 Anonynous Status= Disabled

FlexMaster:
 Status= Disabled
 Address=
 Interval= 15

login warning:
 Status= Disabled
 content= "Warning, you are logging into device for authorized user only. If you
are not an authorized user, please click Quit; otherwise click Continue to login."

EAPoL Key no Retry:
 Status= Disabled

AAA:
 ID:
  1:
   Name= Local Database
   Type= Local

  2:
   Name= Guest Accounts
   Type= Guest


DHCP servers for DHCP relay agent:

Administrator Name/Password:
 Name= super
```

```
 Password= ********
 Authenticate:
  Mode= Authenticate using the admin name and password

Management ACL:

AP:
 ID:
  1:
   MAC Address= 24:c9:a1:04:2a:20
   Model= zf7372
   Approved= Yes
   Device Name= RuckusAP
   Description=
   Location=
   GPS=
   CERT = Complex
   Bonjour-policy=
   Group Name= System Default
   Channel Range:
    A/N= 36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136
(Disallowed= )
    B/G/N= 1,2,3,4,5,6,7,8,9,10,11,12,13 (Disallowed= )
   Radio a/n:
    Channelization= Auto
    Channel= Auto
    WLAN Services enabled= Yes
    Tx. Power= Auto
    WLAN Group Name= Default
    Call Admission Control= OFF
    SpectraLink Compatibility= Disabled
   Radio b/g/n:
    Channelization= Auto
    Channel= Auto
    WLAN Services enabled= Yes
    Tx. Power= Auto
    WLAN Group Name= Default
    Call Admission Control= OFF
    SpectraLink Compatibility= Disabled
   Override global ap-model port configuration= No
   Network Setting:
    Protocol mode= Use Parent Setting
    Device IP Settings= Keep AP's Setting
    IP Type= Static
    IP Address= 192.168.0.11
    Netmask= 255.255.255.0
    Gateway= 192.168.0.1
```

```
      Primary DNS Server=
      Secondary DNS Server=

      Device IPv6 Settings= Keep AP's Setting
      IPv6 Type= Auto Configuration
      IPv6 Address= fc00::1
      IPv6 Prefix Length= 7
      IPv6 Gateway=
      IPv6 Primary DNS Server=
      IPv6 Secondary DNS Server=
    Mesh:
      Status= Disabled
    LLDP:
      Status = Use Parent Setting
    LAN Port:
      0:
        Interface= eth0
        Dot1x= None
        LogicalLink= Down
        PhysicalLink= Down
        Label=  LAN1
      0:
        Interface= eth0
        Dot1x= None
        LogicalLink= Down
        PhysicalLink= Down
        Label=  LAN2

  2:
    MAC Address= 2c:5d:93:28:8d:f0
    Model= zf7372
    Approved= Yes
    Device Name= RuckusAP
    Description=
    Location=
    GPS=
    CERT = Complex
    Bonjour-policy=
    Group Name= System Default
    Channel Range:
      A/N= 36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136
(Disallowed= )
      B/G/N= 1,2,3,4,5,6,7,8,9,10,11,12,13 (Disallowed= )
    Radio a/n:
      Channelization= Auto
      Channel= Auto
      WLAN Services enabled= Yes
```

```
  Tx. Power= Auto
  WLAN Group Name= Default
  Call Admission Control= OFF
  SpectraLink Compatibility= Disabled
 Radio b/g/n:
  Channelization= Auto
  Channel= Auto
  WLAN Services enabled= Yes
  Tx. Power= Auto
  WLAN Group Name= Default
  Call Admission Control= OFF
  SpectraLink Compatibility= Disabled
 Override global ap-model port configuration= No
 Network Setting:
  Protocol mode= Use Parent Setting
  Device IP Settings= Keep AP's Setting
  IP Type= Static
  IP Address= 192.168.0.13
  Netmask= 255.255.255.0
  Gateway= 192.168.0.1
  Primary DNS Server=
  Secondary DNS Server=

  Device IPv6 Settings= Keep AP's Setting
  IPv6 Type= Auto Configuration
  IPv6 Address= fc00::1
  IPv6 Prefix Length= 7
  IPv6 Gateway=
  IPv6 Primary DNS Server=
  IPv6 Secondary DNS Server=
 Mesh:
  Status= Disabled
 LLDP:
  Status = Use Parent Setting
 LAN Port:
  0:
   Interface= eth0
   Dot1x= None
   LogicalLink= Down
   PhysicalLink= Down
   Label=  LAN1
  0:
   Interface= eth0
   Dot1x= None
   LogicalLink= Down
   PhysicalLink= Down
   Label=  LAN2
```

```
  3:
    MAC Address= e0:10:7f:2c:0e:d0
    Model= zf7372
    Approved= Yes
    Device Name= RuckusAP
    Description=
    Location=
    GPS=
    CERT = Complex
    Bonjour-policy=
    Group Name= System Default
    Channel Range:
      A/N= 36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136
(Disallowed= )
      B/G/N= 1,2,3,4,5,6,7,8,9,10,11,12,13 (Disallowed= )
    Radio a/n:
      Channelization= Auto
      Channel= Auto
      WLAN Services enabled= Yes
      Tx. Power= Auto
      WLAN Group Name= Default
      Call Admission Control= OFF
      SpectraLink Compatibility= Disabled
    Radio b/g/n:
      Channelization= Auto
      Channel= Auto
      WLAN Services enabled= Yes
      Tx. Power= Auto
      WLAN Group Name= Default
      Call Admission Control= OFF
      SpectraLink Compatibility= Disabled
    Override global ap-model port configuration= No
    Network Setting:
      Protocol mode= Use Parent Setting
      Device IP Settings= Keep AP's Setting
      IP Type= Static
      IP Address= 192.168.0.12
      Netmask= 255.255.255.0
      Gateway= 192.168.0.1
      Primary DNS Server=
      Secondary DNS Server=

