Mendelova univerzita v Brně
Provozně ekonomická fakulta

Řešení dynamické konfigurace IPv6 klientů v počítačové síti MENDELU

Bakalářská práce

Vedoucí práce:
Ing. Martin Pokorný, Ph.D.

Barbora Chumlenová

Brno 2015

Poděkování

Tímto bych chtěla poděkovat vedoucímu této bakalářské práce Ing. Martinovi Pokornému Ph.D. za konzultace, cenné připomínky, užitečné rady a mnoho stráveného času při zpracování této práce. Dále bych chtěla poděkovat Bc. Tomáši Filipovi za pomoc při práci v síťové laboratoři a cenné rady. V neposlední řadě děkuji také své rodině za podporu po celou dobu studia.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Řešení dynamické konfigurace IPv6 klientů v počítačové síti MENDELU**
vypracoval/a samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*

Jsem si vědom/a, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.

Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmětná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brně dne 15. května 2015 _____

Abstract

CHUMLENOVÁ, B. *Dynamic host IPv6 configuration in MENDELU computer network.* Bachelor thesis. Brno 2015.

In the first part of this bachelor thesis, there is an explanation and analysis of IPv6 network protocol basic features, which is becoming used as standard for network communication in this time. In the next parts of the thesis, there is an explanation of different variants of dynamic configuration. The SLAAC mechanism in combination with statefull and stateless DHCPv6. These variants were verified and tested in the laboratory of Computer Networking at the Department of Informatics FBE MENDELU. The goal of this thesis was to test these variants and choose the most suitable configuration of clients, which should be used in the production network MENDELU.

Keywords

IPv6, DHCPv6, SLAAC, dynamic configuration, end nodes

Abstrakt

CHUMLENOVÁ, B. *Řešení dynamické konfigurace IPv6 klientů v počítačové síti MENDELU.* Bakalářská práce. Brno 2015

V první části práce budou v teoretické rovině popsány a rozebrány základní vlastnosti síťového protokolu IPv6, který se začíná v dnešní době používat jako standard pro síťovou komunikaci. V dalších částech práce jsou pak postupně rozebrány a rozpracovány různé varianty dynamické konfigurace. Jedná se o použití mechanismu SLAAC v kombinaci s bezstavovým a stavovým DHCPv6. Tyto varianty jsou pak aplikovány a testovány v Laboratoři síťových technologií ÚI PEF MENDELU. Cílem této práce bylo otestovat tyto varianty a vybrat nejvhodnější konfiguraci klientů, která má být aplikována v síti produkční síti MENDELU.

Klíčová slova

IPv6, DHCPv6, SLAAC, dynamická konfigurace, koncové uzly

Obsah

1 Úvod 9

2 Cíl práce 11

3 Publikační review 12

3.1 Výběrová kritéria 12

3.2 Zdroje 12

4 Popis technologického aparátu 15

4.1 IPv6 adresace 15

4.1.1 Adresní prostor a zápis adresy 15

4.1.2 Typy adres 15

4.2 ICMPv6 17

4.3 Objevování sousedů 17

4.4 Automatická konfigurace 19

4.4.1 Bezstavová konfigurace – SLAAC 19

4.4.2 Stavová konfigurace 21

4.5 VLAN 23

5 Metodika 25

6 Analýza 26

6.1 Model sítě 26

6.2 Analýza technického vybavení 27

6.2.1 Aktivní síťové prvky 27

6.2.2 Koncová zařízení 28

6.3 Dynamická konfigurace 29

6.4 Shrnutí 30

7 Návrh řešení 31

7.1 Fáze 1 32

7.1.1 Shrnutí fáze 1 36

7.2 Fáze 2 37
7.2.1 Shrnutí fáze 2 39
7.3 Shrnutí 40

8 Řešení 41
8.1 Implementace fáze 1 41
8.1.1 Konfigurace výchozí brány 41
8.1.2 Konfigurace bezstavového ISC DHCPv6 serveru 43
8.1.3 Konfigurace koncových klientů 44
8.2 Implementace fáze 2 45
8.2.1 Konfigurace výchozí brány 45
8.2.2 Konfigurace stavového ISC DHCPv6 serveru 47
8.2.3 Konfigurace koncových klientů 49
8.3 Testování 50
8.3.1 Testování fáze 1 52
8.3.2 Testování fáze 2 58

9 Ekonomické zhodnocení 64

10 Závěr 66

11 Literatura 68

A Nastavení rozhraní fáze 1 73

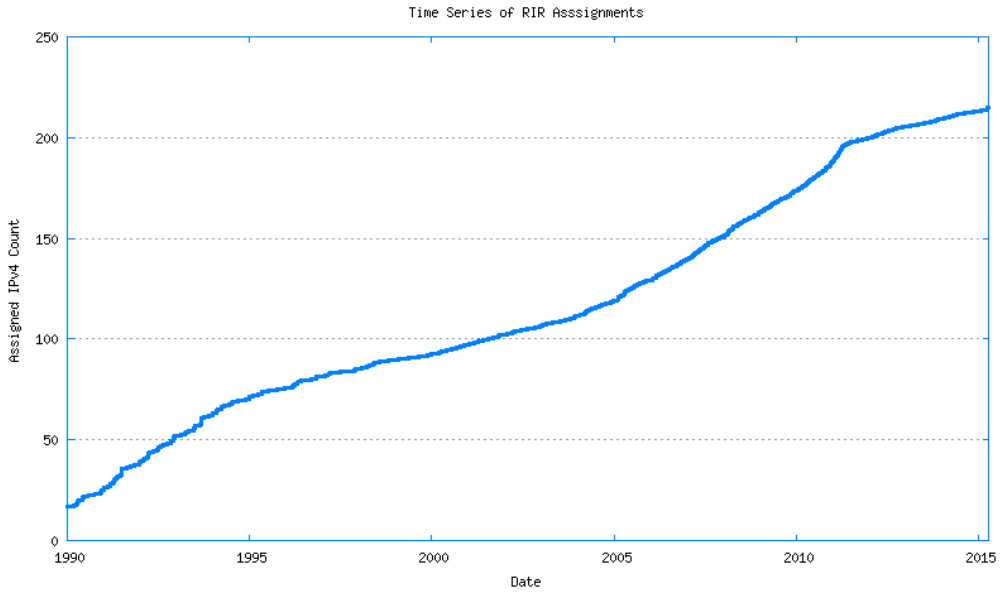
B Nastavení rozhraní fáze 2 75

1 Úvod

Se vznikem internetu souvisí také vznik počítačových sítí. Tyto sítě se neustále rozšiřují. Aby mohly počítače a další zařízení v síti mezi sebou komunikovat, potřebují být jednoznačně identifikovány. K jejich identifikaci slouží takzvaná IP adresa – 32 bitový numerický identifikátor, která je součástí IP protokolu. Tento protokol je základním kamenem internetu.

V současné době se převážně používá protokol IPv4. Adresní prostor u tohoto protokolu je 2^{32} adres. Vzhledem k neustálé expanzi internetu začalo být zřejmé, že brzy dojde k vyčerpání adresního prostoru. To vedlo k navržení nové verze protokolu s označením IPv6. Tento adresní prostor nabízí 2^{128} adres. Odom (2010) uvádí, že použití nového protokolu poskytuje nejlepší řešení problému nedostatku IPv4 adres.

Přestože specifikace protokolu byla připravena, s implementací se nezačalo. Podle Satrapy (2011) byl přechod na IPv6 natolik ožehavou a nejistou půdou, že se většina firem věnovala raději snaze o rozvoj IPv4, než aby se angažovala v IPv6, protože návratnost investic byla v prvním případě rychlejší.



Obr. 1 Spotřeba IPv4 adres (Potaroo.net, 2015)

Na obrázku 1 je znázorněna spotřeba IPv4 adres mezi roky 1990 a 2015. Můžeme si povšimnout, že v 90. letech se mírně snížila spotřeba IPv4 adres. Toto snížení je vyvoláno některými opatřeními z 1. poloviny 90. let. Mezi ně patří zpřísnění přidělování IPv4 adres, používání CIDRu nebo zavedení technologie NAT pro překlad adres. Po roce 2000 však potřeba opět rapidně stoupá, čímž dochází k znovuobnovení zájmu o IPv6 a jeho postupnému uvedení.

Na rozšíření IPv6 protokolu má značný vliv zejména ochota velkých institucí jej implementovat do svých sítí. Mezi tyto instituce můžeme zahrnout například ministerstva, veřejnou správu nebo vysoké školy. Pro podporu IPv6 v sítích státní

správy vydala vláda již v roce 2009 prohlášení o povinnosti podporovat na svých serverech jak protokol IPv4, tak IPv6. Také jednotlivé vysoké školy se rozhodly nový protokol implementovat do svých stávajících sítí. (Průša, 2014)

Vzhledem k požadavku Mendelovy univerzity na zavedení protokolu IPv6 do počítačové sítě MENDELU bylo zadáno několik vysokoškolských prací zabývající se danou problematikou.

Tato bakalářská práce, zabývající se výhradně dynamickou konfigurací koncových klientů, je vytvářena současně s diplomovou prací Návrh integrace IPv6 do počítačové sítě Mendelovy univerzity v Brně v oblasti směrování autora Bc. Tomáše Filipa a diplomovou prací Návrh integrace IPv6 do počítačové sítě Mendelovy univerzity v Brně v oblasti bezpečnosti a síťových služeb autora Bc. Michala Šturmy.

K dispozici byla poskytnuta síťová laboratoř pro vytvoření a zprovoznění navrženého modelu univerzitní sítě. Dále byla poskytnuta relevantní část dokumentace počítačové sítě MENDELU. Všechny IP adresy, identifikátory, čísla VLAN a ostatní číselná označení jsou smyšlená tak, aby pouze odrážela realitu skutečné sítě. Díky tomu budou získané výsledky odpovídat jednotlivým principům a budou reálně využitelné při nasazení.

2 Cíl práce

Cílem mé práce je navrhnout a v podobě případové studie ověřit různé způsoby dynamické konfigurace IPv6 klientů v počítačové síti Mendelovy univerzity v Brně. Dynamická konfigurace v sítích IPv6 s sebou přináší určité komplikace, a proto bude důležitý zejména správný návrh dynamické konfigurace IPv6 klientů. Návrh je nutno ověřit v laboratoři UI PEF MENDELU. Poté bude následovat implementace v produkční síti MENDELU. Mezi uvažované technologie patří například stavové a bezstavové DHCPv6 nebo mechanismus SLAAC.

3 Publikační review

3.1 Výběrová kritéria

Vyhledávání publikací probíhalo na základě stanovených klíčových slov souvisejících s danou problematikou. Nalezené práce jsem dále třídila podle několika kritérií. Hlavní důraz byl kladen na aktuálnost publikace. Do výběru jsem zahrnula pouze práce publikované po roce 2006, s výjimkou některých RFC dokumentů, které vyšly již dříve, avšak od té doby se nijak výrazně nezměnily. Dalším kritériem je použitelnost obsahu.

Klíčová slova, podle kterých jsem vyhledávala: IPv6, DHCPv6, implementace IPv6, dynamická konfigurace, přechod na IPv6, SLAAC.

3.2 Zdroje

Literatura, z které jsem čerpala inspiraci pro vypracování této bakalářské práce, je v souladu se samotným zadáním práce. Většina zdrojů se zabývá problematikou IPv6. Další velkou skupinou jsou zdroje zabývající se přímo dynamickou konfigurací IPv6 klientů a implementací DHCPv6 serveru.

Vysokoškolské práce - dostupné z www.thesis.cz, www.vut.brno

Veselý (2014) se ve své diplomové práci zaobírá problematikou IPv6 bezpečnosti. Největší část práce tvoří popis mnoha různých útoků, které mohou nastat v IPv6 sítích. Následně jsou zde popsány také možnosti obrany před těmito útoky. Autor také zmiňuje nástroje, díky nimž je možno útoky v IPv6 sítích provádět. K testování IPv6 implementace dochází právě za použití těchto nástrojů.

Diplomová práce Dvořáka (2014) se zaměřuje na implementaci protokolu IPv6 ve firemním prostředí. K tomuto účelu je využita reálná firma, která si však nepřeje být zmíněna, a proto v práci po celou dobu vystupuje pod názvem XXX spol. s.r.o. Po teoretickém úvodu, ve kterém jsou zmíněny základní vlastnosti nového protokolu, následuje část praktická, která se zabývá zkoumáním současného stavu sítě zmíněné firmy. Na základě této analýzy jsou navržena možná řešení implementace pro tuto společnost.

Koutecký (2014) ve své diplomové práci řeší implementační projekt zabývající se zavedením IPv6 do prostředí vysoké školy. Práce se zaměřuje na možnosti implementace tohoto protokolu. V úvodu se nachází teoretické pojednání o základních vlastnostech tohoto protokolu. Následně je provedena analýza současného stavu síťové infrastruktury. Na základě této analýzy je vybrána nejvhodnější přechodová metoda. Na závěr jsou zhodnoceny přínosy IPv6 pro školu.

Kalina (2012) představuje mechanismy internetového protokolu IPv6, zejména jejich funkčnost a analýzu. Úvodem autor popisuje referenční model

ISO/OSI a také historii a vývoj protokolu IPv6. V rámci teoretické části je detailně provedena analýza protokolu IPv6. V praktické části autor vytvořil pro výše zmíněné mechanismy výukovou animaci v programu Adobe Flash Professional C5.

Tlačbaba (2012) se ve své práci zaměřil na tunelovací mechanismy IPv6 paketů skrze IPv4 síť. Úvodem popisuje základní vlastnosti IPv6 protokolu. Poté se věnuje třem možnostem tunelování, které postupně porovnává podle vlastností, jako je například šířka pásma, zpoždění, ztrátovost paketů nebo rozptyl zpoždění.

Bakalářská práce, jejímž autorem je Priesnitz (2012) je zaměřena na implementaci protokolu IPv6 v prostředí podnikové sítě Teplárny Brno, a.s. První část práce je věnována teoretickému úvodu. Jsou zde popsány rozdíly oproti IPv4 a také základní principy fungování. Druhá část práce je věnována konkrétnímu praktickému řešení. Je zde provedena analýza současného stavu síťové infrastruktury a následný návrh implementačních řešení.

Hrachovský (2012) se v této práci zabývá přechodem počítačových sítí z IPv4 na IPv6. Na úvod nás autor seznamuje s novým protokolem a také možnostmi přechodu. Poté autor poukazuje na rozdíly mezi oběma protokoly a popisuje zejména rozdílnou konfiguraci jednotlivých síťových prvků.

Zima (2012) se zaměřil na přechodové mechanismy mezi protokolem IPv4 a IPv6. Nejprve je nastíněna současná situace obou protokolů a poté následuje seznámení se současnými přechodovými mechanismy. Na základě těchto mechanismů je navržen a poté implementován překladač adres. Následně je provedeno testování tohoto překladače.

Bakalářská práce Joudala (2011) se zabývá jednotlivými aspekty zavedení IPv6 na Jihočeské univerzitě v Českých Budějovicích. Autor se nejprve zabývá vlastnosti protokolu IPv6. Následně analyzuje současný stav sítě na JU. Dále se zde zabývá otázkami, jako jsou finanční náklady nebo význam a přínosy přechodu z IPv4 na IPv6 v podmínkách vysokých škol.

Geyer (2011) se ve své diplomové práci zabývá zabezpečením počítačových sítí využívajících protokol IPv6. Autor nejprve nastiňuje danou problematiku útoků na lokální IPv6 sítě. V další části jsou popsány možnosti ochrany proti těmto útokům. Na závěr autor uvádí přesnou metodiku, tedy jak postupovat při zabezpečení sítí IPv6.

Úvodem své práce se Pangrác (2010) věnuje obecnému popisu protokolu IPv6. Následně uvádí několik možností pro přechod z protokolu IPv4 na IPv6. Celá problematika je popsána na modelové situaci firmy působící jako poskytovatel připojení. Tato práce obsahuje také zhodnocení od vedoucích firmy včetně časového a finančního plánu.

Práce Hlouška (2008) se týká implementace DHCPv6 serveru pro operační systém Linux. Úvodem jsou nastíněny základní vlastnosti protokolu DHCPv6. Dále se autor věnuje popisu implementace a metodiky testování. Součástí je také příloha, v níž jsou uvedeny jednotlivé implementační kódy.

V této práci Vilímek (2007) popisuje protokol IPv6 a následnou implementaci tohoto protokolu ve společnosti UPC Česká republika, a.s. Úvodem popisuje vlastnosti a základní principy fungování tohoto protokolu. Poté se autor věnuje popisu UPC sítě a její podrobné analýze. V poslední části této práce je uvedena skutečná implementace v prostředí výše zmíněné společnosti.

Shrnutí

Zmíněné práce, které jsou výše stručně popsány, představují společně s odbornou literaturou prostředky k seznámení se s danou problematikou a poskytují dostačující základ pro sepsání této bakalářské práce.

Většina uvedených závěrečných prací se zabývá zejména implementací protokolu IPv6 ve firemním prostředí. Jsou zde však práce, které se zabývají přímo implementací v prostředí vysoké školy, například práce Joudala (2011) nebo Kouteckého (2014). Další početně zastoupenou skupinou jsou práce věnující se zabezpečení IPv6 sítí. Mezi tyto patří zejména práce Veselého (2014) a Geyera (2011).

Žádná z uvedených prací však detailně neřeší problém dynamické konfigurace koncových zařízení, který bude zpracován v této bakalářské práci.

4 Popis technologického aparátu

4.1 IPv6 adresace

4.1.1 Adresní prostor a zápis adresy

Nový protokol IPv6 s sebou přináší z dnešního pohledu nevyčerpatelné množství adres. Jedná se zhruba o 3,4 x 10^{38} použitelných adres. Oproti starému protokolu se změnil zejména formát datagramu. Cílem bylo zefektivnit zpracování datagramu, a tím urychlit směrování paketů. Z tohoto důvodu došlo k minimalizaci počtu položek. Základní hlavička má tedy konstantní délku a všechny volitelné položky z dřívějšího protokolu byly přesunuty do samostatných hlaviček. (Satrapa, 2011)

IPv6 adresa má oproti IPv4 adrese čtyřnásobnou délku. Zapisuje se pomocí číslic šestnáctkové soustavy. Ty jsou uspořádány do osmi skupin po čtyřech číslicích oddělených od sebe dvojtečkami. Podrobný popis délky a podoby adresy lze nalézt v RFC 3513 (2003).

Existuje několik pravidel umožňujících vynechání některých znaků k vytvoření zkráceného tvaru adresy. V adrese dochází k častému výskytu hodnoty nula. Jednou z možností zkrácení je vynechání počátečních nul v každé čtveřici. Blok adresy ve tvaru „0001“ je tedy možno vynecháním počátečních nul zkrátit pouze na „1“. Dále lze vynechat nulové šestnáctibitové bloky jdoucí za sebou pomocí zástupného znaku „::“, ale to však pouze jedenkrát, aby bylo možno rekonstruovat původní tvar adresy. (RFC 3513, 2003)

Původní adresa	2001:0000:a000:**000**1:**0000**:**0000**:**0000**:**0000**
Zkrácená adresa	2001:**000**0:a000:1:**0**:**0**:**0**:**0**
Zkrácená adresa	2001:0:a000:1**::**

Tab. 1 Příklad zkracování adres

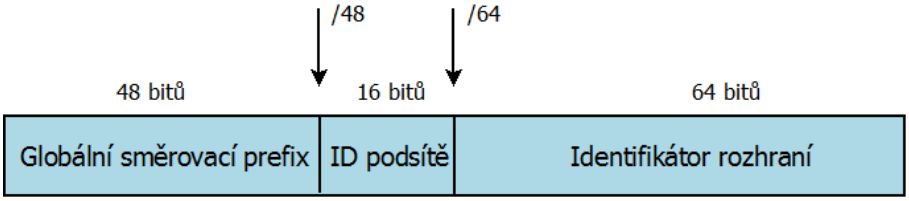
4.1.2 Typy adres

Adresní prostor byl rozdělen na několik typů adres. Mezi základní tři typy patří individuální, skupinové a výběrové adresy. (Graziany, 2013)

- *Individuální* (unicast) adresy identifikují právě jedno rozhraní, na které budou data doručena.
- *Skupinové* (multicast) adresy identifikují skupinu rozhraní náležících různým zařízením. Paket odeslaný na skupinovou adresu je doručen všem zařízením identifikovaným danou adresou.
- *Výběrové* (anycast) adresy jsou adresy přiřazené opět skupině zařízení. Paket odeslaný na výběrovou adresu je však doručen pouze tomu zařízení, které je nejblíže.

Individuální (unicast) adresy jsou nejrozšířenějším druhem adres. Dále se však dělí na několik typů (Odom,2010):

- *Unicast globální* adresy identifikují zařízení v rámci celého internetu, jsou tedy jedinečné na celém světě.
- *Unicast lokální linkové* adresy nejsou celosvětově jedinečné. Jejich dosah je omezen pouze na lokální síť. Používají se proto při bezstavové konfiguraci nebo při objevování sousedů.
- *Unicast unikátní individuální lokální* adresy nejsou směrovatelné a slouží tedy pouze k lokální komunikaci. Jsou celosvětově jednoznačné.

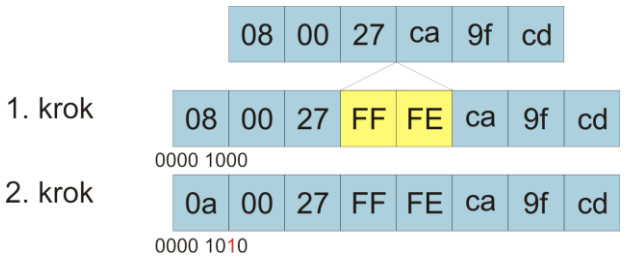


Obr. 2 Schéma globální individuální adresy

Jak je možno vidět na obrázku výše, IPv6 adresa je rozdělena na 3 části. Globální směrovací prefix je přidělen poskytovatelem připojení k identifikaci sítě. Identifikátor podsítě slouží k určení jednotlivých podsítí v rámci určité sítě. Druhá polovina adresy je celá věnována identifikátoru rozhraní.

Existuje několik způsobů k vytvoření tohoto identifikátoru. Jednou z možností je nastavit jej staticky. Další způsoby nabízí vytvoření identifikátoru pomocí mechanismu EUI-64 nebo Privacy Extensions. Identifikátor vytvořený pomocí EUI-64 je odvozen z MAC adresy. Vzhledem k jedinečnosti MAC adresy se předpokládá, že identifikátor z ní odvozený bude také unikátní. (Odom, 2010)

Transformací se 48 bitová MAC adresa zvětší na 64 bitovou hodnotu, a to vložením 16 bitů. MAC adresa se rozdělí na dvě poloviny o velikosti 3 bajty a doprostřed se vloží hexadecimální FFFE. Je zapotřebí obrátit příznak globality, jedná se o předposlední bit v prvním bajtu. Hodnota 0 značí globální adresu, hodnota 1 značí adresu lokální. (RFC 4291, 2006)



Obr. 3 Postup při vytváření EUI-64

Vzhledem k jednoduchosti tohoto mechanismu lze snadno identifikovat jednotlivá koncová zařízení a získat informace nejen o tom v jaké síti se nacházejí, ale také k jaké službě přistupují. Aby bylo zabráněno tomuto stopování klientů, byl navržen bezpečnostní mechanismus s názvem Privacy Extensions, který je po-

drobněji popsán v RFC 4941 (2007). Princip spočívá v nahodilém generování hostitelské části IPv6 adresy. Tyto adresy se pravidelně obměňují a vznikají nové. Nelze predikovat jejich podobu ani změnu. Z tohoto důvodu je pro správce nemožné identifikovat jednotlivá zařízení v síti. (Lupa.cz, 2011)

Tento stupeň anonymity je standardně podporován ve všech operačních systémech od firmy Microsoft určených pro uživatele. (Msdn.com, 2010)

Pro příklad lze uvést operační systém Windows 7, jehož výchozí nastavení obsahuje rovnou dvě vygenerované globální adresy. Jedná se o tzv. dočasnou adresu s náhodným identifikátorem a trvalou adresu s náhodným identifikátorem. Dočasná adresa je použita při navázání spojení do internetu, a to z důvodu zajištění soukromí. Tato adresa je generována každých 7 dnů. Trvalá adresa je neměnná a bývá použita jako fixní bod pro navázání komunikace nebo pro záznam do DNS. Použití dočasných adres lze vypnout tak, aby pro veškerou komunikaci byla použita adresa trvalá. Lze vypnout také generování náhodných identifikátorů pro vynucení použití mechanismu EUI-64. (Nic.cz, 2011)

4.2 ICMPv6

ICMPv6 představuje přepracovanou verzi dřívějšího protokolu ICMP. Je to režijní protokol a jeho podrobná definice se nachází v dokumentu RFC 4443 (2006). Tento protokol bývá používán převážně k výměně provozních informací, k testování dosažitelnosti a ohlašování jednotlivých chybových stavů. Zprávy protokolu jsou distribuovány pomocí datagramu ICMPv6. ICMP zpráva je rozdělena do tří částí (Graziani, 2013): Typ (Type) – identifikuje typ dané ICMPv6 zprávy, Kód (Code) – poskytuje další podrobnosti o typu, Kontrolní součet (Checksum) – používá se k detekci poškozených dat v ICMPv6 zprávě.

