Mendelova univerzita v Brně
Provozně ekonomická fakulta

Návrh integrace IPv6 do počítačové sítě Mendelovy univerzity v Brně v oblasti směrování

Diplomová práce

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

Bc. Tomáš Filip

Brno 2015

Mé poděkování patří Ing. Martinovi Pokornému, Ph.D., za odborné vedení, trpělivost, vstřícnost a ochotu, kterou mi v průběhu zpracování této diplomové práce věnoval.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Návrh integrace IPv6 do počítačové sítě Mendelovy univerzity v Brně v oblasti směrování**
vypracoval 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, 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 30. dubna 2015 .....

Abstract

Filip, T. The integration of IPv6 protocol into the Mendel University computer network in the area of routing. Master thesis. Brno 2015

This master thesis deals with integration of IPv6 network protocol into production computer network of Mendel University in Brno in the routing field. The integration includes the Dual Stack transition mechanism, IPv6 address plan, static routing at the perimeter of the university network, and OSPFv3 and MP–BGP routing protocols. Proposed integration plan was verified in the Laboratory of computer networking at the Department of Informatics at FBE MENDELU, and it serves as a template for a final implementation in the production network.

Keywords

IPv6, OSPFv3, MP–BGP, VRF, Cisco, university, routing, implementation

Abstrakt

Filip, T. Návrh integrace IPv6 do počítačové sítě Mendelovy univerzity v Brně v oblasti směrování. Diplomová práce. Brno 2015

Tato diplomová práce se zabývá vytvořením optimálního návrhu integrace síťového protokolu IPv6 do produkční počítačové sítě Mendelovy univerzity v Brně v oblasti směrování. Návrh zahrnuje přechodový mechanismus Dual Stack, adresní plán IPv6, statické směrování na perimetru univerzitní sítě MENDELU a směrovací protokoly OSPFv3 a MP–BGP. Zpracovaný návrh integrace byl verifikován v prostředí Laboratoře síťových technologií Ústavu informatiky na PEF MENDELU a představuje předlohu finální implementace do produkční sítě.

Klíčová slova

IPv6, OSPFv3, MP–BGP, VRF, Cisco, univerzitní, směrování, implementace

Obsah

1 Úvod

Z geografického hlediska se počítačová síť Mendelovy univerzity rozprostírá na několika místech v Brně a také v obci Lednice na Moravě, kde sídlí Zahradnická fakulta (ZF). V univerzitním kampusu v Brně – Černých Polích se nachází nejvýznamnější a největší část počítačové sítě Mendelovy univerzity. Tato část univerzitní sítě MENDELU je dále rozdělena do menších lokalit. Jednou z těchto lokalit je i Fakulta regionálního rozvoje a mezinárodních studií (FRRMS), která se ovšem nachází přibližně 1 km severně od univerzitního kampusu rovněž v brněnské části Černá Pole. Součástí univerzitní sítě MENDELU jsou i vysokoškolské koleje Jana Amose Komenského (JAK; Brno – Černá Pole) a koleje Josefa Taufera (TAK; Brno – Královo Pole).

Univerzitní síť je každodenně využívána více než 1500 zaměstnanci a 12000 studenty a v současné době je k ní stabilně připojeno několik tisíc koncových uzlů.

Kromě běžných uživatelských koncových stanic v kancelářích nebo učebnách mohou uživatelé pro připojení svých soukromých přenosných zařízení (například notebooky, tablety, chytré telefony apod.) k univerzitní síti MENDELU využít bezdrátovou technologii Wi–Fi nebo vyhrazené volně přístupné datové zásuvky. Zaměstnancům je rovněž umožněn přístup do univerzitní sítě z domova prostřednictvím VPN.

Mendelova univerzita v Brně disponuje unikátním Univerzitním informačním systémem (UIS), jehož významnou součástí je implementace technologického subsystému určeného pro správu univerzitní sítě. V tomto subsystému je možné například evidovat jednotlivé koncové uzly, evidovat všechny její VLAN, konfigurovat porty na přístupové vrstvě (využíváno například pedagogickými pracovníky pro povolení přístupu do Internetu stanicím studentů) a také generovat zónové soubory DNS a konfigurační soubory pro DHCP.

V současné době je celá infrastruktura univerzitní sítě MENDELU vybudována převážně na zařízeních společnosti Cisco Systems, Inc.

Nosným komunikačním protokolem univerzitní sítě je internetový protokol verze 4 (IPv4). Od této skutečnosti se odvíjí známé problémy, jako například již zcela nedostatečný adresní prostor a s tím související vynucené využívání technologie NAT. Jedním z trvalých řešení těchto problémů, které se vztahují k provozu IPv4, je přechod univerzitní sítě na internetový protokol verze 6 (IPv6).

IPv6 existuje již mnoho let a v současnosti se jeho nasazování do produkčních sítí značně zrychluje. Protokol IPv6 se stále vyvíjí, protože při praktické implementaci se odhalují mezery samotného protokolu nebo metodologie jeho nasazení. Na Mendelově univerzitě v Brně nebyl doposud zpracován žádný koncept integrace a následné implementace IPv6 do univerzitní počítačové sítě. Jednou z motivací této diplomové práce je pomoci tento nepříznivý stav zvrátit.

Integrace IPv6 do produkční univerzitní sítě MENDELU je natolik rozsáhlý problém, že není možné jej vyřešit v rámci jediné závěrečné práce. Tato diplomová práce je tak součástí skupiny závěrečných prací, jež se zabývají návrhy nasazení IPv6

do počítačové sítě Mendelovy univerzity v Brně v různých oblastech implementace tohoto protokolu. Výsledkem těchto prací bude postupná integrace IPv6 do všech geografických a sférických částí (aktivní síťové prvky, servery, síťové služby, koncové uzly atd.) univerzitní sítě MENDELU.

Oblastí zájmu návrhu integrace této diplomové práce je **směrování IPv6**. Nasazení nového síťového protokolu je prozatím plánováno pouze v geografických oblastech kampusu Mendelovy univerzity v Brně a Fakulty regionálního rozvoje a mezinárodních studií (FRRMS). Nachází se zde totiž páteř univerzitní sítě a dva spoje k síti ISP.

Tato diplomová práce se nezabývá nasazením IPv6 na vysokoškolských kolejích JAK a TAK ani na Zahradnické fakultě, která se nachází v obci Lednice na Moravě.

Souběžně s touto diplomovou prací jsou zpracovávány další závěrečné práce zabývající se návrhy nasazení IPv6 do univerzitní sítě MENDELU v jiných oblastech implementace:

1. Bakalářská práce s názvem *Řešení dynamické konfigurace IPv6 klientů v počítačové síti Mendelovy univerzity v Brně* autorky Barbory Chumlenové, jež se zabývá automatickou konfigurací IPv6 uživatelských stanic v univerzitní síti MENDELU a následnému zabezpečení.
2. Diplomová práce s názvem *Návrh integrace IPv6 do počítačové sítě Mendelovy univerzity v Brně v oblasti bezpečnosti a síťových služeb* autora Bc. Michala Šturmy zabývající se zabezpečením univerzitní sítě v kontextu s nasazením IPv6 a síťovými službami, zejména DNS.

Je vhodné zdůraznit, že každá ze závěrečných prací byla zpracována individuálně jejím autorem, přestože se v průběhu práce nebylo možné vyhnout určité kooperaci.

2 Cíl práce

Primárním cílem této diplomové práce je na základě provedené analýzy současného stavu produkční univerzitní sítě Mendelovy univerzity v Brně, analýzy uživatelských požadavků a seznámení se se situací nasazení protokolu IPv6 na jiných vysokých školách v České republice připojených k akademické síti CESNET zpracování optimálního návrhu integrace protokolu IPv6 do geografických lokací produkční počítačové sítě Mendelovy univerzity situovaných v univerzitním kampusu a budově FRRMS v Brně – Černých Polích a jeho následná verifikace prostřednictvím fyzického modelu univerzitní sítě MENDELU navrženého a zkonstruovaného v podmínkách Laboratoře síťových technologií Ústavu informatiky Provozně ekonomické fakulty Mendelovy univerzity v Brně na základě získaných poznatků z jednotlivých analýz a zpracovaného návrhu.

3 Specifikace požadavků

V této kapitole je uveden seznam požadavků na návrh integrace protokolu IPv6 do produkční počítačové sítě Mendelovy univerzity v Brně, které byly předloženy odpovědnými zástupci Ústavu informačních technologií.

3.1 Metodika integrace protokolu IPv6

Nasazení protokolu IPv6 do produkční univerzitní sítě MENDELU musí být zrealizováno bez narušení stávajícího provozu univerzitní počítačové sítě prostřednictvím přechodového mechanismu Dual Stack. Podstatou této metody přechodu je rozšíření současné konfigurace L3 prvků o atributy IPv6. To znamená, že síťová zařízení budou mít konfigurovány oba typy IP adres. Poskytovatel internetových služeb CESNET z.s.p.o. plně podporuje IPv6. Nebude zapotřebí žádný typ tunelování ani překládání adres. Síťové uzly s podporou IPv6 budou komunikovat nativně prostřednictvím nového protokolu. Obě verze síťového protokolu budou v univerzitní síti fungovat vedle sebe, aniž by se jakkoli vzájemně ovlivňovaly. Budou pouze sdílet systémové prostředky síťových zařízení.

3.2 Adresní plán IPv6

Princip přidělování síťových prefixů IPv6 jednotlivým VLAN univerzitní sítě musí být proveden s ohledem na minimalizaci množství záznamů ve směrovacích tabulkách infrastrukturních L3 prvků univerzitní sítě MENDELU. Rovněž je kladen důraz na snadnou identifikaci konkrétní VLAN při vizuálním pohledu na její přiřazený IPv6 prefix. Identifikací konkrétní VLAN je myšleno zejména její umístění v topologii univerzitní sítě MENDELU.

3.3 Směrování protokolu IPv6

Síťový provoz protokolu IPv6 musí být směrován na základě totožných principů, jako tomu je v současnosti v případě směrování síťového provozu přes protokol IPv4. To znamená zejména navržení implementace směrovacích protokolů BGP a OSPF, které jsou v současnosti provozovány pro směrování síťového provozu IPv4, také pro IPv6. Výsledkem návrhu směrování protokolu IPv6 by měly být především logicky shodné záznamy ve směrovacích tabulkách L3 prvků na páteři a perimetru univerzitní sítě MENDELU.

3.4 Verifikace navrženého řešení

Zpracovaný návrh integrace IPv6 do univerzitní sítě je nutné před ostrým nasazením verifikovat v prostředí Laboratoře síťových technologií ÚI PEF MENDELU. Na základě analýzy topologie produkční univerzitní sítě MENDELU je zapotřebí

navrhnout a zkonstruovat její model s využitím technického vybavení této laboratoře. Na tomto modelu budou následně provedeny verifikační testy, jenž rozhodnou o správnosti zpracovaného návrhu integrace IPv6 do univerzitní sítě MENDELU.

3.5 Utajení citlivých informací

Z důvodu zachování míry zabezpečení produkční univerzitní sítě je nezbytné zachovat v utajení některé její atributy. Jedná se zejména o skutečné:

- IP adresy,
- identifikátory VLAN,
- identifikátory oblastí OSPF,
- identifikátory VRF.

4 Metodika řešení

Postup vedoucí k dosažení specifikovaného cíle této diplomové práce lze shrnout do následujících kroků:

1. Podrobné seznámení se s problematikou protokolu IPv6 z různých zdrojů (odborná literatura, RFC dokumenty apod.). Výsledkem je stručný popis jednotlivých technologií, které jsou pro vyřešení problému této závěrečné práce nezbytné.
2. Analýza akademických prací zabývajících se stejným nebo podobným problémem – integrace protokolu IPv6 do libovolné produkční počítačové sítě. Účelem je získání užitečných poznatků a principů, které by bylo možné uplatnit při řešení této závěrečné práce.
3. Analýza stavu nasazení protokolu IPv6 na jiných českých univerzitách, jejichž počítačové sítě jsou připojeny k totožnému poskytovateli internetových služeb (ISP). Podklady byly získány od odpovědných zástupců jednotlivých univerzit, kteří poskytli cenné informace o stávajícím provozu IPv6 ve svých univerzitních sítích. Účelem je získání představy o nasazení protokolu IPv6 do produkčních sítí podobného rozsahu, jako je univerzitní síť MENDELU.
4. Analýza současného stavu produkční počítačové sítě Mendelovy univerzity v Brně, která je zaměřena zejména na její topologii a principy směrování.
5. Na základě provedených analýz a získaných teoretických znalostí problematiky IPv6 je v souladu s požadavky zpracován optimální návrh integrace internetového protokolu verze 6 do produkční počítačové sítě Mendelovy univerzity v Brně. Návrh zahrnuje požadovaný přechodový mechanismus Dual Stack, adresní plán IPv6, návrh realizace statického směrování na perimetru univerzitní sítě a obecné návrhy implementací směrovacích protokolů OSPFv3 a MP–BGP.
6. Vytvořený návrh integrace protokolu IPv6 je následně prakticky implementován prostřednictvím fyzického modelu univerzitní sítě MENDELU, jenž byl zkonstruován pomocí technických prostředků Laboratoře síťových technologií ÚI PEF MENDELU. Topologie modelu vychází z topologie produkční univerzitní sítě a je v něm zároveň implementován i soudobý síťový protokol IPv4.
7. Za účelem ověření správnosti navrženého řešení integrace protokolu IPv6 do univerzitní sítě MENDELU bylo na jejím modelu provedeno několik verifikačních testů zaměřujících se na funkčnost principů směrování.

5 Popis technologického aparátu

5.1 IPv6 – Internet Protocol verze 6

Je nástupcem současného internetového protokolu (IPv4). (Satrapa, 2011)
Jeho základní specifikace je uvedena v RFC 2460 (2007).

Formát datagramu

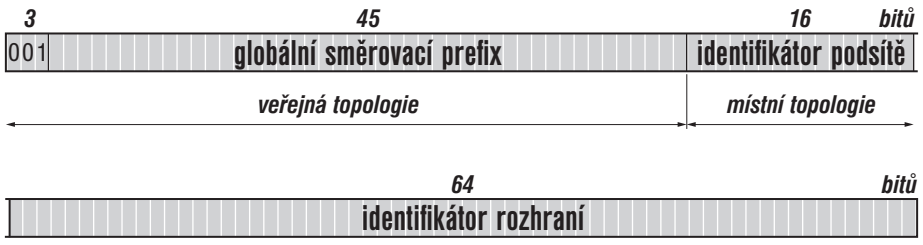
V souvislosti se směrováním jsou podstatné následující atributy IPv6 datagramu:

- *Maximální počet skoků* (Hop limit) je podle RFC 2460 (2007) náhradou dřívější životnosti datagramu (TTL).
- *Zdrojová adresa* – IPv6 adresa odesílatele datagramu.
- *Cílová adresa* – IPv6 adresa příjemce datagramu.

Nejdůležitější typy IPv6 adres

Globální individuální adresy – podle Satrapy (2011, s. 60) se jedná o „normální“ adresy – protipól veřejných adres současného IPv4. Jsou unikátní v rámci celého Internetu. Jejich obvyklá struktura je znázorněna na obr. 1 a je složena ze tří podstatných částí:

1. *Globální směrovací prefix* je identifikátorem koncové sítě. Je přidělován lokálním internetovým registrem (LIR) – zpravidla jím bývá místní poskytovatel internetových služeb (ISP).
2. *Identifikátor podsítě* slouží k rozlišení jednotlivých podsítí v rámci dané sítě. Délka identifikátoru podsítě plus délka globálního směrovacího prefixu musí mít délku právě 64 bitů.
3. *Závěrečný identifikátor rozhraní* zabírá celou polovinu adresy, tj. zbylých 64 bitů.



Obr. 1: Obvyklá struktura globální individuální adresy. Převzato od: Satrapa (2011, s. 60)

Lokální linkové adresy (link local) nejsou unikátní v rámci Internetu. Jejich platnost je vymezena lokální sítí. Tyto adresy začínají prefixem `fe80::/10`. Dalších 54 bitů je nulových. Za nimi se nachází 64bitový identifikátor rozhraní, který je nejčastěji získán aplikací modifikovaného EUI–64. (Satrapa, 2011, s. 64)

Přidělování adresního prostoru IPv6

Satrapa (2011, s. 91) uvádí, že procedura přidělování adres je dnes totožná pro oba protokoly: centrální autoritou je *IANA*[1], která přiděluje velké bloky adres *regionálním registrům* (RIR). Regionální registr pro Evropu je RIPE NCC[2].