      Device IPv6 Settings= Keep AP's Setting
      IPv6 Type= Auto Configuration
      IPv6 Address= fc00::1
      IPv6 Prefix Length= 7
```

```
      IPv6 Gateway=
      IPv6 Primary DNS Server=
      IPv6 Secondary DNS Server=
    Mesh:
      Status= Disabled
    LLDP:
      Status = Use Parent Setting
    LAN Port:
      0:
        Interface= eth0
        Dot1x= None
        LogicalLink= Down
        PhysicalLink= Down
        Label=  LAN1
      0:
        Interface= eth0
        Dot1x= None
        LogicalLink= Down
        PhysicalLink= Down
        Label=  LAN2


Smart Redundancy:
  Status= Disabled
  Peer IP/IPv6 Address=
  Shared Secret=

IPv4 Management Interface:
  Status= Disabled
  IP Address=
  Netmask=
  Gateway Status= Disabled
  Gateway Address=
  VLAN= 1

IPv6 Management Interface:
  Status= Disabled
  IPv6 Address=
  IPv6 Prefix=
  Gateway Status= Disabled
  Gateway Address=
  VLAN= 1

L2/MAC ACL:
  ID:
    1:
      Name= System
```

```
    Description= System
    Restriction= Deny only the stations listed below
    Stations:



SNMP Agent:
 Status= Disabled
 Contact= https://support.ruckuswireless.com/contact_us
 Location= 350 West Java Dr. Sunnyvale, CA 94089 US
 RO Community= public
 RW Community= private

SNMP Trap:
 Format= Version2
 Status= Disabled

SNMPV3 Agent:
 Status= Disabled
 Ro:
  User=
  Authentication Type= MD5
  Authentication Pass Phrase=
  Privacy Type= DES
  Privacy Phrase=
 Rw:
  User=
  Authentication Type= MD5
  Authentication Pass Phrase=
  Privacy Type= DES
  Privacy Phrase=

SNMP Trap:
 Format= Version3
 Status= Disabled

WLAN Service:
 ID:
  1:
   NAME = TEST-Ruckus-ZD1106
   Tx. Rate of Management Frame(2.4GHz) = 2.0Mbps
   Tx. Rate of Management Frame(5GHz)   = 6.0Mbps
   Beacon Interval = 100ms
   SSID = TEST-Ruckus-ZD1106
   Description = TEST-Ruckus-ZD1106
   Type = Standard Usage
   Authentication = open
```

Encryption = wpa2
Algorithm = aes
Passphrase = 1234567899
FT Roaming = Enabled
802.11k Neighbor report = Enabled
Web Authentication = Disabled
Authentication Server = Disabled
Called-Station-Id type = wlan-bssid
Tunnel Mode = Disabled
Background Scanning = Enabled
Max. Clients = 100
Isolation per AP = Disabled
Isolation across AP = Disabled
Zero-IT Activation = Enabled
Priority = High
Load Balancing = Disabled
Band Balancing = Disabled
Dynamic PSK = Enabled
Dynamic PSK Passphrase Length = 62
Dynamic PSK Type = secure
Dynamic PSK Expire Time = unlimited
Dynamic PSK Validity Period = first-use
Limit Dynamic PSK = Disabled
Rate Limiting Uplink = Disabled
Rate Limiting Downlink = Disabled
Auto-Proxy configuration:
  Status = Disabled
Inactivity Timeout:
   Status = Enabled
   Timeout = 5 Minutes
VLAN-ID = 1
Dynamic VLAN = Disabled
Closed System = Disabled
Https Redirection = Disabled
OFDM-Only State = Disabled
Multicast Filter State = Disabled
802.11d State = Enabled
Force DHCP State = Disabled
Force DHCP Timeout = 10
DHCP Option82:
   Status = Disabled
   Option82 sub-Option1 = Disabled
   Option82 sub-Option2 = Disabled
   Option82 sub-Option150 = Disabled
   Option82 sub-Option151 = Disabled
Ignore unauthorized client statistic = Disabled
STA Info Extraction State = Enabled

```
    BSS Minrate = Disabled
    Call Admission Control State = Disabled
    PMK Cache Timeout= 720 minutes
    PMK Cache for Reconnect= Enabled
    NAS-ID Type= wlan-bssid
    Roaming Acct-Interim-Update= Disabled
    PAP Message Authenticator = Enabled
    Send EAP-Failure = Disabled
    L2/MAC = No ACLS
    L3/L4/IP Address = No ACLS
    L3/L4/IPv6 Address = No ACLS
    Precedence = Default
    Proxy ARP = Disabled
    Device Policy = No ACLS
    Vlan Pool = No Pools
    Role based Access Control Policy = Disabled
    SmartRoam = Disabled  Roam-factor = 1
    White List = No ACLS
    Application Visibility = disabled
    Apply Policy Group = No_Denys


WLAN Group:
 ID:
  1:
    Name= Default
    Description= Default WLANs for Access Points
    WLAN Service:
     WLAN1:
      NAME= TEST-Ruckus-ZD1106
      VLAN=


Mosquitto bridge global index file does not exist!
```

10.2 Výstupy měření

10.2.1 Výstupy měření programem Ping Plotter

10.2.1.1 Síť se samostatnými Wi-Fi přístupovými body (Ping Plotter