V rámci ICMPv6 rozlišujeme dva typy zpráv. Prvním typem jsou zprávy chybové, druhým typem jsou zprávy informační. Mezi chybové zprávy zahrnujeme tyto druhy chybových zpráv: Nedosažitelnost, Nadměrný datagram, Vypršení životnosti datagramu a Chybný datagram. Nedosažitelnost informuje o tom, že cílová adresa je nedosažitelná. Nadměrný datagram informuje o nižší hodnotě MTU, než je velikost datagramu. Zpráva Vypršení životnosti datagramu informuje o tom, že danému datagramu vypršela jeho doba životnosti. Chybný datagram informuje o tom, že doručený datagram je nesrozumitelný. (Hotský, 2013)

4.3 Objevování sousedů

Stejně jako u IPv4, tak i u IPv6, je zapotřebí determinovat přítomnost jednotlivých klientů na stejné síti, zjistit linkovou adresu ostatních klientů nacházejících se ve stejné lokální síti a současně ověřit jejich dostupnost. V rámci IPv4 sítí byla tato potřeba zajištěna pomocí protokolu ARP (Address Resolution Protocol).

Obdobou ARP v prostředí IPv6 se stal nový mechanismus pro objevování sousedů. Vystupuje pod názvem Neighbor Discovery (ND). Nabízí stejnou funkcionalitu jako ARP, navíc však disponuje dalšími funkcemi. To znamená, že kromě zjištění

linkových adres uzlů ve stejné lokální síti umožňuje například hledání směrovačů, rychlé aktualizace při změně linkových adres, detekci duplicitních adres nebo zjišťování síťových parametrů, které jsou nezbytné pro automatickou konfiguraci. (Odom, 2010)

V okamžiku, kdy IPv6 klient nebo směrovač potřebuje zaslat paket jinému klientu nebo směrovači nacházejícímu se ve stejné lokální síti, jako první zkontroluje svoji databázi sousedů – cache sousedů. Tato databáze obsahuje seznam sousedních IPv6 adres společně s odpovídajícími linkovými adresami. Pokud v této databázi nenachází záznam odpovídající dané IPv6 adrese, využije pro dynamické zjištění hledané MAC adresy již výše zmíněný Neighbor Discovery Protocol (NDP).

NDP pro svou činnost využívá pět typů ICMP zpráv a dvě další zprávy SEND, které mají na starost bezpečné objevování sousedů (Secure Neighbor Discovery). (Satrapa, 2011)

Objevování sousedů	
Výzva směrovači	Router solicitation
Ohlášení směrovače	Router advertisement
Výzva sousedovi	Neighbor solicitation
Ohlášení souseda	Neighbor advertisement

Tab. 2 Typy ICMP zpráv pro objevování sousedů (Satrapa, 2011).

Změnou oproti ARP je kromě jednotlivých názvů také adresa, na kterou se dotaz posílá. Tyto skupinové adresy, na něž se posílají jednotlivé dotazy, začínají prefixem ff02::1:ff:0/104. Zbylých 24 bitů (6 hexadecimálních číslic) pochází z IPv6 adresy, na kterou má být zpráva zaslána (destination IP). Pokud uzel hledá linkovou adresu k určité IPv6 adrese, vezme daných 24 bitů a připojí je za výše zmíněný prefix. V případě, že hledá linkovou adresu odpovídající následující IPv6 adrese (Satrapa, 2011)

2001:718:803:2a0:a00:27ff:fec8:b02

svůj dotaz zašle na skupinovou adresu

ff02::1:ffc8:b02

Tato skupinová adresa bývá označována jako adresa pro vyzývaný uzel (Solicited Node Multicast Address). Vzhledem k tomu, že daná adresa reprezentuje pouze uzly se shodnými spodními 24 bity, snižuje se počet skupin, ve kterých může být daný host začleněn. Tím se zamezí zbytečnému obtěžování ostatních uzlů a dotaz je, až na výjimky, doručen správnému uzlu. (Odom, 2010), (Satrapa, 2011)

Proces komunikace probíhá následovně. Vyzývající uzel zašle na skupinovou adresu ICMP zprávu s názvem Výzva sousedovi s požadavkem na jeho MAC adresu. Sousední uzel odpovídá zprávou Ohlášení souseda na adresu vyzyvatele a současně přikládá svoji MAC adresu. Na základě Ohlášení souseda se v cache sousedů zanese nová položka obsahující dvojici tvořenou příslušnou IPv6 adresou a k ní odpovídající linkovou adresou.

Dalšími dvěma důležitými zprávami jsou Výzva směrovači (Router Solitation) a Ohlášení směrovače (Router Advertisement). RA jsou ICMPv6 zprávy, které mají za úkol informovat klienty o síťových parametrech tak, aby se dokázali sami nakonfigurovat. Jsou to zejména konfigurační parametry typu síťový prefix, délka prefixu a MAC adresa výchozí brány. Počítač se díky ohlášení dozví, v jaké síti se nachází, jak se zde komunikuje a kdo je implicitní směrovač. Pokud není v konfiguraci speciálně zakázáno, jsou tyto zprávy posílány v pravidelných intervalech všem uzlům v síti. Uzlům stačí chvíli poslouchat, případně si pro zajištění větší dynamičnosti mohou o dané parametry zažádat, a to prostřednictvím Výzvy směrovači (Router Solicitation). (Blanchet, 2006)

Objevování sousedů se používá také k zjištění, zdali je určitá adresa v síti již přítomna. Tento mechanismus se nazývá Detekce duplicitních adres (Duplicate Address Detection). Uzel pomocí Výzvy sousedovi hledá vlastníka ke své vlastní vygenerované adrese. Problém nastane v případě, že uzel obdrží Ohlášení souseda. V takovém případě je daná adresa v síti již přítomna a uzel ji nemůže začít používat. (Satrapa, 2011)

Dále stojí za zmínění systém ověřující dosažitelnost sousedů. Pro ověření dostupnosti jsou k dispozici dva mechanismy. První mechanismus ověřuje dosažitelnost uzlu za pomoci informací, které čerpá z vyšší síťové vrstvy. Pokud zde probíhá komunikace, pak je zřejmé, že daný uzel je dostupný. Druhý mechanismus využívá pro ověřování zprávy Výzva sousedovi (NS), které aktivně zasílá svým sousedům a očekává jejich odpověď. Přijetím zprávy Ohlášení souseda (NA) je ověřena dostupnost daného souseda. Satrapa (2011) uvádí několik stavů, které jsou přidělovány k jednotlivým položkám v cache sousedů. Jedná se o následující: Nekompletní (Incomplete), Dosažitelná (Reachable), Prošlá (Stale), Odložená (Delay), Testovaná (Probe). Podrobný popis těchto stavů a zároveň i další informace týkající se Objevování sousedů jsou podrobněji popsány v RFC 4861 (2007).

4.4 Automatická konfigurace

Automatická konfigurace je další novinkou ve světě IPv6. Základní požadavek je kladen na co nejmenší počáteční konfiguraci tak, aby zařízení připojené do sítě bylo schopno získat síťové parametry (prefix sítě, délku prefixu, MAC adresu výchozí brány) samo a začalo tak během chvíle komunikovat se svým okolím. Obecně rozlišujeme dva typy automatické konfigurace: stavovou a bezstavovou konfiguraci (Satrapa, 2011).

4.4.1 Bezstavová konfigurace – SLAAC

Prvním typem automatické konfigurace je konfigurace bezstavová. Objevuje se také pod názvem *SLAAC (Stateless Address Autoconfiguration)*. Je považována za součást systému objevování sousedů. Bezstavová konfigurace pro svou komunikaci používá protokol ICMPv6. Využívá se skutečnosti, že se v síti nachází implicitní směrovač, který zná jednotlivé konfigurační parametry potřebné pro komunikaci s ostatními sítěmi. Tyto konfigurační parametry jsou pomocí RA zpráv implicit-

ním směrovačem rozesílány do těch sítí, ve kterých je daný směrovač připojen, a ve kterých je odesílání těchto zpráv povoleno. K těmto parametrům si uzel doplní identifikátor rozhraní. Ten je vytvořen pomocí EUI-64 nebo Privacy Extensions. (RFC 2462, 1998)

Po přijetí této zprávy si uzel aktualizuje svoji směrovací tabulku přidáním nové cesty (default route). Pokud je nastaven flag autokonfigurace, nastaví si také IPv6 adresu z ohlášeného adresního prostoru. (Veselý, 2014)

Aby počítač věděl, odkud získat jednotlivé síťové parametry, nachází se v RA dva speciální příznaky – M flag a O flag. (Lupa.cz, 2011)

M flag	O flag	Způsob konfigurace
0	0	SLAAC
0	1	Bezstavové DHCPv6
1	0	Stavové DHCP

Tab. 3 Přehled speciálních příznaků v RA.

ManagedFlag informuje klienta, že má použít stavovou konfiguraci k doplnění chybějících síťových parametrů.

OtherConfigFlag informuje klienta, aby ke konfiguraci použil bezstavový DHCPv6 server.

Autonomous udává, jestli smí klient nad ohlašovaným prefixem provádět bezstavovou konfiguraci.

Velkou výhodou při použití bezstavové konfigurace je skutečnost, že odpadá nutnost realizovat a udržovat DHCPv6 server. Na druhou stranu je zde velká nevýhoda v podobě absence konfiguračních parametrů obsahující informace o DNS serverech. Tím pádem není umožněna plnohodnotná síťová komunikace. Nabízí se dvě možnosti řešení.

Prvním řešením je využití rozšíření pro bezstavovou konfiguraci, které je popsáno v dokumentu RFC 6106 (2010). *IPv6 Router Advertisement Options for DNS Configuration* je standard, který vyšel v roce 2010 a doplnil do automatické bezstavové konfigurace dvě položky. První položkou je *RDNSS*, obsahující adresy rekurzivních DNS serverů. Druhá položka se nazývá *DNSSL* a obsahuje seznam jednotlivých domén. (Satrapa, 2011)

Zásadní problém je v tom, že podpora RFC 6106 musí být implementována, jak na straně klientů, tak na straně směrovačů. Navíc musí být tento standard podporován všemi síťovými zařízeními. Vše tedy záleží, jak se tvůrci operačních systémů rozhodnou, zda implementovat podporu RFC 6106 do svých systémů, či nikoliv.

Například co se týká operačního systému Windows, podpora RFC 6106 není v žádné stávající verzi. Microsoft se veřejně vyjádřil, že nemá snahu toto rozšíření do budoucna implementovat. (Horley, 2013), (Social.technet.microsoft.com, 2012)

Druhým řešením je zabezpečit předání informací o DNS jiným způsobem, a to například využitím bezstavového DHCPv6 serveru. Jedná se velmi zjednodu-

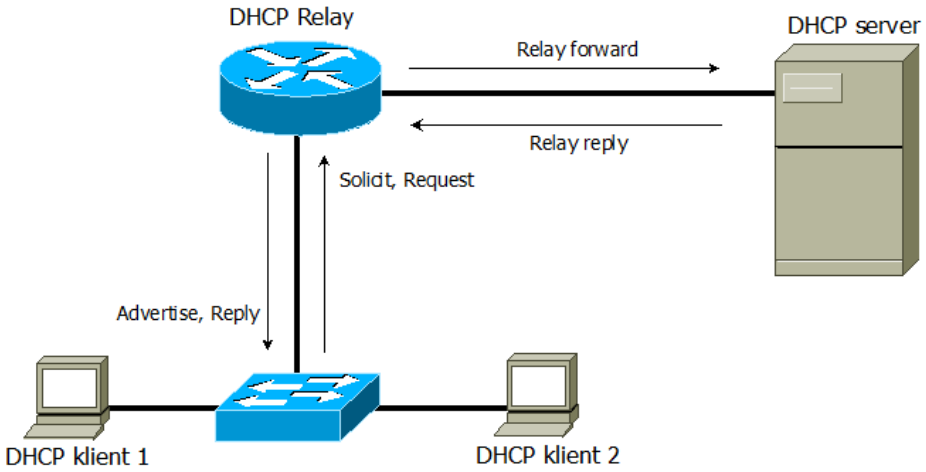
šenou verzi DHCPv6 zaměřenou především na snadnou implementovatelnost a celkovou jednoduchost. Používá pouze dva typy zpráv – žádost o informaci a odpověď. Bezstavový DHCPv6 server slouží zpravidla pouze k tomu, aby klientům v síti poskytl informace o rekurzivních DNS serverech a doplnil tím informace, které klient nemohl získat prostřednictvím mechanismu SLAAC. (RFC 3736, 2004)

4.4.2 Stavová konfigurace

Druhým typem automatické konfigurace je protokol DHCPv6, často označován jako stavová konfigurace. Jedná se o aplikační protokol pro přidělování IPv6 adres a dalších síťových parametrů. Detailní specifikace se nachází v RFC 3315 (2003). Stejně, jako je tomu u DHCPv4, jsou adresy a síťové parametry přidělovány dočasně a je nutno je obnovovat. Získání těchto parametrů probíhá ve 4 fázích (Satrapa, 2011):

1. **Solicit** *(výzva)* – zasílá klient pomocí skupinové adresy všem DHCP agentům a hledá server, který je ochoten poskytnout síťové parametry. Do zprávy může zadat požadované síťové parametry a IA, kterým chce adresy přidělit.
2. **Advertise** *(ohlášení serveru)* – server zpracuje zprávu Solicit. Následně reaguje odpovědí Advertise, ve které uvede příslušné konfigurační parametry a adresy, které může klientovi přidělit.
3. **Request** *(žádost)* – klient přijme všechny ohlášení a podle hodnoty volby Preference se obvykle rozhodne, kterou nabídku z daných serverů použije. Klient si vybere server ze seznamu serverů, který si vytvořil a zasílá zprávu Request pro získání dalších komunikačních parametrů.
4. **Reply** *(odpověď)* – Server následně tuto zprávu vyhodnotí a posílá klientovi vybranou adresu.

Součástí této komunikace jsou 3 typy zařízení. Je zde klient, který poptává informace, server, který informace poskytuje a dále zprostředkovatel *(Relay agent),* který se stará o zajištění komunikace mezi DHCP serverem a jednotlivými DHCP klienty pomocí předávání protokolu DHCPv6, který slouží k přenosu DHCPv6 zpráv.



Obr. 4 Znázornění komunikace mezi DHCP klienty a DHCP serverem prostřednictvím Relay agenta

Na obrázku 4 je vyobrazena komunikace mezi DHCP klientem a DHCP serverem za použití DHCP Relay agenta. Ten přeposílá zprávy od klienta k serveru a naopak a tvoří tím pádem prostředníka této komunikace.

Celý proces dynamického přidělení IPv6 adresy je realizován prostřednictvím čtyř DHCPv6 zpráv. Zprávou Solicit klient hledá DHCPv6 server, který je ochotný přidělit mu požadované parametry. Tato zpráva je přenesena prostřednictvím Relay agenta jako zpráva Relay Forward. Server na základě této zprávy posílá odpověď se síťovými parametry, které může klientovi nabídnout. Toto ohlášení serveru je zasláno nejprve DHCPv6 Relay agentovi ve formě zprávy Relay Reply. Agent zajistí předání zprávy klientovi jako zprávu DHCPv6 Advertise. Klient oznamuje své rozhodnutí pomocí zprávy DHCPv6 Request. Komunikace končí zprávou DHCPv6 Reply, ve které jsou obsaženy síťové parametry zaslané daným DHCPv6 serverem. Jedná se o IPv6 adresu a informaci o rekurzivním DNS serveru.

Otázkou v DHCPv6 komunikaci je především správná identifikace zařízení. K tomu se používá tzv. *DUID (DHCP Unique Identifier)*. Jedná se o jedinečný identifikátor každého zařízení účastnícího se daného procesu komunikace. Bývá přidělen jak klientům, tak serverům. Měl by být stálý a neměnit se ani při výměně síťové karty nebo používaného rozhraní (Ethernet, WiFi). Tím je klient oproštěn od závislosti na daném hardwarovém vybavení. Standard definuje 3 možnosti vytvoření DUID. První způsob definuje vytvoření DUID pomocí MAC adresy a časového razítka. Počátečních 16 bitů označuje typ DUID-LLT (00-01). Následuje časový údaj o velikosti 32 bitů následovaný MAC adresou proměnlivé délky. Druhým způsobem je využití jedinečného identifikátoru poskytnutého výrobcem. DUID vytvořeno tímto způsobem se skládá z 16 bitů označujících daný typ DUID-EN. V tomto případě se jedná o hodnotu 2 (00:02). Následuje výrobní číslo přidělené výrobcem, které může mít libovolnou délku. Poslední možností je využití klasické MAC adresy. Jedná se tedy o obdobu z IPv4. Typ DUID-LL je opět uložen v prvních 16 bitech (00:03). Po nich následuje MAC adresa. Každý operační systém si vytváří DUID jiným způsobem. Máme-li tedy na jednom PC více operačních systémů, každý bude

mít jiný identifikátor DUID. Ke změně DUID dochází také po reinstalaci OS. (Lupa.cz,2011), (RFC 3315, 2003)

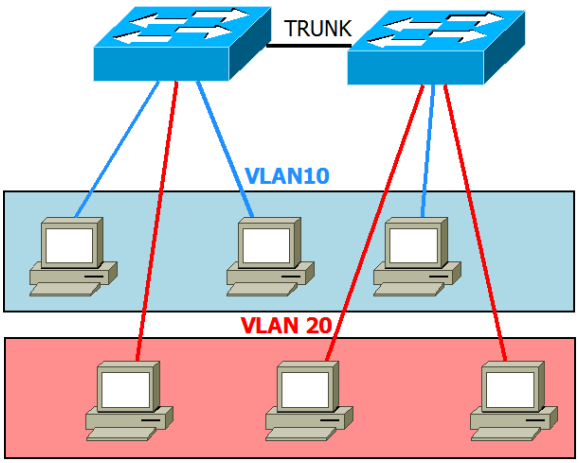
Stavová konfigurace má oproti bezstavové řadu výhod. Za zmínění stojí zejména absolutní kontrola politiky přidělování adres na straně serveru. Správci tím pádem mají kontrolu nad jednotlivými síťovými zařízeními. Další výhodou je možnost posílat další konfigurační parametry, např. adresy DNS serverů. Na základě přidělených adres lze pak následně DNS záznamy aktualizovat.

Na druhou stranu je zde i několik nevýhod oproti bezstavové konfiguraci. Především to, že provoz a údržba DHCP serveru je mnohem náročnější na systémové prostředky. (Hloušek, 2008)

4.5 VLAN

Virtuální lokální sítě jsou vlastně logické segmenty klasických LAN sítí. Umožňují síť logicky rozdělit, a to bez závislosti na fyzickém umístění jednotlivých uzlů. V rámci jedné LAN může existovat velké množství VLAN. Počítače uvnitř VLAN spolu mohou komunikovat jako by byly na stejné LAN. Na základě svého umístění je jim také přidělena IP adresa v rámci dané VLAN.

Technologie VLAN je založena na přepínačích, které přinesly zvýšení propustnosti přetíženým sítím. Porty na L2 přepínačích bývají standardně zahrnuty do jedné broadcast zóny. To umožňuje zahlcování sítě nevyžádanými daty. Při použití VLAN je broadcast odeslaný uvnitř dané VLAN ukončen na hranici této podsítě a nezahlcuje tím pádem ostatní segmenty sítě.



Obr. 5 Ukázková síť s dvěma VLAN a šesti koncovými uzly

Přiřazení do VLANY se provádí na přepínači. Nejčastější metodou je zařazení dle portu. Jedná se o ruční přiřazení, které znamená, že veškerá komunikace procházející přes daný port, spadá do určité VLAN. Správa je jednoduchá a přehledná. Při komunikaci VLAN v rámci jednoho přepínače je v jeho operační paměti uloženo, která komunikace náleží které VLAN a na základě toho je realizováno správné směrování. Tyto porty jsou označovány jako přístupové (Access port). (Samuraj-cz.com, 2007)

Složitější situace nastává v případě, požadujeme-li, aby dané VLAN byly použitelné v rámci celé sítě. Informace o zařazení do jednotlivých VLAN musí být tedy zachovány i při přechodu přes jiný přepínač. Řešením je standard IEEE.1q, který zavádí značkování rámců. Rámec je při posílání na druhý přepínač označen – tagován. Porty, na nichž se taguje odchozí komunikace, se nazývají trunk porty. Při spojení dvou trunk portů vzniká tzv. trunk, nebo také trunk link. (Samuraj-cz.com, 2007)

End-to-end VLAN představuje podsíť, která je realizována na všech L2 zařízeních v rámci dané LAN sítě. Pro zajištění komunikace mezi uživateli z různých VLAN je potřeba ukončit VLAN L3 rozhraním. Realizace se provádí prostřednictvím tzv. virtuálního rozhraní (SVI interface) na distribučních přepínačích. Každé SVI rozhraní má přidělenou svoji IP adresu v rámci dané podsítě a bývá využíváno jako výchozí brána pro všechny uživatele z dané VLAN. (Buček, 2012)

Použití VLAN s sebou přináší několik výhod (Tóth, 2014):

1. **Zvýšení výkonu** – je dosaženo především snížením provozu v síti. Snížení je docíleno vytvořením většího počtu broadcastových domén.
2. **Zjednodušení správy** – díky možnosti seskupování klientů do určitých VLAN vzniká možnost spravovat je jednotně.
3. **Nezávislost na fyzické topologii** – do VLAN lze přidávat nebo z ní odebírat jednotlivé klienty, bez ohledu na to, kde se v síti fyzicky nacházejí.
4. **Zvýšení možnosti zabezpečení** – možnost oddělit uživatele pracující s citlivými údaji do samostatné VLAN.

5 Metodika

V této kapitole bude stručně popsán postup při tvorbě této bakalářské práce. Před samotnou tvorbou práce bylo nutné seznámit se s danou problematikou. Co je IPv6 a jaké novinky s sebou přináší. Poznatky k této práci byly nabyty studiem doporučené odborné literatury a relevantních vysokoškolských prací. Na základě prostudování těchto prací bylo vytvořeno publikační review.

Po seznámení s danou problematikou následovalo první praktické použití IPv6. Na jednoduché virtuální síti tvořené několika virtuálními klienty bylo poprvé otestováno dynamické přidělování adres skrze DHCPv6 server.

Následujícím krokem bylo vyzkoušet stejnou problematiku v síťové laboratoři. Bylo otestováno stavové i bezstavové DHCPv6 na jednoduché síti tvořené linuxovým serverem a několika klienty rozdělenými do dvou VLAN.

Po analýze stávajícího stavu sítě byly navrženy varianty dynamické konfigurace koncových klientů. Jedná se o použití mechanismu SLAAC a DHCPv6 serveru. Byly navrženy dvě využitelné varianty. Z logického pohledu byl další postup rozvržen do dvou fází.

V první fázi byl v laboratorní síti zapojen model univerzitní sítě MENDELU, jehož cílem bylo co nejvíce napodobit reálný stav sítě. Fáze jedna měla za úkol ověřit dynamickou konfiguraci koncových klientů za použití technologie SLAAC s bezstavovým DHCPv6 serverem. Klienti byli umístěni do různých VLAN v rámci jednotlivých oblastí. Po jejich konfiguraci následovalo testování konektivity a sběr show výpisů. Pro každého klienta byly zaznamenány také odchyty komunikace.