Regionální registry přidělují menší bloky *lokálním registrům* (LIR), jimiž jsou zpravidla místní poskytovatelé Internetu. Od nich získávají adresy koncové instituce – zákazníci. Vzhledem k hierarchickému uspořádání přidělovaných rozsahů je zajištěna agregovatelnost. (Satrapa, 2011, s. 91)

Ohlášení směrovače

Formát této zprávy je definován v RFC 4861 (2007), kde se uvádí, že každý směrovač posílá tato ohlášení (RA) v náhodných intervalech do všech sítí, k nimž je připojen. Touto zprávou jsou hostitelům poskytnuty základní informace o síti, v níž se nachází. (Satrapa, 2011, s. 119)

Podle RFC 4861 (2007) se jedná se o jednu z mnoha informačních zpráv ICMPv6 – typ 134.

V souvislosti s oblastí směrování jsou podstatné následující atributy ohlášení směrovače:

- *Omezení skoků* (Cur Hop Limit) – poskytuje lokálním uzlům informaci o tom, jak mají omezovat životnost odesílaných IPv6 datagramů, tj. jakou hodnotu mají vkládat do položky s maximálním počtem skoků v záhlaví vytvářeného IPv6 datagramu.
- *Životnost implicitního směrovače* (Router Lifetime) – udává časový úsek (sekundy), po který má být daný směrovač implicitním pro uzly konkrétní sítě.
- *Preference* (Prf) – ohlašuje-li směrovač nenulovou životnost implicitního směrovače, může si zde nastavit preferenci. (Satrapa, 2011, s. 121)

Nejpodstatnější volbou ohlášení směrovače je *informace o prefixu.*
Dále internetový protokol verze 6 detailně rozebírá Satrapa (2011).

[1] `http://www.iana.org`
[2] `https://www.ripe.net`

5.2 Přechodové mechanismy

McFarland (2011, s. 48) uvádí, že přechodové mechanismy pomáhají přejít od jednoho protokolu k jinému. Z hlediska protokolu IP se v praxi jedná o přechod z protokolu IPv4 na IPv6. Sítě IPv6 časem zcela nahradí dnešní sítě IPv4. V blízké budoucnosti se však nelze obejít bez různých přechodových mechanismů, které umožní souběžný provoz obou protokolů.

Dual Stack nabízí nejplynulejší přechod z prostředí protokolu IPv4 na IPv6. Podle RFC 4213 (2005) není při použití duální sady protokolů u koncových uzlů vyžadováno žádné tunelování ani překlad adres. U všech uzlů v síti (hostitelé, servery, směrovače, přepínače, firewally atd.) jsou povoleny oba protokoly: IPv4 i IPv6.

5.3 Směrování

Kocharians (2014, s. 271) popisuje směrování (routing) jako proces, při němž směrovač přijme paket IP (v4 nebo v6), provede rozhodnutí o jeho dalším odeslání, a poté jej skutečně odešle.

Podle Lammle (2013, s. 356) se rozlišují následující způsoby směrování:

- *Statické směrování* – trasy jsou do směrovací tabulky ukládány ručně.
- *Výchozí směrování* – možnost zasílání paketů vzdáleným cílovým sítím, které nejsou uvedeny ve směrovací tabulce směrovače dalšího přeskoku.
- *Dynamické směrování* – záznamy jsou do směrovací tabulky automaticky ukládány na základě informací od směrovacích protokolů, které jsou rovněž zodpovědné za automatickou konvergenci při změně topologie sítě (například při selhání některého síťového rozhraní nebo celého zařízení).

Administrativní vzdálenost

Kocharians (2014, s. 644) uvádí, že směrovač prostřednictvím administrativní vzdálenosti (AD) porovnává důvěryhodnost tras do konkrétní cílové sítě získaných z více zdrojů. Výchozí hodnoty AD pro vybrané zdroje shrnuje tab. 1. Nižší hodnota AD je lepší.

Tab. 1: Výchozí hodnoty AD vybraných zdrojů tras. Zdroj: Empson (2014, s. 3)

Typ trasy	**Administrativní vzdálenost**
Připojená síť	0
Statická trasa	1
eBGP	20
OSPF	110
iBGP	200
Nedostupná trasa	255

Autonomní systém

Autonomní systém (AS) je množina směrovačů (síť) spadající pod správní kontrolu konkrétní organizace (například firma, univerzita, ISP, apod.). (Odom, 2013, s. 407)

Každému AS je přidělen identifikátor ASN z rozsahu 0–65535. Identifikátory ASN jsou spravovány organizací IANA podobně jako veřejné síťové prefixy. Veřejné, privátní a rezervované rozsahy ASN jsou uvedeny v tab. 2. (Wallace, 2015, s. 550)

Tab. 2: Kategorie rozsahů ASN podle organizace IANA. Zdroj: Wallace (2015, s. 551)

Rozsah ASN	**Účel**
0	Rezervováno
1-64495	Veřejný rozsah ASN, přiděluje IANA
64496-64511	Rezervováno pro účely dokumentace
64512-65534	Privátní rozsah ASN
65535	Rezervováno

Vnitřní a vnější směrovací protokoly

Podle Odom (2013, s. 406) jsou směrovací protokoly rozděleny na:

1. *Vnitřní* (IGP) – směrovací protokoly určené pro provoz uvnitř jediného AS.
2. *Vnější* (EGP) – směrovací protokoly určené pro provoz mezi různými AS.

5.4 Směrovací protokol OSPF

Podle RFC 2328 (1998) patří směrovací protokol OSPF do skupiny vnitřních směrovacích protokolů (IGP) a je založený na principu stavu linky.

Podle Lammle (2013, s. 387) je OSPF charakterizován těmito základními vlastnostmi: Podporuje oblasti a autonomní systémy, podporuje více tras do jednoho cíle se stejnými náklady, má velmi rychlou konvergenci, minimalizuje provoz aktualizací směrování (sousední směrovače si nevyměňují celé směrovací tabulky, ale pouze aktualizace svých linek), umožňuje škálovatelnost, podporuje VLSM/CIDR, má neomezený počet přeskoků, podporuje jej více výrobců síťových zařízení a nepodporuje automatickou sumarizaci tras, pouze manuální.

Wallace (2015) a Lammle (2013) dále uvádějí a vysvětlují následující důležité pojmy, které se vztahují k OSPF: linka, ID směrovače, vztahy sousedství a přilehlosti, protokol Hello, topologická databáze (LSDB), aktualizace stavu linky (LSU), ohlášení stavu linky (LSA), oblast (area), hraniční směrovač oblasti (ABR), páteřní směrovač, určený směrovač (DR) a záložní určený směrovač (BDR).

Základní princip provozu

Podle Wallace (2015, s. 263) lze základní princip provozu OSPF rozdělit do 3 kroků:

1. Objevení sousedních OSPF směrovačů a následná výměna určitých informací, na jejichž základě bude rozhodnuto, zda by si dva sousední směrovače měly posílat data o síťové topologii (tzn. zda bude ustanoven stav přilehlosti). Každý OSPF směrovač si udržuje tabulku sousedů.
2. Výměna informací z topologické databáze vyžaduje, aby každý OSPF směrovač posílal zprávy přilehlým sousedům. Všechny směrovače poté budou mít informace o topologii sítě. Každý OSPF směrovač si ukládá topologické informace do topologické databáze, která obsahuje zejména tyto údaje:
   - ID směrovače každého souseda.
   - Zainteresované rozhraní a IP adresu každého souseda.
   - Seznam směrovačů dosažitelných na všech rozhraních každého z nich.
3. Výpočet tras – všechny zainteresované směrovače provádějí nezávisle na sobě analýzu svých topologických databází a ze získaných informací vybírají nejlepší trasy do všech dostupných sítí ze své vlastní perspektivy. Směrovací protokoly pracující se stavem linky používají pro analýzu dat a vybírání nejlepších tras algoritmus nejkratší cesty (SPF[3]). Pro všechny nejlepší trasy do všech dostupných sítí je určeno správné odchozí rozhraní (resp. rozhraní dalšího přeskoku) a jsou vloženy do směrovací tabulky. (Wallace, 2015, s. 263)

Metrika

Existuje-li více tras do konkrétní cílové sítě, tak interní metrika protokolu OSPF poskytuje možnost porovnání jejich nákladů.

Jejím vstupním parametrem jsou ceny všech rozhraní, které jsou zahrnuty do OSPF procesu. Ve výchozím stavu se cena rozhraní odvíjí od jeho šířky pásma (bandwidth). V případě logických rozhraní je podle Cisco.com (2014) výchozí hodnota bandwith stanovena na 1 Gbit. Cenu každého rozhraní lze také nastavit ručně. (Wallace, 2015, s. 330)

Výsledná metrika trasy je určena součtem cen všech odchozích rozhraní dané trasy. Trasy s minimální metrikou jsou ukládány do směrovací tabulky.

Protokol OSPF podporuje i vícenásobné trasy (až 32) do konkrétní cílové sítě se shodnou minimální metrikou. Na těchto trasách je pak aktivní rovnoměrné vyvažování zátěže (load balancing). (Wallace, 2015, s. 332)

Skupinové adresy

V RFC 2328 (1998) se uvádí, že OSPF používá pro svůj provoz skupinovou IP adresu `224.0.0.5` zahrnující všechny směrovače OSPF a `224.0.0.6` pro všechny určené směrovače.

[3]Shortest Path First, `http://en.wikipedia.org/wiki/Dijkstra's_algorithm`

OSPFv3

V RFC 5340 (2008) se uvádí, že OSPF ve verzi 3 přináší podporu pro dynamické směrování IPv6.

Dále jsou podle RFC 5340 (2008) základní principy a funkce pro OSPFv2 i OSPFv3 totožné. Například v těchto aspektech jsou však rozdíly:

- ID směrovače již není získáno z nejvyšší IP adresy, ale je potřeba jej určit vždy ručně.
- Atributy přilehlosti a rozhraní dalšího přeskoku nyní využívají linkové lokální adresy. I nadále je pro odesílání aktualizací a potvrzení využíváno vícesměrové vysílání. Podle RFC 5340 (2008) jsou pro tyto účely vyhrazené skupinové IPv6 adresy:
  - `ff02::5` – všechny směrovače OSPF,
  - `ff02::6` – všechny určené směrovače OSPF.
- Každému zainteresovanému rozhraní do OSPFv3 procesu je nutné přímo přiřadit ID procesu a ID oblasti, pod kterou spadá.

Další základy problematiky OSPF podrobně popisuje Odom (2013, s. 411) a pokročilými technikami navazuje Wallace (2015, s. 263).

5.5 Směrovací protokol BGP

Účelem směrovacího protokolu BGP je podle RFC 4271 (2006) zjišťování, vybírání a propagace nejlepších tras pro směrování síťového provozu v rámci celého Internetu.

Wallace (2015, s. 545) uvádí, že BGP verze 4 (BGPv4) je v současnosti jediným zástupcem skupiny vnějších směrovacích protokolů (EGP).

Základní princip

BGP používá pro analýzu a výběr tras tzv. algoritmus nejlepší cesty (best–path algorithm). Jedná se o komplexní algoritmus, jehož vstupem je mnoho atributů cesty (PA). (Wallace, 2015, s. 545)

Jedním z mnoha PA je BGP AS_PATH (autonomous system path). Jedná se o základní atribut, který BGP směrovače používají ve výchozí konfiguraci pro výběr nejlepších tras, nemají-li manuálně nastaveny jiné atributy cesty. Propaguje-li směrovač trasu prostřednictvím BGP svému sousedovi, je k síťovému prefixu přidružena množina PA, včetně AS_PATH. Tento atribut poskytuje posloupnost všech identifikátorů AS (ASN), přes které byl prefix propagován. (Wallace, 2015, s. 546)

Směrovače BGP prostřednictvím posloupnosti v AS_PATH také zabraňují směrovacím smyčkám: obdrží-li BGP směrovač aktualizaci s prefixem a v posloupnosti ASN v AS_PATH se již nachází jeho vlastní ASN, tak tuto aktualizaci ignoruje. (Wallace, 2015, s. 549)

Sousedství mezi směrovači

Vztah sousedství je definován staticky prostřednictvím konfigurace BGP procesu u zainteresovaných směrovačů (například v případě směrovačů OSPF je vztah sousedství ustanoven automaticky na základě propagovaných prefixů). Směrovače si následně vyměňují BGP zprávy na portu `179/tcp`. Sousední směrovače nemusí být ve stejné síti a mohou být mezi nimi umístěny další směrovače (neexistuje stav přilehlosti). (Wallace, 2015, s. 546)

Relace sousedství má v BGP dva typy:

1. *Interní* (iBGP) – sousední směrovače se nachází ve stejném AS.
2. *Externí* (eBGP) – sousední směrovače se nachází v odlišných AS.

Způsoby směrování síťového provozu do Internetu

Podle Wallace (2015, s. 551) mají koncové sítě (firemní, univerzitní, apod.) na výběr ze dvou způsobů směrování síťového provozu do Internetu:

1. *Výchozí směrování* – staticky definovaná trasa, kterou směrovač zvolí v případě, že ve směrovací tabulce neexistuje lépe vyhovující trasa do cílové sítě. Prefix cílové sítě se nemusí shodovat ani v jednom bitu.
2. *BGP* – výchozí trasa je propagována poskytovatelem internetových služeb prostřednictvím BGP.

Je-li koncová síť připojena k poskytovateli internetových služeb více než jedním spojem (například dual–homed), Wallace (2015, s. 553) doporučuje využití druhého způsobu směrování prostřednictvím BGP.

Parametr *Weight*

Lacoste (2014) uvádí, že se jedná o proprietární lokální parametr cesty dostupný na zařízeních společnosti Cisco Systems, Inc. Jeho účelem je preference určité trasy do konkrétní cílové sítě, pokud jich směrovač přijal od různých BGP sousedů více. Není součástí množiny PA, které si sousedé BGP mezi sebou vyměňují ve zprávách BGP Update. Vyšší hodnota parametru weight je lepší. Výchozí hodnoty atributu weight jsou 32768 pro lokální trasy a 0 pro ostatní trasy.

Atribut cesty *MED*

Podle Lacoste (2014) představuje atribut MED metriku směrovacího protokolu BGP. Sousední směrovače typu eBGP si vzájemně vyměňují její hodnotu ve zprávách BGP Update. Jejím účelem je upřednostnění určité cesty do konkrétního AS, pokud jich existuje více. Cesta s nižší hodnotou atributu MED je lepší.

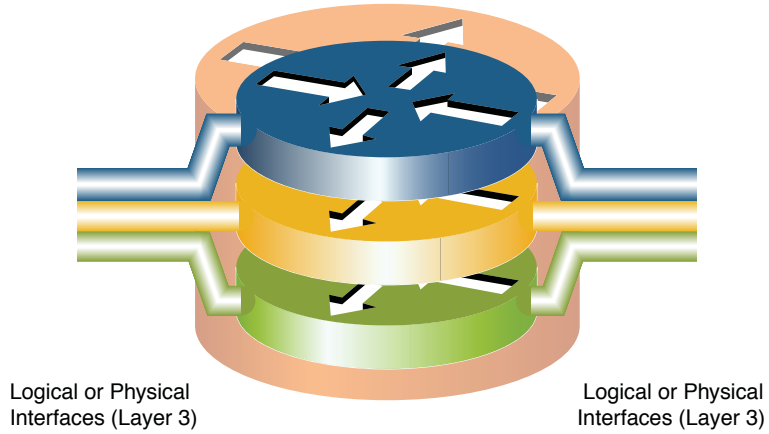
MP–BGP

Multiprotocol BGP je podle RFC 4760 (2007) rozšíření směrovacího protokolu BGPv4 poskytující podporu pro směrování protokolu IPv6.

Dále se protokolem BGP podrobně zabývá Wallace (2015, s. 545).

5.6 Virtual Routing and Forwarding

Bruno (2011, s. 143) uvádí, že VRF je technologie pro virtualizaci směrování. Základní princip spočívá ve vytvoření několika virtuálních směrovacích instancí (virtuálních směrovačů) v jednom konkrétním fyzickém směrovači tak, jako je to znázorněno na obr. 2.



Obr. 2: Grafické znázornění principu VRF. Převzato od: Tiso (2011, s. 305)

Tiso (2011, s. 305) uvádí, že primárním účelem VRF je oddělení síťového provozu ve sdílené síťové infrastruktuře na síťové vrstvě (L3), čímž je dosaženo například většího zabezpečení sítí a také jejich nezávislost (například oddělení sítí zákazníků konkrétního ISP). Další výhodou VRF je možnost nahrazení více fyzických směrovačů jedním s konfigurací VRF.

Podle Tiso (2011, s. 305) zahrnuje každá VRF instance (virtuální směrovač) následující komponenty, které jsou nutné pro proces směrování a předávání paketů:

- Přiřazená fyzická nebo logická L3 rozhraní,
- směrovací tabulka,
- instance směrovacích protokolů.

Každá z komponent konkrétní VRF instance je zcela nezávislá na ostatních, avšak jednotlivé VRF instance sdílí fyzická rozhraní, procesor a paměť hostitelského směrovače. (Tiso, 2011, s. 303)

5.7 Virtuální sítě VLAN

Podle Hucaby (2014, s. 95) je virtuálními lokálními sítěmi VLAN virtualizována linková vrstva (L2).