```
Host Information
1,10.16.11.81,10.16.11.81
Sample Information
2018-03-18 14:25:48Z,2.80
```

2018-03-18 14:25:49Z,1.78
2018-03-18 14:25:49Z,1.83
2018-03-18 14:25:50Z,1.51
2018-03-18 14:25:50Z,1.59
2018-03-18 14:25:51Z,1.75
2018-03-18 14:25:51Z,5.09
2018-03-18 14:25:52Z,2.06
2018-03-18 14:25:52Z,2.05
2018-03-18 14:25:53Z,1.67
2018-03-18 14:25:53Z,2.40
2018-03-18 14:25:54Z,2.59
2018-03-18 14:25:54Z,2.75
2018-03-18 14:25:55Z,3.35
2018-03-18 14:25:55Z,3.03
2018-03-18 14:25:56Z,4.32
2018-03-18 14:25:56Z,2.38
2018-03-18 14:25:57Z,2.03
2018-03-18 14:25:57Z,2.31
2018-03-18 14:25:58Z,2.37
2018-03-18 14:25:58Z,3.48
2018-03-18 14:25:59Z,2.35
2018-03-18 14:25:59Z,2.32
2018-03-18 14:26:00Z,2.05
2018-03-18 14:26:00Z,2.34
2018-03-18 14:26:01Z,2.31
2018-03-18 14:26:01Z,3.45
2018-03-18 14:26:02Z,8.04
2018-03-18 14:26:02Z,2.90
2018-03-18 14:26:03Z,2.19
2018-03-18 14:26:03Z,4.91
2018-03-18 14:26:04Z,2.87
2018-03-18 14:26:04Z,5.35
2018-03-18 14:26:05Z,3.20
2018-03-18 14:26:05Z,3.64
2018-03-18 14:26:06Z,2.88
2018-03-18 14:26:06Z,2.70
2018-03-18 14:26:07Z,2.55
2018-03-18 14:26:07Z,6.63
2018-03-18 14:26:08Z,94.23
2018-03-18 14:26:08Z,*
2018-03-18 14:26:09Z,1.75
2018-03-18 14:26:09Z,1.89
2018-03-18 14:26:10Z,1.86
2018-03-18 14:26:10Z,1.90

```
2018-03-18 14:26:11Z,1.68
2018-03-18 14:26:11Z,2.44
2018-03-18 14:26:12Z,1.62
2018-03-18 14:26:12Z,1.73
2018-03-18 14:26:13Z,1.56
2018-03-18 14:26:13Z,1.91
2018-03-18 14:26:14Z,1.01
2018-03-18 14:26:14Z,1.71
2018-03-18 14:26:15Z,2.71
2018-03-18 14:26:15Z,1.60
2018-03-18 14:26:16Z,1.70
2018-03-18 14:26:16Z,1.97
2018-03-18 14:26:17Z,2.62
2018-03-18 14:26:17Z,1.69
2018-03-18 14:26:18Z,1.68
2018-03-18 14:26:18Z,1.79
2018-03-18 14:26:19Z,2.36
2018-03-18 14:26:19Z,4.04
2018-03-18 14:26:19Z,4.04
2018-03-18 14:26:20Z,2.28
2018-03-18 14:26:20Z,2.60
2018-03-18 14:26:21Z,4.34
2018-03-18 14:26:21Z,1.43
2018-03-18 14:26:22Z,4.75
2018-03-18 14:26:22Z,2.06
2018-03-18 14:26:23Z,3.61
2018-03-18 14:26:23Z,2.34
2018-03-18 14:26:24Z,3.72
2018-03-18 14:26:24Z,2.18
2018-03-18 14:26:25Z,6.90
2018-03-18 14:26:25Z,3.23
2018-03-18 14:26:26Z,4.46
2018-03-18 14:26:26Z,3.57
2018-03-18 14:26:27Z,2.39
2018-03-18 14:26:27Z,2.31
2018-03-18 14:26:28Z,3.34
2018-03-18 14:26:28Z,160.39
2018-03-18 14:26:29Z,*
2018-03-18 14:26:29Z,2.49
2018-03-18 14:26:30Z,1.71
2018-03-18 14:26:30Z,1.90
2018-03-18 14:26:31Z,1.36
2018-03-18 14:26:31Z,3.56
2018-03-18 14:26:32Z,1.54
```

```
2018-03-18 14:26:32Z,1.64
2018-03-18 14:26:33Z,1.30
2018-03-18 14:26:33Z,1.83
2018-03-18 14:26:34Z,2.15
2018-03-18 14:26:34Z,1.83
2018-03-18 14:26:35Z,1.55
2018-03-18 14:26:35Z,1.95
```

10.2.1.2 Síť s využitím Wi-Fi kontroleru Cisco WLC2504