Druhá fáze byla obdobou fáze jedna. Opět byl zapojen daný laboratorní model, s tím rozdílem, že fáze dva byla zaměřena na použití stavového DHCPv6 serveru za předpokladu statických vazeb pro jednotlivé klienty prostřednictvím jejich DUID. Správná funkčnost byla opět ověřena prostřednictvím testů konektivity a posbíráním jednotlivých výpisů.

Co se týká samotného členění, práce se skládá z několika kapitol. V publikačním review je vytvořen přehled o podobných pracích zpracovaných na problematiku IPv6. Kapitola Popis technologického aparátu představuje stručný teoretický přehled o vlastnostech protokolu IPv6. Další kapitoly se věnují praktické části této bakalářské práce. Je zde analýza stávajícího stavu sítě. Dále jsou zde rozebrány jednotlivé varianty dynamické konfigurace a také problémy, které s sebou přináší. V první fázi se jedná zejména o identifikátor rozhraní a vynucení jeho vytvoření prostřednictvím mechanismu EUI-64. V druhé fázi se pak setkáváme s problémem týkajícím se identifikace koncových klientů v DHCPv6 komunikaci. Jedná se o problém nestabilního DUID. Následující kapitola se zabývá implementací navržených variant a také jejich testováním. Poslední kapitoly jsou věnovány závěrečnému a finančnímu zhodnocení.

6 Analýza

V této kapitole bude zanalyzován současný stav síťové infrastruktury produkční sítě Mendelovy univerzity v Brně. Jedná se o velmi důležitou kapitolu, která pomáhá přiblížit realitu, a tím i skutečný stav sítě. Analýza je použita i v pozdějších fázích, zejména při návrhu řešení a při samotném řešení. Větší pozornost bude věnována především stávající dynamické konfiguraci koncových zařízení.

Mendelova univerzita v Brně byla založena v roce 1919. Nese název po významném vědci Johannu Gregoru Mendelovi. Skládá se z pěti fakult a jednoho vysokoškolského ústavu. Mimo areál školy se nachází několik vysokoškolských kolejí a školních zemědělských podniků – Lednice a Žabčice. Pro účely této práce se však bude brát v úvahu pouze ta část sítě, nacházející se v areálu Mendelovy univerzity v Brně.

6.1 Model sítě

Pro snadnější zobrazení skutečného stavu sítě poslouží následující model síťové infrastruktury. Díky tomuto modelu se můžeme snadněji orientovat v rozložení jednotlivých síťových prvků. Následující model může být využit také pro následný návrh řešení.

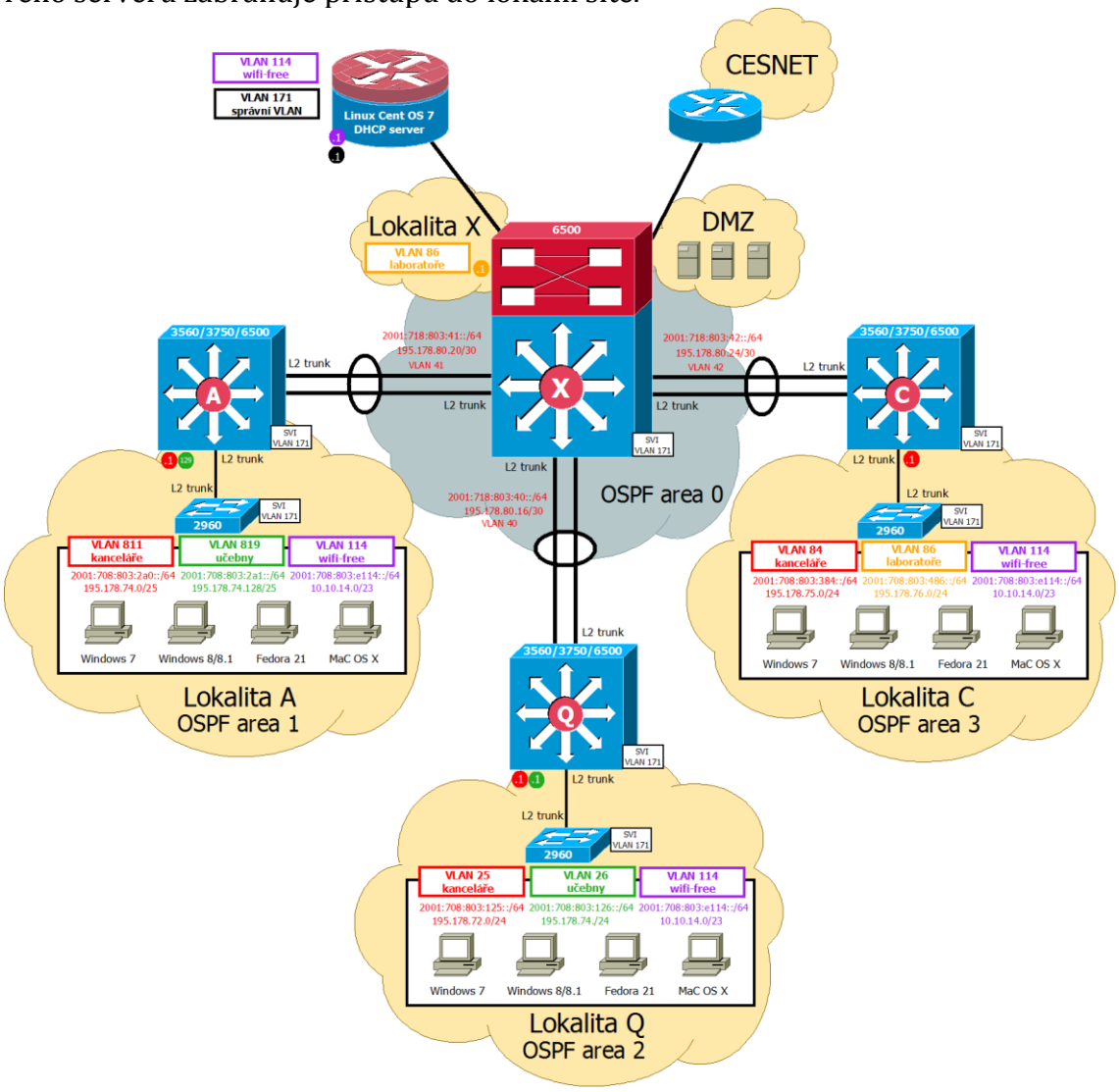
Model byl vytvořen na základě poskytnutých informací tak, aby co nejlépe odpovídal skutečnému stavu produkční sítě MENDELU. Podrobné informace o této síti však nemohly být poskytnuty z důvodu ochrany interních údajů Mendelovy univerzity. Všechna číselná označení, která se budou dále v této práci vyskytovat, jsou smyšlená a pouze odráží realitu.

Samotná síť MENDELU je tvořena cca 300 aktivními síťovými prvky, které umožňují stabilní komunikaci v síti. Hlavním síťovým prvkem je L3 přepínač umístěný na budově X. Reálně se jedná o dva fyzické přepínače typu Cat6500, které jsou logicky propojeny dohromady pomocí VSS (Virtual Switching System). Tento jeden logický L3 přepínač je následně rozdělen na několik virtuálních směrovačů VRF. V rámci této bakalářské práci je uvažována pouze VRF Internet a VRF Černá Pole.

K tomuto L3 přepínači jsou připojeny jednotlivé distribuční přepínače. Ty jsou k páteřní síti připojeny pomocí EtherChannelu tak, aby byla zátěž rovnoměrně rozložena mezi linky a v případě výpadku jednoho linku se o komunikaci postaral link druhý. Tím je docíleno vyšší rychlosti a také spolehlivosti. Distribuční přepínače slouží k propojení jednotlivých budov v rámci areálu školy. Uvnitř budovy se dále nachází velké množství přístupových přepínačů, nejčastěji se jedná o Cat2960. K nim jsou už přímo připojeny jednotlivé VLAN s koncovými zařízeními. Počítačová síť je využívána především studenty a zaměstnanci školy. Z tohoto důvodu zde existuje několik virtuálních lokálních sítí. Koncová zařízení se mohou nacházet v rámci jednotlivých učeben, kanceláří, anebo volně při použití bezdrátového připojení. Studenti se k internetu připojují pomoci bezdrátové sítě Eduroam. Internetové připojení Mendelově univerzitě v Brně poskytuje CESNET. K řízení bezpečnos-

ti síťového provozu a k přístupu do veřejného internetu se používá linuxový firewall. Na tomto linuxovém stroji běží také ISC DHCP server.

Existuje zde také tzv. demilitarizovaná zóna DMZ. Ta slouží k umístění školních serverů, které jsou primárně dostupné z veřejného internetu. V podstatě se jedná o podsíť, která chrání tyto servery před útoky z venku a při napadení některého serveru zabraňuje přístupu do lokální sítě.



Obr. 6 Model síťové infrastruktury produkční sítě MENDELU

6.2 Analýza technického vybavení

6.2.1 Aktivní síťové prvky

V produkční síti MENDELU se nachází cca 300 aktivních prvků. Jedná se zejména o L2 a L3 přepínače. Obecně lze tyto prvky rozdělit do tří kategorií, a to podle toho, v jaké části sítě se nacházejí. Existují zde 3 typy vrstev, ve kterých se aktivní prvky

mohou vyskytovat. Prvním typem je vrstva přístupová. Síťové prvky umístěné v přístupové L2 vrstvě slouží k propojení koncových zařízení a k jejich zařazení do VLAN. V síti MENDELU tuto funkci plní přepínače Cat2960, kterých může být na každém patře umístěno hned několik. Na této úrovni je také zajišťováno zabezpečení přístupu do sítě, a to prostřednictvím Port Security. Díky této metodě se na daném portu ověřuje, zda se uživatel přihlašuje do sítě s povolenou MAC adresou. Mezi další zabezpečovací funkci přístupové vrstvy patří DHCP Snooping. Touto funkcí jsou všechny porty považovány za nedůvěryhodné. Porty, ke kterým je připojen DHCP server nebo porty, které propojují jednotlivé přepínače pomocí trunků, nastavíme jako důvěryhodné. Komunikace z nedůvěryhodných portů je zahazována.

Druhou vrstvou je vrstva distribuční. Tato vrstva navzájem propojuje jednotlivá přístupová zařízení a slouží k distribuci služeb a funkcí. Dále slouží k ukončení některých VLAN a zajišťuje směrování mezi nimi (inter-VLAN routing). V této vrstvě se nacházejí L3 přepínače Cat3750, Cat4500 a někde se objevuje i Cat6500. Zpravidla bývá na každé budově alespoň jeden distribuční prvek.

Poslední vrstvou je vrstva páteřní, která propojuje distribuční prvky pomocí redundantních spojů umožňujících spolehlivé a rychlé směrování. V této vrstvě se nachází dva Cat6500, které jsou navzájem propojeny pomocí VSS (Virtual Switching System) a dále pak rozděleny do jednotlivých VRF.

Zařízení	Výrobce	Typ	Podpora IPv6
L3 přepínač	Cisco	Catalyst 6500	ano
L3 přepínač	Cisco	Catalyst 3750	ano
L3 přepínač	Cisco	Catalyst 4500	ano
přepínač	Cisco	Catalyst 2960	ano

Tab. 4 Aktivní prvky v síti

6.2.2 Koncová zařízení

Koncovými zařízeními se obecně rozumí jednotlivá fyzická zařízení, na kterých uživatelé pracují a pomocí kterých se připojují do sítě. Tato koncová zařízení můžeme rozdělit na několik typů podle toho, kde jsou umístěny, a jakým způsobem se konfigurují.

Prvním typem jsou desktopové počítače a tiskárny, které se nacházejí v jednotlivých učebnách a kancelářích. K získání IPv4 adresy využívají ISC DHCP server, a jsou tedy konfigurovány dynamicky. Dynamicky jsou konfigurovány také klientské stanice, které se do sítě připojují bezdrátově pomocí WLC (Wireless LAN Controller), který umožňuje jednotnou správu jednotlivých přístupových bodů. Do této skupiny patří především notebooky studentů, tablety nebo mobilní zařízení.

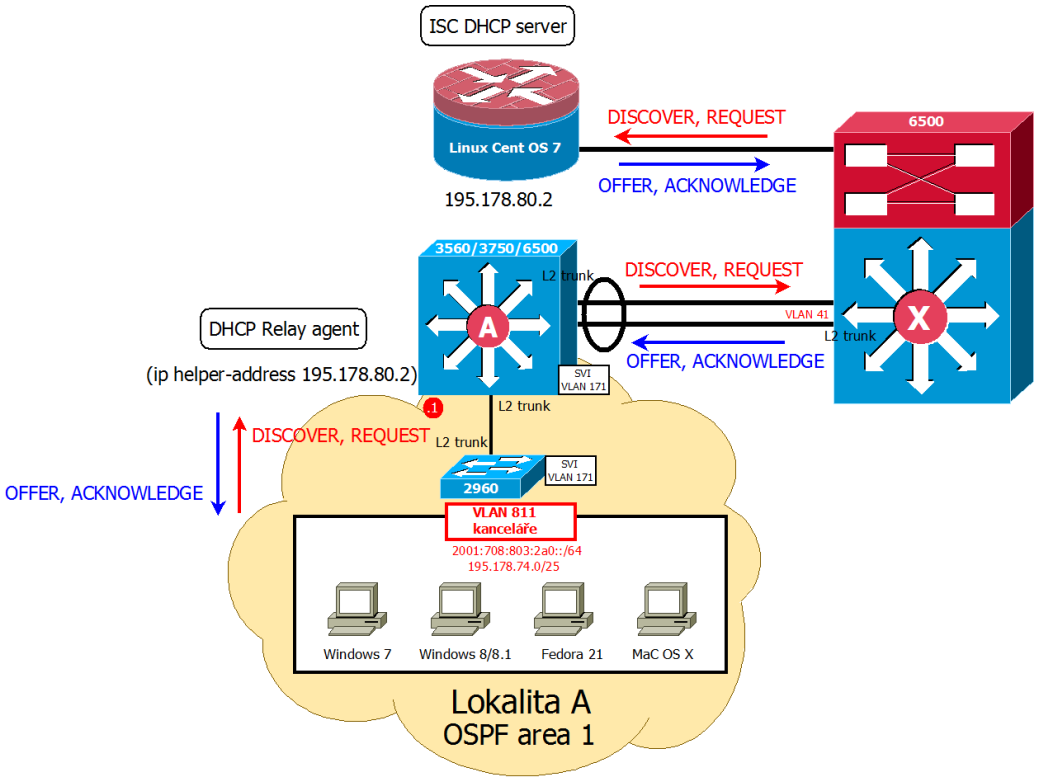
Mezi koncové zařízení patří i servery, které mají za úkol poskytovat klientům služby. IPv4 adresa je všem serverům a výchozím branám přidělena staticky, především z důvodu toho, aby měl správce přehled o síti, a aby byla zajištěna stálá dosažitelnost těchto serverů. Poslední skupinou zařízení v produkční síti MENDE-

LU jsou různá technologická zařízení, jako například čtečky karet, monitorovací kamery nebo různá čidla.

Zastoupení jednotlivých operačních systémů používaných klienty v síti MENDELU je velmi různorodé. Nejpočetnější skupinou jsou pravděpodobně klienti s operačním systémem Windows. Jedná se o Windows 7, Windows 8 a Windows 8.1. Dále se zde vyskytují uživatelé s operačním systémem Linux. Vynechat nelze ani uživatele používající operační systém Mac OS X. Všechny zmíněné operační systémy plně podporují protokol IPv6.

6.3 Dynamická konfigurace

Jak bylo zmíněno výše, v síti MENDELU se používají dva možné přístupy pro přidělování adres. Je zde manuální přidělování IPv4 adres serverům a výchozím branám a dynamické přidělování adres pomocí ISC DHCP serveru běžícím na linuxovém firewallu. Pro každý segment sítě obsahující DHCP klienty je potřeba mít dostupný DHCP server. Vzhledem k tomu, že máme v síti tento server pouze jeden, musíme v síti realizovat tzv. DHCP Relay agenty.



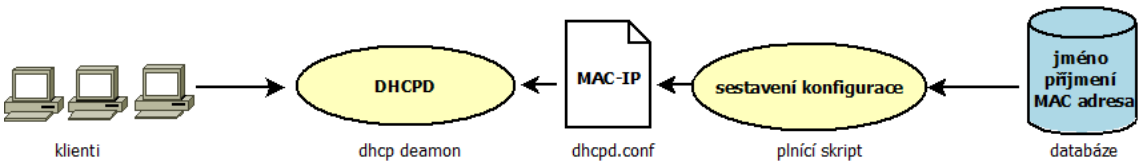
Obr. 7 Znázornění komunikace mezi DHCP klienty a DHCP serverem prostřednictvím Relay agenta

Funkci DHCP Relay agentů v produkční síti MENDELU plní všechny distribuční L3 přepínače a také páteřní L3 přepínač, vše záleží na tom, kde se nachází výchozí

brány pro jednotlivé VLAN. DHCP server je realizován na linuxovém stroji a je v celé síti pouze jeden.

Na obrázku 7 je zobrazen výřez z infrastrukturního modelu produkční sítě MENDELU. Na tomto výřezu je pak naznačena výměna DHCP zpráv mezi klienty z VLAN 811 a DHCP serverem prostřednictvím distribučního L3 přepínače, který zde plní funkci Relay agenta a tvoří prostředníka této komunikace. Existují dva způsoby jak klientům přidělovat IPv4 adresy prostřednictvím dynamické konfigurace. Prvním způsobem je přidělit klientovi adresu z předem definovaného rozsahu. Tento rozsah je nazýván pool adres. Konfiguračně složitějším způsobem je propojení klientovy MAC adresy se zvolenou IPv4 adresou. Tímto způsobem jsou konfigurovány koncové uzly v učebnách a kancelářích.

Je zřejmé, že v rozsáhlé síti obsahující velký počet klientů je toto propojení velmi časové náročné. V současné síti MENDELU je provozována databáze obsahující informace o jednotlivých uživatelích, včetně MAC adresy jejich zařízení. Dále existuje skript, který je schopen získat informace o MAC adrese z této databáze a automaticky naplnit konfigurační soubor DHCP serveru. Klientům je IPv4 adresa přidělena na základě jejich MAC adresy. DHCP deamon z konfiguračního souboru přečte dvojici MAC-IP a danou IPv4 klientovi přidělí.



Obr. 8 Plnění konfiguračního souboru dhcpd.conf informace z databáze

6.4 Shrnutí

Jak je z této kapitoly zřejmé, současná produkční sít MENDELU je v plně funkčním stavu. Otázkou tedy zůstává, proč navrhovat něco jiného. Hlavním důvodem pro implementaci nového protokolu IPv6 je zejména vyčerpání dostupných veřejných prefixů. Poskytovatel sítě CESNET odmítá nadále přidělovat další adresy.

Další velmi významný důvod, proč chce vedení školy zavést nový protokol, souvisí se současným trendem aktivního přechodu technických univerzit na novou verzi protokolu. Implementací IPv6 na MENDELU má univerzita možnost připojit se k ostatním univerzitám a držet s nimi krok. To má vliv také na udržení dobrého jména univerzity.

7 Návrh řešení

V této kapitole bude na základě předchozí analýzy uveden návrh dynamické konfigurace koncových klientů. Při implementaci nového protokolu bude zachována celá páteřní topologie stávající produkční sítě MENDELU. Také zůstane zachováno logické členění segmentů sítě do jednotlivých VLAN. Stávající síťové prvky budou také nadále součástí sítě, což by neměl být problém, s ohledem na jejich podporu IPv6 protokolu. Vzhledem k tomu, že poskytovatel CESNET nebuduje pouze IPv6 sítě, ale dual-stack, budou k dispozici oba dva protokoly současně.

Návrh řešení dynamické konfigurace koncových zařízení byl rozdělen do dvou fází, a to podle využitých technologií a mechanismů pro přidělování adres a získávání síťových parametrů.

Fáze jedna představuje zkušební provoz IPv6 v síti MENDELU. Je založena na automatické konfiguraci klientů pomocí mechanismu SLAAC. Tím odpadá nutnost realizovat stavový DHCPv6 server. Tato fáze byla vybrána vedením ÚIT Mendelovy univerzity v Brně na dobu přibližně jednoho roku. Poté se plánuje přechod na fázi dva, která je založena na využití stavového DHCPv6 serveru. Při stavové konfiguraci je zde kladen požadavek, aby klienti získávali IPv6 adresy na základě svého identifikátoru tak, aby měl správce přehled o jednotlivých zařízeních v síti. Jak již bylo řečeno, ruční plnění konfiguračního souboru je velmi časově náročné. Klíčový pro přechod na tuto fázi je tedy především vývoj skriptu umožňujícího automatické plnění konfiguračního souboru dhcpd.conf informacemi z databáze tak, jako je tomu v současnosti na IPv4. Tento problém by měly vyřešit již zadané vysokoškolské práce. Diplomová práce autora Bc. Olivera Horečného má za úkol implementaci webového rozhraní, které umožní správci zadávat potřebné informace. Diplomová práce autora Bc. Daniela Smolinského se pak následně bude zabývat skriptem, který umožní aktualizovat konfigurační soubor na základě dat z webové aplikace.

Dynamická konfigurace se týká především přístupové vrstvy, ve které jsou umístěni koncoví klienti v jednotlivých VLAN. Distribuční a páteřní vrstvu již zmiňovaného modelu síťové infrastruktury řeší diplomová práce autora Bc. Tomáše Filipa.

Globální IPv6 adresa, která je klientovi v jednotlivých fázích přidělena se skládá ze tří částí. Prvních 48 bitů je tzv. globální směrovací prefix. Tato část adresy je odvozena z prefixu, který byl Mendelově univerzitě v Brně přidělen lokálním poskytovatelem CESNET a je ve tvaru 2001:718:803::/48. (Ripe.net, 2015)

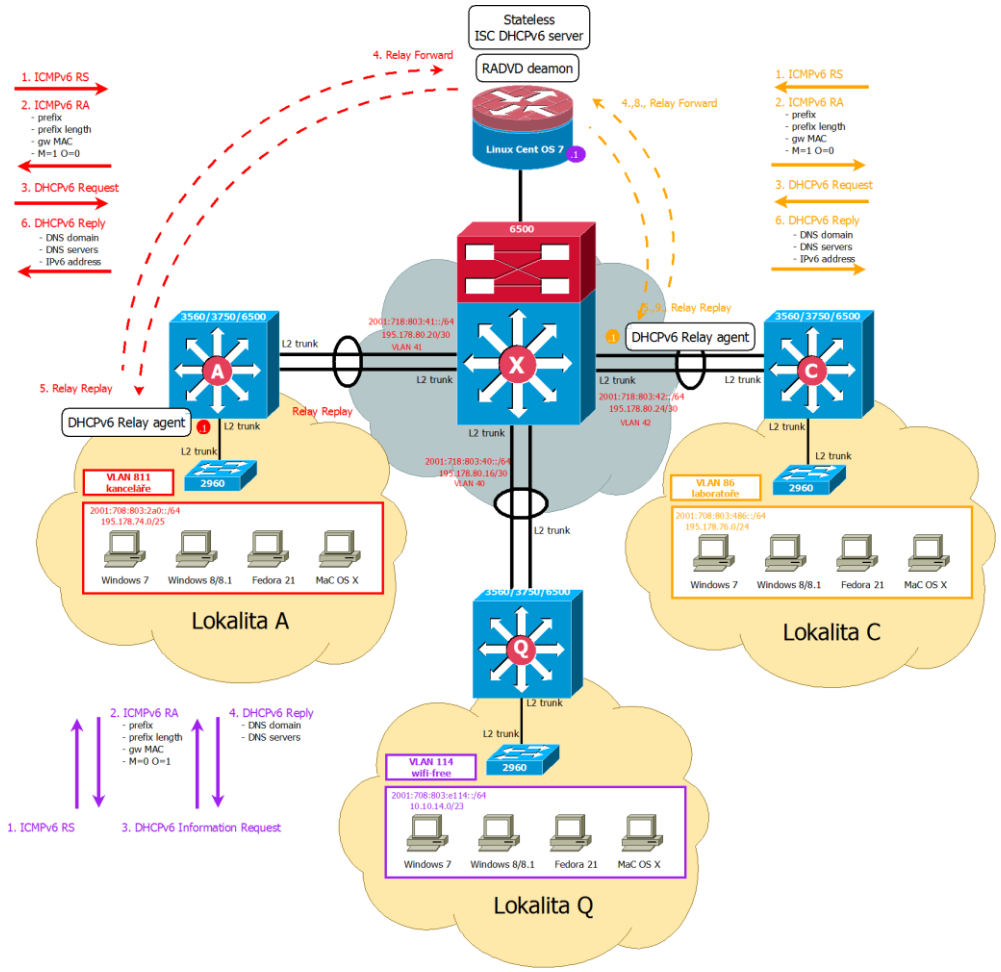
Po globálním směrovacím prefixu následuje 16 bitů pro identifikaci podsítě. Návrh adresace této části adresy má na starosti Bc. Tomáš Filip ve své diplomové práci. Zbylých 64 bitů představuje identifikátor rozhraní, jehož vytvoření je předmětem této bakalářské práce.