Konkrétní virtuální síť se vyskytuje na jednom nebo více přepínačích a utváří tak jedinou virtuální všesměrovou doménu. Tímto způsobem je možné rozdělit jediný fyzický přepínač na několik virtuálních. (Hucaby, 2015)

SVI (Switched Virtual Interface) je logické rozhraní používané pro přiřazení L3 adresy (IP, IPv6) v rámci konkrétní VLAN.

VLAN trunk je fyzický L2 spoj, po němž lze přenášet síťový provoz více VLAN prostřednictvím logického značení („tagování“ VLAN).

Přístupové rozhraní přepínače pak slouží k připojení koncového uzlu – tento typ L2 rozhraní spadá do jediné VLAN.

Technologii virtuálních lokálních sítí VLAN podrobně popisuje Hucaby (2014, s. 95).

5.8 Spanning Tree Protocol

Podle Hucaby (2014, s. 154) je účelem provozu protokolu STP je zamezení vzniku L2 smyček, jejichž důsledkem mohou být tzv. všesměrové bouře. Jedná se o situaci, kdy přepínač, který na některé ze svých L2 rozhraní zahrnuté v L2 smyčce obdrží všesměrový rámec (tj. rámec s cílovou MAC adresou `FF:FF:FF:FF:FF:FF`). Následně jej odesílá na všechna svá ostatní L2 rozhraní, vyjma toho, na kterém byl všesměrový rámec přijat. Z jednoho všesměrového rámce tak putuje po síti několik jeho kopií. Rámce nemají žádný mechanismus, kterým by bylo určeno, po jakou dobu mohou v síti existovat. V případě, že se všesměrový rámec ocitne v L2 smyčce mezi přepínači, které si jej mezi sebou neustále přeposílají a zároveň s každým odesláním vytvářejí jeho nové kopie (přičemž ty staré nemizí a počet nových roste exponenciálně), dojde k úplnému zahlcení komunikačních linek. Síť následně přestává úplně fungovat, protože není schopna obsluhovat běžný datový provoz.

Protokol STP eliminuje vznik L2 smyček blokací některého ze zúčastněných rozhraní, čímž ji přeruší. Zablokované rozhraní nadále přijímá provozní zprávy STP BPDU, ale nepřijímá běžný síťový provoz.

STP dále podrobně rozebírá Hucaby (2014, s. 151).

6 Analýza podobných akademických prací

V této kapitole je provedena analýza akademických prací, které se zabývají stejným nebo podobným problémem – integrace IPv6 do produkční sítě. Účelem analýzy je možné získání poznatků, které mohou být uplatněny v této diplomové práci.

Analýza zahrnuje vybrané bakalářské (BP) a diplomové práce (DP) za posledních 10 let, které byly dostupné v archívech jednotlivých vysokých škol nebo v databázi vysokoškolských kvalifikačních pracích[4], kterou provozuje Fakulta informatiky Masarykovy univerzity.

Pro vyhledávání byla použita klíčová slova: implementation IPv6, integration IPv6, deployment IPv6, transition IPv6, implementace IPv6, integrace IPv6, nasazení IPv6, přechod IPv6.

6.1 BP Návrh integrace protokolu IPv6 ve firmě Z–Ware

Tato bakalářská práce navrhuje a diskutuje metody a postupy implementace IPv6 do počítačové sítě firmy Z–Ware. Zabývá se praktickým nastavením směrovačů, serverů a klientských stanic.

Hakl (2013) uvádí, že firma Z–Ware má dvě hlavní střediska. První z nich se nachází v Brně a druhé v Jihlavě. Další servisní místa jsou v Praze, Břeclavi, Lanškrouně a Ostravě. Každé lokalitě byl přidělen globální směrovací IPv6 prefix délky 64 bitů.

Pouze tři ze čtyř poskytovatelů internetových služeb podporují IPv6, z čehož vyplývá, že je nutné zprovoznit některé z tunelových řešení. Autor provedl testování tří tunelových řešení: 6to4, Hurricane Electric a Sixxs.

6.2 BP Přechod počítačových sítí z IPv4 na IPv6

Bakalářská práce se rovněž zabývá problematikou počítačových sítí protokolu IPv4 a jejího následného přechodu na verzi IPv6.

Hrachovský (2012) zde testuje tunelové řešení Teredo na operačních systémech Ubuntu 10.04, Windows 7 Home Edition a Windows XP SP2. Hrachovský (2012) zde uvádí, že na rozdíl od tunelu typu 6to4 nevyžaduje Teredo veřejnou IP adresu.

Autor se dále zabývá praktickou konfigurací směrovacího protokolu OSPFv3 na Router Boardech Mikrotik s verzí firmware 5.16. Tento směrovací protokol byl zvolen pro jeho plnou podporu na této platformě.

6.3 BP Integrace protokolu IPv6 ve firmě Znovín Znojmo, a.s.

Tato bakalářská práce si klade za cíl integraci protokolu IPv6 do produkční počítačové sítě firmy Znovín Znojmo, a.s.

[4]Dostupné na: `http://www.theses.cz`

Podle Viklického (2015) se tato firemní síť skládá ze tří poboček. Dvě se nachází v Šatově a jedna je ve Znojmě.

Poskytovatelem internetových služeb je společnost NET EXPERT, v.o.s, která by byla schopna zajistit nativní podporu pro tuto firemní síť, avšak tento krok důrazně nedoporučila z toho důvodu, že by spojení nemuselo být tak stabilní jako stávající a že ze své strany nemůže zajistit stoprocentní zabezpečení firemní sítě. Viklický (2015)

6.4 DP Problematika přechodu na IPv6 v podnikových sítích

Diplomová práce nastiňuje problematiku nového protokolu IPv6 jak z hlediska teoretického, tak z hlediska praktického. Objasňuje současný stav implementace protokolu IPv6 v páteřních sítích a naznačuje postup, jak je možné v podnikových podmínkách na IPv6 přejít.

Petlach (2006) v této diplomové práci porovnává a shrnuje všechny možné přístupy a techniky přechodu počítačových sítí na IPv6 v různých oblastech implementace tohoto protokolu.

Jedná se spíše o referenční příručku správce sítě, než o práci, ze které by bylo možné převzít praktické poznatky pro integraci IPv6 do univerzitní sítě.

6.5 DP Implementace IPv6 v BIVŠ

Tato diplomová práce popisuje implementační projekt protokolu IPv6 do prostředí Bankovního institutu Vysoké školy Praha. Bankovní institut Vysoká škola a.s. je soukromá vysoká škola v České republice a v současné době má 6 poboček.

Autor v této práci velmi přívětivým způsobem přibližuje stav školní počítačové sítě. Koutecký (2014) uvádí, že propojené jsou pouze pobočky v Praze a Teplicích.

Práce se však postupně zabývá více technickým vybavením infrastruktury školní sítě a jeho podporou IPv6 a porovnáváním přechodových mechanismů.

6.6 Shrnutí podstatných poznatků z analýzy

Z analyzovaných akademických prací nelze převzít žádný poznatek nebo princip, který by bylo možné uplatnit při návrhu integrace protokolu IPv6 do univerzitní sítě MENDELU.

Primárně je to způsobeno skutečností, že počítačová síť Mendelovy univerzity v Brně je svojí složitostí zcela mimo rozsah sítí, které byly předloženy v analyzovaných závěrečných pracích. Žádný z autorů například neměl k dispozici globální směrovací IPv6 prefix v délce 48 bitů, který by umožňoval komplexnější přístup k návrhu adresního plánu IPv6 pro daný subjekt. Žádná ze sítí rovněž není připojena k ISP podobné velikosti, jako je CESNET z.s.p.o.

7 Analýza adresních plánů IPv6 na jiných univerzitách

Před zpracováním optimálního adresního plánu IPv6 pro počítačovou síť Mendelovy univerzity v Brně je rozumné analyzovat adresní plány IPv6 ostatních českých univerzit[5], jejichž ISP je rovněž provozovatel páteřní akademické sítě CESNET z.s.p.o. Touto analýzou mohou být odhaleny určité poznatky užitečné pro tvorbu adresního plánu IPv6 pro univerzitní síť MENDELU.

Jednotlivými zástupci významných českých univerzit byly poskytnuty informace o adresních plánech IPv6 v různé míře podrobností. Nicméně je zapotřebí klást důraz zejména na následující atributy adresních plánů IPv6 ostatních českých univerzit:

- Přidělený globální směrovací IPv6 prefix,
- způsob jeho rozdělení v rámci jednotlivých univerzitních sítí.

Není nezbytně nutné nahlížet na úplné detaily jednotlivých adresních plánů IPv6, protože každá univerzitní síť je vybudována jiným způsobem a v konečných detailech se budou vždy lišit.

7.1 České vysoké učení technické v Praze

Přidělený globální směrovací IPv6 prefix je `2001:718:2::/48`.

Vaněk (2010) uvádí, že jednotlivým lokalitám této univerzitní sítě jsou přidělovány síťové IPv6 prefixy o délce 56 bitů.

Na obr. 3 je znázorněno podrobné schéma adresního plánu IPv6 areálu Karlova náměstí v Praze, kde se nachází Fakulta elektrotechnická.

7.2 Masarykova univerzita

Přidělený globální směrovací IPv6 prefix je `2001:718:801::/48`.

Podle Rohledera (2012) je jednotlivým lokalitám přidělován prefix o délce 56 bitů. Koncovým sítím v nich obsaženým jsou následně poskytnuty prefixy o délce 64 bitů, resp. 60 bitů pro případné experimenty.

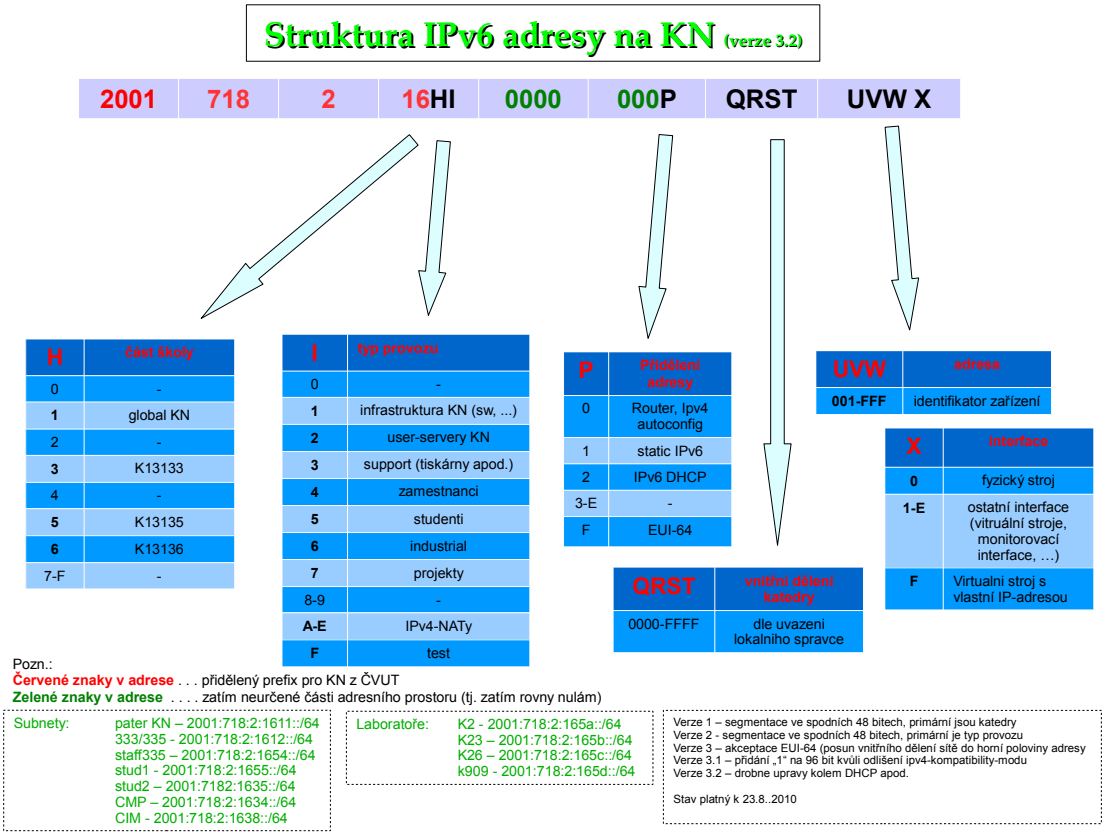
Rozhraní směrovače koncové sítě mají vždy staticky konfigurovanou IPv6 adresu ve tvaru `<globální prefix>:<prefix koncové sítě>::1`.

Je plánováno, že uživatelské stanice budou konfigurovány prostřednictvím bezstavového DHCPv6.

7.3 Slezská univerzita v Opavě

Přidělený globální směrovací IPv6 prefix je `2001:718:2201::/48`.

[5]Tyto informace byly získány na základě elektronické komunikace s odpovědnými zástupci jednotlivých českých univerzit a také z dokumentů dostupných na `http://archiv.cesnet.cz/ipv6/wg/`



Obr. 3: Schéma adresního plánu IPv6 Fakulty elektrotechnické ČVUT.

Žádné dělení na lokality se zde neprovádí. Macura (2010) uvádí, že jednotlivým koncovým sítím jsou přidělovány přímo prefixy o délce 64 bitů.

Ve čtvrtém oktetu IPv6 adresy jsou promítnuty číslice třetího bajtu IPv4 adresy. Například síti `193.84.208.0/24` je přidělen prefix `2001:718:2201:208::/64`.

Servery mají IPv6 adresy konfigurovány staticky.

7.4 Technická univerzita v Liberci

Přidělený globální směrovací IPv6 prefix je `2001:718:1c01::/48`.

Koncovým sítím jsou přidělovány prefixy délky 64 bitů. Jsou použita „vizuálně stejná“ čísla podsítí. Například síti `147.230.72.0/21` je přidělen IPv6 prefix `2001:718:1c01:72::/64`. (Satrapa, 2010)

Serverům jsou IPv6 adresy přidělovány staticky, uživatelským stanicím pak prostřednictvím bezstavového DHCPv6.

7.5 Vysoká škola báňská – Technická univerzita Ostrava

Přidělený globální směrovací IPv6 prefix je `2001:718:1001::/48`.

Každé lokalitě je přidělen prefix o délce 56 bitů. Jednotlivým koncovým sítím v nich obsaženým jsou následně přiřazeny prefixy dlouhé 64 bitů. (Pustka, 2010)

Servery jsou konfigurovány staticky. Uživatelské stanice získávají IPv6 konfiguraci prostřednictvím stavového DHCPv6.

7.6 Vysoké učení technické v Brně

Přidělený globální směrovací IPv6 prefix je `2001:718:802::/48`.

Podle Lampy (2009) jsou pro topologicky oddělené areály VUT v přiděleném adresním prostoru IPv6 rezervovány alokační bloky o délce síťového IPv6 prefixu 52–53 bitů (8–16 bloků délky 56 bitů). Tyto bloky jsou voleny tak, aby číselně odpovídaly stávajícímu přidělení síťových prefixů IPv4.

Fakulty a organizační jednotky srovnatelné velikosti mají přiděleny z rezervovaných alokačních bloků prefixy o délce 56 bitů podle dislokace fakulty.

Globálně směrované koncové sítě mají přiřazen síťový prefix délky 64 bitů.

Point–To–Point sítě propojující směrovače mají přidělen síťový prefix o délce 112 bitů. Tyto prefixy jsou alokovány ze společného rezervovaného bloku `2001:718:802:ffff::/64`. (Lampa, 2009)

7.7 Západočeská univerzita v Plzni

Přidělený globální směrovací IPv6 prefix je `2001:718:1801::/48`.

Kostěnec (2010) uvádí, že jednotlivým lokalitám univerzitní sítě ZČU jsou přiřazeny prefixy o délce 52 bitů.

IPv6 adresy na rozhraních mají tvar `2001:718:1801:LSSS::/64`, kde:

- `L` představuje lokalitu `1` až `F`,
- segment `S` odpovídá vizuálně IPv4.

Například k rozhraní s IPv4 adresou `147.228.1.70` bude přiřazena IPv6 adresa `2001:718:1801:1001::1:70`. (Kostěnec, 2010)

7.8 Shrnutí podstatných poznatků z analýzy

Provedenou analýzou adresních plánů IPv6 na jiných univerzitách byl získán zcela zásadní a velmi užitečný poznatek:

- Je-li konkrétní univerzitní síť rozdělena do lokalit, jsou přiřazovány síťové IPv6 prefixy nejdříve jim, a sice o délkách 52, 56 nebo 60 bitů. Až následně jsou koncovým sítím v nich obsaženým přiřazeny síťové prefixy IPv6 o délce 64 bitů.
- Není-li konkrétní univerzitní síť rozdělena do lokalit, jsou jednotlivým koncovým sítím přímo přiřazeny síťové prefixy IPv6 o délce 64 bitů.