```
Host Information
1,M1-PRACOVNA-
HER,10.16.11.81
Sample Information
2018-03-18T18:37:57,2.00
2018-03-18T18:37:58,2.00
2018-03-18T18:37:58,2.00
2018-03-18T18:37:59,2.00
2018-03-18T18:37:59,3.00
2018-03-18T18:38:00,2.00
2018-03-18T18:38:00,2.00
2018-03-18T18:38:01,2.00
2018-03-18T18:38:01,2.00
2018-03-18T18:38:02,2.00
2018-03-18T18:38:02,2.00
2018-03-18T18:38:03,3.00
2018-03-18T18:38:03,1.00
2018-03-18T18:38:04,3.00
2018-03-18T18:38:04,2.00
2018-03-18T18:38:05,2.00
2018-03-18T18:38:05,3.00
2018-03-18T18:38:06,3.00
2018-03-18T18:38:06,2.00
2018-03-18T18:38:07,3.00
2018-03-18T18:38:07,3.00
2018-03-18T18:38:08,3.00
2018-03-18T18:38:08,2.00
2018-03-18T18:38:09,3.00
2018-03-18T18:38:09,5.00
2018-03-18T18:38:10,4.00
2018-03-18T18:38:10,4.00
2018-03-18T18:38:11,2.00
2018-03-18T18:38:11,4.00
2018-03-18T18:38:12,3.00
2018-03-18T18:38:12,3.00
```

2018-03-18T18:38:13,2.00
2018-03-18T18:38:13,4.00
2018-03-18T18:38:14,4.00
2018-03-18T18:38:14,4.00
2018-03-18T18:38:15,3.00
2018-03-18T18:38:15,4.00
2018-03-18T18:38:16,2.00
2018-03-18T18:38:16,2.00
2018-03-18T18:38:17,88.00
2018-03-18T18:38:17,4.00
2018-03-18T18:38:18,2.00
2018-03-18T18:38:18,2.00
2018-03-18T18:38:19,2.00
2018-03-18T18:38:19,2.00
2018-03-18T18:38:20,2.00
2018-03-18T18:38:20,2.00
2018-03-18T18:38:21,2.00
2018-03-18T18:38:21,2.00
2018-03-18T18:38:22,2.00
2018-03-18T18:38:22,2.00
2018-03-18T18:38:23,4.00
2018-03-18T18:38:23,2.00
2018-03-18T18:38:24,2.00
2018-03-18T18:38:24,2.00
2018-03-18T18:38:25,2.00
2018-03-18T18:38:25,3.00
2018-03-18T18:38:26,2.00
2018-03-18T18:38:26,2.00
2018-03-18T18:38:27,2.00
2018-03-18T18:38:27,4.00
2018-03-18T18:38:28,3.00
2018-03-18T18:38:28,2.00
2018-03-18T18:38:29,2.00
2018-03-18T18:38:29,2.00
2018-03-18T18:38:30,2.00
2018-03-18T18:38:30,3.00
2018-03-18T18:38:31,7.00
2018-03-18T18:38:31,3.00
2018-03-18T18:38:31,3.00
2018-03-18T18:38:32,3.00
2018-03-18T18:38:32,3.00
2018-03-18T18:38:33,12.00
2018-03-18T18:38:33,*
2018-03-18T18:38:34,4.00

2018-03-18T18:38:34,2.00
2018-03-18T18:38:35,2.00
2018-03-18T18:38:35,3.00
2018-03-18T18:38:36,2.00
2018-03-18T18:38:36,2.00
2018-03-18T18:38:37,2.00
2018-03-18T18:38:37,2.00
2018-03-18T18:38:38,2.00
2018-03-18T18:38:38,2.00
2018-03-18T18:38:39,2.00
2018-03-18T18:38:39,2.00
2018-03-18T18:38:40,2.00
2018-03-18T18:38:40,2.00
2018-03-18T18:38:41,2.00
2018-03-18T18:38:41,2.00
2018-03-18T18:38:42,2.00
2018-03-18T18:38:42,2.00
2018-03-18T18:38:43,2.00
2018-03-18T18:38:43,2.00
2018-03-18T18:38:44,2.00
2018-03-18T18:38:44,6.00
2018-03-18T18:38:45,3.00
2018-03-18T18:38:45,2.00
2018-03-18T18:38:46,6.00
2018-03-18T18:38:46,6.00
2018-03-18T18:38:47,3.00
2018-03-18T18:38:47,2.00