7.1 Fáze 1

Jak bylo řečeno výše, první fáze bude zaměřena na bezstavovou dynamickou konfiguraci. Pro získání síťových parametrů bude zkombinován mechanismus SLAAC spolu s bezstavovým DHCPv6 serverem, který doplní potřebné informace pro plnohodnotnou síťovou komunikaci. Kombinace je nutná z toho důvodu, že odpadá možnost využít standard definovaný v RFC 6106 (2010), který by klientům doplnil potřebné informace o DNS.

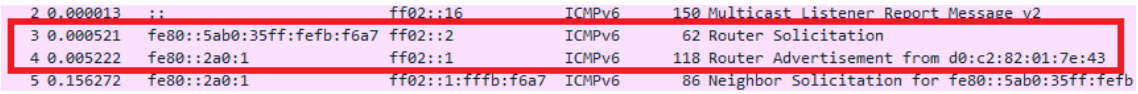
V předchozí kapitole byla zmíněna důležitost identifikátoru rozhraní a také to, jakým způsobem bude v každé fázi vytvořen. V první fázi se setkáme s několika způsoby vytvoření tohoto identifikátoru. K jeho vytvoření může být použit mechanismus EUI-64. Jednotliví klienti jsou pro správce snadno identifikovatelní na základě své MAC adresy.

Tento způsob vytvoření je současně požadavkem vedení ÚIT univerzity na tuto fázi. Právě kvůli snadné identifikaci koncových zařízení implementují některé operační systémy tzv. Privacy Extensions, které identifikátor rozhraní vytváří naprosto náhodně. Po připojení do sítě si však klient vygeneruje nejen trvalou adresu s náhodným identifikátorem, ale i dočasnou adresu s náhodným identifikátorem.



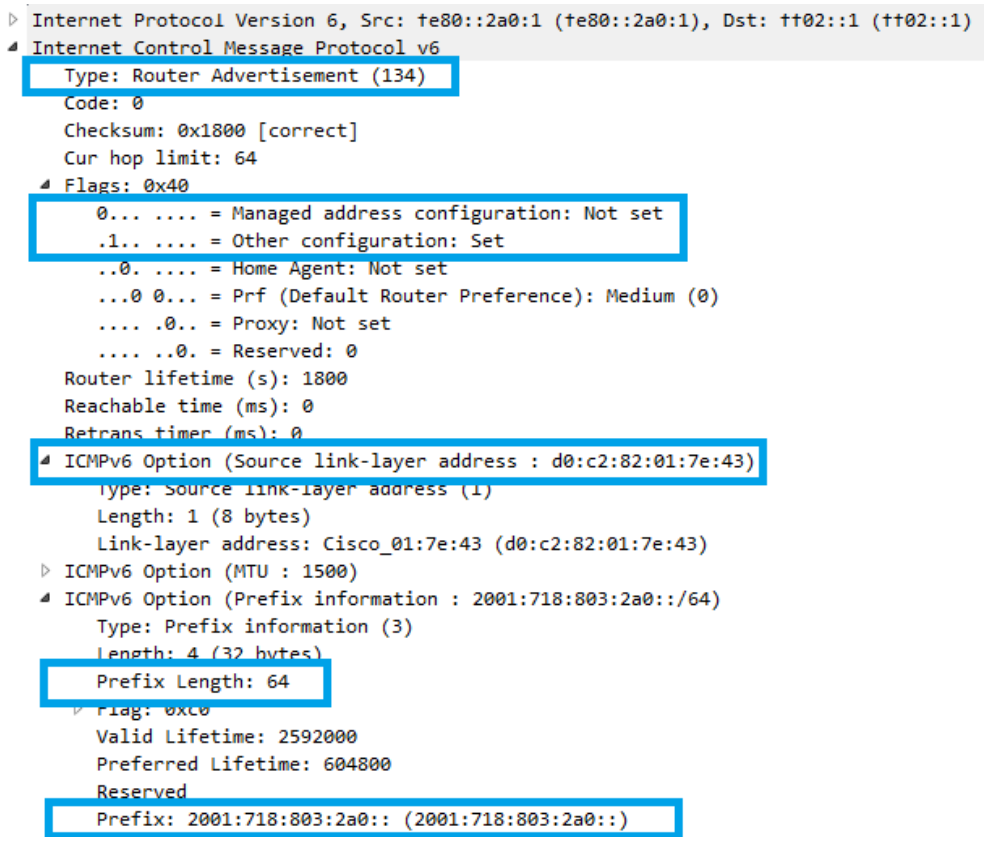
Obr. 9 Model produkční sítě MENDELU ve fázi 1

Na obrázku 9 je znázorněn model univerzitní sítě spolu s postupem získání IPv6 adresy a zbylých síťových parametrů. Klíčové jsou v této fázi již zmiňované ICMPv6 zprávy Router Solicitation a Router Advertisement. RS zprávy jsou zasílány klienty pro zjištění přítomnosti směrovače v síti. Tím je dosaženo větší dynamičnosti celé komunikace, než v případě, kdy klient čeká, až směrovač sám zašle tyto informace prostřednictvím zprávy RA.



Obr. 10 Záznam komunikace mezi klientem a směrovačem

Na obrázku 10 vidíme, jak probíhá komunikace mezi klientem a směrovačem, a tedy jakým způsobem klient získává jednotlivé síťové parametry. Můžeme si povšimnout, že nejprve klient aktivně zažádal o poslání informací zasláním zprávy RS na multicastovou adresu ff02::2. Jako odpověď mu přichází zpráva RA odeslaná směrovačem na multicastovou adresu ff02::01. Zpráva klienta informuje o síťových parametrech typu síťový prefix, délka prefixu a MAC adresa výchozí brány. Podrobný obsah RA zprávy je zobrazen na obrázku 11.



Obr. 11 Zpráva Router advertisement

Můžeme si povšimnout, že ohlášení směrovače neobsahuje informace o rekurzivním DNS serveru, které jsou ovšem nezbytné pro plnohodnotnou síťovou ko-

munikaci. Existuje zde rozšíření pro bezstavovou konfiguraci, které do ní doplňuje dvě položky. První z položek rozšiřuje bezstavovou konfiguraci o informaci o rekurzivním DNS serveru a druhá položka obsahuje seznam jednotlivých domén. Vše je detailně popsáno v dokumentu RFC 6106 (2010). Hlavním problémem je to, že tento standard musí být implementován nejen na směrovači, ale také na koncovém zařízení. U některých operačních systémů není snaha tento standard v budoucnu implementovat. Příkladem je například OS Windows. (Horley, 2013)

Tyto informace je tedy nutno získat jiným způsobem. Nabízí se použití DHCPv6 serveru. Z tohoto důvodu se v ohlášení směrovače nachází další dvě velmi důležité položky. Jedná se o flagy oznamující, jakým způsobem bude probíhat zjišťování zbylých síťových parametrů. Konkrétně se jedná o dva flagy (Managed Config Flag a Other Config Flag). V případě bezstavové konfigurace je nastaven flag M na hodnotu 0 a flag O na hodnotu 1. Nastavení těchto flagů opět vidíme na obrázku 11. Klient se díky tomu dozvídá, že pro získání zbylých informací o DNS se má obrátit na bezstavový DHCPv6 server.

Ke komunikaci se serverem používají klienti zprávy DHCPv6 Information Request a DHCPv6 Reply. Tyto zprávy zabalí DHCPv6 Relay agent do zpráv předání (Relay Forward) a odesílá je na bezstavový DHCPv6 server. Odpověď serveru obsahující záznamy o rekurzivním DNS serveru jsou pomocí zpráv zprostředkování (Relay Reply) zaslány DHCPv6 Relay agentovi, který tuto odpověď dále předává klientovi prostřednictvím zprávy DHCPv6 Reply.

Primárním problémem první fáze je již zmiňované vytvoření identifikátoru rozhraní pomocí mechanismu EUI-64. U Fedory tento problém odpadá, ve výchozím nastavení si sama vytvoří adresu podle výše zmíněného identifikátoru. Tento problém se však týká operačních systému Windows a Mac OS X. Oba dva tyto systémy ve výchozím nastavení povolují vytváření dočasných adres. Vynutit vytvoření identifikátoru použitím EUI-64 a zároveň zakázat vytváření náhodných a dočasných adres je možno provést následujícími příkazy.

Windows

```
netsh interface ipv6 set privacy state=disabled store=persistent
netsh interface ipv6 set global randomizeidentifiers=disabled sto-
re=persistent
```

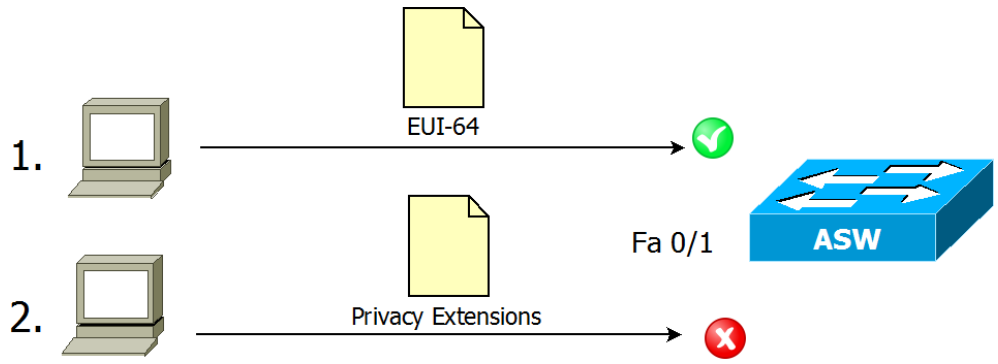
Mac OS X

```
/usr/sbin/sysctl net.inet6.ip6.use_tempaddr=0
```

V síti, která však obsahuje velký počet klientů je toto ruční zadávání příkazů velmi neefektivní a je zde problém, jak přinutit jednotlivé uživatele, aby na svém zařízení příkazy skutečně provedli. Bohužel zde není ani způsob, jak vynutit EUI-64 ze sítě, například nastavením určitého flagu. Jako jedno z možných řešení se nabízí použití kontrolních seznamů ACL (Access Control List) přímo na přístupových L2 zařízeních. Tyto seznamy slouží k řízení síťového provozu a k vynucování síťové politiky. IPv6 ACL lze aplikovat přímo na L2 port nebo na L3 směrovač, tedy na SVI určité VLAN. Na základě definovaných pravidel můžeme pakety na daném portu povolit (permit) nebo zakázat (deny). Tímto tedy můžeme do sítě propouštět

pouze pakety zaslané klientem využívajícím identifikátor EUI-64. Potřebné informace pro vytvoření kontrolního seznamu lze využívat například z databáze obsahující informace o jednotlivých uživatelích. Jelikož v současné síti používáme bezpečnostní mechanismus Port Security, obsahuje tato databáze také informaci o MAC adrese každé klientské stanice, která jednoduše poslouží k vytvoření klientova EUI-64 identifikátoru. Níže je ukázka možného nastavení IPv6 PACL na L2 portu.

```
Cat2960(config)#ipv6 access-list EUI64
Cat2960(config-ipv6-acl)# permit ipv6 host 2001:718:803:2a0:a00:27ff:fec8:b02
any
Cat2960(config-ipv6-acl)#exit
Cat2960(config)#interface fa0/1
Cat2960(config-if)#ipv6 traffic-filter EUI64 in
Cat2960(config-if)#exit
```



Obr. 12 Příklad přechodu paketů přes přístupový prvek

IPv6 PACL nám tedy zajistí stav zobrazený na obrázku 12. Pakety zaslané klientem vlastnícím identifikátor rozhraní podle EUI-64 bez problému projdou přes přístupový síťový prvek. Pokud však klient pro svou komunikaci používá Privacy Extensions, jeho pakety přes přístupovou úroveň neprojdou, a budou tedy zahozeny.

S bezpečnostní politikou vytvářenou na portech souvisí také vlastnost DHCP Snooping, která umožňuje filtraci DHCP zpráv. Ve výchozím nastavení jsou všechny porty považovány za nedůvěryhodné a my nastavujeme ty, které budou důvěryhodné. Lze vytvářet také DHCP Binding Database, kde jsou zaneseny informace o všech přidělených IP adresách a také informace o daných rozhraních. Následně je tato databáze porovnávána se zdrojovou adresou klienta, od kterého pakety přicházejí. Pokud komunikace vychází z nedůvěryhodného portu, pakety se zahazují. Pro následnou blokaci nepovolených IP adres se využívá IP Source Guard.

Velkou nevýhodou je především to, že jak IPv6 PACL, tak IPv6 Source Guard jsou dostupné pro Cat2960 pouze od verze IOS 15.0(2) a pozdější. (Cisco, 2015) V produkční síti MENDELU se ovšem vyskytují Cat2960, které mají verzi IOS nižší.

Z tohoto důvodu není možné vyzkoušet tyto způsoby v síťové laboratoři, ani je nelze použít při implementaci.

Poslední dostupný způsob vynucení EUI-64 je přímo na linuxovém firewallu. Jedná se o nejzazší dostupnou variantu, protože by bylo vhodné zabezpečit tento problém již na přístupových zařízeních. Samotné řešení a implementace tohoto řešení bude popsána v diplomové práci Bc. Michala Šturmy.

7.1.1 Shrnutí fáze 1

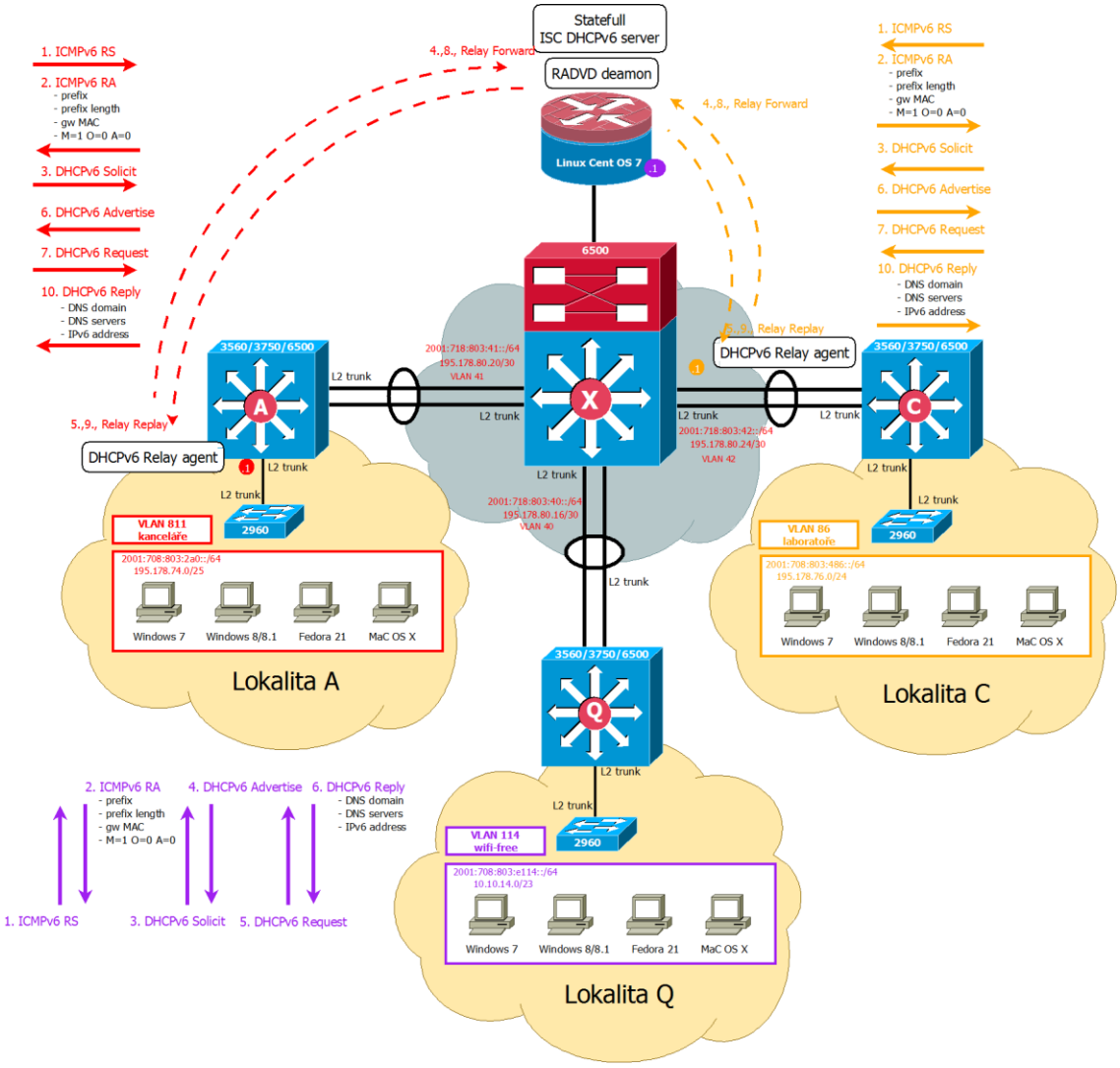
Aby bylo možno implementovat a následně ověřit první fázi, je dobré stanovit si přesný pracovní postup.

1. Nejprve je nutno nastavit jednotlivé výchozí brány pro dané VLAN. Tento krok vyžaduje nejprve aktivovat dual-stack v SDM (Switch Database Manager) pro společný provoz IPv4 a IPv6. Dále zde nastavujeme podporu směrování IPv6. Každému SVI přiřadíme statickou IPv6 adresu. Velmi důležitým krokem je nastavení ohlášení směrovače, jak na Ciscu, tak v radvd.conf. V rámci tohoto kroku budou nastaveny také flagy M na hodnotu 0 a flag O na hodnotu 1. Zde taktéž dojde ke konfiguraci DHCPv6 Relay agentů, aby byla zajištěna komunikace mezi DHCPv6 klientem a DHCPv6 serverem, nacházejícím se na linuxovém firewallu.
2. Dále bude provedeno nastavení bezstavového DHCPv6 serveru.
3. Vynucení identifikátoru EUI-64 u koncových klientů.
4. Posledním krokem je nastavení koncových klientů a nastavení dynamického získávání IPv6 adresy.

7.2 Fáze 2

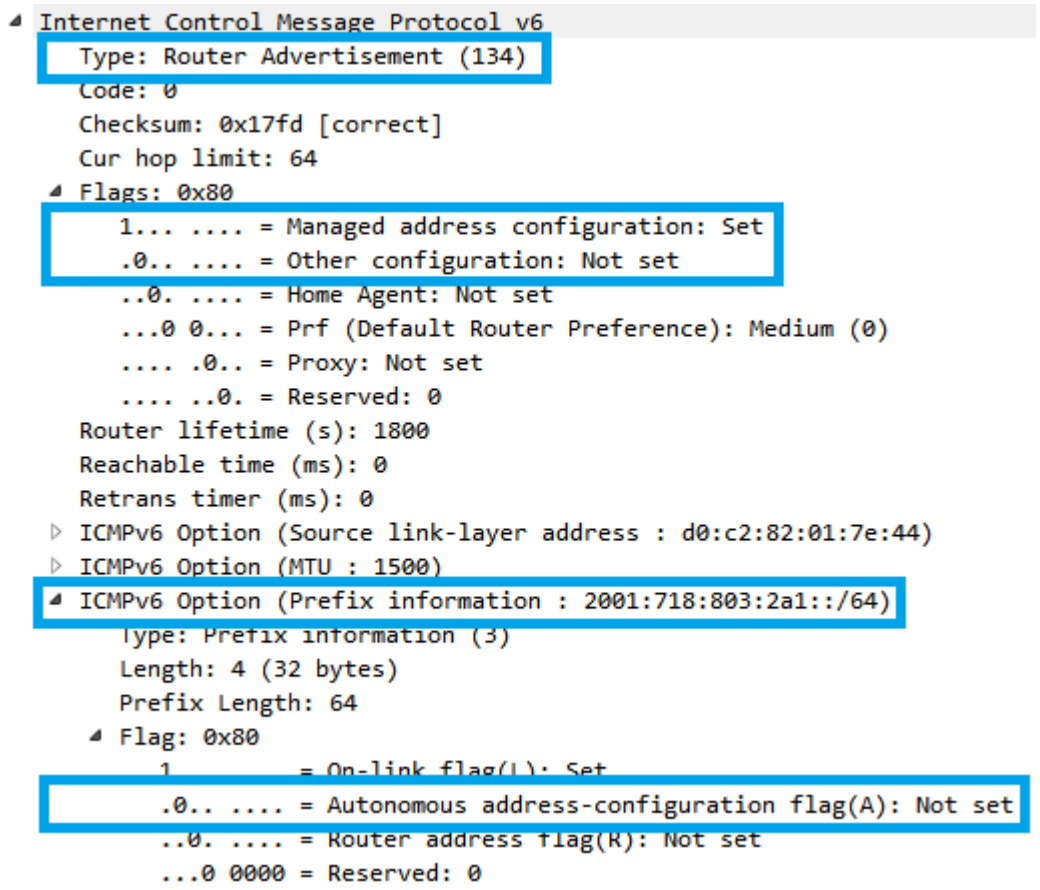
Druhá fáze je obdobou fáze první, avšak podstatou tohoto návrhu je využití stavového DHCPv6 serveru pro dynamické přidělování IPv6 adres a dalších síťových parametrů. Základním požadavkem pro tuto fázi je získání adresy ze stavového DHCPv6 serveru, a to takovým způsobem, že tato adresa bude klientovi přiřazena na základě jeho jedinečného identifikátoru. To správci sítě zajistí dostatečný přehled a kontrolu nad jednotlivými zařízeními připojenými v síti.

Obrázek 13 vyobrazuje navržený model produkční sítě MENDELU ve fázi dva. Je zde opět znázorněna komunikace klientů jak se směrovači, tak s DHCPv6 serverem.



Obr. 13 Model produkční sítě MENDELU ve fázi 2

Získávání adres opět začíná zasláním zprávy Router Solicitation, kterou klient žádá směrovač o zaslání potřebných parametrů prostřednictvím zprávy Router Advertisement. V této fázi je opět klíčové nastavení flagů M a O.



Obr. 14 Zpráva Router Advertisement – nastavení flagů M a O

Jak vidíme na obrázku 14, při využití stavové konfigurace pro dynamické získání IPv6 adresy je nastaven flag M na hodnotu 1 a flag O na hodnotu 0. Klient tedy ví, že zbylé informace mu poskytne stavový DHCPv6 server. Komunikace s tímto serverem opět probíhá jako ve fázi jedna prostřednictvím DHCPv6 Relay agenta. Komunikace mezi klientem a serverem je zajištěna prostřednictvím čtyř zpráv – Solicit, Advertise, Request a Reply. Všechny zprávy procházejí skrze DHCPv6 Relay agenta tak, jako tomu bylo ve fázi jedna. K tomu jsou využity zprávy Relay Forward a Relay Reply.

Ve zprávě DHCPv6 Reply, která ukončuje celou komunikaci, jsou obsaženy síťové parametry zaslané daným DHCPv6 serverem. Jedná se o IPv6 adresu a informaci o rekurzivním DNS serveru a seznamu jednotlivých domén. Navíc zde však přibyla položka o poskytnuté IPv6 adrese.