8 Analýza současného stavu sítě MENDELU

V této kapitole je provedena podrobná analýza všech klíčových aspektů současného stavu univerzitní sítě MENDELU, jež se týkají síťové vrstvy (L3).

Předpokladem úspěšného zpracování analýzy současného stavu univerzitní sítě bylo poskytnutí některých fragmentů její dokumentace ze strany *Ústavu informačních technologií (ÚIT) MENDELU*. Tyto informace byly poskytnuty dne 15. 10. 2014 na základě podepsané dohody o zachování mlčenlivosti. Tímto aktem byl zároveň definován rozhodný den stavu počítačové sítě Mendelovy univerzity v Brně, na kterém je analýza provedena. Změny v univerzitní síti provedené po tomto dni nemají žádný dopad na principiální vlastnosti jejího provozu a především způsobů směrování, které podléhají analýze.

Pro potřeby analýzy byla Ústavem informačních technologií poskytnuta část dokumentace univerzitní sítě MENDELU, která popisuje:

- **Vnitřní část univerzitní sítě** – podklad pro analýzu topologie a směrování na páteři univerzitní sítě a v jejích lokalitách. Většina těchto lokalit je geograficky situována v univerzitním kampusu v Brně – Černých Polích na ulici Zemědělská. Další zainteresovanou lokalitou je geograficky vzdálená oblast Fakulty regionálního rozvoje a mezinárodních studií (FRRMS), která se nachází na ulici tř. Generála Píky (vzdálenost přibližně 1 km od univerzitního kampusu) v budově Z.
- **Perimetr univerzitní sítě** – podklad pro analýzu topologie a směrování na perimetru univerzitní sítě.
- **Připojení univerzitní sítě MENDELU k ISP** – podklad pro analýzu topologie a detailů směrování v rámci připojení univerzitní sítě MENDELU k poskytovateli internetových služeb (ISP).

8.1 Utajení citlivých informací

Vzhledem k povaze poskytnutých informací ze strany *ÚIT MENDELU* bylo rozhodnuto, že se v této diplomové práci nevyskytnou žádné skutečné identifikátory. Tímto omezením jsou dotčeny zejména IP adresy, identifikátory VLAN, identifikátory oblastí OSPF, identifikátory VRF apod. Primárním účelem tohoto rozhodnutí je zachování míry zabezpečení počítačové sítě Mendelovy univerzity v Brně.

V případě IP adres je v celé diplomové práci pro adresování všech L3 rozhraní na vnitřní straně hraničního směrovače univerzitní sítě MENDELU využíváno veřejného adresního rozsahu `195.178.72.0-195.178.80.255`. Privátní síťové prefixy jsou rovněž fiktivní, avšak je u nich zachována vazba na identifikátory VLAN (VID) stejným způsobem jako v produkční síti.

Identifikátory VLAN, OSPF oblastí, VRF apod. jsou pak zcela smyšlené.

8.2 Metodika provedení analýzy

Pro zpřehlednění postupu analýzy současného stavu je topologie univerzitní sítě MENDELU dekomponována na následující části: vnitřní univerzitní síť, perimetr univerzitní sítě, demilitarizovaná zóna a připojení univerzitní sítě k ISP. Každá tato komponenta topologie univerzitní sítě je analyzována zvlášť, zejména z hledisek topologie a směrování.

Účelem analýzy každé komponenty topologie univerzitní sítě MENDELU je získání informací o všech typech VLAN, které v ní existují. Získané typy VLAN jsou pro potřeby návrhu integrace IPv6 následně pojmenovány, protože každý z nich je vhodné v IPv6 adresovat jiným způsobem.

Z analýzy směrování síťového provozu v jednotlivých komponentách topologie univerzitní sítě jsou získány informace o způsobech směrování (statické, dynamické, výchozí) v jednotlivých částech univerzitní sítě a také záznamy ve směrovacích tabulkách zainteresovaných L3 prvků na perimetru a na páteři.

8.3 Geografické oblasti univerzitní sítě

Univerzitní síť MENDELU lze rozdělit do pěti geograficky oddělených oblastí:

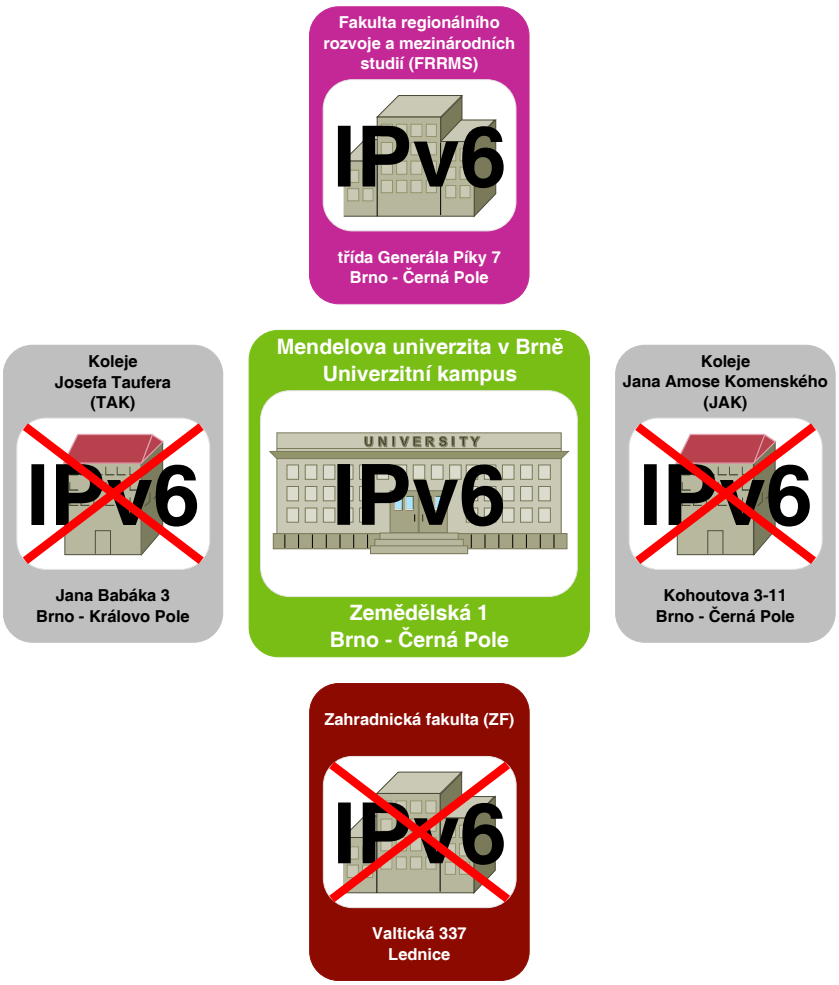
1. Kampus Mendelovy univerzity v Brně
2. Fakulta regionálního rozvoje a mezinárodních studií (FRRMS)
3. Zahradnická fakulta (ZF)
4. Koleje Jana Amose Komenského (JAK)
5. Koleje Josefa Taufera (TAK)

Jak znázorňuje obr. 4, integrace IPv6 je prozatím plánována pouze pro geografické oblasti kampus Mendelovy univerzity v Brně a Fakultu regionálního rozvoje a mezinárodních studií.

V ostatních oblastech se s nasazením IPv6 v krátkodobém časovém horizontu nepočítá, tudíž nejsou podrobeny analýze.

8.4 Ústřední logický L3 přepínač *Core*

Pro další postup analýzy současného stavu univerzitní sítě MENDELU je nezbytné vysvětlit některé detaily provozu jejího ústředního *logického* L3 přepínače s názvem **Core**.



Obr. 4: Geografické oblasti počítačové sítě Mendelovy univerzity v Brně. Pro „přeškrtnuté“ oblasti není prozatím nasazení IPv6 plánováno.

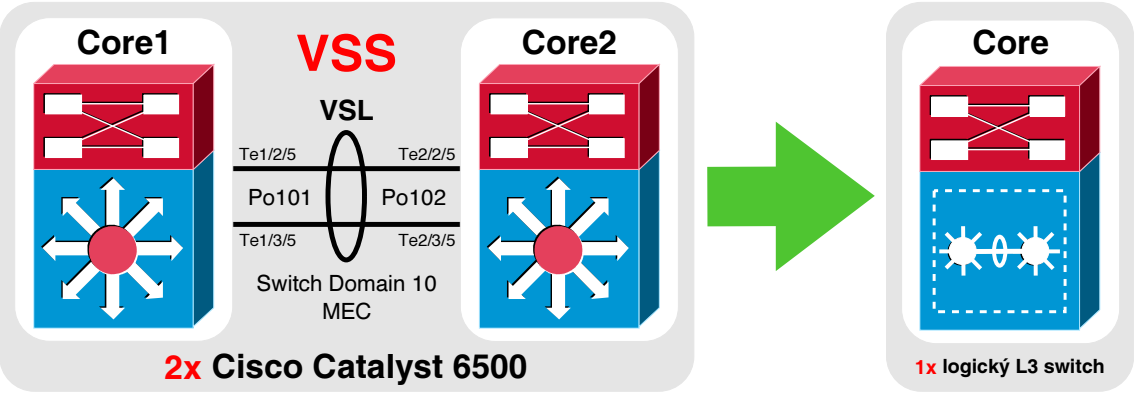
Virtual Switching System

Po *fyzické* stránce je *Core* tvořen dvojicí L3 přepínačů *Cisco Catalyst 6500 Series*. Touto platformou je podporována proprietární technologie společnosti Cisco nazvaná Virtual Switching System (VSS)[6].

Na obr. 5 je demonstrováno, že tyto dva fyzické L3 přepínače s názvy *Core1* a *Core2* jsou prostřednictvím VSS domény sloučeny jako jediný logický L3 přepínač s názvem *Core* s integrovanou správou fyzických zdrojů (například fyzická rozhraní obou L3 přepínačů se tváří, jako kdyby patřila jedinému zařízení). Z pohledu síťového návrhu může logický přepínač VSS domény obecně vystupovat v roli jediného L3 přepínače s výhodou redundance.

Fyzické propojení dvou zainteresovaných fyzických L3 přepínačů je realizováno prostřednictvím speciálního spoje Multichassis EtherChannel (MEC), který se v kon-

[6]Dalšími podporovanými platformami jsou *4500R* a *8500*. (Hucaby, 2015, s. 372)



Obr. 5: Fyzická a logická podoba ústředního L3 přepínače univerzitní sítě *Core*.

textu s VSS nazývá Virtual Switch Link (VSL). Toto propojení umožňuje jednomu z dvojice fyzických L3 přepínačů (například *Core1*) spravovat systémové prostředky partnera (*Core2*) dané VSS domény. Spoj VSL je sestaven ze dvou 10 Gbit rozhraní na každém z dvojice fyzických L3 přepínačů. Navíc každé z agregovaných fyzických rozhraní je umístěno v jiném slotu šasi. Tímto způsobem propojení je zajištěna maximální míra vysoké dostupnosti.

Virtual Routing and Forwarding

Na ústředním logickém L3 přepínači *Core* je nakonfigurováno několik virtuálních směrovacích instancí prostřednictvím virtualizační technologie VRF–lite[7]. K analýze univerzitní sítě MENDELU pro účely zpracování návrhu integrace IPv6 je zapotřebí uvést dva virtuální směrovače, které na *Core* existují:

1. **VRF CernaPole** – ústřední L3 prvek páteře univerzitní sítě.
2. **VRF Internet** – *hraniční směrovač* univerzitní sítě, kterým je připojena k ISP.

8.5 Vnitřní část univerzitní sítě

Páteř univerzitní sítě

Primárním účelem páteře univerzitní sítě MENDELU je spojení všech jejích koncových podsítí do jednoho logického celku.

Na páteři se nachází 9 aktivních L3 prvků (fyzické i virtuální), jejichž přehled je uveden v tab. 3. Většina z nich je fyzicky umístěna ve vybraných budovách kampusu

[7]Označení VRF–lite používá společnost Cisco pro provoz VRF bez MPLS (Multiprotocol Label Switching), což je technologie zcela mimo rámec této diplomové práce.

Mendelovy univerzity v Brně. Další se nachází v budově Z, v níž sídlí Fakulta regionálního rozvoje a mezinárodních studií geograficky vzdálená přibližně 1 km severně od univerzitního kampusu MENDELU.

Tab. 3: L3 prvky páteře univerzitní sítě MENDELU.

Fyzické umístění	**Název páteřního L3 prvku**
Budova X	*Core* – výhradně *VRF CernaPole*
Budova X	*Nexus2*
Budova A	*core–A*
Budova C	*core–C*
Budova B	*core–B*
Budova Q	*core–Q*
Budova E	*core–E*
Budova T	*core–T*
Budova Z	*core–Z*

Všechny uvedené páteřní L3 přepínače jsou připojeny k ústřednímu L3 přepínači *Core*. Páteř univerzitní sítě MENDELU je tak uspořádána do téměř čisté[8] hvězdicové topologie, jež je vyobrazena na obr. 6.

Ústředním L3 prvkem páteře je virtuální směrovač *VRF CernaPole*, který je zprovozněný na ústředním logickém L3 přepínači *Core*.

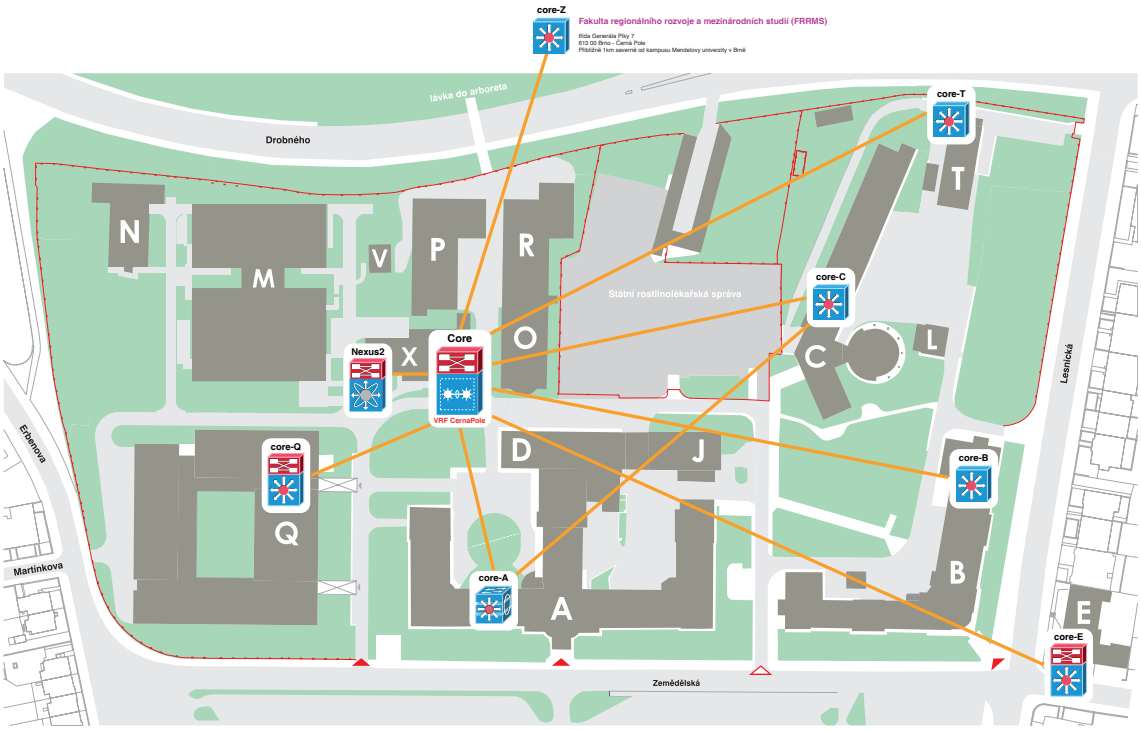
Všechny páteřní L3 přepínače jsou připojeny na ústřední L3 přepínač *Core* prostřednictvím spojů typu EtherChannel pracujícím na standardním protokolu LACP. Primárními účely konfigurace EtherChannelu je vysoká dostupnost a zvýšení propustnosti páteřních spojů. Na každém páteřním L3 přepínači je do EtherChannelu zahrnuta vždy dvojice fyzických rozhraní na každý páteřní spoj. Každá dvojice agregovaných fyzických rozhraní vytváří na každém páteřním L3 přepínači logické rozhraní nazývané PortChannel (Po). Tato logická rozhraní jsou konfigurována jako L2 trunky.

Fyzická rozhraní přímého spoje mezi páteřními L3 přepínači *core–A* a *core–C* jsou rovněž konfigurována jako L2 trunky.

Na těchto L2 trunk rozhraních je povolen provoz spojovacích (Point–To–Point) sítí, které budou nadále nazývány jako **páteřní VLAN**. Účelem tohoto typu VLAN je logické propojení všech L3 prvků páteře univerzitní sítě. V současnosti jich v univerzitní síti existuje celkem 9 a jejich VID jsou v intervalu **40** až **48**. Všechny *páteřní VLAN* mají délku síťového prefixu 30 bitů. IP adresy jsou následně přiřazeny k SVI *páteřních VLAN*, která se nacházejí na všech L3 prvcích páteře.