2018-03-18T18:38:48,3.00
2018-03-18T18:38:48,2.00
2018-03-18T18:38:49,2.00
2018-03-18T18:38:49,2.00
2018-03-18T18:38:50,14.00
2018-03-18T18:38:50,2.00
2018-03-18T18:38:51,3.00
2018-03-18T18:38:51,5.00
2018-03-18T18:38:52,3.00
2018-03-18T18:38:52,3.00

10.2.1.3 Síť s využitím Wi-Fi kontroleru Ruckus ZoneDirector 1106

Host Information
1,M1-PRACOVNA-HER,10.16.11.81
Sample Information
2018-03-18T18:42:32,0.00

2018-03-18T18:42:32,2.00
2018-03-18T18:42:33,2.00
2018-03-18T18:42:33,2.00
2018-03-18T18:42:34,2.00
2018-03-18T18:42:34,3.00
2018-03-18T18:42:35,3.00
2018-03-18T18:42:35,2.00
2018-03-18T18:42:36,2.00
2018-03-18T18:42:36,2.00
2018-03-18T18:42:37,2.00
2018-03-18T18:42:37,2.00
2018-03-18T18:42:38,2.00
2018-03-18T18:42:38,2.00
2018-03-18T18:42:39,2.00
2018-03-18T18:42:39,2.00
2018-03-18T18:42:40,2.00
2018-03-18T18:42:40,2.00
2018-03-18T18:42:41,2.00
2018-03-18T18:42:41,2.00
2018-03-18T18:42:42,2.00
2018-03-18T18:42:42,2.00
2018-03-18T18:42:43,2.00
2018-03-18T18:42:43,2.00
2018-03-18T18:42:44,2.00
2018-03-18T18:42:44,2.00
2018-03-18T18:42:45,2.00
2018-03-18T18:42:45,3.00
2018-03-18T18:42:46,2.00
2018-03-18T18:42:46,2.00
2018-03-18T18:42:47,3.00
2018-03-18T18:42:47,3.00
2018-03-18T18:42:48,3.00
2018-03-18T18:42:48,2.00
2018-03-18T18:42:49,2.00
2018-03-18T18:42:49,2.00
2018-03-18T18:42:50,2.00
2018-03-18T18:42:50,3.00
2018-03-18T18:42:51,2.00
2018-03-18T18:42:51,3.00
2018-03-18T18:42:52,2.00
2018-03-18T18:42:52,37.00
2018-03-18T18:42:53,2.00
2018-03-18T18:42:53,2.00
2018-03-18T18:42:54,3.00

2018-03-18T18:42:54,3.00
2018-03-18T18:42:55,3.00
2018-03-18T18:42:55,3.00
2018-03-18T18:42:56,2.00
2018-03-18T18:42:56,3.00
2018-03-18T18:42:57,3.00
2018-03-18T18:42:57,2.00
2018-03-18T18:42:58,2.00
2018-03-18T18:42:58,2.00
2018-03-18T18:42:59,2.00
2018-03-18T18:42:59,2.00
2018-03-18T18:43:00,2.00
2018-03-18T18:43:00,2.00
2018-03-18T18:43:01,2.00
2018-03-18T18:43:01,2.00
2018-03-18T18:43:02,2.00
2018-03-18T18:43:02,2.00
2018-03-18T18:43:03,2.00
2018-03-18T18:43:03,2.00
2018-03-18T18:43:04,2.00
2018-03-18T18:43:04,2.00
2018-03-18T18:43:05,2.00
2018-03-18T18:43:05,2.00
2018-03-18T18:43:06,2.00
2018-03-18T18:43:06,2.00
2018-03-18T18:43:07,2.00
2018-03-18T18:43:07,2.00
2018-03-18T18:43:08,2.00
2018-03-18T18:43:08,2.00
2018-03-18T18:43:09,55.00
2018-03-18T18:43:09,5.00
2018-03-18T18:43:10,2.00
2018-03-18T18:43:10,2.00
2018-03-18T18:43:11,3.00
2018-03-18T18:43:11,5.00
2018-03-18T18:43:12,6.00
2018-03-18T18:43:12,5.00
2018-03-18T18:43:13,5.00
2018-03-18T18:43:13,2.00
2018-03-18T18:43:14,3.00
2018-03-18T18:43:14,2.00
2018-03-18T18:43:15,3.00
2018-03-18T18:43:15,3.00
2018-03-18T18:43:16,2.00