V druhé fázi je také potřeba vynutit, aby klienti využívali adresu, kterou jim DHCPv6 server přidělí. Některé operační systémy si vytváří pro zajištění vyšší bezpečnosti tzv. dočasné adresy pomocí prefixu získaného z ohlášení směrovače. Je

tedy potřeba zajistit, aby klienti nad ohlašovaným prefixem neprováděli bezstavovou konfiguraci. K tomu slouží flag A, který se nachází ve zprávě Router Advertisement a je součástí volby informace o prefixu. Řešením je vynulování tohoto flagu tak, jako je zobrazeno na obrázku 14 prostřednictvím následujícího příkazu.

```
ipv6 nd prefix 2001:718:803:xxxx::/64 no-autoconfig
```

Klientům lze přidělovat adresy dvěma způsoby. První a konfiguračně nejsnazší možností je definovat určitý rozsah neboli tzv. pool adres, ze kterého bude klientovi adresa přidělena. Těchto rozsahů bývá vytvořeno několik, obvykle pro každou virtuální lokální síť. Pomocí příkazu range6 pak následně určíme rozmezí zadáním první a poslední adresy, kterou je možno klientům z dané podsítě přidělit.

Druhou o něco komplikovanější variantou je navázat přesně definovanou IPv6 adresu na identifikátor klienta. V případě IPv4 se jednalo o MAC adresu klienta, která sloužila pro jeho jednoznačné určení. V IPv6 je nově klient identifikován pomocí DUID. Jak již bylo dříve zmíněno, existuje několik způsobů, jak lze DUID vytvořit. Zjištění DUID probíhá na každém operačním systému jiným způsobem. Nejsnadnější zjištění poskytuje operační systém Windows. DUID klienta je přímo součástí výpisu ipconfig /all. K vypsání DUID na Mac OS X slouží příkaz ipconfig getv6packet en1. Na Fedoře je potřeba hledat DUID v souboru obsahujícím informaci o jednotlivých zápůjčkách. Cesta k tomuto souboru je následující /var/lib/dhclient/dhclient6.leases. Navázání IPv6 adresy na DUID klienta probíhá prostřednictvím příkazu fixed-address6 v konfiguračním souboru dhcpd.conf.

Hlavním problémem této varianty je již zmiňované navázání IPv6 adresy na DUID klienta. Při velkém počtu připojujících se klientů je ruční plnění konfiguračního souborů téměř nerealizovatelné. Řešením je využití databáze a skriptu, který ji s konfiguračním souborem propojí a bude automaticky aktualizovat. Správce v aplikaci vyplní údaje k určitému uživateli včetně jeho DUID a tyto informace se přenesou do konfiguračního souboru. Dalším problémem je fakt, že DUID, jako klientův jednoznačný identifikátor, je poměrně nestálé. Pokud na jednom stroji realizujeme více operačních systémů, pak každý tento systém bude mít své vlastní DUID. Nevýhodné je také přeinstalování stávajícího operačního systému, které zapříčiní opět změnu tohoto identifikátoru.

Pokud by se řešení s identifikátorem DUID do budoucna ukázalo jako nevyhovující, existuje i alternativní řešení. Na základě e-mailové konverzace se správcem sítě UCEEB ČVUT vyplynulo, že při řešení problému s nestabilitou DUID zvolili stavový DHCPv6 Dibbler server, který umožňuje klientům rezervovat adresy na základě MAC adresy nebo lokální linkové adresy. Detailní informace o tomto přidělování lze nalézt v uživatelské příručce pro Dibbler server. (Klub.com.pl, 2015, s. 71)

7.2.1 Shrnutí fáze 2

Také při řešení druhé fáze je vhodné stanovit jednotlivé kroky pro provedení druhé fáze takovým způsobem, aby tato fáze správně fungovala a vyhovovala předem daným požadavkům.

1. Na začátku je opět nutno nastavit jednotlivé výchozí brány pro dané VLAN. Nejprve opět aktivujeme dual-stack v SDM a povolíme také IPv6 směrování. Dále přiřadíme statické IPv6 adresy jednotlivým rozhraním. Následuje nastavení flagu M na hodnotu 1 a flagu O na hodnotu 0. V dalším kroku nastavíme potřebné DHCPv6 Relay agenty, kteří budou přenášet DHCPv6 komunikaci mezi DHCPv6 klienty a DHCPv6 serverem.
2. Dalším krokem je nastavení stavového DHCPv6 serveru, tudíž je nutno navázat zde jednotlivé IPv6 adresy na DUID zvolených klientů a také uvést potřebné informace o DNS.
3. Na závěr je potřeba nastavit na koncových klientech, aby si IPv6 adresu získali dynamicky.

7.3 Shrnutí

Jak již bylo řečeno, dynamická konfigurace s sebou přináší určité komplikace, a proto je zásadní vybrat správnou variantu, která nám tuto konfiguraci umožní.

Je potřeba zohlednit jednotlivé možnosti každé varianty. Například, že ohlášení směrovače neobsahuje informace o IPv6 adresách rekurzivních DNS serverů, které jsou nezbytné pro plnohodnotnou komunikaci v síti. Je tedy zřejmé, že tyto informace bude nutno předat jiným způsobem. Zde se nabízí možnost použít variantu popsanou ve fázi jedna a zkombinovat mechanismus SLAAC s bezstavovým serverem DHCPv6. Pokud bychom chtěli využít pouze protokol DHCPv6, opět narazíme na překážku. Tento protokol dokáže předat všechny síťové parametry, až na jeden velmi důležitý, a to adresu výchozí brány. Nutno tedy vycházet z varianty popsané ve fázi dva a použít tento server společně s ohlášením směrovače.

Jako řešení se tedy nabízí možnost zkombinovat zcela odlišné mechanismy a protokoly, kdy jeden bez druhého nemůže plnohodnotně fungovat. V každém případě je však potřeba mít na směrovači nastaveno posílání RA zpráv, pomocí nichž určíme, jak bude komunikace dále probíhat.

Osobně se přikláním k variantě navržené v první fázi. Především díky velké výhodě spočívající v tom, že není nutno realizovat stavový DHCPv6 server a není potřeba řešit navázání IPv6 adres na klientovo nestálé DUID. V lednu 2015 bylo rozhodnuto vedením ÚIT o způsobu dynamické konfigurace koncových klientů při reálném nasazení IPv6 do produkční sítě MENDELU. Byla vybrána bezstavová konfigurace popsaná ve fázi 1. Hlavním důvodem, proč nebyl zvolen stavový DHCPv6 server, byla obtížná realizace navázání identifikátorů klientů na dané IPv6 adresy. Čeká se tedy na vytvoření již zmíněného skriptu, který usnadní plnění konfiguračního souboru DHCPv6 serveru. V okamžiku, kdy tento skript vznikne, se může začít pracovat na přechodu z první testovací fáze 1 do požadované konečné fáze 2. Výhledově se jedná o časový horizont minimálně jednoho roku.

8 Řešení

8.1 Implementace fáze 1

Konfigurace fáze jedna se bude opírat o jednotlivé body stanovené v předchozí kapitole. Postupně budou rozepsány jednotlivé kroky, až na předposlední krok, který není možno v laboratoři vyzkoušet.

8.1.1 Konfigurace výchozí brány

Prvním úkolem je zajistit společný provoz jak protokolu IPv4, tak protokolu IPv6 a zajistit také IPv6 směrování.

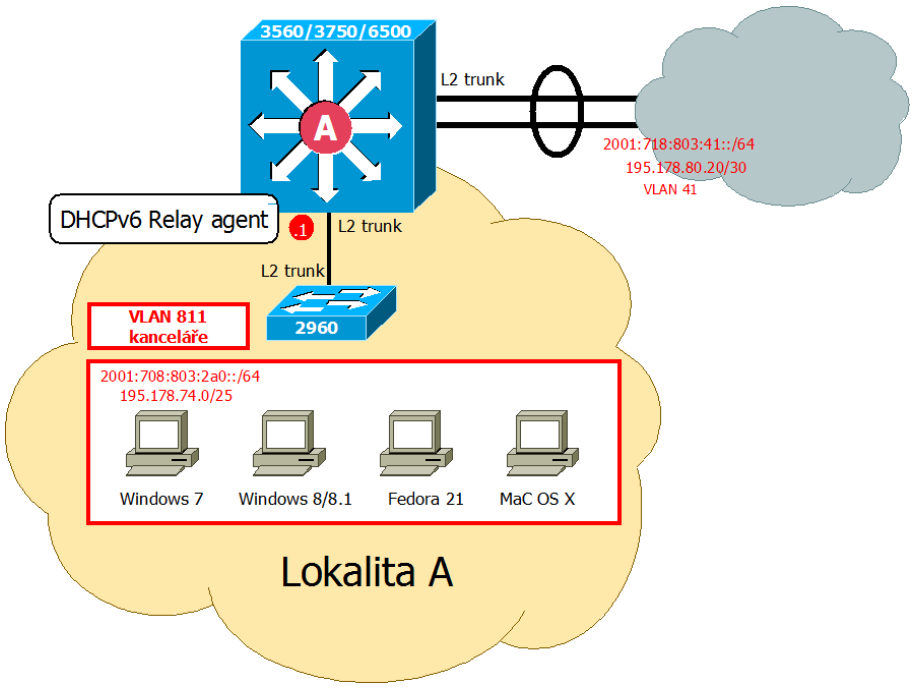
```
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#ipv6 unicast-routing
```

Následně pro každou VLAN obsahující koncové klienty nastavíme výchozí bránu. Nejprve určíme, o jaké rozhraní se jedná. Následně pro toto rozhraní přiřadíme IPv4 a IPv6 adresu, z toho důvodu, že v provozu budou oba dva protokoly současně. Za IPv4 adresu přidáme také masku sítě. Pro zasílání informací o prefixu zde uvedeme také prefix a samozřejmě jeho délku.

Na Ciscu jsou ohlášení směrovače ve výchozím stavu posílána automaticky. My však můžeme nastavit interval, ve kterém se tyto zprávy budou klientům rozesílat v případě, že si o ně sami aktivně nepožádají. Na linuxovém firewallu nastavíme zasílání směrovače v konfiguračním souboru radvd.conf.

Dále je klíčové správné nastavení ManagedConfig flagu a OtherConfig flagu. Vzhledem k tomu, že se tato fáze zabývá bezstavovou konfigurací, je nutno nastavit flag M na hodnotu 0 příkazem no ipv6 nd managed-config-flag a flag O na hodnotu 1 příkazem ipv6 nd other-config-flag. Tím zajistíme, aby se klient z ohlášení směrovače dozvěděl, odkud získat chybějící informace.

Výchozí brány fungují také jako prostředníci DHCPv6 komunikace. Z tohoto důvodu zde nastavíme helper adresy, které umožňují těmto Relay agentům přeposílat zprávy od klientů na server. U IPv4 se jedná o příkaz helper-address, v případě IPv6 použijeme relay destination.



Obr. 15 VLAN 811 v lokalitě A

Pro zjednodušení bude uvedena konfigurace pouze pro jedno rozhraní z vybrané lokality a také konfigurace rozhraní na linuxovém firewallu. Ostatní konfigurace budou součástí příloh. Pro lepší orientaci poslouží obrázek č. 15.

Lokalita A

```
Switch(config)#interface vlan811
Switch(config-if)#ip address 195.178.74.1 255.255.255.128
Switch(config-if)#ip helper-address 195.178.80.2
Switch(config-if)#ipv6 address 2001:718:803:2a0::1/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:2a0::/64
Switch(config-if)#no ipv6 nd managed-config-flag
Switch(config-if)#ipv6 nd other-config-flag
Switch(config-if)#ipv6 nd ra interval 600 198 # intervaly pro zasílání RA
Switch(config-if)#ipv6 dhcp relay destination 2001:718:803:f21::2
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Linuxový firewall

Nastavování výchozí brány na linuxovém firewallu probíhá jiným způsobem. Nejprve je potřeba nastavit rozhraní, které bude plnit funkci výchozí brány. Tomuto rozhraní přiřadíme především IPv4 adresu, masku sítě a IPv6 adresu včetně délky prefixu.

```
DEVICE=eth0.114 # označení rozhraní
VLAN=yes # jedná se o VLAN
```

```
NM_CONTROLLED=no # rozhraní nebude spravováno pomocí Network Managera
ONBOOT=yes # rozhraní bude aktivováno při zapnutí

USERCTL=no  # pouze root může spravovat toto rozhraní
BOOTPROTO=none # nebude použit protokol bootp ani dhcp
IPADDR=10.10.14.1 # ipv4 adresa
NETMASK=255.255.254.0 # maska sítě

IPV6INIT=yes # povoluje ipv6 inicializaci na tomto rozhraní
IPV6ADDR=2001:718:803:e114::1/64 # ipv6 adresa
IPV6_AUTOCONF=no # na tomto rozhraní nejsou přijímány ani přesměrovávány RA zprávy
IPV6_ROUTER=no # RA z tohoto rohraní nebudou zasílána
IPV6TO4INIT=no # zakazuje inicializaci 6to4 na tomto rozhraní
```

Druhým krokem je nastavení zasílání ohlášení směrovače pro end-to-end VLAN 114. To provedeme nastavením konfiguračního souboru /etc/radvd.conf. Hlavní rozdíl oproti výše zmíněné konfiguraci Cisco zařízení je ten, že v radvd musíme zasílání RA ručně povolit. Velmi důležité je opět správné nastavení flagů M na hodnotu 0 a flagu O na hodnotu 1.

```
interface eth0.114
{
       AdvSendAdvert on; # aktivace posílání RA
       AdvManagedFlag off; # flag M je nastaven na hodnotu 0
       AdvOtherConfigFlag on; # flag O je nastaven na hodnotu 1
       MinRtrAdvInterval 198; # minimální interval pro posílání RA
       MaxRtrAdvInterval 600; # maximální interval pro posílání RA
       prefix 2001:718:803:e114::/64 {}; # prefix, který bude RA oznamovat
};
```

8.1.2 Konfigurace bezstavového ISC DHCPv6 serveru

Konfigurace DHCPv6 serveru probíhá v souboru /etc/dhcpd6.conf, je velmi jednoduchá, není nutno nijak explicitně sdělovat, že se jedná o bezstavovou konfiguraci, pouze stačí vynechat údaje týkající se přidělení adres.

Dalšími velmi důležitými údaji jsou v konfiguračním souboru informace o rekurzivním DNS serveru.

DNS

```
option dhcp6.name-servers 2001:718:803:f21::2;
option dhcp6.domain-search "mendelu.cz";
```

VLAN obsahující DHCPv6 server

```
subnet6 2001:718:803:f21::/64 {} # nebudou ignorovány požadavky v VLAN, ve které
                                   je DHCPv6 server umístěn
```

End-to-End VLAN114

```
subnet6 2001:718:803:e114::/64 {}
```

Lokalita Q

```
subnet6 2001:718:803:125::/64 {}
subnet6 2001:718:803:126::/64 {}
```

Lokalita A

```
subnet6 2001:718:803:2a0::/64 {}
subnet6 2001:718:803:2a1::/64 {}
```

Lokalita C

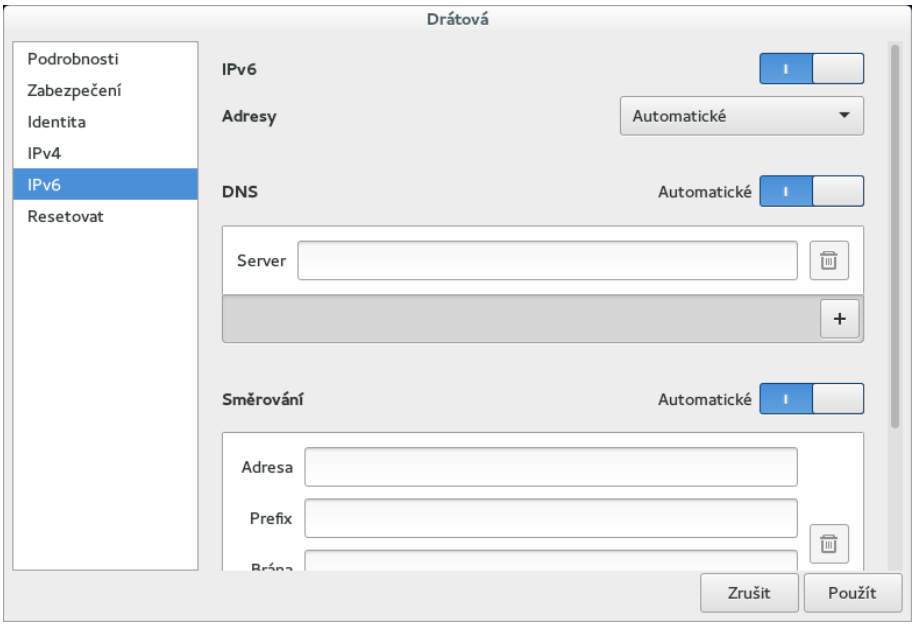
```
subnet6 2001:718:803:384::/64 {}
```

Lokalita X

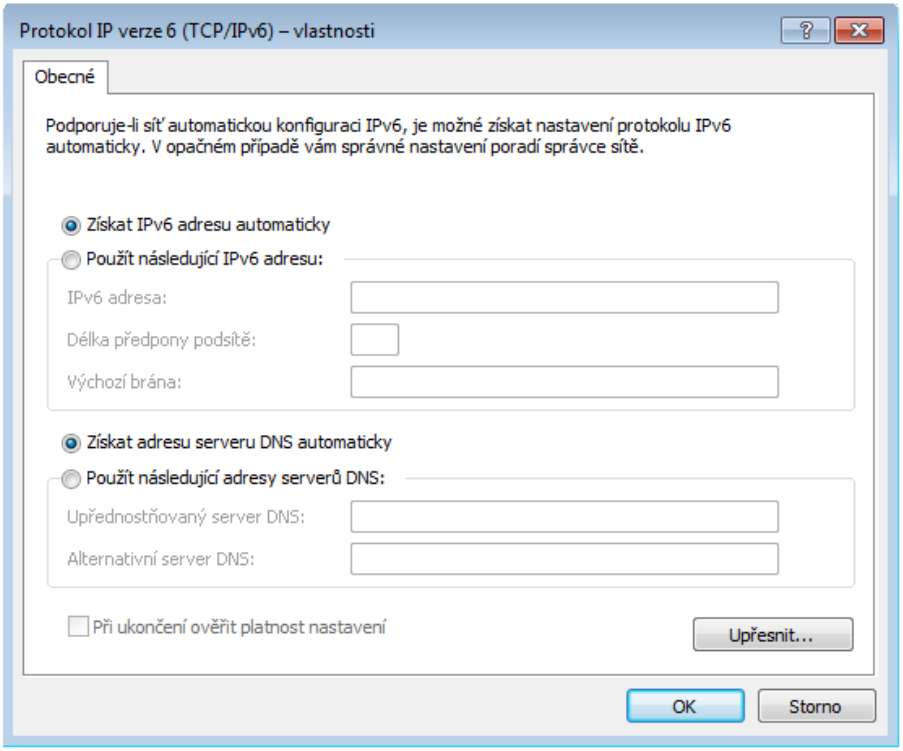
```
subnet6 2001:718:803:486::/64 {}
```

8.1.3 Konfigurace koncových klientů

Samotná konfigurace jednotlivých klientů proběhla velmi jednoduše. Jediné, co bylo potřeba na koncových klientech nastavit, bylo dynamické získávání IPv6 adresy. Pro příklad je uvedeno nastavení na klientech s operačním systémem Linux (konkrétně se jedná o distribuci Fedora 21) a operačním systémem Windows 7.



Obr. 16 Nastavení dynamického získávání IPv6 adresy na Fedoře 21



Obr. 17 Nastavení dynamického získávání IPv6 adresy na Windows 7

8.2 Implementace fáze 2

Také implementace této fáze bude založena na bodech z kapitoly Návrh řešení. Nejprve bude nastavena výchozí brána, včetně zasílání RA a nastavení DHCPv6 Relay agentů. Dále bude uvedeno nastavení konfiguračního souboru dhcp.conf pro stavový DHPCv6 server. Posledním krokem bude obdobně jako ve fázi jedna nastavení koncových klientů.

8.2.1 Konfigurace výchozí brány

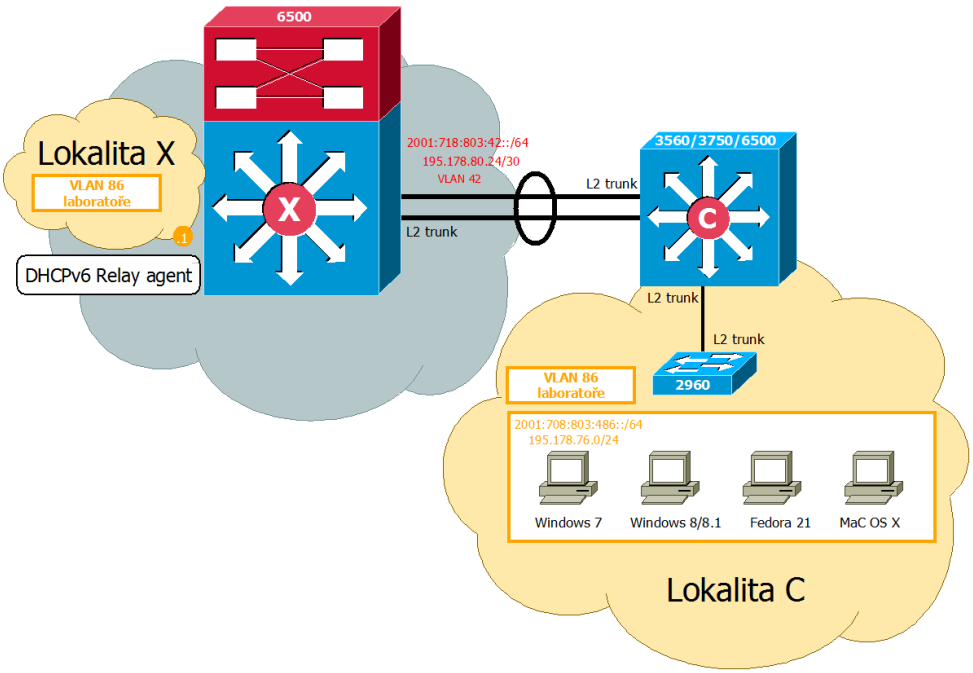
Zde také nejprve aktivujeme společný provoz obou protokolů a zajistíme IPv6 směrování pomocí následujících dvou příkazů.