Popisovaná logická topologie páteře univerzitní sítě je znázorněna na obr. 7.

[8]Hvězdicová topologie je porušena přímým spojem mezi páteřními L3 přepínači *core–A* a *core–C*. Jedná se o „památku“ na předchozí topologii páteře univerzitní sítě, jenž byla uspořádána do kruhu. Podle posledních informací bude tento pozůstatek z předešlé topologie v dohledné době odstraněn.



Obr. 6: Plán kampusu Mendelovy univerzity v Brně s fyzickým rozmístěním L3 prvků páteře počítačové sítě. Podkladový materiál byl poskytnut *Stavebním oddělením PRO OK REK MENDELU*.

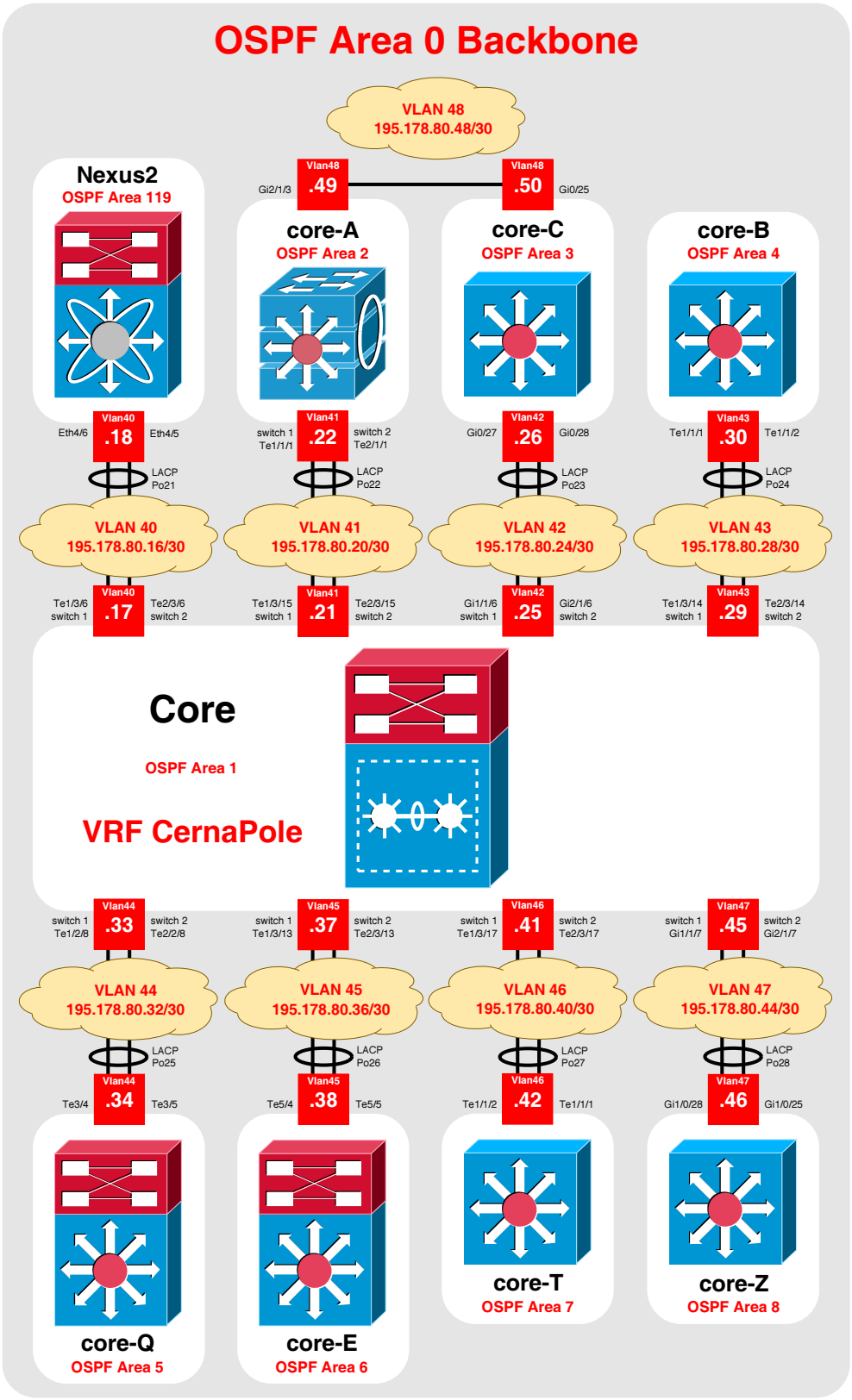
Lokality univerzitní sítě

Vnitřní část univerzitní sítě je rozdělena do devíti lokalit. Každá z nich je tvořena právě jedním L3 prvkem páteře. Je účelné jednotlivé lokality pojmenovat – ponesou vždy označení budovy, ve které se fyzicky nachází jejich přidružený páteřní L3 prvek. Přehled lokalit univerzitní sítě MENDELU je uveden tab. 4.

Některé lokality v sobě zahrnují více budov univerzitního kampusu. Jedná se o budovy, ve kterých není umístěn žádný páteřní L3 prvek, ale vyskytují se v nich L2 přepínače a koncové uzly připojené k univerzitní síti MENDELU. Mezi tyto budovy patří například *D*, *L*, *M* a další.

V jednotlivých lokalitách univerzitní sítě existují koncové sítě, které budou nadále nazývány jako **lokalitní VLAN**. Každý exemplář tohoto typu VLAN se vždy vyskytuje pouze v rámci jediné lokality – každá *lokalitní VLAN* existuje vždy pouze na jediném páteřním L3 prvku. Všechny páteřní L3 prvky mají pro připojené *lokalitní VLAN* vždy konfigurováno právě jedno SVI, které pro každou z nich slouží jako výchozí brána.

Vzhledem k velkému množství *lokalitních VLAN* v univerzitní síti jich bude v této diplomové práci prezentována pouze nepatrná část. Ukázková topologie vybraných lokalit s modelovými *lokalitními VLAN* je znázorněna na obr. 8.



Obr. 7: Logická topologie páteře univerzitní sítě MENDELU.

Tab. 4: Seznam lokalit univerzitní sítě MENDELU.

L3 prvek páteře	**Připojená lokalita**
VRF CernaPole	Lokalita **X**
Nexus2	Lokalita **X2**
core–A	Lokalita **A**
core–C	Lokalita **C**
core–B	Lokalita **B**
core–Q	Lokalita **Q**
core–E	Lokalita **E**
core–T	Lokalita **T**
core–Z	Lokalita **Z**

Směrování

Existují dva hlavní důvody, proč je zapotřebí procesu směrování ve vnitřní části univerzitní sítě:

1. Konektivita mezi koncovými uzly různých *lokalitních VLAN* (Inter–VLAN routing) v odlišných lokalitách,
2. konektivita mezi koncovými uzly *lokalitních VLAN* a uzly v DMZ a v Internetu.

Požadované konektivity je dosaženo tím, že se ve směrovacích tabulkách páteřních L3 prvků nachází záznamy:

- Všech *páteřních VLAN*,
- všech *lokalitních VLAN*,
- výchozí trasy.

Výchozí trasa

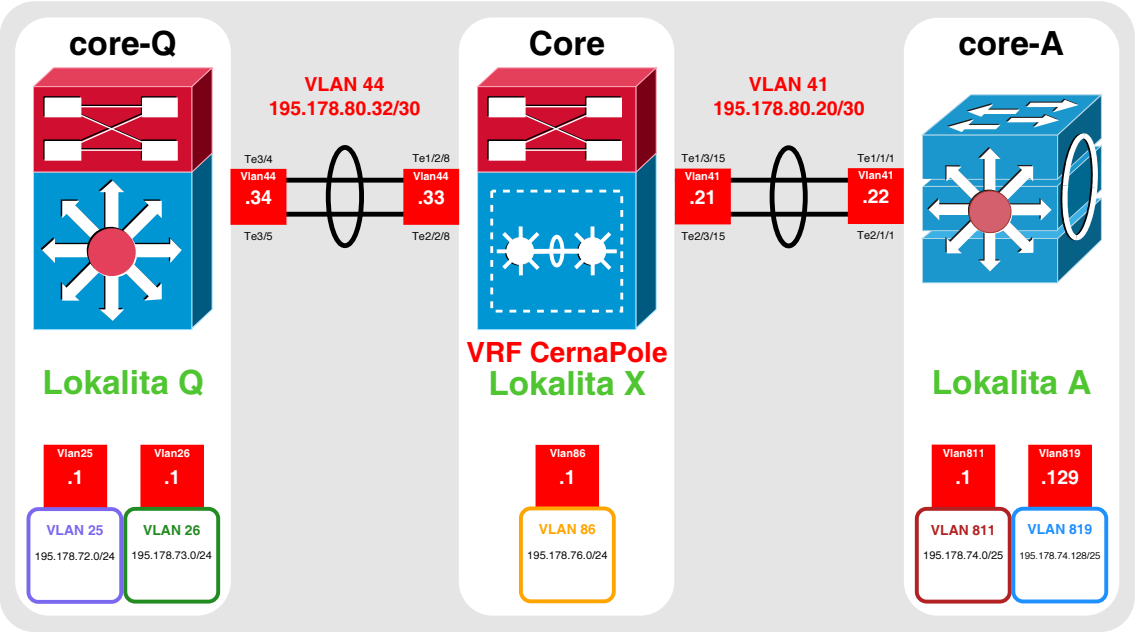
Ústřední směrovač páteře *VRF CernaPole* má ve své směrovací tabulce staticky uloženu výchozí trasu (default route), jejímž prostřednictvím je směrován veškerý síťový provoz z vnitřní části univerzitní sítě adresovaný uzlům v DMZ nebo v Internetu:

- `S* 0.0.0.0/0 [1/0] via 195.178.80.2`

Rozhraním dalšího přeskoku této výchozí trasy je inside rozhraní univerzitního firewallu s IP adresou `195.178.80.2`. Další detaily ohledně firewallu budou následovat v rámci analýzy perimetru univerzitní sítě MENDELU.

Provoz směrovacího protokolu OSPF

Ve vnitřní části univerzitní sítě MENDELU je nasazen směrovací protokol OSPF, který je primárně odpovědný za:



Obr. 8: Topologie vybraných lokalit s modelovými *lokalitními VLAN* univerzitní sítě MENDELU.

- Propagaci síťových prefixů *páteřních* a *lokalitních VLAN* mezi všemi L3 prvky páteře,
- propagaci výchozí trasy na všechny L3 prvky páteře,
- automatickou konvergenci univerzitní sítě při změně její topologie (například přidání nebo odebrání libovolné *páteřní* či *lokalitní* VLAN, selhání rozhraní apod.).

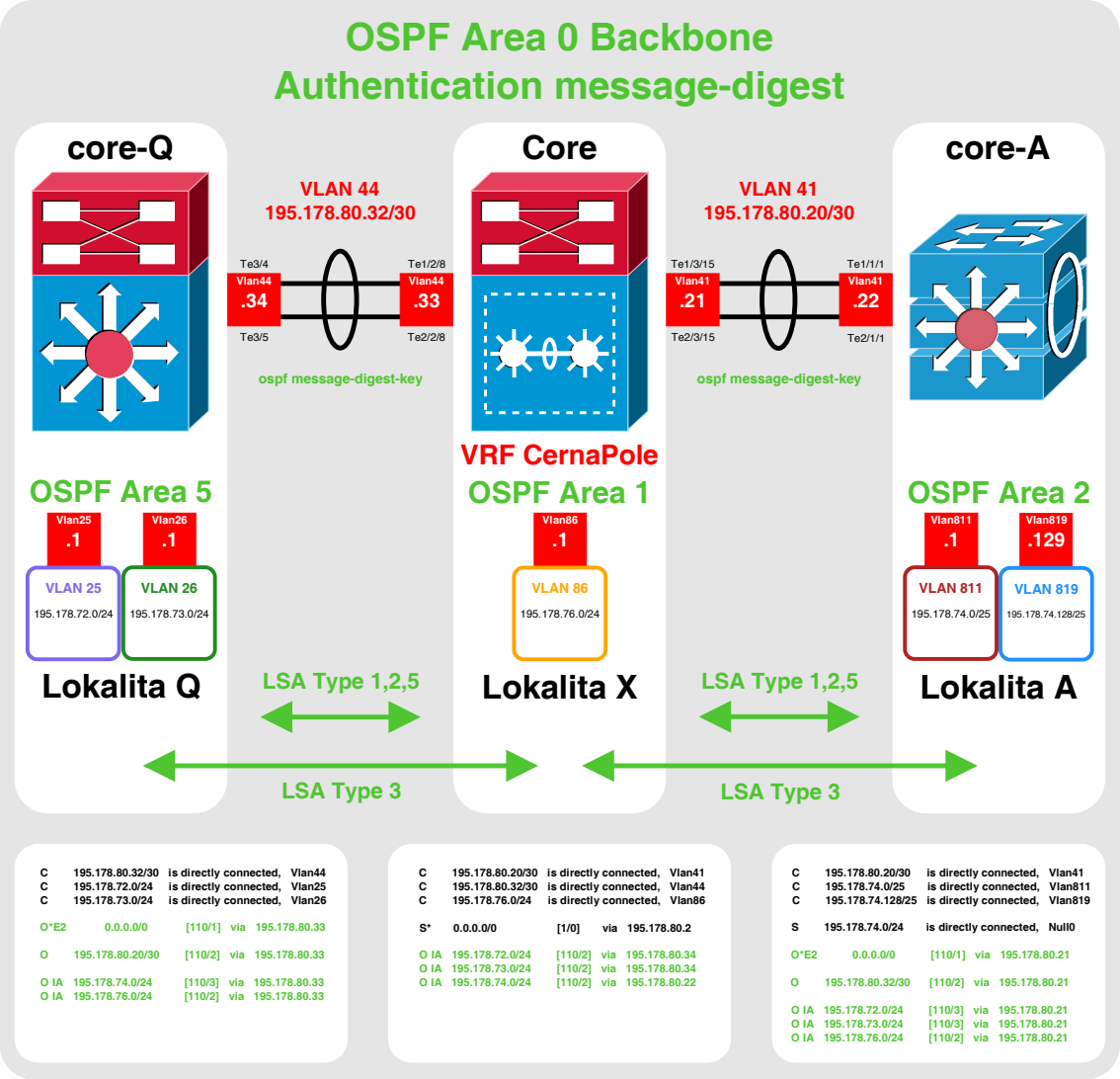
Princip dynamického směrování prostřednictvím směrovacího protokolu OSPF ve vnitřní části univerzitní sítě MENDELU komplexně znázorňuje na vybraných lokalitách obr. 9.

Vnitřní část univerzitní sítě MENDELU je rozdělena do 10 OSPF oblastí:

- Páteř je umístěna v oblasti 0 (páteřní oblast OSPF).
- Lokality jsou umístěny do svých spádových OSPF oblastí. Jejich přehled uvádí tab. 5.

Mezi výhody rozdělení univerzitní sítě do OSPF oblastí patří snížení provozní režie protokolu OSPF, urychlení konvergence a omezení případné nestability sítě pouze na postiženou oblast.

Téměř všechny páteřní L3 prvky univerzitní sítě mají právě jednoho přilehlého souseda – ústřední směrovač *VRF CernaPole*. Je to dáno uspořádáním *páteřních*



Obr. 9: Směrování ve vnitřní části univerzitní sítě MENDELU prostřednictvím OSPF.

VLAN, v nichž jsou vždy zahrnuty právě dva L3 prvky páteře. Výjimku tvoří páteřní L3 prvky *core–A* a *core–C*, protože jsou navíc propojeny přímo mezi sebou a jsou si tak vzájemně přilehlými sousedy.

Všechna SVI *páteřních VLAN* jsou na páteřních L3 prvcích umístěna do oblasti 0 a všechna SVI *lokalitních VLAN* do svých spádových OSPF oblastí. L3 prvky páteře tak vystupují jako hraniční směrovače oblasti (ABR).

Páteřní L3 prvky si vzájemně vyměňují své topologické databáze, které obsahují směrovací informace *páteřních VLAN*, *lokalitní VLAN* a výchozí trasy, kterou propaguje ústřední směrovač páteře *VRF CernaPole*. Tyto informace si páteřní L3 prvky mezi sebou vyměňují prostřednictvím OSPF zpráv LSA, přičemž:

Tab. 5: Seznam lokalit a přidružených OSPF oblastí.

Lokalita	OSPF oblast
X	1
X2	119
A	2
C	3
B	4
Q	5
E	6
T	7
Z	8

- Prefixy *páteřních VLAN* jsou získávány na základě zpráv LSA typu 1 (Router LSA) a 2 (Network LSA; Intra–Area),
- prefixy *lokalitních VLAN* jsou přímo obsaženy ve zprávách LSA typu 3 (Inter–Area),
- prefix *výchozí trasy* je přímo obsažen ve zprávách LSA typu 5 jako externí trasa typu E2.