```
2018-03-18T18:43:16,3.00
2018-03-18T18:43:17,2.00
2018-03-18T18:43:17,2.00
2018-03-18T18:43:18,2.00
2018-03-18T18:43:18,2.00
2018-03-18T18:43:19,2.00
2018-03-18T18:43:19,2.00
2018-03-18T18:43:20,2.00
2018-03-18T18:43:20,2.00
2018-03-18T18:43:21,2.00
2018-03-18T18:43:21,2.00
2018-03-18T18:43:22,3.00
2018-03-18T18:43:22,2.00
2018-03-18T18:43:23,1.00
2018-03-18T18:43:23,2.00
2018-03-18T18:43:24,2.00
2018-03-18T18:43:24,4.00
2018-03-18T18:43:25,2.00
2018-03-18T18:43:25,2.00
2018-03-18T18:43:26,2.00
2018-03-18T18:43:26,2.00
```

10.2.2 Výstupy měření programem iPerf

10.2.2.1 Síť se samostatnými Wi-Fi přístupovými body

```
C:\iperf-3.1.3-win64>iperf.exe -c 10.16.11.81 -P 1 -i 1 -p 5001 -f k -t 60
------------------------------------------------------------
Client connecting to 10.16.11.81, TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  3] local 10.16.11.139 port 1663 connected with 10.16.11.81 port 5001
[ ID] Interval       Transfer     Bandwidth
[300]  0.0- 1.0 sec  3944 KBytes  32309 Kbits/sec
[300]  1.0- 2.0 sec  4752 KBytes  38928 Kbits/sec
[300]  2.0- 3.0 sec  4808 KBytes  39387 Kbits/sec
[300]  3.0- 4.0 sec  4656 KBytes  38142 Kbits/sec
[300]  4.0- 5.0 sec  4760 KBytes  38994 Kbits/sec
[300]  5.0- 6.0 sec  4328 KBytes  35455 Kbits/sec
[300]  6.0- 7.0 sec  4512 KBytes  36962 Kbits/sec
[300]  7.0- 8.0 sec  4464 KBytes  36569 Kbits/sec
[300]  8.0- 9.0 sec  4640 KBytes  38011 Kbits/sec
[300]  9.0-10.0 sec  4144 KBytes  33948 Kbits/sec
[300] 10.0-11.0 sec  3960 KBytes  32440 Kbits/sec
[300] 11.0-12.0 sec  4008 KBytes  32834 Kbits/sec
[300] 12.0-13.0 sec  3600 KBytes  29491 Kbits/sec
```

[300]	13.0-14.0	sec	3424	KBytes	28049 Kbits/sec
[300]	14.0-15.0	sec	3936	KBytes	32244 Kbits/sec
[300]	15.0-16.0	sec	3664	KBytes	30015 Kbits/sec
[300]	16.0-17.0	sec	3528	KBytes	28901 Kbits/sec
[300]	17.0-18.0	sec	3592	KBytes	29426 Kbits/sec
[300]	18.0-19.0	sec	3200	KBytes	26214 Kbits/sec
[300]	19.0-20.0	sec	2560	KBytes	20972 Kbits/sec
[300]	20.0-21.0	sec	2048	KBytes	16777 Kbits/sec
[300]	21.0-22.0	sec	1664	KBytes	13631 Kbits/sec
[300]	22.0-23.0	sec	1408	KBytes	11534 Kbits/sec
[300]	23.0-24.0	sec	128	KBytes	1049 Kbits/sec
[300]	24.0-25.0	sec	0.00	KBytes	0.00 Kbits/sec
[300]	25.0-26.0	sec	0.00	KBytes	0.00 Kbits/sec
[300]	26.0-27.0	sec	2560	KBytes	20972 Kbits/sec
[300]	27.0-28.0	sec	4032	KBytes	33030 Kbits/sec
[300]	28.0-29.0	sec	4616	KBytes	37814 Kbits/sec
[300]	29.0-30.0	sec	4064	KBytes	33292 Kbits/sec
[300]	30.0-31.0	sec	3872	KBytes	31719 Kbits/sec
[300]	31.0-32.0	sec	4176	KBytes	34210 Kbits/sec
[300]	32.0-33.0	sec	4176	KBytes	34210 Kbits/sec
[300]	33.0-34.0	sec	3928	KBytes	32178 Kbits/sec
[300]	34.0-35.0	sec	3736	KBytes	30605 Kbits/sec
[300]	35.0-36.0	sec	3776	KBytes	30933 Kbits/sec
[300]	36.0-37.0	sec	3696	KBytes	30278 Kbits/sec
[300]	37.0-38.0	sec	3720	KBytes	30474 Kbits/sec
[300]	38.0-39.0	sec	3520	KBytes	28836 Kbits/sec
[300]	39.0-40.0	sec	3168	KBytes	25952 Kbits/sec
[300]	40.0-41.0	sec	2656	KBytes	21758 Kbits/sec
[300]	41.0-42.0	sec	1920	KBytes	15729 Kbits/sec
[300]	42.0-43.0	sec	1152	KBytes	9437 Kbits/sec
[300]	43.0-44.0	sec	0.00	KBytes	0.00 Kbits/sec
[300]	44.0-45.0	sec	0.00	KBytes	0.00 Kbits/sec
[300]	45.0-46.0	sec	2656	KBytes	21758 Kbits/sec
[300]	46.0-47.0	sec	4280	KBytes	35062 Kbits/sec
[300]	47.0-48.0	sec	4464	KBytes	36569 Kbits/sec
[300]	48.0-49.0	sec	3720	KBytes	30474 Kbits/sec
[300]	49.0-50.0	sec	3760	KBytes	30802 Kbits/sec
[300]	50.0-51.0	sec	3656	KBytes	29950 Kbits/sec
[300]	51.0-52.0	sec	3592	KBytes	29426 Kbits/sec
[300]	52.0-53.0	sec	3224	KBytes	26411 Kbits/sec
[300]	53.0-54.0	sec	3904	KBytes	31982 Kbits/sec
[300]	54.0-55.0	sec	4696	KBytes	38470 Kbits/sec
[300]	55.0-56.0	sec	4288	KBytes	35127 Kbits/sec
[300]	56.0-57.0	sec	4480	KBytes	36700 Kbits/sec
[300]	57.0-58.0	sec	4264	KBytes	34931 Kbits/sec
[300]	58.0-59.0	sec	4032	KBytes	33030 Kbits/sec
[300]	59.0-60.0	sec	4616	KBytes	37814 Kbits/sec

10.2.2.2 Síť s využitím Wi-Fi kontroleru Cisco WLC2504