```
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#ipv6 unicast-routing
```

Dále pro každou lokalitu nastavíme potřebné výchozí brány pro jednotlivé virtuální lokální sítě z infrastrukturního modelu. Vybranému rozhraní přiřadíme opět obě IP adresy včetně masky sítě a prefixu sítě s jeho délkou. Provedeme nastavení intervalu pro zasílání ohlášení směrovače a následně nastavíme pro tyto rozhraní helper adresy pro komunikaci s DHCP serverem.

V následujícím kroku bude zásadní změna oproti fázi jedna, a to v nastavení již zmiňovaných flagů M a O. Vzhledem k tomu, že podstatou fáze dva je stavová konfigurace, a tedy použití stavového DHCPv6 serveru, je flag M nastaven na hodnotu

1 a flag O na hodnotu 0. Zde je také velmi důležité vynulování flagu A diskutovaného v kapitole Návrh řešení fáze dva. Tím zajistíme, aby klienti neprováděli nad ohlašovaným prefixem bezstavovou konfiguraci a docílíme toho, aby adresa přidělaná DHCPv6 serverem byla jediná, kterou klienti budou používat.



Obr. 18 VLAN86 v lokalitě X

Také zde bude pro zjednodušení zobrazena konfigurace pouze rozhraní VLAN 86, která má výchozí bránu v lokalitě X a také konfigurace linuxového firewallu.

Lokalita X

```
Switch(config-if)#interface vlan86
Switch(config-if)#ip address 195.178.76.1 255.255.255.0
Switch(config-if)#ip helper-address 195.178.80.2
Switch(config-if)#ipv6 address 2001:718:803:486::1/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:486::/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:125::/64 no-autoconfig # flag A
Switch(config-if)#no ipv6 other-config-flag
Switch(config-if)#ipv6 managed-config-flag
Switch(config-if)#ipv6 dhcp relay destination 2001:718:803:f21::2
Switch(config-if)#ipv6 nd ra interval 600 198 # intervaly pro zasílání RA
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Linuxový firewall

Na linuxovém stroji opět nastavíme IP adresy pro výchozí bránu VLAN 114, která je v rámci celé sítě. Z tohoto rozhraní se budou zasílat také ohlášení směrovače se správně nastavenými flagy M a O pro zajištění stavové konfigurace.

```
DEVICE=eth0.114 # označení rozhraní
VLAN=yes # jedná se o VLAN
NM_CONTROLLED=no # rozhraní nebude spravováno pomocí Network Managera
ONBOOT=yes # rozhraní bude aktivováno při zapnutí

USERCTL=no  # pouze root může spravovat toto rozhraní
BOOTPROTO=none # nebude použit protokol bootp ani dhcp
IPADDR=10.10.14.1 # ipv4 adresa
NETMASK=255.255.254.0 # maska sítě

IPV6INIT=yes # povoluje ipv6 inicializaci na tomto rozhraní
IPV6ADDR=2001:718:803:e114::1/64 # ipv6 adresa
IPV6_AUTOCONF=no # na tomto rozhraní nejsou přijímány ani přesměrovávány RA zprávy
IPV6_ROUTER=no # RA z tohoto rohraní nebudou zasílána
IPV6TO4INIT=no # zakazuje inicializaci 6to4 na tomto rozhraní
```

Po nastavení rozhraní eth0.114 provedeme nastavení ohlášení směrovače v příslušném konfiguračním souboru /etc/radvd.conf.

```
interface eth0.114
{
       AdvSendAdvert on; # aktivace posílání RA
       AdvOtherConfigFlag off;  # flag O je nastaven na hodnotu 0
       AdvManagedFlag on; # flag M je nastaven na hodnotu 1
       MinRtrAdvInterval 198; # minimální interval pro posílání RA
       MaxRtrAdvInterval 600; # maximální interval pro posílání RA
       prefix 2001:718:803:e114::/64 {};  # prefix, který bude RA oznamovat
};
AdvSendAdvert on;  # aktivace posílání RA
       AdvManagedFlag off;  # flag M je nastaven na hodnotu 0
       AdvOtherConfigFlag on;  # flag O je nastaven na hodnotu 1
       MinRtrAdvInterval 198;  # minimální interval pro posílání RA
       MaxRtrAdvInterval 600;  # maximální interval pro posílání RA
       prefix 2001:718:803:e114::/64 {};  # prefix, který bude RA oznamovat
```

8.2.2 Konfigurace stavového ISC DHCPv6 serveru

Nejsnadnější variantou konfigurace stavového DHCPv6 je dynamické přidělování adres z určitého rozsahu pomocí příkazu range6. Tento rozsah definujeme zadáním první a poslední přidělitelné adresy. Jeden z požadavků na fázi dva však vyžaduje, aby klientovi byla adresa přidělena na základě jeho DUID. To je docíleno příkazem fixed-address6. Toto přidělení má vyšší váhu než definování daného rozsa-

hu. Manuální vypisování je však opravdu zdlouhavé a vytvořit rezervaci pro každého klienta v síti je téměř nerealizovatelné. Z toho důvodu je do budoucna plánováno využití již zmíněné webové aplikace a plnícího skriptu autorů Bc. Olivera Horečného a Bc. Daniela Smolinského.

DNS

```
option dhcp6.name-servers 2001:718:803:f21::2;
option dhcp6.domain-search "mendelu.cz";
```

VLAN obsahující DHCPv6 server

```
subnet6 2001:718:803:f21::/64 {} #nebudou ignorovány požadavky v VLAN, ve které
                                    je DHCPv6 server umístěn
```

End-to-End VLAN114

```
subnet6 2001:718:803:e114::/64 {}
```

Lokalita Q

```
subnet6 2001:718:803:125::/64 {
        range6 2001:718:803:125::11 2001:718:803:125::ffff;
}
subnet6 2001:718:803:126::/64 {
        range6 2001:718:803:126::11 2001:718:803:126::ffff;
}
```

Lokalita A

```
subnet6 2001:718:803:2a0::/64 {
        range6 2001:718:803:2a0::11 2001:718:803:2a0::ffff;
}
subnet6 2001:718:803:2a1::/64 {
        range6 2001:718:803:2a1::11 2001:718:803:2a1::ffff;
}
```

Lokalita C

```
subnet6 2001:718:803:384::/64 {
        range6 2001:718:803:384::11 2001:718:803:384::ffff;
}
```

Lokalita X

```
subnet6 2001:718:803:486::/64 {
        range6 2001:718:803:486::11 2001:718:803:486::ffff;
}
```

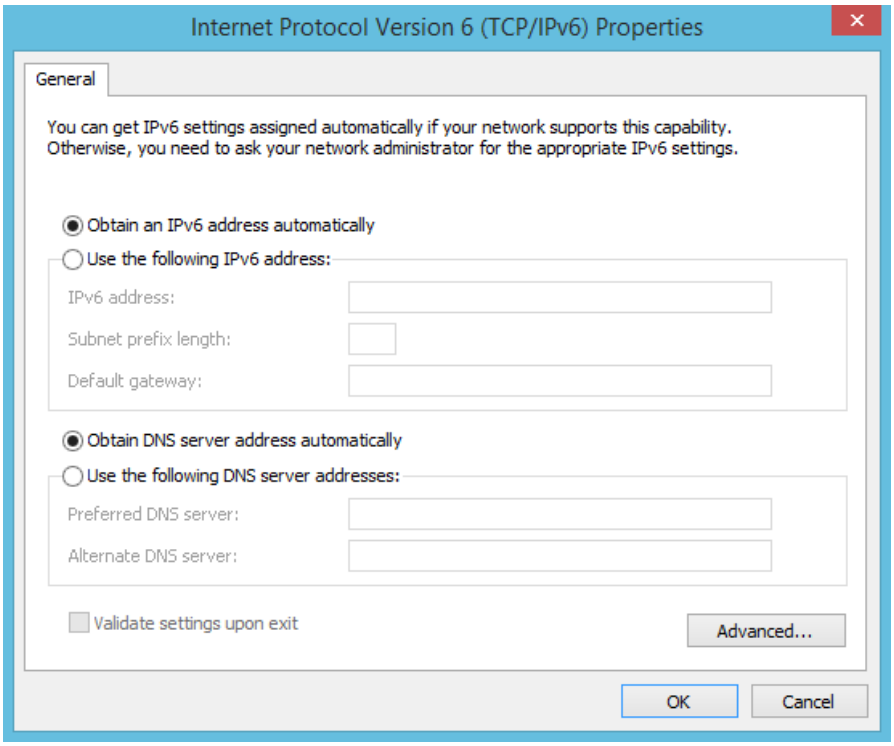
Klienti s pevně danou rezervací adresy

```
host NBVirtBoxWin80 {
  host-identifier option dhcp6.client-id
00:01:00:01:1a:14:14:a0:00:15:5d:e6:c5:fa;
  fixed-address6 2001:718:803:126::10;
}
```

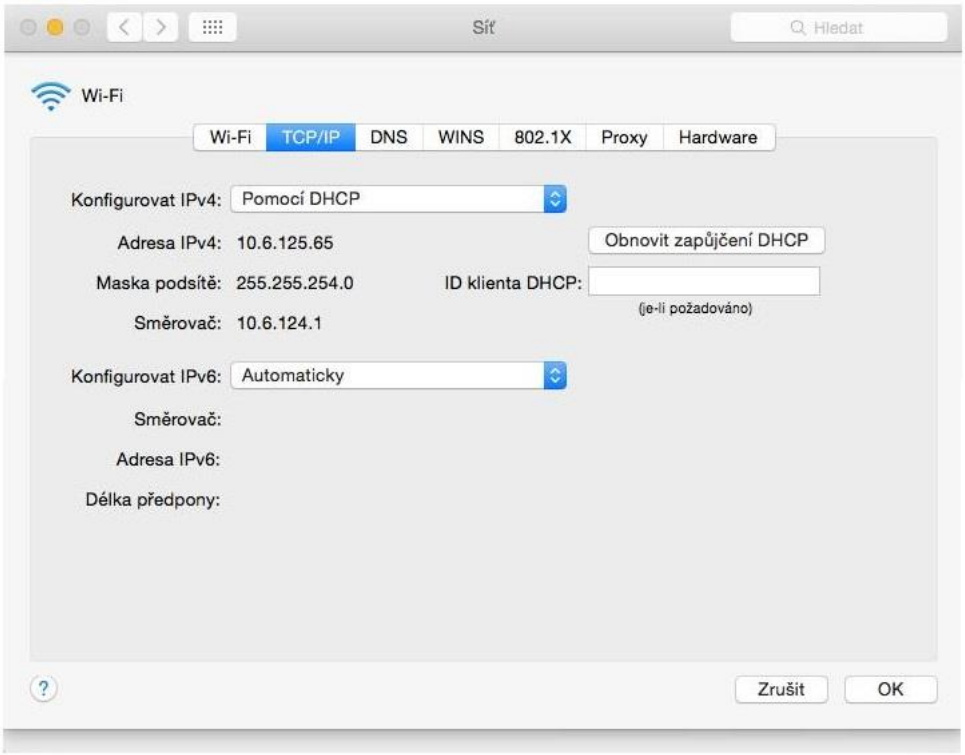
```
host NBVirtBoxWin81 {
  host-identifier option dhcp6.client-id
00:01:00:01:19:f2:0b:06:00:15:5d:e6:c5:dc;
  fixed-address6 2001:718:803:126::20;
}
host NBVirtBoxFedora21 {
  host-identifier option dhcp6.client-id
00:04:49:dd:7a:68:c5:9b:8d:08:b4:e5:af:88:e6:9a:83:8f;
  fixed-address6 2001:718:803:126::30;
}
host Pokuston2Win7 {
  host-identifier option dhcp6.client-id
00:01:00:01:18:36:b3:c4:08:00:27:79:ef:9b;
  fixed-address6 2001:718:803:2a1::10;
}
host AppleMacOSX {
  host-identifier option dhcp6.client-id
00:01:00:01:1c:a5:a6:f2:58:b0:35:fb:f6:a7;
  fixed-address6 2001:718:803:2a1::20;
}
```

8.2.3 Konfigurace koncových klientů

Posledním krokem této fáze je konfigurace koncových klientů. Jediné, co je nutno v této části zajistit, je nastavit dynamické získávání IPv6 adresy. Pro změnu je zde uvedeno nastavení na klientovi s operačním systémem Windows 8.1 a na klientovi s operačním systémem Mac OS X.



Obr. 19 Nastavení dynamického získávání IPv6 adresy na Windows 8.1



Obr. 20 Nastavení dynamického přidělení IPv6 adresy na Mac OS X

8.3 Testování

Po implementaci každé fáze bylo potřeba ověřit, zda dynamické přidělení, ať už s použitím mechanismu SLAAC a bezstavového DHCPv6 serveru nebo za pomoci stavového DHCPv6 serveru, proběhlo úspěšně. K tomu jsem využila následujících příkazů.

Windows 7, 8/8.1:

- `ipconfig all/renew/release`,
- `route PRINT`,
- `netsh int ipv6 show addr`,
- `netsh int ipv6 show route`,
- `netsh int ipv6 show dns`,
- `netsh int ipv6 show joins`,
- `netsh int ipv6 show privacy`,
- `netsh int ipv6 show global`,
- `netsh int ipv6 show neighbors`,
- `arp -n`.

Fedora 21:

- `ip link`,
- `ip addr show, ip -6 addr show`,
- `ip route show, ip -6 route show`,

- cat /etc/resolv.conf,
- ip neighbor show, ip -6 neighbor show,
- iptables -L -vn, ip6tables -L -vn.

Mac OS X:

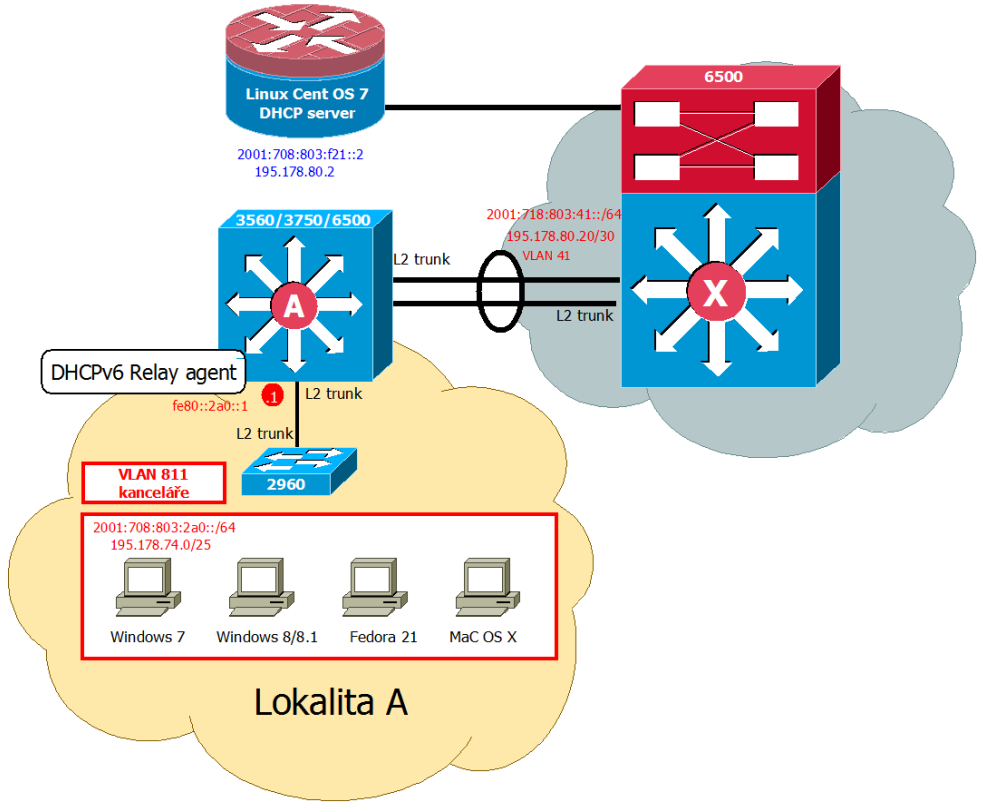
- ifconfig,
- arp -an,
- ndp -an,
- netstat -f inet –rn, netstat -f inet6 -rn.

Na všech těchto klientech byly provedeny testy konektivity prostřednictvím příkazu ping, popřípadě ping6. Byla ověřena konektivita s výchozí bránou, klientem ze stejné VLAN, klientem z jiné VLAN, dále pak dostupnost na firewall inside a outside a VRF inside, server v DMZ a nakonec i konektivita na CESNET. Detailní přehled všech těchto výpisů, screenshotů a záznamů komunikace programem Wireshark je součástí příloh nacházejících se na CD.

Testování pro každou fázi bude rozděleno do tří částí. Nejprve bude ověřeno nastavení výchozí brány a správné zasílání RA. Dále bude prověřena funkčnost DHCPv6 serveru a komunikace s DHCPv6 Relay agentem. Nakonec je nutno ověřit správné nastavení koncového klienta a zjistit, zda získal požadované síťové parametry. Ověření bude podloženo jednotlivými záznamy komunikace z Wiresharku a výpisy zvolených příkazů.

8.3.1 Testování fáze 1

Jak bylo řečeno, nejdříve ověříme nastavení výchozí brány, tedy nastavení rozhraní pro VLAN 811. Dále je nutno zkontrolovat, zda je tato VLAN přímo připojená k distribučnímu prvku. K tomuto účelu slouží výpis příkazu show ipv6 interface brief a příkazu show ipv6 route. Pro testování fáze jedna byl vybrán klient s OS Windows 7, jakožto pravděpodobně nejpočetnější zástupce klientů v univerzitní síti.



Obr. 21 Výřez infrastrukturního modelu s VLAN 811

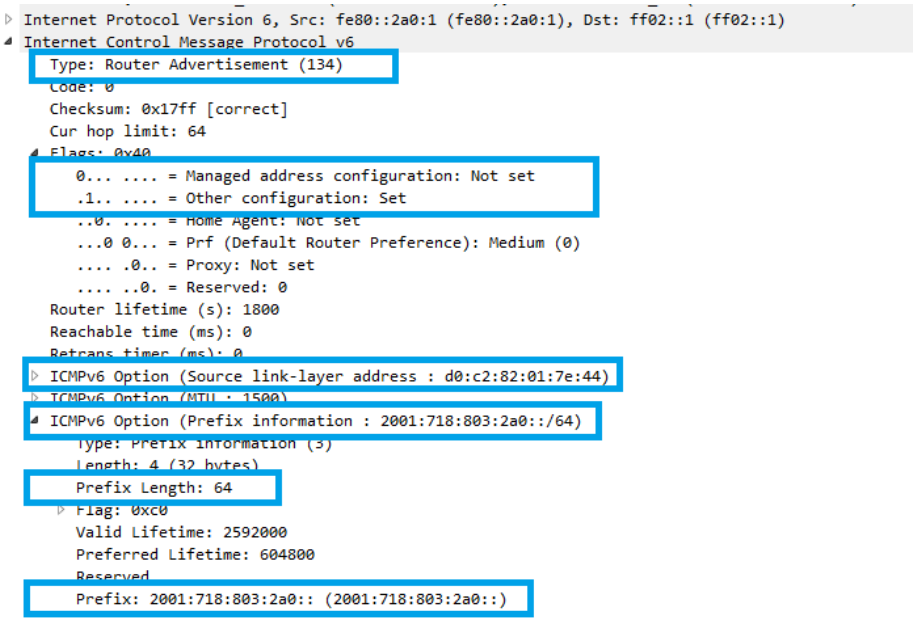
```
3560-core-A#show ipv6 interface brief
Vlan1                      [up/up]
    unassigned
Vlan41                     [up/up]
    FE80::41:2
    2001:718:803:41::2
Vlan43                     [up/up]
    FE80::43:1
    2001:718:803:43::1
Vlan171                    [up/up]
    FE80::E171:4
Vlan811                    [up/up]
    FE80::2A0:1
    2001:718:803:2A0::1
Vlan819                    [up/up]
    FE80::2A1:1
    2001:718:803:2A1::1
```

Obr. 22 Nastavení SVI VLAN 811

```
3560-core-A#show ipv6 route
IPv6 Routing Table - default - 16 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       R - RIP, ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OE2 ::/0 [110/1], tag 1
     via FE80::41:1, Vlan41
O    2001:718:803:40::/64 [110/2]
     via FE80::41:1, Vlan41
C    2001:718:803:41::/64 [0/0]
     via Vlan41, directly connected
L    2001:718:803:41::2/128 [0/0]
     via Vlan41, receive
O    2001:718:803:42::/64 [110/2]
     via FE80::41:1, Vlan41
C    2001:718:803:43::/64 [0/0]
     via Vlan43, directly connected
L    2001:718:803:43::1/128 [0/0]
     via Vlan43, receive
OI   2001:718:803:100::/56 [110/3]
     via FE80::41:1, Vlan41
O    2001:718:803:200::/56 [110/0]
     via Null0, directly connected
C    2001:718:803:2A0::/64 [0/0]
     via Vlan811, directly connected
L    2001:718:803:2A0::1/128 [0/0]
     via Vlan811, receive
C    2001:718:803:2A1::/64 [0/0]
```

Obr. 23 Směrovací tabulka distribučního prvku

Dále zkontrolujeme záznam komunikace zprávy Router Advertisment.



Obr. 24 Záznam komunikace zprávy Router Advertisement při bezstavové konfiguraci

Na obrázku 24 vidíme obsah zprávy Router Advertisement odchycené na koncové stanici s operačním systémem Windows 7. Jak vidíme podle natavení flagů, jedná se skutečně o bezstavovou konfiguraci.

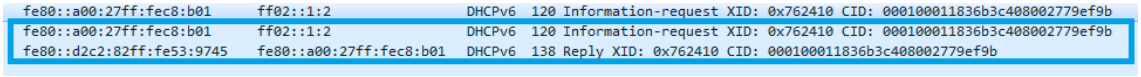
Dále z obrázku vyčteme informace o MAC adrese výchozí brány, prefixu a délce prefixu. Klientovi v tomto okamžiku chybí záznamy o DNS, pro které se obrací na bezstavový DHCPv6 server.

Nejprve tedy ověříme, zda je DHCPv6 spuštěný a na jakém portu poslouchá. K tomuto účelu poslouží výpis příkazu netstat --inet6 -anp.

```
[root@firewall _Lab]# netstat --inet6 -anp
Aktivní Internetová spojení (servery a navázaná spojení)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 :::37704                    :::*                        LISTEN      2284/rpc.statd
tcp        0      0 :::111                      :::*                        LISTEN      2161/rpcbind
tcp        0      0 :::53                       :::*                        LISTEN      5946/named
tcp        0      0 :::22                       :::*                        LISTEN      2473/sshd
tcp        0      0 ::1:631                     :::*                        LISTEN      2336/cupsd
tcp        0      0 ::1:953                     :::*                        LISTEN      5946/named
tcp        0      0 ::1:25                      :::*                        LISTEN      2553/master
udp        0      0 :::111                      :::*                                    2161/rpcbind
udp        0      0 2001:718:803:f22::2:123     :::*                                    5909/ntpd
udp        0      0 fe80::21b:21ff:fec8:40c2:123 :::*                                   5909/ntpd
udp        0      0 2001:718:803:f21::2:123     :::*                                    5909/ntpd
udp        0      0 ::1:123                     :::*                                    5909/ntpd
udp        0      0 2001:718:803:e114::1:123    :::*                                    5909/ntpd
udp        0      0 2001:718:803:e171::1:123    :::*                                    5909/ntpd
udp        0      0 :::123                      :::*                                    5909/ntpd
udp        0      0 :::640                      :::*                                    2161/rpcbind
udp        0      0 :::547                      :::*                                    5884/dhcpd
udp        0      0 :::54699                    :::*                                    2284/rpc.statd
udp        0      0 :::53                       :::*                                    5946/named
raw        0      0 :::58                       :::*                        7           4613/radvd
```

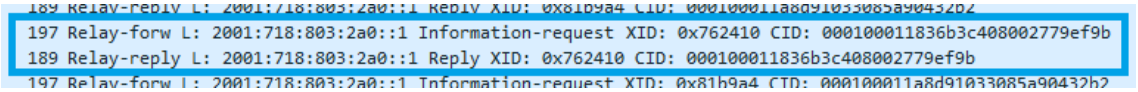
Obr. 25 Výpis služeb běžících na firewallu

Z obrázku 25 vidíme, že DHCPv6 server poslouchá na portu 547. Nyní ověříme, zda probíhá komunikace mezi DHCPv6 klientem a DHCPv6 Relay agentem.



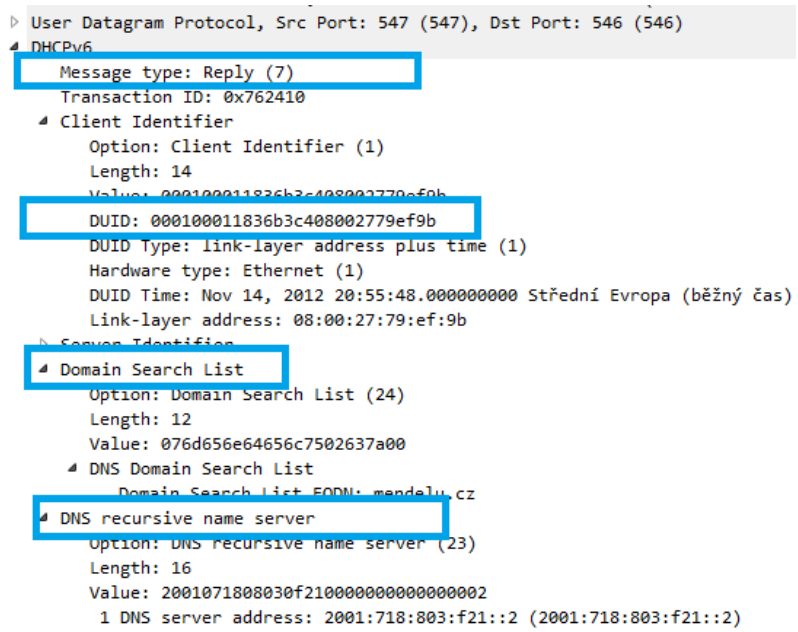
Obr. 26 Komunikace mezi bezstavovým DHCPv6 serverem a DHCPv6 Relay agentem

Následně ověříme, zda klientův požadavek přišel na server. U bezstavové komunikace očekáváme zprávy Relay Forward a Relay Reply, které zprostředkovávají přenos požadavku klienta a odpovědi serveru pomocí Relay agenta.