Interní metrika OSPF

Interní metrikou OSPF je součet cen všech odchozích rozhraní konkrétní cesty do cílové sítě.

Směrovací protokol OSPF určuje cenu (cost) každého rozhraní podle vzorce:

$$Cost = \frac{ReferenceBandwidth}{InterfaceBandwidth}$$

Výchozí hodnota OSPF ReferenceBandwidth je u zařízení Cisco rovna 10^8. Tuto hodnotu lze případně změnit, ale zpravidla by měly mít všechny zainteresované L3 prvky tuto hodnotu shodnou.

Hodnota InterfaceBandwidth je totožná s atributem bandwidth, který je definován u každého rozhraní. U fyzických rozhraní vychází z jejich skutečné šířky pásma. Například fyzické 10 Gbit rozhraní má tuto hodnotu rovnu 10^{10}.

Směrovací protokol OSPF však v případě univerzitní sítě nemá žádné informace o fyzických rozhraních L3 prvků páteře, protože do procesu OSPF jsou zahrnuta pouze SVI *páteřních VLAN*. Pokud není nastaveno jinak, všechna logická rozhraní mají hodnotu bandwidth rovnu 10^9. Z toho plyne, že všechna rozhraní zahrnutá do procesu OSPF v univerzitní síti MENDELU mají stejnou cenu, ačkoli jsou některé spoje složeny z 1 Gbit fyzických rozhraní a jiné z 10 Gbit fyzických rozhraní.

Výsledky všech výpočtů cen SVI *páteřních VLAN* jsou rovny 0,1. Minimální hodnota ceny rozhraní v OSPF je však 1. Všechna SVI *páteřních VLAN* tak mají cenu rovnu **1**.

Sumarizace síťových prefixů *lokalitních VLAN*

Na obr. 9 je dále naznačena sumarizace síťových prefixů *lokalitních VLAN* 811 a 819 v lokalitě A. Jejich síťové prefixy `195.178.74.0/25` a `195.178.74.128/25` byly sumarizovány[9] pod jediný souhrnný síťový prefix `195.178.74.0/24`, pod nímž jsou tyto dvě *lokalitní VLAN* prostřednictvím OSPF propagovány všem ostatním L3 prvkům páteře univerzitní sítě. Na každém z nich je tímto způsobem v případě těchto dvou *lokalitních VLAN* ušetřen jeden záznam ve směrovací tabulce. V produkční univerzitní síti se principu sumarizace síťových prefixů využívá všude, kde to situace umožňuje.

Zároveň je k síťovému prefixu souhrnné trasy ve směrovací tabulce propagujícího L3 prvku uveden statický záznam tzv. discard route, jehož odchozím rozhraním je logické rozhraní `Null0`:

- `S 195.178.74.0/24 is directly connected, Null0`

Tímto záznamem je zamezeno bloudění paketů v L3 smyčce v případě, že jeden z dílčích síťových prefixů souhrnné trasy přestane být využíván (například dojde k odstranění jedné ze zmíněných *lokalitních VLAN*).

Autentizace OSPF

Účelem vzájemné OSPF autentizace přilehlých L3 prvků je zamezení podvržení falešných zpráv LSA z jiného zdroje. Každá zpráva LSA obsahuje MD5 otisk předem definovaného řetězce, který se musí na rozhraních přilehlých sousedů shodovat. Neshodují-li se, jsou podvržené LSA zprávy likvidovány.

V univerzitní síti je OSPF autentizace aktivována pro celou páteřní oblast 0 a na SVI všech *páteřních VLAN*.

8.6 Perimetr univerzitní sítě

Účelem uspořádání perimetru univerzitní sítě MENDELU je bezpečné oddělení jejího vnitřního, relativně bezpečného, prostředí od veřejného a potenciálně nebezpečného prostředí Internetu.

Perimetr obecně rozděluje síť do tzv. bezpečnostních domén, které jsou propojeny prostřednictvím firewallu.

V univerzitní síti MENDELU se vyskytují dvě kategorie uzlů:

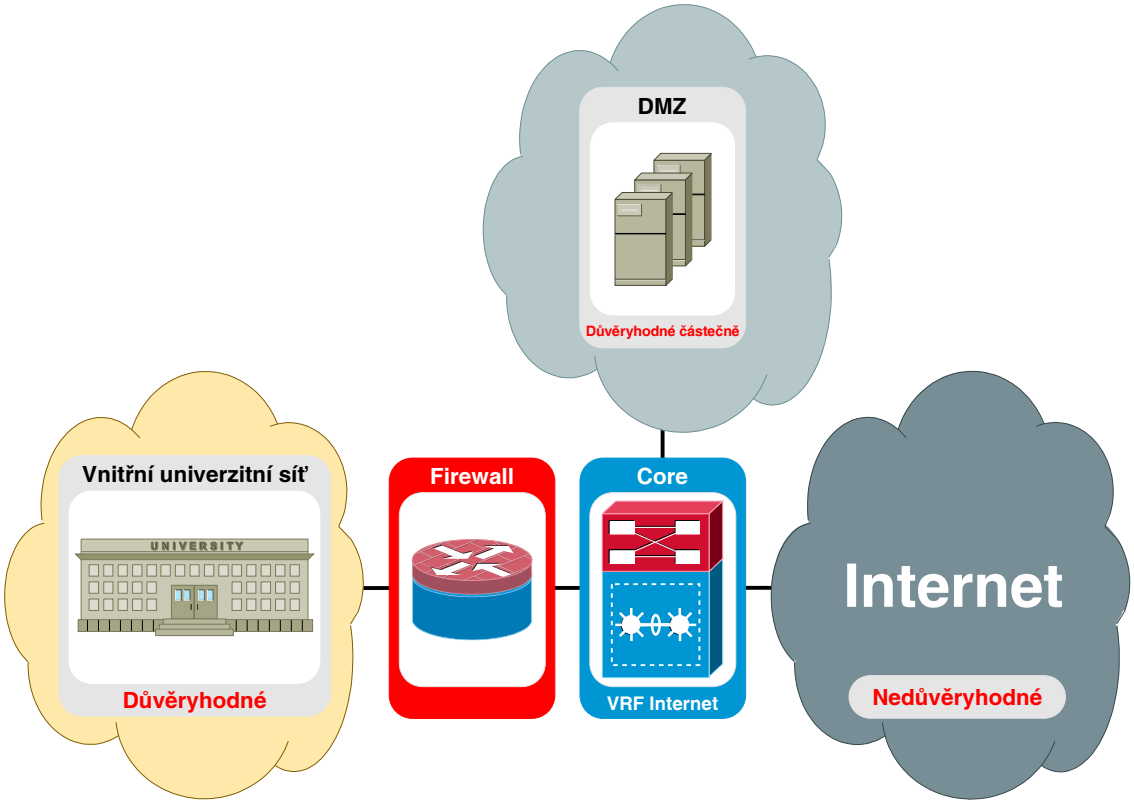
- Nedostupné z veřejného Internetu – například notebooky studentů,
- dostupné z veřejného Internetu – například univerzitní webový server.

Univerzitní síť je tak na perimetru rozdělena do 3 bezpečnostních domén:

[9] K vytváření souhrnných tras lze použít přívětivou webovou aplikaci dostupnou na `http://www.netmatics.net/IPv4Calcs/SupernetCalculator.aspx`

1. **Vnitřní univerzitní síť**, kde jsou umístěny všechny uzly nedostupné z veřejného Internetu.
2. **Demilitarizovaná zóna (DMZ)**, kde jsou umístěny všechny uzly dostupné z veřejného Internetu.
3. **Internet**, kde se nachází všechny uzly mimo univerzitní síť MENDELU.

Schématické rozdělení univerzitní sítě MENDELU do bezpečnostních domén znázorňuje obr. 10. Zároveň je zde uvedena míra důvěryhodnosti síťových uzlů v jednotlivých bezpečnostních doménách.



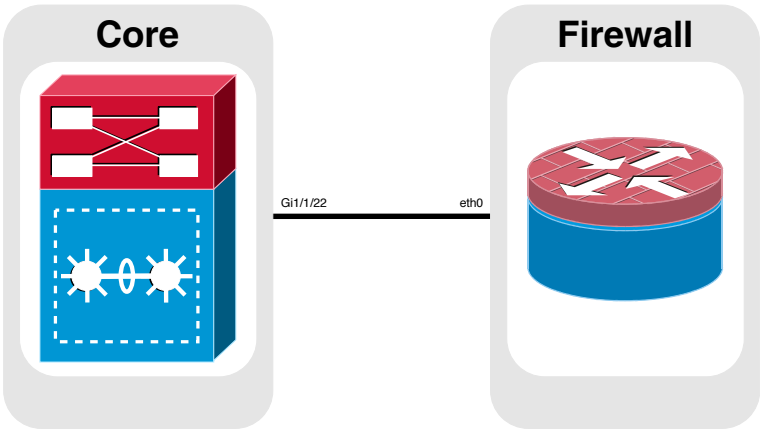
Obr. 10: Bezpečnostní domény perimetru univerzitní sítě MENDELU.

Komunikace síťových uzlů mezi bezpečnostní doménou *vnitřní univerzitní síť* a bezpečnostními doménami *demilitarizovaná zóna* a *Internet* probíhá výhradně prostřednictvím univerzitního firewallu, který je odpovědný za uplatňování bezpečnostní politiky na perimetru univerzitní sítě MENDELU.

Účel umístění uzlů univerzitní sítě dostupných z veřejného Internetu do zvláštní bezpečnostní domény DMZ spočívá v tom smyslu, že při vnějším útoku na některý z těchto uzlů, není narušena bezpečnost uzlů ve vnitřní části univerzitní sítě.

Topologie

Fyzická topologie perimetru univerzitní sítě zahrnuje logický ústřední L3 přepínač *Core* a univerzitní firewall. Je znázorněna na obr. 11.



Obr. 11: Fyzická topologie perimetru univerzitní sítě MENDELU.

Univerzitní firewall je zařízení, na kterém běží operační systém Linux, distribuce CentOS. Tento aktivní prvek bude nadále nazýván jako **Firewall**. Na tomto stroji je nakonfigurován nástroj iptables, jenž slouží pro definici pravidel firewallu v jádře tohoto operačního systému.

Logická topologie perimetru univerzitní sítě je tvořena virtuálními směrovači VRF *CernaPole* a VRF *Internet*, které jsou zprovozněny na logickém ústředním L3 přepínači *Core*, a *Firewallem*, který se nachází mezi nimi. Logická topologie perimetru univerzitní sítě MENDELU je znázorněna na obr. 12.

Všechny tři uvedené aktivní L3 prvky na perimetru jsou propojeny prostřednictvím dvou virtuálních sítí, které budou nadále nazývány jako **perimetrové VLAN**:

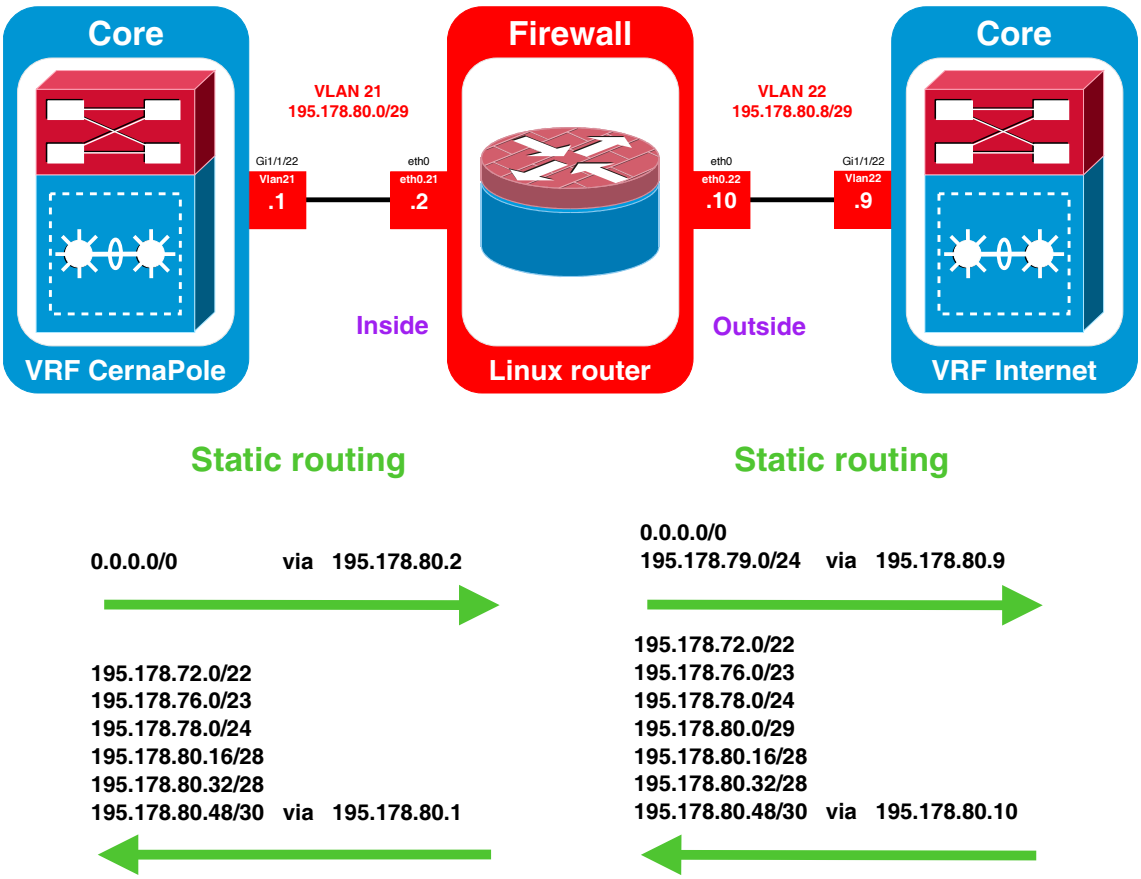
- VLAN **21** s prefixem `195.178.80.0/29` spojuje *Firewall* a *VRF CernaPole*,
- VLAN **22** s prefixem `195.178.80.8/29` spojuje *Firewall* a *VRF Internet*.

Směrování

Směrovače na perimetru univerzitní sítě směrují síťový provoz prostřednictvím statických tras. Toto statické směrování rovněž demonstruje obr. 12.

Hraniční směrovač univerzitní sítě *VRF Internet* obsahuje ve své směrovací tabulce statické záznamy souhrnných síťových prefixů, kterými jsou adresovány všechny VLAN existující v univerzitní síti MENDELU. Odchozím rozhraním těchto statických tras je outside rozhraní *Firewallu* `eth0.22` s IP adresou `195.178.80.10`.

Jediným statickým záznamem směrovací tabulky ústředního směrovače páteře univerzitní sítě *VRF CernaPole* je výchozí trasa, jejímž prostřednictvím je směrován



Obr. 12: Logická topologie a statické směrování perimetru univerzitní sítě MENDELU.

veškerý síťový provoz z vnitřní univerzitní sítě určený uzlům v DMZ nebo v Internetu. Odchozím rozhraním této výchozí trasy je inside rozhraní *Firewallu* `eth0.21` s IP adresou `195.178.80.2`.

Firewall směruje síťový provoz adresovaný uzlům ve vnitřní univerzitní síti na základě statických záznamů se souhrnnými prefixy *páteřních* a *lokalitních VLAN*. IP adresa dalšího přeskoku je `195.178.80.1`, což je SVI `Vlan21` směrovače *VRF CernaPole*.