```
C:\iperf-3.1.3-win64>iperf.exe -c 10.16.11.81 -P 1 -i 1 -p 5001 -f k -t 60
------------------------------------------------------------
Client connecting to 10.16.11.81, TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[ ID] Interval       Transfer     Bandwidth
[300]  0.0- 1.0 sec  2688 KBytes  22020 Kbits/sec
[300]  1.0- 2.0 sec  4752 KBytes  38928 Kbits/sec
[300]  2.0- 3.0 sec  4808 KBytes  39387 Kbits/sec
[300]  3.0- 4.0 sec  4656 KBytes  38142 Kbits/sec
[300]  4.0- 5.0 sec  4760 KBytes  38994 Kbits/sec
[300]  5.0- 6.0 sec  4864 KBytes  39846 Kbits/sec
[300]  6.0- 7.0 sec  4752 KBytes  38928 Kbits/sec
[300]  7.0- 8.0 sec  4808 KBytes  39387 Kbits/sec
[300]  8.0- 9.0 sec  4608 KBytes  37749 Kbits/sec
[300]  9.0-10.0 sec  4608 KBytes  37749 Kbits/sec
[300] 10.0-11.0 sec  4352 KBytes  35652 Kbits/sec
[300] 11.0-12.0 sec  3600 KBytes  29491 Kbits/sec
[300] 12.0-13.0 sec  3584 KBytes  29360 Kbits/sec
[300] 13.0-14.0 sec  4008 KBytes  32834 Kbits/sec
[300] 14.0-15.0 sec  3456 KBytes  28312 Kbits/sec
[300] 15.0-16.0 sec  3072 KBytes  25166 Kbits/sec
[300] 16.0-17.0 sec  2048 KBytes  16777 Kbits/sec
[300] 17.0-18.0 sec  1664 KBytes  13631 Kbits/sec
[300] 18.0-19.0 sec  1152 KBytes  9437  Kbits/sec
[300] 19.0-20.0 sec  640  KBytes  5243  Kbits/sec
[300] 20.0-21.0 sec  2560 KBytes  20972 Kbits/sec
[300] 21.0-22.0 sec  3968 KBytes  32506 Kbits/sec
[300] 22.0-23.0 sec  3840 KBytes  31457 Kbits/sec
[300] 23.0-24.0 sec  4736 KBytes  38797 Kbits/sec
[300] 24.0-25.0 sec  4352 KBytes  35652 Kbits/sec
[300] 25.0-26.0 sec  3840 KBytes  31457 Kbits/sec
[300] 26.0-27.0 sec  3968 KBytes  32506 Kbits/sec
[300] 27.0-28.0 sec  3456 KBytes  28312 Kbits/sec
[300] 28.0-29.0 sec  3712 KBytes  30409 Kbits/sec
[300] 29.0-30.0 sec  4352 KBytes  35652 Kbits/sec
[300] 30.0-31.0 sec  4736 KBytes  38797 Kbits/sec
[300] 31.0-32.0 sec  3968 KBytes  32506 Kbits/sec
[300] 32.0-33.0 sec  4608 KBytes  37749 Kbits/sec
[300] 33.0-34.0 sec  3712 KBytes  30409 Kbits/sec
[300] 34.0-35.0 sec  3872 KBytes  31719 Kbits/sec
[300] 35.0-36.0 sec  3600 KBytes  29491 Kbits/sec
[300] 36.0-37.0 sec  3168 KBytes  25952 Kbits/sec
[300] 37.0-38.0 sec  2656 KBytes  21758 Kbits/sec
[300] 38.0-39.0 sec  1920 KBytes  15729 Kbits/sec
```

[300]	39.0-40.0	sec	0.00	KBytes	0.00 Kbits/sec
[300]	40.0-41.0	sec	2560	KBytes	20972 Kbits/sec
[300]	41.0-42.0	sec	3840	KBytes	31457 Kbits/sec
[300]	42.0-43.0	sec	4352	KBytes	35652 Kbits/sec
[300]	43.0-44.0	sec	4224	KBytes	34603 Kbits/sec
[300]	44.0-45.0	sec	4224	KBytes	34603 Kbits/sec
[300]	45.0-46.0	sec	4144	KBytes	33948 Kbits/sec
[300]	46.0-47.0	sec	3072	KBytes	25166 Kbits/sec
[300]	47.0-48.0	sec	3456	KBytes	28312 Kbits/sec
[300]	48.0-49.0	sec	3712	KBytes	30409 Kbits/sec
[300]	49.0-50.0	sec	3200	KBytes	26214 Kbits/sec
[300]	50.0-51.0	sec	4096	KBytes	33554 Kbits/sec
[300]	51.0-52.0	sec	3968	KBytes	32506 Kbits/sec
[300]	52.0-53.0	sec	4096	KBytes	33554 Kbits/sec
[300]	53.0-54.0	sec	3328	KBytes	27263 Kbits/sec
[300]	54.0-55.0	sec	2688	KBytes	22020 Kbits/sec
[300]	55.0-56.0	sec	4104	KBytes	33620 Kbits/sec
[300]	56.0-57.0	sec	4160	KBytes	34079 Kbits/sec
[300]	57.0-58.0	sec	4280	KBytes	35062 Kbits/sec
[300]	58.0-59.0	sec	4096	KBytes	33554 Kbits/sec
[300]	59.0-60.0	sec	4224	KBytes	34603 Kbits/sec

10.2.2.3 Síť s využitím Wi-Fi kontroleru Ruckus ZoneDirector 1106