Obr. 27 Komunikace mezi DHCPv6 Relay agentem a DHCPv6 klientem

Z obrázků 26 a 27 je patrné, že komunikace mezi klientem a serverem prostřednictvím DHCPv6 Relay agenta probíhá úspěšně. Následně tedy zkontrolujeme záznam komunikace zprávy DHCPv6 Reply na koncové stanici. Ověříme, zda obsahuje všechny potřebné informace.



Obr. 28 Záznam komunikace zprávy DHPCv6 Reply při bezstavové konfiguraci

Jak lze ze zprávy vidět, bezstavový DHCPv6 server doplnil klientovi informace jak o rekurzivním DNS serveru, tak seznamu doménových jmen. Klient v tuto chvíli zná všechny síťové parametry pro plnohodnotnou síťovou komunikaci.

Pro ověření, zda si klient nakonfigurovat IPv6 adresu a získal informace o DNS z bezstavového DHCPv6 serveru, poslouží výpis klientova síťového nastavení.

```
C:\Users\root>ipconfig /all

Konfigurace protokolu IP systému Windows

   Název hostitele . . . . . : p01-site
   Primární přípona DNS. . . . . :
   Typ uzlu  . . . . . : hybridní
   Povoleno směrování IP . . . . . : Ne
   WINS Proxy povoleno . . . . . : Ne
   Prohledávací seznam přípon DNS. . : mendelu.cz

Adaptér sítě Ethernet Připojení k místní síti:

   Přípona DNS podle připojení . . . : mendelu.cz
   Popis . . . . . : Intel(R) PRO/1000 MT - adaptér pro stolní
počítač
   Fyzická Adresa. . . . . : 08-00-27-C8-0B-02
   Protokol DHCP povolen . . . . . : Ano
   Automatická konfigurace povolena  : Ano
   IPv6 adresa. . . . . : 2001:718:803:2a0:a00:27ff:fec8:b02(Prefero
vané)
   Místní IPv6 adresa v rámci propojení . . . : fe80::a00:27ff:fec8:b02%11(Prefe
rované)
   Adresa IPv4 . . . . . : 195.178.74.11(Preferované)
   Maska podsítě . . . . . : 255.255.255.128
   Zapůjčeno . . . . . : 18. března 2015 18:28:20
   Zápůjčka vyprší . . . . . : 19. března 2015 6:28:16
   Výchozí brána . . . . . : fe80::2a0:1%11
                                 195.178.74.1
   Server DHCP . . . . . : 195.178.80.2
   IAID DHCPv6 . . . . . : 235405351
   DUID klienta DHCPv6. . . . . : 00-01-00-01-18-36-B3-C4-08-00-27-79-EF-9B

   Servery DNS . . . . . : 2001:718:803:f21::2
                                 195.178.80.2
   Rozhraní NetBios nad protokolem TCP/IP . . . . . : Povoleno
   Seznam hledání přípon DNS specifických pro připojení:
                                 mendelu.cz
```

Obr. 29 Výpis příkazu ipconfig /all

Můžeme si povšimnout, že klientova adresa je nakonfigurována skutečně bezstavově a podle FFFE poznáme, že se jedná o identifikátor EUI-64 vytvořený na základě klientovy MAC adresy. Je to současně jediná adresa, kterou si klient vygeneroval, a to díky dříve zmíněným příkazům pro vynucení identifikátoru EUI-64 a zakázání vytváření dočasných adres. Že se dočasné a náhodné adresy těmito příkazy skutečně netvoří, můžeme ověřit následujícími dvěma výpisy.

```
C:\Users\root>netsh int ipv6 show global
Dotaz na aktivní stav...

Obecné globální parametry
----------------------------------------------
Výchozí limit počtu směrování: 128 směrování
Limit mezipaměti sousedních uzlů: 256 položek na rozhraní
Limit mezipaměti směrování: 128 položek na oddíl
Limit nového sestavení: 33550784 bajtů
Přesměrování ICMP: enabled
Chování směrování zdroje: dontforward
Převedení úlohy: enabled
Rozpoznávání médií DHCP: enabled
Protokolování rozpoznávání médií: disabled
Úroveň protokolu MLD: all
Verze protokolu MLD: version3
Předávání vícesměrového vysílání: disabled
Fragmenty předané skupinou: disabled
Náhodné identifikátory: disabled
Odpověď masky adresy: disabled

Aktuální globální statistika
----------------------------------------------
Počet oddílů                  : 1
Počet klientů NL              : 7
Počet zprostředkovatelů FL    : 4
```

Obr. 30 Vypnutí náhodných adres ve výpisu netsh int ipv6 show global

```
C:\Users\root>netsh int ipv6 show privacy
Dotaz na aktivní stav...

Parametry dočasných adres

Použít dočasné adresy                  : disabled
Pokusy o zjištění duplicitních adres   : 5
Maximální doba platnosti               : 7d
Maximální doba preferování             : 1d
Doba opětovného vytvoření              : 5s
Maximální náhodná doba                 : 10m
Náhodná doba                           : 0s
```

Obr. 31 Vypnutí dočasných adres ve výpisu netsh int ipv6 show privacy

Na závěr přikládám výpis z příkazu netsh int ipv6 show route, pomocí něhož vidíme klientovu směrovací tabulku.

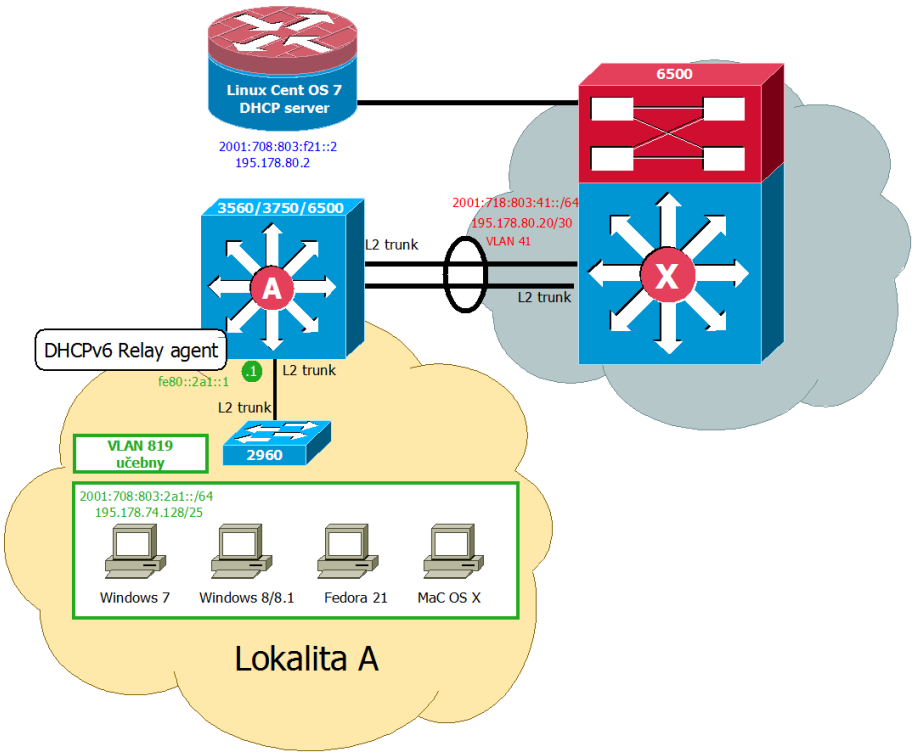
```
C:\Users\root>netsh int ipv6 show route

Publik.  Typ      Metr.  Předpona                    Idx  Název brány/rozhraní
-------  -------  -----  --------------------------  ---  --------------------
Ne       Ručně      256  ::/0                         11  fe80::2a0:1
Ne       Ručně      256  ::1/128                       1  Loopback Pseudo-Interface
 1
Ne       Ručně        8  2001:718:803:2a0::/64        11  Připojení k místní síti
Ne       Ručně      256  2001:718:803:2a0:a00:27ff:fec8:b02/128   11  Připojení k
 místní síti
Ne       Ručně      256  fe80::/64                    11  Připojení k místní síti
Ne       Ručně      256  fe80::a00:27ff:fec8:b02/128   11  Připojení k místní sít
i
Ne       Ručně      256  ff00::/8                      1  Loopback Pseudo-Interface
 1
Ne       Ručně      256  ff00::/8                     11  Připojení k místní síti
```

Obr. 32 Směrovací tabulka klienta

8.3.2 Testování fáze 2

Pro znázornění testování druhé fáze, která byla zaměřena na využití stavového DHCPv6 serveru, byl tentokrát vybrán klient s Mac OS X. Stejně jako v testování přechozí fáze ověříme nejprve rozhraní na distribučním prvku. Zajímá nás především rozhraní VLAN 819, ve které se zvolený klient nachází. Dále ověříme přímé připojení VLAN 819. Opět využiji příkazů show ipv6 interface brief a show ipv6 route.



Obr. 33 Výřez infrastrukturního modelu s VLAN 819

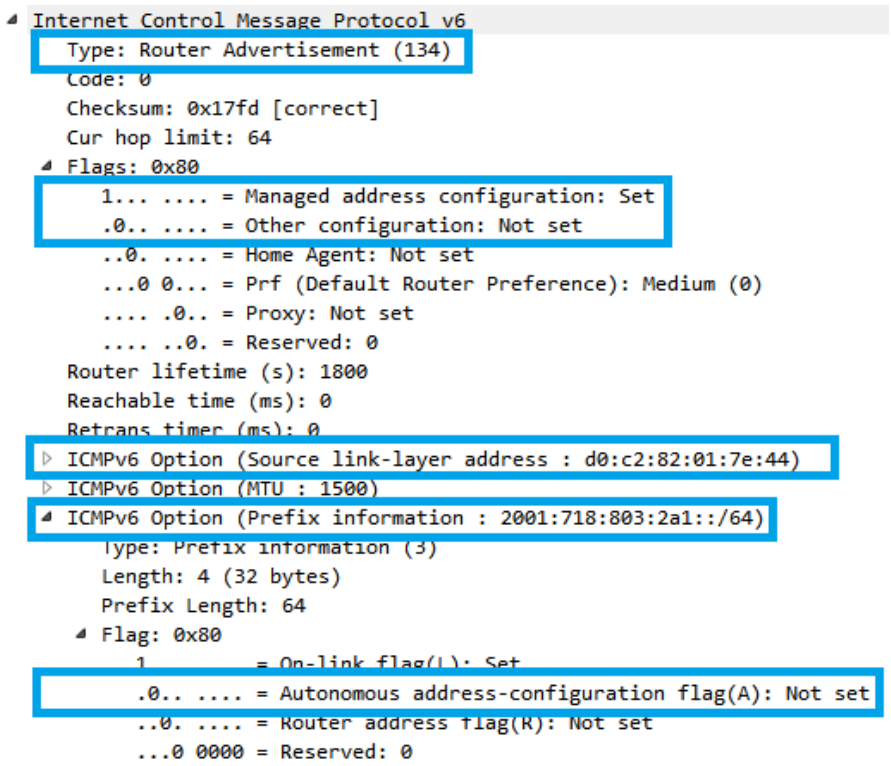
```
3560-core-A#show ipv6 interface brief
Vlan1                  [up/up]
    unassigned
Vlan41                 [up/up]
    FE80::41:2
    2001:718:803:41::2
Vlan43                 [up/up]
    FE80::43:1
    2001:718:803:43::1
Vlan171                [up/up]
    FE80::E171:4
Vlan811                [up/up]
    FE80::2A0:1
    2001:718:803:2A0::1
Vlan819                [up/up]
    FE80::2A1:1
    2001:718:803:2A1::1
FastEthernet0/1        [up/up]
```

Obr. 34 Nastavení SVI VLAN 819

```
3560-core-A#show ipv6 route
IPv6 Routing Table - default - 16 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       R - RIP, ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OE2 ::/0 [110/1], tag 1
     via FE80::41:1, Vlan41
O   2001:718:803:40::/64 [110/2]
     via FE80::41:1, Vlan41
C   2001:718:803:41::/64 [0/0]
     via Vlan41, directly connected
L   2001:718:803:41::2/128 [0/0]
     via Vlan41, receive
O   2001:718:803:42::/64 [110/2]
     via FE80::41:1, Vlan41
C   2001:718:803:43::/64 [0/0]
     via Vlan43, directly connected
L   2001:718:803:43::1/128 [0/0]
     via Vlan43, receive
OI  2001:718:803:100::/56 [110/3]
     via FE80::41:1, Vlan41
O   2001:718:803:200::/56 [110/0]
     via Null0, directly connected
C   2001:718:803:2A0::/64 [0/0]
     via Vlan811, directly connected
L   2001:718:803:2A0::1/128 [0/0]
     via Vlan811, receive
C   2001:718:803:2A1::/64 [0/0]
     via Vlan819, directly connected
L   2001:718:803:2A1::1/128 [0/0]
     via Vlan819, receive
OI  2001:718:803:300::/56 [110/3]
     via FE80::41:1, Vlan41
```

Obr. 35 Směrovací tabulka distribučního prvku

Nyní je na řadě kontrola zasílání ohlášení směrovače, a tedy prozkoumání zprávy Router Advertisement.



Obr. 36 Záznam komunikace zprávy Router Advertisement při stavové konfiguraci klientů

Na obrázku 36 vidíme všechny sítové parametry poskytnuté směrovačem. Je zde také názorně vidět nastavení flagů M a O při stavové konfiguraci. Dále si můžeme povšimnout vynulování flagu A. To by mělo zajistit, že adresa přidělená DHPCv6 serverem bude jediná, kterou následně uvidíme ve výpisu klientova ifconfigu.

Pro získání chybějících DNS záznamů, a především přidělení IPv6 adresy, se klient obrací na stavový DHCPv6 server. Je tedy opět potřeba ověřit, zda tento server poslouchá pomocí příkazu netstat --inet -anp.

Pro stavovou konfiguraci jsou obvykle velmi důležité i dhcpd6.leases, ve kterých obvykle uvidíme informace o jednotlivých zápůjčkách. Je zde identifikátor klienta, přidělená adresa a také životnost zápůjčky a datum, kdy vyprší. Vzhledem k tomu, že při implementaci druhé fáze jsme klientům rezervovali adresy na základě jejich DUID, a to pomocí příkazu fixed-addresss6, nenachází se v souboru se zápůjčkami žádné položky, tento soubor obsahuje pouze záznamy adres přidělené z určitého rozsahu, tedy poolu. (Isc.org, 2012)

```
[root@firewall _Lab]# netstat --inet6 -anp
Aktivní Internetová spojení (servery a navázaná spojení)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 :::53                       :::*                        LISTEN      18282/named
tcp        0      0 :::22                       :::*                        LISTEN      2457/sshd
tcp        0      0 ::1:631                     :::*                        LISTEN      2318/cupsd
tcp        0      0 :::36279                    :::*                        LISTEN      2119/rpc.statd
tcp        0      0 ::1:953                     :::*                        LISTEN      18282/named
tcp        0      0 ::1:25                      :::*                        LISTEN      2539/master
tcp        0      0 :::111                      :::*                        LISTEN      2099/rpcbind
udp        0      0 :::547                      :::*                                    18209/dhcpd
udp        0      0 :::53                       :::*                                    18282/named
udp        0      0 :::38109                    :::*                                    2119/rpc.statd
udp        0      0 :::1002                     :::*                                    2099/rpcbind
udp        0      0 :::111                      :::*                                    2099/rpcbind
udp        0      0 fe80::f21:2:123             :::*                                    18237/ntpd
udp        0      0 fe80::f22:2:123             :::*                                    18237/ntpd
udp        0      0 fe80::e114:1:123            :::*                                    18237/ntpd
udp        0      0 fe80::e171:1:123            :::*                                    18237/ntpd
udp        0      0 fe80::21b:21ff:fec8:40c2:123 :::*                                   18237/ntpd
udp        0      0 fe80::21b:21ff:fec8:40c2:123 :::*                                   18237/ntpd
udp        0      0 fe80::21b:21ff:fec8:40c2:123 :::*                                   18237/ntpd
udp        0      0 fe80::21b:21ff:fec8:40c2:123 :::*                                   18237/ntpd
udp        0      0 fe80::21b:21ff:fec8:40c2:123 :::*                                   18237/ntpd
udp        0      0 2001:718:803:f21::2:123     :::*                                    18237/ntpd
udp        0      0 2001:718:803:f22::2:123     :::*                                    18237/ntpd
udp        0      0 ::1:123                     :::*                                    18237/ntpd
udp        0      0 2001:718:803:e114::1:123    :::*                                    18237/ntpd
udp        0      0 :::123                      :::*                                    18237/ntpd
raw        0      0 :::58                       :::*                        7           6823/radvd
```

Obr. 37 Výpis běžících služeb na firewallu

Je nutno ověřit, zda probíhá komunikace mezi klientem a Relay agentem. Tedy, jestli jsou všechny čtyři zprávy přeneseny od klienta k serveru.

```
fe80::5ab0:35ff:fefb:f6a7 ff02::1:2               DHCPv6 114 Solicit XID: 0x96c29a CID: 000100011ca5a6f258b035fbf6a7
fe80::2a1:1               fe80::5ab0:35ff:fefb:f6a7 DHCPv6 182 Advertise XID: 0x96c29a IAA: 2001:718:803:2a1::20 CID: 000100011ca5a6f258b035fbf6a7
fe80::5ab0:35ff:fefb:f6a7 ff02::1:2               DHCPv6 160 Request XID: 0xd05d8 CID: 000100011ca5a6f258b035fbf6a7 IAA: 2001:718:803:2a1::20
fe80::2a1:1               fe80::5ab0:35ff:fefb:f6a7 DHCPv6 182 Reply XID: 0xd05d8 IAA: 2001:718:803:2a1::20 CID: 000100011ca5a6f258b035fbf6a7
```

Obr. 38 Komunikace mezi DHCPv6 klientem DHCPv6 Relay agentem při stavové konfiguraci

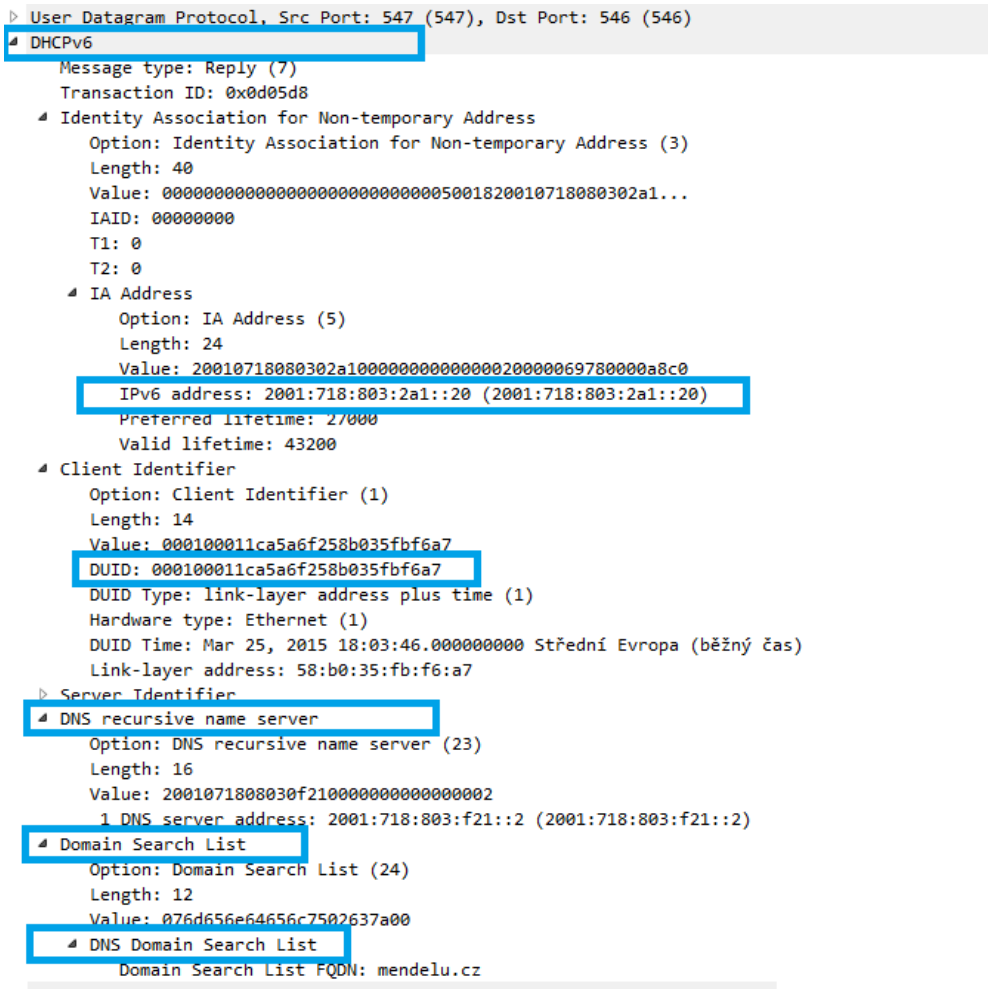
Dalším krokem je ověření komunikace také mezi DHCPv6 serverem a DHCPv6 Relay agentem. U stavové konfigurace zde očekáváme celkem čtyři zprávy – Solicit, Advertise, Request a Reply.

```
191 Relay-forw L: 2001:718:803:2a1::1 Solicit XID: 0x96c29a CID: 000100011ca5a6f258b035fbf6a7
233 Relay-reply L: 2001:718:803:2a1::1 Advertise XID: 0x96c29a IAA: 2001:718:803:2a1::20 CID: 000100011ca5a6f258b035fbf6a7
237 Relay-forw L: 2001:718:803:2a1::1 Request XID: 0xd05d8 CID: 000100011ca5a6f258b035fbf6a7 IAA: 2001:718:803:2a1::20
233 Relay-reply L: 2001:718:803:2a1::1 Reply XID: 0xd05d8 IAA: 2001:718:803:2a1::20 CID: 000100011ca5a6f258b035fbf6a7
```

Obr. 39 Komunikace mezi DHCPv6 Relay agentem a DHCPv6 serverem při stavové konfiguraci

Bylo ověřeno, že komunikace mezi DHCPv6 klientem a DHCPv6 serverem probíhá úspěšně prostřednictvím DHCPv6 Relay agenta, jak je vidět na obrázcích 38 a 39 výše.

Zbývá tedy ověřit, zda klientovi přišly všechny potřebné síťové parametry. K tomu využijeme opět zprávu DHCPv6 Reply odchycenou přímo na klientské stanici.



Obr. 40 Záznam komunikace zprávy DHCPv6 Reply při stavové konfiguraci klientů

Na obrázku 40 vidíme odpověď DHCPv6 serveru, která obsahuje všechny parametry, které server klientovi přidělil. Opět se zde objevuje informace o rekurzivním DNS serveru a také o seznamu doménových jmen. Co je oproti přechozí fázi odlišné, je poskytnutá IPv6 adresa. Z obrázku poznáme, že IPv6 adresa nebyla přidělena z definovaného rozsahu, ale na základě příkazu fixed-address6 v konfiguračním souboru. Kontrolou je samozřejmě výpis síťového natavení přímo na klientovi pomocí příkazu ifconfig.