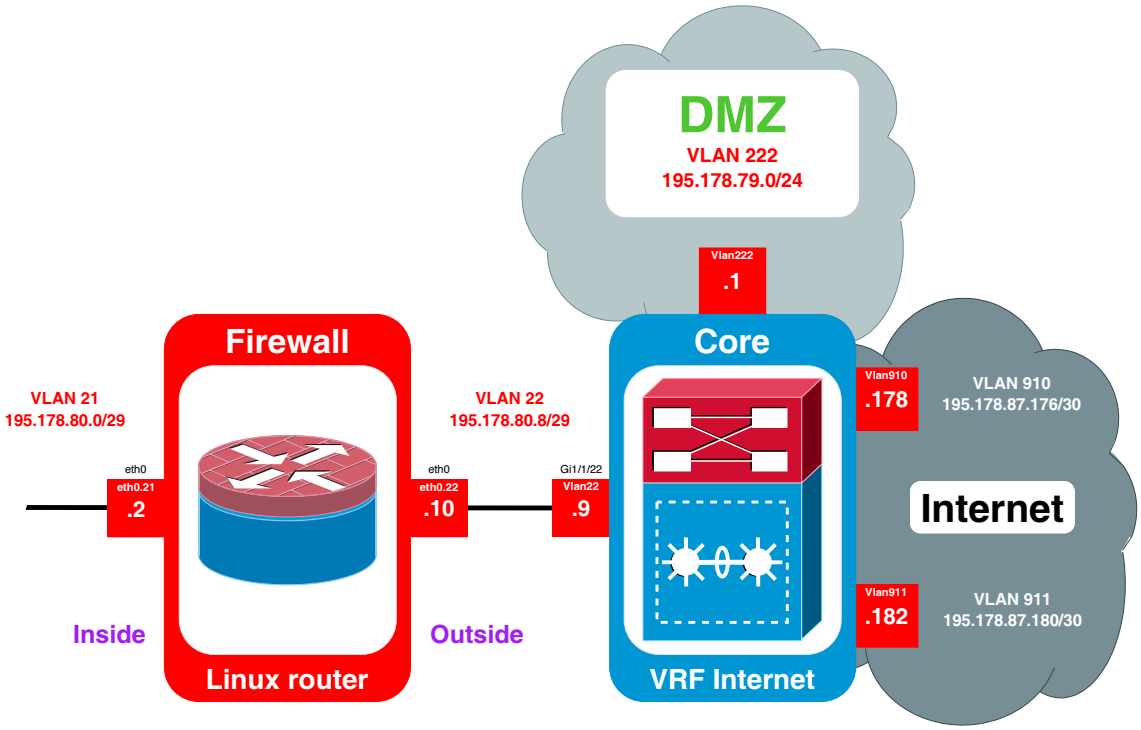
Směrovací tabulka *Firewallu* rovněž obsahuje statické záznamy s prefixy výchozí trasy a *demilitarizované VLAN*, jejichž prostřednictvím je směrován síťový provoz adresovaný uzlům v DMZ a v Internetu. IP adresa dalšího přeskoku je `195.178.80.9` náležící SVI `Vlan22` na hraničním směrovači *VRF Internet*.

8.7 Demilitarizovaná zóna

DMZ je realizována jako VLAN **222**, která je přímo připojená k hraničnímu směrovači *VRF Internet* a nachází se tak na vnější straně (outside) *Firewallu*. Tato VLAN bude nadále nazývána jako **demilitarizovaná VLAN**.

Síťový prefix *demilitarizované VLAN* 222 je `195.178.79.0/24` a její výchozí bránou je SVI `Vlan222` na hraničním směrovači *VRF Internet* s IP adresou `195.178.79.1`.

Umístění DMZ v části topologie perimetru univerzitní sítě MENDELU je znázorněno na obr. 13.



Obr. 13: Umístění DMZ v části topologie perimetru univerzitní sítě MENDELU.

V *demilitarizované VLAN* jsou umístěny uzly, u kterých je vyžadována přímá dostupnost z Internetu. Komunikace uzlů v DMZ s uzly ve vnitřní části univerzitní sítě je však kvůli bezpečnosti omezena prostřednictvím *Firewallu*.

8.8 End–To–End VLAN

V univerzitní síti MENDELU se vyskytuje určité množství VLAN, které jsou prostřednictvím L2 trunků rozprostřeny po následujících částech univerzitní sítě:

- Vnitřní univerzitní síť – stejná L2 trunk rozhraní jako *páteřní* a *lokalitní VLAN*,
- perimetr – stejná L2 trunk rozhraní jako *perimetrové VLAN*,
- DMZ – stejná L2 trunk rozhraní jako *demilitarizovaná VLAN* 222.

Tento typ sítí je označen jako **End–To–End VLAN**.

Z dosud představených typů VLAN jsou *End–To–End VLAN* jediné, které jsou adresovány privátními síťovými prefixy specifikovanými v RFC 1918:

- `10.0.0.0-10.255.255.255` (prefix `10.0.0.0/8`)
- `172.16.0.0-172.31.255.255` (prefix `172.16.0.0/12`)
- `192.168.0.0-192.168.255.255` (prefix `192.168.0.0/16`)

Výchozí bránou každé *End–To–End VLAN* je jejich SVI nacházející se na *Firewallu*[10], kde je pro ně zároveň zprovozněn NAT, resp. varianta PAT, která umožňuje sdílení jediné veřejné IP adresy teoreticky více než 60000 hostitelům.

Mezi dobře známé *End–To–End VLAN* univerzitní sítě MENDELU patří například bezdrátová síť Eduroam, jejímž prostřednictvím mohou studenti získat konektivitu s uzly v Internetu pro svá soukromá přenosná zařízení (notebooky, chytré telefony apod.).

Na obr. 14 je vyobrazena částečně zjednodušená topologie modelové *End–To–End VLAN* **114** se smyšleným síťovým prefixem `10.10.14.0/23`. Podstatné je zejména SVI `eth0.114` umístěné na *Firewallu*.

8.9 Správa aktivních prvků infrastruktury univerzitní sítě

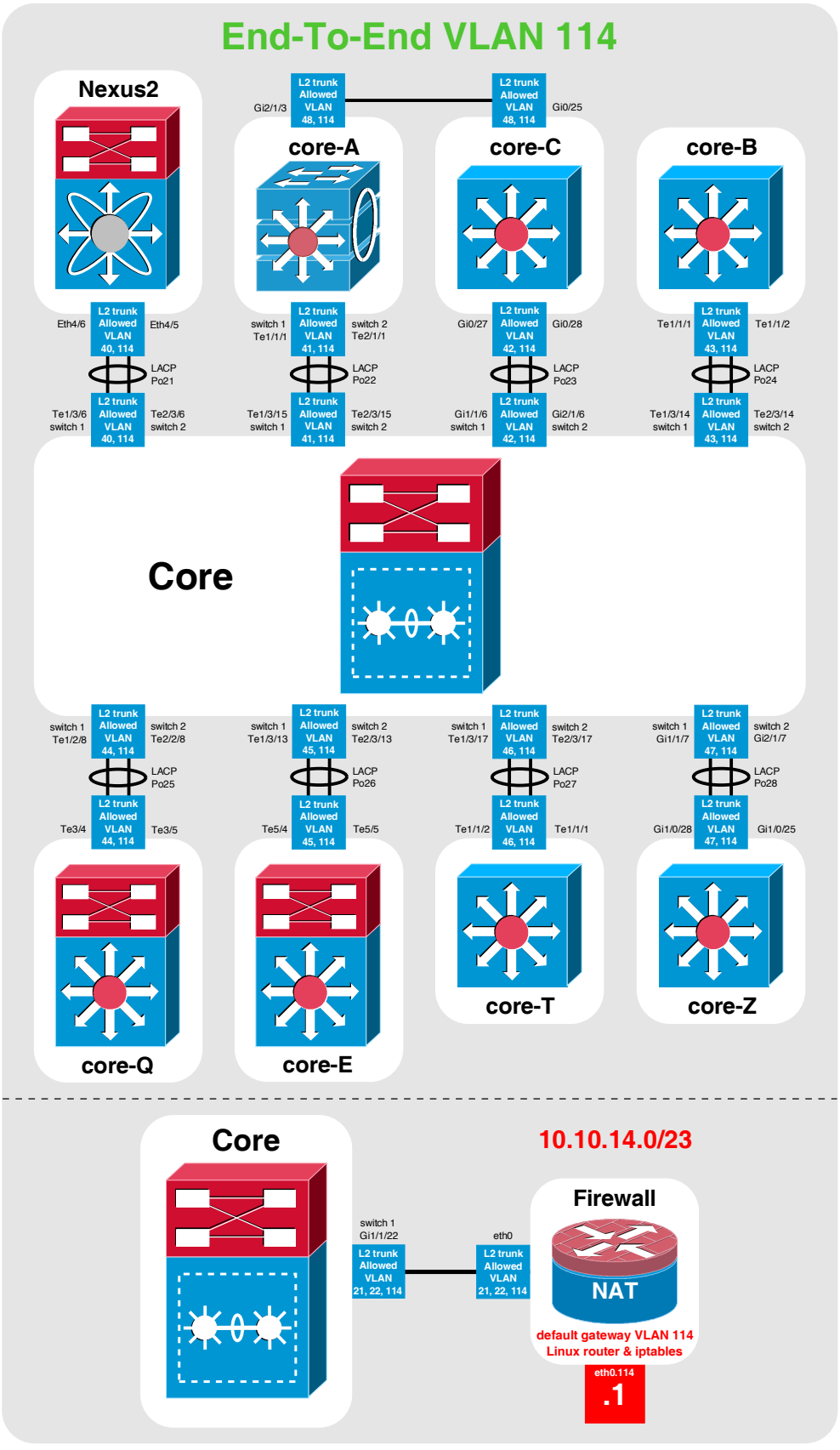
Všechny aktivní prvky (zejména L2 a L3 přepínače Cisco *Catalyst*) univerzitní sítě jsou zahrnuty do speciální VLAN, jejímž prostřednictvím mohou být vzdáleně spravovány. Tento typ zvláštní virtuální sítě bude označen jako **správní VLAN** (VLAN pro síťový management). Její fiktivní VID je **171**. Tato síť je zcela oddělena od všech ostatních VLAN univerzitní sítě.

Správní VLAN je rozprostřena po celé univerzitní síti stejným způsobem jako *End–To–End VLAN*. Podstatným rozdílem je však skutečnost, že každý aktivní prvek infrastruktury univerzitní sítě má nakonfigurováno SVI *správní VLAN*, k němuž je staticky přiřazena IP adresa z privátního rozsahu `10.7.1.0/23` (u páteřních L3 prvků je jejich IP adresa *správní VLAN* zároveň Router ID v rámci směrovacího protokolu OSPF).

Výchozí bránou je zvláštní server s OS Linux, ze kterého lze jednotlivé aktivní prvky vzdáleně spravovat prostřednictvím protokolů Telnet (nezabezpečená komunikace) nebo SSH (šifrovaná komunikace). Tento stroj je pro infrastrukturní aktivní prvky zároveň NTP serverem.

Konfigurace SVI *správní VLAN* a přiřazení IP adresy zapříčiní minimálně u L3 prvků páteře univerzitní sítě, že se síťový prefix *správní VLAN* ocitne v jejich směrovacích tabulkách jako přímo připojená síť. Je však krajně nebezpečné, aby do *správní VLAN* byla povolena komunikace z uzlů všech ostatních VLAN univerzitní sítě. Proto je nezbytné takovou komunikaci filtrovat prostřednictvím přístupových seznamů (ACL).

[10]Jedná se o určité zjednodušení skutečnosti, protože některé *End–To–End VLAN* v produkční univerzitní síti mají výchozí bránu na jiném firewallu, než je hlavní univerzitní *Firewall* na perimetru, který byl představen. Toto zjednodušení neovlivňuje podstatu této diplomové práce.

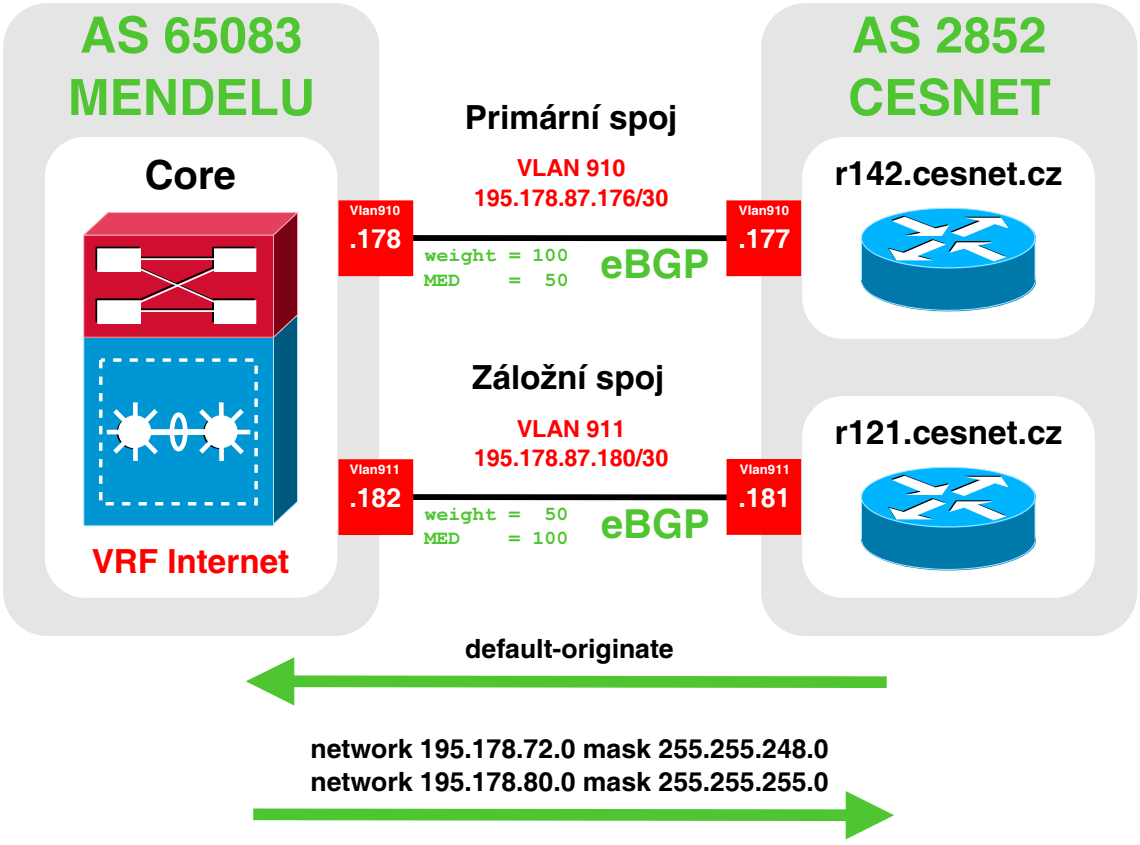


Obr. 14: Zjednodušená topologie modelové End–To–End VLAN 114.

8.10 Připojení univerzitní sítě MENDELU k ISP

Počítačová síť Mendelovy univerzity v Brně je připojena k páteřní akademické počítačové síti České republiky, jejímž provozovatelem je sdružení **CESNET z.s.p.o.**[11] Tento subjekt je zároveň poskytovatelem internetových služeb (ISP) Mendelovy univerzity v Brně.

Topologie



Obr. 15: Topologie připojení univerzitní sítě MENDELU k ISP.

Univerzitní síť MENDELU je k ISP připojena prostřednictvím dvou fyzických 10 Gbit dvoubodových (Point–To–Point) spojů. Oba tyto spoje jsou na straně univerzitní sítě připojeny do ústředních L3 přepínačů *Core1* a *Core2* (jak již bylo řečeno, dohromady tvoří jediný logický L3 přepínač s názvem *Core*). Na straně ISP pak vedou ke dvěma zcela nezávislým fyzickým směrovačům pojmenovaným *r142.cesnet.cz (R142)* a *r121.cesnet.cz (R121)*. Celou situaci znázorňuje obr. 15. Tato topologie je

[11] Jedná se o sdružení, které bylo založeno vysokými školami a Akademií věd České republiky v roce 1996. Další informace jsou dostupné na `http://www.cesnet.cz`

označována jako *dual–homed* a její hlavní výhoda spočívá v zamezení ztráty konektivity s ISP v případě selhání kterékoli komponenty některého ze spojů (zařízení, rozhraní, optický kabel apod.). V topologii připojení univerzitní sítě MENDELU a ISP je spoj mezi *Core* a *R142* zvolen jako primární a spoj mezi *Core* a *R121* jako záložní.

Fyzická rozhraní obou spojů jsou nakonfigurována jako L2 trunky, u nichž je povolen provoz **spojovacích VLAN 910** a **911**. IP adresy jsou pak přiřazeny k SVI těchto VLAN (`Vlan910` a `Vlan911`). Na straně *Core* jsou obě SVI přiřazena k virtuálnímu směrovači *VRF Internet*. Obě *spojovací VLAN* mají délku síťového prefixu 30 bitů (Point–To–Point VLAN).

Poskytnuté veřejné síťové prefixy

Mendelově univerzitě v Brně bylo ze strany ISP přiděleno množství veřejných síťových IPv4 prefixů. Jak již bylo uvedeno v sekci *Utajení citlivých informací*, bude v této diplomové práci z tohoto množství prezentována pouze nepatrná část. Hierarchie poskytnutí tohoto veřejného adresního prostoru je znázorněna v tab. 6, přičemž:

- *RIPE NCC* vystupuje v roli regionálního registru, RIR,
- *CESNET* (ISP) představuje lokální registr, LIR,
- *MENDELU* je koncovým subjektem.

Tab. 6: Část veřejných síťových prefixů IPv4 poskytnutých univerzitní síti MENDELU.

RIPE NCC	CESNET	MENDELU
`195.0.0.0/8`	`195.178.64.0/19`	`195.178.72.0/21`
		`195.178.80.0/24`

Provoz směrovacího protokolu BGP

Hraniční směrovač univerzitní sítě *VRF Internet* je umístěn do privátního autonomního systému s ASN 65083. Oba styčné směrovače ISP *R142* a *R121* spadají do veřejného autonomního systému s ASN 2852.