```
C:\iperf-3.1.3-win64>iperf.exe -c 10.16.11.81 -P 1 -i 1 -p 5001 -f k -t 60
------------------------------------------------------------
Client connecting to 10.16.11.81, TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
```

[ID]	Interval		Transfer	Bandwidth
[3]	0.0- 1.0	sec	2560 KBytes	20972 Kbits/sec
[3]	1.0- 2.0	sec	4280 KBytes	35062 Kbits/sec
[3]	2.0- 3.0	sec	4608 KBytes	37749 Kbits/sec
[3]	3.0- 4.0	sec	4352 KBytes	35652 Kbits/sec
[3]	4.0- 5.0	sec	4280 KBytes	35062 Kbits/sec
[3]	5.0- 6.0	sec	4736 KBytes	38797 Kbits/sec
[3]	6.0- 7.0	sec	4808 KBytes	39387 Kbits/sec
[3]	7.0- 8.0	sec	4608 KBytes	37749 Kbits/sec
[3]	8.0- 9.0	sec	4752 KBytes	38928 Kbits/sec
[3]	9.0-10.0	sec	3968 KBytes	32506 Kbits/sec
[3]	10.0-11.0	sec	3712 KBytes	30409 Kbits/sec
[3]	11.0-12.0	sec	4224 KBytes	34603 Kbits/sec
[3]	12.0-13.0	sec	3712 KBytes	30409 Kbits/sec
[3]	13.0-14.0	sec	3968 KBytes	32506 Kbits/sec
[3]	14.0-15.0	sec	1536 KBytes	12583 Kbits/sec
[3]	15.0-16.0	sec	3072 KBytes	25166 Kbits/sec
[3]	16.0-17.0	sec	2816 KBytes	23069 Kbits/sec
[3]	17.0-18.0	sec	4096 KBytes	33554 Kbits/sec

[3]	18.0-19.0	sec	3712	KBytes	30409 Kbits/sec
[3]	19.0-20.0	sec	4224	KBytes	34603 Kbits/sec
[3]	20.0-21.0	sec	3584	KBytes	29360 Kbits/sec
[3]	21.0-22.0	sec	3584	KBytes	29360 Kbits/sec
[3]	22.0-23.0	sec	3328	KBytes	27263 Kbits/sec
[3]	23.0-24.0	sec	4224	KBytes	34603 Kbits/sec
[3]	24.0-25.0	sec	4096	KBytes	33554 Kbits/sec
[3]	25.0-26.0	sec	4096	KBytes	33554 Kbits/sec
[3]	26.0-27.0	sec	4280	KBytes	35062 Kbits/sec
[3]	27.0-28.0	sec	4808	KBytes	39387 Kbits/sec
[3]	28.0-29.0	sec	4608	KBytes	37749 Kbits/sec
[3]	29.0-30.0	sec	4752	KBytes	38928 Kbits/sec
[3]	30.0-31.0	sec	4864	KBytes	39846 Kbits/sec
[3]	31.0-32.0	sec	4808	KBytes	39387 Kbits/sec
[3]	32.0-33.0	sec	4280	KBytes	35062 Kbits/sec
[3]	33.0-34.0	sec	4808	KBytes	39387 Kbits/sec
[3]	34.0-35.0	sec	4760	KBytes	38994 Kbits/sec
[3]	35.0-36.0	sec	4808	KBytes	39387 Kbits/sec
[3]	36.0-37.0	sec	4160	KBytes	34079 Kbits/sec
[3]	37.0-38.0	sec	4808	KBytes	39387 Kbits/sec
[3]	38.0-39.0	sec	4736	KBytes	38797 Kbits/sec
[3]	39.0-40.0	sec	3712	KBytes	30409 Kbits/sec
[3]	40.0-41.0	sec	3968	KBytes	32506 Kbits/sec
[3]	41.0-42.0	sec	3968	KBytes	32506 Kbits/sec
[3]	42.0-43.0	sec	3072	KBytes	25166 Kbits/sec
[3]	43.0-44.0	sec	768	KBytes	6291 Kbits/sec
[3]	44.0-45.0	sec	1664	KBytes	13631 Kbits/sec
[3]	45.0-46.0	sec	2560	KBytes	20972 Kbits/sec
[3]	46.0-47.0	sec	4096	KBytes	33554 Kbits/sec
[3]	47.0-48.0	sec	3584	KBytes	29360 Kbits/sec
[3]	48.0-49.0	sec	3584	KBytes	29360 Kbits/sec
[3]	49.0-50.0	sec	3328	KBytes	27263 Kbits/sec
[3]	50.0-51.0	sec	4096	KBytes	33554 Kbits/sec
[3]	51.0-52.0	sec	4608	KBytes	37749 Kbits/sec
[3]	52.0-53.0	sec	4224	KBytes	34603 Kbits/sec
[3]	53.0-54.0	sec	4760	KBytes	38994 Kbits/sec
[3]	54.0-55.0	sec	4808	KBytes	39387 Kbits/sec
[3]	55.0-56.0	sec	4608	KBytes	37749 Kbits/sec
[3]	56.0-57.0	sec	4736	KBytes	38797 Kbits/sec
[3]	57.0-58.0	sec	4352	KBytes	35652 Kbits/sec
[3]	58.0-59.0	sec	4736	KBytes	38797 Kbits/sec
[3]	59.0-60.0	sec	4752	KBytes	38928 Kbits/sec

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor: **Jiří Mareš**

Studium: I14527

Studijní program: B1802 Aplikovaná informatika

Studijní obor: Aplikovaná informatika

Název bakalářské práce: **Analýza přístupů a řešení problematiky roamingu ve Wi-Fi sítích v prostředí Cisco a Ruckus**

Název bakalářské práce AJ: Analysis of approaches and solutions to the problems of roaming in WiFi networks in an environment of Cisco and Ruckus

Cíl, metody, literatura, předpoklady:

Cílem práce je představit principy a navrhnout technické řešení roamingu WiFi sítí s využitím technologií Cisco. Autor práce představí důvody využívání a principy roamingu WiFi sítí s důrazem na technické řešení dané problematiky. V praktické části autor představí modelové řešení, provede jeho realizaci a provede měření základních parametrů síťového provozu za využití kontrolerů WLC2504, ZoneDirector 1106 a v prostředí bez jejich využití. Osnova práce: Úvod Principy přenosu dat s využitím WiFi WiFi roaming ? principy a možnosti využití Představení vybraných kontrolerů Návrh modelového řešení Metodika měření Výsledky měření a jejich vyhodnocení Závěr

WEI, Hung-Yu, Jaroqniew RYKOWSKI a Sudhir DIXIT. WiFi, WiMAX and LTE multi-hop mesh networks: basic communication protocols and application areas. Hoboken, N.J.: Wiley, c2013, 1 online zdroj (xxv, 254 p.). Wiley series on information and communications technologies. TEARE, Diane, Bob VACHON a Rick GRAZIANI. Implementing Cisco IP routing (ROUTE): CCNP ROUTE 300-101. Indianapolis, IN: Cisco Press, 2015, xxxiii, 726 pages. Cisco Press foundation learning guide. ISBN 1587204568.

Garantující pracoviště: Katedra informačních technologií,
Fakulta informatiky a managementu

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Datum zadání závěrečné práce: 21.10.2014