Jak lze vidět na obrázku 41 klient má skutečně přidělenou adresu na základě svého identifikátoru DUID a tato adresa je současně jediná globální adresa, kterou ve výpisu vidíme. Na závěr je připojen také výpis z příkazu ndp -an.

```
Last login: Wed Apr  1 19:40:16 on ttys000
midget1:~ site$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet6 ::1 prefixlen 128
        inet 127.0.0.1 netmask 0xff000000
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=1<PERFORMNUD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=b<RXCSUM,TXCSUM,VLAN_HWTAGGING>
        ether 58:b0:35:fb:f6:a7
        inet6 fe80::5ab0:35ff:fefb:f6a7%en0 prefixlen 64 scopeid 0x4
        inet 195.178.74.139 netmask 0xffffff80 broadcast 195.178.74.255
        inet6 2001:718:803:2a1::20 prefixlen 64 dynamic
        nd6 options=1<PERFORMNUD>
        media: autoselect (100baseTX <full-duplex>)
        status: active
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether f8:1e:df:f2:8d:34
        inet6 fe80::fa1e:dfff:fef2:8d34%en1 prefixlen 64 scopeid 0x5
        inet 10.10.4.109 netmask 0xfffffe00 broadcast 10.10.5.255
        nd6 options=1<PERFORMNUD>
        media: autoselect
        status: active
fw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 4078
        lladdr d8:30:62:ff:fe:fe:14:2a
        nd6 options=1<PERFORMNUD>
        media: autoselect <full-duplex>
        status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
        ether 0a:1e:df:f2:8d:34
        media: autoselect
        status: inactive
```

Obr. 41 Výpis příkazu ifconfig na klientovi Mac OS X při stavové konfiguraci

```
midget1:~ site$ ndp -an
Neighbor                        Linklayer Address  Netif Expire    St Flgs Prbs
2001:718:803:2a1::20            58:b0:35:fb:f6:a7    en0 permanent R
fe80::1%lo0                     (incomplete)         lo0 permanent R
fe80::2a1:1%en0                 d0:c2:82:1:7e:44     en0 23h57m42s S  R
fe80::5ab0:35ff:fefb:f6a7%en0   58:b0:35:fb:f6:a7    en0 permanent R
fe80::fa1e:dfff:fef2:8d34%en1   f8:1e:df:f2:8d:34    en1 permanent R
```

Obr. 42 Výpis příkazu ndp –an

9 Ekonomické zhodnocení

V této kapitole bude provedeno zhodnocení po finanční stránce. Z hlediska koncových klientů nebude přechod sítě MENDELU na nový protokol znamenat pro univerzitu velkou finanční přítěž.

Všechny typy testovaných koncových klientů, které odráží skutečné zastoupení klientů v univerzitní síti, plně podporují nový protokol. Při implementaci protokolu IPv6 nedojde ani ke změně současného logického rozložení jednotlivých segmentů sítě, a to včetně jednotlivých síťových prvků. Není tedy potřeba natahovat novou kabeláž, ani nakupovat nové aktivní prvky. Všechny stávající prvky podporují IPv6 a jsou připraveny na její zavedení.

Jsou zde však určité funkce IPv6, které stávající prvky nepodporují. Jedná se například o podporu IPv6 PACL nebo IPv6 Source Guard, které jsou podporovány až od verze IOS 15.0(2) a vyšší. Je zde mnoho aktivních prvků, které by potřebovaly aktualizovat na novější verzi IOS. Upgrade všech těchto zařízení je však velmi finančně náročný, a proto nebude započítán mezi nákladové položky stejně tak, jako řešení otázek zabezpečení.

Vyčíslitelnou položkou jsou náklady na konfiguraci jednotlivých klientských a serverových strojů. Konfigurace bude probíhat v plně funkční IPv4 síti. Z toho důvodu je průměrná doba konfigurace odhadnuta na 20 hodin. Podle ČSÚ se průměrný hrubý měsíční plat v oblasti informačních a komunikačních technologiích pohybuje okolo 48 000 Kč. (Czsu.cz, 2015) Vezmeme-li v úvahu 20 pracovních dní a 8 hodinovou pracovní směnu, dostáváme se k částce za hodinu. Získáváme tedy průměrný hodinový výdělek technika, který odpovídá výši cca 300 Kč/hod.

Popis	Počet hodin	Kč/hod	Kč
Konfigurace koncových klientů	15	300	4500
Instalace a konfigurace DHCPv6 serveru	5	350	1750
Konfigurace výchozí brány a Relay agantů	5	350	1750
Nákup licencí	0	0	0
CELKOVÉ NÁKLADY			**8000**

Tab. 5 Přehled nákladových položek

Velmi obtížné je však určení zisku, který Mendelově univerzitě v Brně přinese zavedení nového protokolu. Je zde možnost vyjádřit jej pouze v teoretické rovině v podobě oportunitních nákladů, tedy v takových nákladech, které se rovnají ušlému zisku v případě, že by škola nový protokol neimplementovala.

V tomto případě by se muselo najít jiné východisko pro řešení nedostatku veřejných adres. Například by bylo nutno rozdělit síť do více segmentů, které by navenek vystupovaly pod jednou veřejnou adresou, což by zabralo desítky hodin práce. Připojení Mendelovy univerzity v Brně k ostatním školám již implementujícím IPv6 bude mít vliv zejména na dobré jméno univerzity.

Zavedení nového protokolu IPv6 do současné produkční sítě MENDELU není, jak se zdá, z pohledu koncových klientů velmi finančně náročné. Dalo by se tvrdit, že finanční náročnost odpovídá tvorbě klasických IPv4 sítí.

10 Závěr

Cílem této práce bylo zanalyzovat současný stav počítačové sítě MENDELU a na základě těchto poznatků následně navrhnout různé způsoby dynamické konfigurace pro IPv6 klienty nacházející se v této počítačové síti. Tyto navržené způsoby bylo nutno otestovat v síťové laboratoři na klientech, kteří se v počítačové síti MENDELU vyskytují nejčastěji. Jednalo se o klienty s operačním systémem Windows 7, Windows 8/8.1, distribuce Linuxu - Fedora 21 a také Mac OS X.

V kapitole Publikační review byly nejprve rozebrány vysokoškolské práce zabývající se problematikou IPv6 a jejím nasazením jak ve firemním, tak vysokoškolském prostředí. Žádná z těchto prací se však nezaměřila na dynamickou konfiguraci koncových klientů, z toho důvodu mělo smysl vypracovat tuto bakalářskou práci zabývající se převážně danou tématikou dynamické konfigurace.

Kapitola Popis technologického aparátu následně seznámila čtenáře s problematikou IPv6 a také s novými vlastnostmi tohoto protokolu. Nachází se zde i struční popis problémů, které s sebou dynamická konfigurace přináší.

Další kapitoly práce jsou věnovány praktickému naplnění cílů. Je zde provedena požadovaná analýza stávajícího stavu sítě, jak z pohledu aktivních síťových prvků, tak i koncových zařízení. Zaměřuji se především na tato koncová zařízení a také na způsob, jakým jsou konfigurovány v současnosti.

Na základě vypracované analýzy byla navržena dvě možná řešení pro dynamické nakonfigurování klientů. Tato řešení jsem rozdělila do dvou samostatných fází, kdy každá varianta dynamické konfigurace byla rozebrána v samostatné podkapitole.

Každá fáze s sebou přinesla určitý problém. V případě první fáze byla řešena potřeba vynucení identifikátoru EUI-64 pro vytvoření klientova identifikátoru rozhraní. K dispozici se nabízelo několik řešení. Jednalo se o využití IPv6 PACL a IPv6 Source Guard. Tyto vlastnosti protokolu IPv6 jsou však podporovány od vyšší verze IOS, než jsou dostupné na stávajících aktivních prvcích. Z tohoto důvodu se nepodařilo vyzkoušet vynucení identifikátoru EUI-64 jiným způsobem, než pomocí ručního zadání příkazů k tomu určených.

Ve druhé fázi jsem se setkala s problémem identifikace koncových klientů v DHCPv6 komunikaci pomocí jejich identifikátoru DUID. Ukázalo se, že tento identifikátor je velmi nestálý a není tedy příliš vhodný pro jednoznačnou identifikaci klientů. Na rozdíl od MAC adresy se DUID po reinstalaci změní. Máme-li v konfiguračním souboru napevno rezervované adresy pro klienty na základě jejich DUID, po reinstalaci operačního systému změna DUID zapříčiní, že klient nezíská rezervovanou adresu. Řešení možná přinesou již zmiňované diplomové práce zabývající se tvorbou webového rozhraní a skriptu umožňujícího automatické plnění konfiguračního souboru DHCPv6 serveru. Dále se nabízí jít cestou ČVUT a využít Dibbler server.

Po návrhu následovala implementace obou fází v síťové laboratoři. Pro každou fázi bylo nutno ověřit, zda funguje podle očekávání. Pro účely testování jsem na každém klientovi sesbírala relevantní výpisy, pořídila screenshoty a také zá-

znamy komunikace. Na základě těchto výsledků je možno tvrdit, že obě fáze proběhly úspěšně. V první fázi si klienti na základě ohlášení směrovače nakonfigurovali svou IPv6 adresu a z bezstavového DHPCv6 serveru získali informace o DNS. Ve druhé fázi klient úspěšně získal adresu, která mu byla rezervována v konfiguračním souboru.

Na základě ekonomického zhodnocení, které bylo na závěr provedeno, můžeme říct, že z hlediska koncových klientů zavedení nového protokolu IPv6 v produkční síti MENDELU nepředstavuje finančně náročnou investici. Je to především z toho důvodu, že není potřeba nakupovat nový hardware a jediné náklady jsou tedy na konfiguraci jednotlivých zařízení.

Na závěr lze tedy říct, že zavedení nového protokolu do stávající počítačové sítě je realizovatelná záležitost. IPv6 s sebou sice přináší určité problémy a bezpečnostní rizika, přechod je však nevyhnutelný.

11 Literatura

BLANCHET, M. *Migrating to IPv6: a practical guide to implementing IPv6 in mobile and fixed networks*. Chichester: Wiley, c2006, xxxii, 418 s. ISBN 04-714-9892-0.

BLOG.NIC.CZ. *Pomůže usnesení vlády k většímu rozšíření IPv6 a DNSSEC?* [online]. 2014 [cit 2015-04-06]. Dostupné z: <http://blog.nic.cz/2014/01/13/pomuze-usneseni-vlady-k-vetsimu-rozsireni-ipv6-a-dnssec/>

BUČEK, O. *Komplexní návrh počítačové sítě pro firmu střední velikosti* [online]. 2012 [cit. 2015-04-13]. Bakalářská práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Eva Hladká. Dostupné z: <http://is.muni.cz/th/359390/fi_b/>

CISCO.COM. *Configuring IPv6 routing* [online]. 2015 [cit. 2015-04-14]. Dostupné z: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/15-0_2_se/configuration/guide/scg2960/swipv6.html#52487>

CZSU.CZ. *Průměrné mzdy – 4. čtvrtletí 2014* [online]. 2015 [cit. 2015-05-03]. Dostupné z: <https://www.czso.cz/documents/11350/20568277/pmz031115_1.xlsx/4f9539ed-34e0-4476-9856-c46d4b40d50f?version=1>

KLUB.COM.PL. *Dibbler – a portable DHCPv6 User's guider* [online]. 2015 [cit. 2015-05-07]. Dostupné z: <http://klub.com.pl/dhcpv6/doc/dibbler-user.pdf>

DVOŘÁK, P. *Návrh implementace IPv6 protokolu ve společnosti* [online]. 2014 [cit. 2015-03-20]. Diplomová. Vysoké učení technické v Brně. Vedoucí práce Viktor Ondrák. Dostupné z: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=72442>

GEYER, L. *Zabezpečení sítí s protokolem IPv6* [online]. 2011 [cit. 2014-04-15]. Diplomová práce. Vysoká učení technické v Brně. Vedoucí práce Karel Burda. Dostupné z: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=53953>

GRAZIANI, R. *Ipv6 Fundamentals: A Straightforward Approach to Understanding Ipv6*. Indianapolis: Cisco Press, 2013. ISBN-13: 978-1-58714-313-7.

HLOUŠEK, V. *Implementace DHCPv6 serveru* [online]. 2008 [cit. 2014-04-27]. Diplomová práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce David Antoš. Dostupné z: <http://theses.cz/id/3ui6q3/>.

HORLEY, E. *Practical IPv6 for Windows Administrators*, 2013, ISBN 978-1430263708.

HOTSKÝ, O. *Protokol IPv6 a jeho praktické využití* [online]. 2013 [cit. 2015-04-06]. Diplomová práce. Bankovní institut vysoká škola, Bankovní institut vysoká škola. Vedoucí práce Vladimír Beneš. Dostupné z: <http://is.bivs.cz/th/21517/bivs_m/>.

HRACHOVSKÝ, J. *Přechod počítačových sítí z IPv4 na IPv6* [online]. 2012 [cit. 2014-04-07]. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce Miroslav Matýsek. Dostupné z: <http://theses.cz/id/azyd1a/>.

IETF. *RFC 2462*. 1998. [cit. 2015-04-06]. Dostupné z: <https://www.ietf.org/rfc/rfc2462.txt>

IETF. *RFC 3513*. 2003. [cit. 2015-03-05]. Dostupné z: <https://www.ietf.org/rfc/rfc3513.txt>

IETF. *RFC 4941*. 2007. [cit. 2015-02-15]. Dostupné z: <https://www.ietf.org/rfc/rfc4941.txt>

IETF. *RFC 4291*. 2006 [cit. 2014-12-02]. Dostupné z: <https://www.ietf.org/rfc/rfc4291.txt>

IETF. *RFC 4443*. 2006 [cit. 2014-11-06]. Dostupné z: <https://www.ietf.org/rfc/rfc4443.txt>

IETF. *RFC 4861*. 2007 [cit. 2015-04-08]. Dostupné z: <https://www.ietf.org/rfc/rfc4861.txt>

IETF. *RFC 6106*. 2010. [cit. 2015-04-07]. Dostupné z: <https://www.ietf.org/rfc/rfc6106.txt>

IETF. *RFC 3315*. 2003. [cit. 2015-03-06]. Dostupné z: <https://www.ietf.org/rfc/rfc3315.txt>

IETF. *RFC 3736*. 2010. [cit. 2015-04-15]. Dostupné z: <https://www.ietf.org/rfc/rfc3736.txt>

ISC.ORG. *Not able to see lease logs in dhcpd6.leases* [online]. 2015 [cit. 2015-05-10]. Dostupné z: <https://lists.isc.org/pipermail/dhcp-users/2012-June/015676.html>

JOUDAL, J. *Implementace IPv6 Na PřF JU* [online]. 2011 [cit. 2014-04-27]. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích, Přírodovědecká fakulta. Vedoucí práce Rudolf Vohnout. Dostupné z: <http://theses.cz/id/rkiodq/>.

KALINA, J. *Výuková interaktivní animace síťového protokolu IPv6* [online]. 2012 [cit. 2014-04-27]. Bakalářská práce. Masarykova univerzita, Fakulta informatiky.

Vedoucí práce Tomáš Rebok. Dostupné z: <http://theses.cz/id/jlf1st/>

KOUTECKÝ, T. *Implementace IPv6 v BIVŠ* [online]. 2014 [cit. 2015-04-11]. Bakalářská práce. Bankovní institut vysoká škola Praha. Vedoucí práce Jan Háněl. Dostupné z: <http://is.bivs.cz/th/22453/bivs_m/>

MSDN.MICROSOFT.COM. *IPv6 Interface Identifiers* [online]. 2010 [cit 2015-04-06]. Dostupné z: <https://msdn.microsoft.com/en-us/library/aa915616.aspx/>

NIC.CZ. *Adresy v internetovém protokolu verze 6 (II*) [online]. 2011 [cit 2015-04-12]. Dostupné z: <https://www.nic.cz/files/nic/doc/Computerworld_IPv6_04 2011.pdf>

ODOM, W. *CCNP Route 642-902 official certification guide. Indianapolis*: Cisco Press, c2010, xxxiv, 730 s. ISBN 978-1-58720-253-7.

PANGRÁC, V*. Podpora IPv6 u menších poskytovatelů internetového připojení* [online]. 2010 [cit. 2014-04-27]. Bakalářská práce. Vysoká škola ekonomická v Praze. Vedoucí práce Luboš Pavlíček. Dostupné z: <http://theses.cz/id/qwca6f/>

PODERMAŃSKI, T. *IPv6 Mýty a skutečnost*: *díl II*. [online]. [cit. 2015-04-06]. Dostupné z: <http://www.lupa.cz/clanky/ipv6-myty-a-skutecnost-dil-ii-adresovy-prostor/>.

PODERMAŃSKI, T. a GRÉGR, M. *IPv6 Mýty a skutečnost: díl IV.* [online]. [cit. 2014-05-14]. Dostupné z: <http://www.lupa.cz/clanky/ipv6-myty-a-skutecnost-dil-iv-podpora-autokonfigurace/>.

POTAROO.NET. *IPv4 address report* [online]. 2015 [cit 2015-04-12]. Dostupné z: <http://www.potaroo.net/tools/ipv4/fig08.png>

PRIESNITZ, P. *Implementace protokolu IPv6 ve firemní síti* [online]. 2012 [cit. 2014-03-25]. Bakalářská práce. Vysoké učení technické v Brně. Vedoucí práce Viktor Ondrák. Dostupné z: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=57732>

RIPE.NET. *Lookup results* [online]. 2015 [cit. 2015-04-17]. Dostupné z: < https://apps.db.ripe.net/search/lookup.html?source=ripe&key=2001%3A718%3A803%3A%3A/48&type=inet6num>.

SAMURAJ-CZ.COM. *VLAN – virtual local area network* [online]. 2007 [cit 2015-04-12]. Dostupné z: <http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/>

SATRAPA, P. *IPv6: internetový protokol IPv6*. Praha: CZ.NIC, 2011, CZ.NIC. ISBN 978-80-904248-0-7.

SOCIAL.TECHNET.MICROSOFT.COM. *Does Win7 or W2K8 server support RFC 6106?* [online]. 2012 [cit. 2014-05-14]. Dostupné z: <https://social.technet.microsoft.com/forums/windowsserver/en-US/5757980a-5983-4efc-a5f3-27687b90fe41/does-win7-or-w2k8-server-support-rfc-6106>.

TLAČBABA, M. *Přechod IPv4 <-> IPv6* [online]. 2012 [cit. 2014-04-27]. Bakalářská práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Eva Hladká. Dostupné z: <http://theses.cz/id/mscp5u/>.

TÓTH, G. *Systém pro delegaci přístupu k síťovým prvkům* [online]. 2014 [cit. 2015-04-11]. Bakalářská práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Petr Holub. Dostupné z: <http://is.muni.cz/th/255648/fi_b_b1/>

VESELÝ, J. *IPv6 a bezpečnost* [online]. 2014 [cit. 2014-04-27]. Diplomová práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Eva Hladká. Dostupné z: <http://theses.cz/id/pm0z8i/>.

VILÍMEK, J. *Implementace protokolu IPv6 u ISP* [online]. 2007 [cit. 2014-04-27]. Bakalářská práce. Vysoká škola ekonomická v Praze. Vedoucí práce Luboš Pavlíček. Dostupné z: <http://theses.cz/id/7vqfzq/>.

ZIMA, M. *Přechod IPv4 / IPv6* [online]. 2012 [cit. 2014-04-27]. Bakalářská práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Eva Hladká. Dostupné z: <http://theses.cz/id/zani7r/>.

Přílohy

A Nastavení rozhraní fáze 1

Lokalita Q

```
Switch(config)#interface vlan25
Switch(config-if)#ip address 195.178.72.1 255.255.255.0
Switch(config-if)#ip helper-address 195.178.80.2
Switch(config-if)#ipv6 address 2001:718:803:125::1/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:125::/64
Switch(config-if)#no ipv6 nd managed-config-flag
Switch(config-if)#ipv6 nd other-config-flag
Switch(config-if)#ipv6 nd ra interval 600 198
Switch(config-if)#ipv6 dhcp relay destination 2001:718:803:f21::2
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

```
Switch(config)#interface vlan26
Switch(config-if)#ip address 195.178.73.1 255.255.255.0
Switch(config-if)#ip helper-address 195.178.80.2
Switch(config-if)#ipv6 address 2001:718:803:126::1/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:126::/64
Switch(config-if)#no ipv6 nd managed-config-flag
Switch(config-if)#ipv6 nd other-config-flag
Switch(config-if)#ipv6 nd ra interval 600 198
Switch(config-if)#ipv6 dhcp relay destination 2001:718:803:f21::2
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Lokalita C

```
Switch(config)#interface vlan84
Switch(config-if)#ip address 195.178.75.1 255.255.255.0
Switch(config-if)#ip helper-address 195.178.80.2
Switch(config-if)#ipv6 address 2001:718:803:384::1/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:384::/64
Switch(config-if)#ipv6 nd managed-config-flag
Switch(config-if)#no ipv6 nd other-config-flag
Switch(config-if)#ipv6 nd ra interval 600 198
Switch(config-if)#ipv6 dhcp relay destination 2001:718:803:f21::2
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Lokalita X

```
Switch(config-if)#interface vlan86
Switch(config-if)#ip address 195.178.76.1 255.255.255.0
Switch(config-if)#ip helper-address 195.178.80.2
Switch(config-if)#ipv6 address 2001:718:803:486::1/64
```

```
Switch(config-if)#ipv6 nd prefix 2001:718:803:486::/64
Switch(config-if)#no ipv6 nd managed-config-flag
Switch(config-if)#ipv6 nd other-config-flag
Switch(config-if)#ipv6 nd ra interval 600 198
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

B Nastavení rozhraní fáze 2

Lokalita Q

```
Switch(config)#interface vlan25
Switch(config-if)#ip address 195.178.72.1 255.255.255.0
Switch(config-if)#ip helper-address 195.178.80.2
Switch(config-if)#ipv6 address 2001:718:803:125::1/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:125::/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:125::/64 no-autoconfig
Switch(config-if)#no ipv6 other-config-flag
Switch(config-if)#ipv6 managed-config-flag
Switch(config-if)#ipv6 nd ra interval 600 198
Switch(config-if)#ipv6 dhcp relay destination 2001:718:803:f21::2
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

```
Switch(config)#interface vlan26
Switch(config-if)#ip address 195.178.73.1 255.255.255.0
Switch(config-if)#ip helper-address 195.178.80.2
Switch(config-if)#ipv6 address 2001:718:803:126::1/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:126::/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:126::/64 no-autoconfig
Switch(config-if)#no ipv6 other-config-flag
Switch(config-if)#ipv6 managed-config-flag
Switch(config-if)#ipv6 nd ra interval 600 198
Switch(config-if)#ipv6 dhcp relay destination 2001:718:803:f21::2
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Lokalita A

```
Switch(config)#interface vlan811
Switch(config-if)#ip address 195.178.74.1 255.255.255.128
Switch(config-if)#ip helper-address 195.178.80.2
Switch(config-if)#ipv6 address 2001:718:803:2a0::1/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:2a0::/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:2a0::/64 no-autoconfig
Switch(config-if)#no ipv6 other-config-flag
Switch(config-if)#ipv6 managed-config-flag
Switch(config-if)#ipv6 nd ra interval 600 198
Switch(config-if)#ipv6 dhcp relay destination 2001:718:803:f21::2
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#interface vlan819
```

```
Switch(config-if)#ip address 195.178.74.129 255.255.255.128
Switch(config-if)#ip helper-address 195.178.80.2
Switch(config-if)#ipv6 address 2001:718:803:2a1::1/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:2a1::/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:125::/64 no-autoconfig
Switch(config-if)#no ipv6 other-config-flag
Switch(config-if)#ipv6 managed-config-flag
Switch(config-if)#ipv6 nd ra interval 600 198
Switch(config-if)#ipv6 dhcp relay destination 2001:718:803:f21::2
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Lokalita C

```
Switch(config)#interface vlan84
Switch(config-if)#ip address 195.178.75.1 255.255.255.0
Switch(config-if)#ip helper-address 195.178.80.2
Switch(config-if)#ipv6 address 2001:718:803:384::1/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:384::/64
Switch(config-if)#ipv6 nd prefix 2001:718:803:125::/64 no-autoconfig
Switch(config-if)#no ipv6 other-config-flag
Switch(config-if)#ipv6 managed-config-flag
Switch(config-if)#ipv6 nd ra interval 600 198
Switch(config-if)#ipv6 dhcp relay destination 2001:718:803:f21::2
Switch(config-if)#no shutdown
Switch(config-if)#exit
```