Síťové prefixy do cílových destinací jsou mezi hraničními směrovači AS univerzitní sítě a ISP propagovány dynamicky prostřednictvím směrovacího protokolu BGP. Proces BGP je v případě logického L3 přepínače *Core* konfigurován pouze pro směrovací instanci *VRF Internet*.

Sousední dvojice směrovačů – *VRF Internet* s *R142* a *VRF Internet* s *R121* – jsou v relaci sousedství typu eBGP, protože *VRF Internet* je umístěn v jiném autonomním systému, než směrovače ISP *R142* a *R121*.

Směrovače ISP *R142* a *R121* jsou nakonfigurovány tak, že prostřednictvím zpráv BGP Update propagují na *VRF Internet* výchozí trasu (default route), jejímž prostřednictvím lze směrovat síťový provoz do vzdálených cílových destinací, jenž nejsou uvedeny ve směrovací tabulce *VRF Internet* (například veřejné síťové prefixy společnosti Google Inc.).

Zprávy BGP Update s propagací výchozí trasy jsou posílány oběma směrovači ISP *R142* a *R121* současně. Hraniční směrovač *VRF Internet* na straně univerzitní sítě je nakonfigurován tak, že trasu propagovanou směrovačem *R142* upřednostňuje. Je to dáno konfigurací BGP atributu *weight*. Hodnoty atributu weight jsou přiřazeny k obdrženým trasám do cílových sítí podle toho, od jakého sousedního směrovače byly přijaty. V případě atributu weight je zvolena trasa s vyšší hodnotou. Ve směrovací tabulce *VRF Internet* je tak uveden záznam:

- `B* 0.0.0.0/0 [20/0] via 195.178.87.177`

`195.178.87.177` je IP adresa L3 rozhraní směrovače *R142*, který je prostřednictvím vyšší hodnoty BGP atributu weight upřednostněn.

Kromě výchozí trasy není žádný další prefix ze strany ISP prostřednictvím BGP do univerzitní sítě MENDELU propagován.

Hraniční směrovač univerzitní sítě *VRF Internet* propaguje směrovačům ISP *R142* a *R121* prostřednictvím zpráv BGP Update všechny veřejné síťové prefixy, jimiž univerzitní síť MENDELU disponuje. Tyto zprávy jsou posílány oběma sousedním směrovačům ISP současně. Je nezbytné, aby oba styčné směrovače ISP upřednostňovaly zvolený primární spoj mezi sousedy *VRF Internet* a *R142* (VLAN 910). Toho je dosaženo prostřednictvím konfigurace BGP atributu *MED*.

Na záložním spoji mezi směrovači *VRF Internet* a *R121* (VLAN 911) se za normálních okolností vyskytují pouze zprávy BGP Update. Zásluhou směrovacího protokolu BGP bude na tento záložní spoj automaticky přeřazen síťový provoz mezi MENDELU a ISP v případě selhání kterékoli komponenty primárního spoje.

8.11 Spanning Tree Protocol

STP je záležitostí linkové vrstvy (L2). Jeho analýza je ovšem důležitá pro pozdější vytvoření modelu univerzitní sítě, jehož prostřednictvím bude verifikován návrh integrace IPv6 do univerzitní sítě MENDELU.

V současnosti se v univerzitní síti MENDELU nachází jediná L2 smyčka, která je způsobena přímým spojem mezi páteřními L3 přepínači *core–A* a *core–C*.

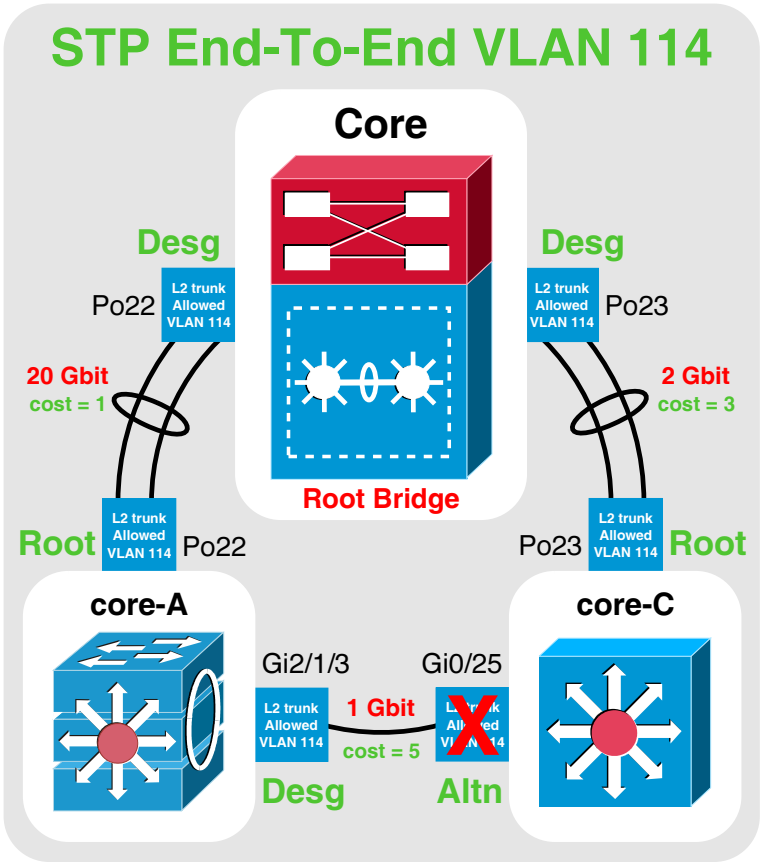
V univerzitní síti je konfigurována proprietární implementace STP od společnosti Cisco Rapid PVST+. Největší výhodou tohoto řešení je možnost konfigurace instancí STP pro jednotlivé VLAN. Na L3 přepínačích páteře je tak vytvořeno několik instancí STP – pro každou VLAN jedna.

STP je konfigurován pro několik typů VLAN představených v dosavadním průběhu analýzy. Avšak nejdůležitějším typem VLAN, pro které jsou vytvořeny instance STP, jsou *End–To–End VLAN*. Pro ostatní typy VLAN je STP konfigurován jako

prevence selhání lidského faktoru (například chybná konfigurace L2 trunku, chybné fyzické propojení přepínačů apod.).

Kořenovým mostem pro všechny *End–To–End VLAN* je ústřední L3 přepínač *Core*. Nebudou zde rozebírány podrobnosti volby kořenového mostu v STP, protože v univerzitní síti je kořenový most pro všechny *End–To–End VLAN* uměle zvolen snížením hodnoty priority L3 přepínače *Core* pod výchozí prahovou hodnotu 32768.

Na obr. 16 je znázorněn příklad eliminace L2 smyčky v případě modelové *End–To–End VLAN* 114. Činností STP procesu zde bylo zablokováno rozhraní `Gi0/25` páteřního L3 přepínače *core–C*, což způsobilo přerušení L2 smyčky.



Obr. 16: Eliminace L2 smyčky na páteři univerzitní sítě MENDELU prostřednictvím STP.

Nevýhodou provozu STP je jeho relativně nákladná režie v univerzitní síti.

8.12 Podpora IPv6 na stávajících aktivních prvcích

Přechod na nový internetový protokol úzce souvisí s technickým vybavením infrastruktury univerzitní sítě MENDELU. Některými staršími aktivními prvky totiž

nemusí být IPv6 vůbec podporován (nelze například žádným způsobem přiřadit IPv6 adresu libovolnému L3 rozhraní). V jiných případech může být nutné pouze aktualizovat operační systém konkrétního aktivního prvku na aktuální verzi.

Fyzická infrastruktura univerzitní počítačové sítě MENDELU je téměř kompletně vybudována na zařízeních společnosti Cisco Systems, Inc.

L3 přepínače univerzitní sítě

Univerzitní síť MENDELU je vybavena množstvím L3 přepínačů. Většina z nich se nachází na perimetru a na páteři univerzitní sítě a musí být u nich zajištěna dostatečná podpora IPv6, protože tyto L3 přepínače jsou zodpovědné za směrování síťového provozu v celé univerzitní síti i mimo ni. Všechny nezbytné informace pro analýzu stávající podpory IPv6 na všech páteřních L3 přepínačích univerzitní sítě MENDELU jsou uvedeny v tab. 7.

Tab. 7: L3 přepínače univerzitní sítě MENDELU.

Umístění	Hostname	Model Cisco	Cisco IOS Image
Budova X	*Core*	2x Catalyst 6500	[illegible]
Budova A	*core–A*	2x Catalyst 3750	[illegible]
Budova C	*core–C*	1x Catalyst 3560	[illegible]
Budova B	*core–B*	1x Catalyst 3750	[illegible]
Budova Q	*core–Q*	1x Catalyst 6800	[illegible]
Budova E	*core–E*	1x Catalyst 6500	[illegible]
Budova T	*core–T*	1x Catalyst 3750	[illegible]
Budova Z	*core–Z*	1x Catalyst 3750	[illegible]
Budova X	*Nexus2*	1x Nexus 7000	[illegible]

Analýza a vyhodnocení míry podpory IPv6 na páteřních L3 přepínačích univerzitní sítě jsou provedeny prostřednictvím webové aplikace *Cisco Feature Navigator*[12], která umožňuje konfrontaci konkrétní verze síťového operačního systému Cisco IOS se všemi funkcemi (features), které společnost Cisco nabízí.

Pro plnohodnotnou integraci IPv6 do univerzitní sítě MENDELU je v systému Cisco IOS na všech páteřních L3 přepínačích nutná podpora následujících funkcí (názvosloví podle společnosti Cisco):

- IPv6 (Internet Protocol Version 6)
- IPv6 Access Services: DHCPv6 Prefix Delegation
- IPv6 Access Services: DHCPv6 Relay Agent
- IPv6 Data Link: VLANs using IEEE 802.1Q Encapsulation
- IPv6 Dual Stack
- IPv6 Neighbor Discovery
- IPv6 Routing: OSPF for IPv6 (OSPFv3)

[12]Dostupné na `http://tools.cisco.com/ITDIT/CFN/`

- IPv6 Routing: OSPF for IPv6 (OSPFv3) Authentication Support with IPsec
- IPv6 Routing: Static Routing
- IPv6 Routing: Unicast Routing
- IPv6 Security: Secure Shell SSH support over IPv6
- IPv6 Services: Cisco Discovery Protocol (CDP)
- IPv6 Services: DNS Lookups over an IPv6 Transport
- IPv6 Services: Extended Access Control Lists
- IPv6 Services: Standard Access Control Lists
- IPv6 Stateless Auto–configuration
- IPv6: ICMPv6
- IPv6: Neighbor Discovery Duplicate Address Detection

Navíc je na ústředním logickém L3 přepínači *Core* nezbytná přítomnost následujících funkcí:

- IPv6 Multicast: Address Family Support for Multiprotocol BGP
- IPv6 Routing: Multiprotocol BGP Extensions for IPv6
- IPv6 Routing: Multiprotocol BGP Link–Local Address Peering
- OSPFv3 Address Families
- OSPFv3 VRF–Lite/PE–CE

Výsledek konfrontace stávajících verzí systému Cisco IOS páteřních L3 přepínačů univerzitní sítě MENDELU s požadovanými funkcemi IPv6 je uveden v tab. 8.

Tab. 8: Stávající podpora požadovaných funkcí IPv6 páteřními L3 přepínači univerzitní sítě MENDELU.

Feature	**Core**	**A**	**C**	**B**	**Q**	**E**	**T**	**Z**	**Nexus2**
IPv6 (Internet Protocol Version 6)	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Access Services: DHCPv6 Prefix Delegation	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Access Services: DHCPv6 Relay Agent	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Data Link: VLANs using IEEE 802.1Q Encapsulation	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Dual Stack	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Neighbor Discovery	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Routing: OSPF for IPv6 (OSPFv3)	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Routing: OSPF for IPv6 (OSPFv3) Authentication Support with IPsec	yes	no	no	no	yes	yes	no	no	no
IPv6 Routing: Static Routing	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Routing: Unicast Routing	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Security: Secure Shell SSH support over IPv6	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Services: Cisco Discovery Protocol (CDP)	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Services: DNS Lookups over an IPv6 Transport	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Services: Extended Access Control Lists	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Services: Standard Access Control Lists	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Stateless Auto–configuration	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6: ICMPv6	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6: Neighbor Discovery Duplicate Address Detection	yes	yes	yes	yes	yes	yes	yes	yes	yes
IPv6 Multicast: Address Family Support for Multiprotocol BGP	yes								
IPv6 Routing: Multiprotocol BGP Extensions for IPv6	yes								
IPv6 Routing: Multiprotocol BGP Link–Local Address Peering	yes								
OSPFv3 Address Families	yes								
OSPFv3 VRF–Lite/PE–CE	yes								

Z výsledků konfrontace vyplývá, že funkce *IPv6 Routing: OSPF for IPv6 (OSPFv3) Authentication Support with IPsec* zajišťující autentizaci směrovacího protokolu OSPFv3 není podporována současnými verzemi systému Cisco IOS na L3 přepínačích:

- *Cisco Catalyst 3560* v budově **C**;
- *Cisco Catalyst 3750* v budovách **A**, **B**, **T** a **Z**;
- *Cisco Nexus 7000* v budově **X**.

Podle webové aplikace Cisco Feature Navigator je:

- tato funkce pro *Cisco Catalyst 3560* nedostupná;
- nezbytné aktualizovat *Cisco Catalyst 3750* na Cisco IOS verze **15.0(2)SE**;
- tato funkce pro *Cisco Nexus 7000* nedostupná.

Na základě provedené analýzy bude nutné zvážit výměnu L3 přepínačů, pro něž je autentizace OSPFv3 nedostupná za novější modely, nebo tuto funkci do univerzitní sítě neimplementovat.

L2 přepínače univerzitní sítě

L2 přepínače na přístupové vrstvě musí podporovat IPv6 pouze za účelem přiřazení IPv6 adresy k SVI *správní VLAN*.

Na přístupových vrstvách všech lokalit univerzitní sítě MENDELU je dohromady umístěno více než 200 kusů L2 přepínačů *Cisco Catalyst 2950* a *2960*. Přepínače *Cisco Catalyst 2950* nepodporují IPv6 ani v nejnovější verzi Cisco IOS dostupné pro tuto platformu. Přepínače *Cisco Catalyst 2960* podporují IPv6 od verze Cisco IOS **12.2(40)SE**.

Z výše uvedených informací vyplývá, že implementace podpory IPv6 na L2 přepínačích univerzitní sítě je složena ze dvou kroků:

1. Nahrazení všech přepínačů *Cisco Catalyst 2950* za model *Cisco Catalyst 2960*,
2. aktualizace všech přepínačů *Cisco Catalyst 2960* minimálně na Cisco IOS image `c2960-lanbasek9-mz.122-40.SE.bin`.

Vzhledem ke značnému množství L2 přepínačů, které by musely být nahrazeny, resp. aktualizovány, se implementace IPv6 na přístupovou vrstvu nevyplatí a je rozumné ponechat správu sítě na protokolu IPv4.

8.13 Shrnutí podstatných poznatků z analýzy

V průběhu analýzy současného stavu univerzitní sítě MENDELU byly získány informace, které jsou zcela nezbytné pro zpracování optimálního návrhu integrace IPv6

do produkční počítačové sítě Mendelovy univerzity v Brně. Tyto důležité poznatky lze rozdělit do následujících celků:

- **Typy VLAN**, které v univerzitní síti MENDELU existují. Na základě těchto informací bude zpracován optimální adresní plán IPv6. Představenými typy VLAN jsou:
  - *Páteřní VLAN* – spojují všechny L3 prvky páteře univerzitní sítě do téměř čisté hvězdicové topologie.
  - *Lokalitní VLAN* – zahrnují koncové síťové uzly vnitřní univerzitní sítě v jednotlivých lokalitách.
  - *Perimetrové VLAN* – spojují virtuální směrovače *VRF Internet* a *VRF CernaPole* s *Firewallem* na perimetru univerzitní sítě.
  - *Demilitarizovaná VLAN* – zahrnuje síťové uzly univerzitní sítě přímo připojené do veřejného Internetu.
  - *End–To–End VLAN* – jsou privátní sítě rozprostřené v mnoha částech celé univerzitní sítě.
  - *Správní VLAN* – zvláštní izolovaná síť, jejímž prostřednictvím je umožněna vzdálená správa aktivních prvků infrastruktury univerzitní sítě.
  - *Spojovací VLAN* – spojují virtuální hraniční směrovač univerzitní sítě *VRF Internet* se směrovači ISP *R142* a *R121*.
- **Způsoby směrování** síťového provozu v jednotlivých částech univerzitní sítě MENDELU, na jejichž základě budou navrženy totožné způsoby směrování v IPv6:
  - *Dynamické směrování* prostřednictvím směrovacího protokolu OSPF – směrování síťového provozu na páteři a mezi lokalitami ve vnitřní části univerzitní sítě MENDELU.
  - *Statické směrování* – směrování síťového provozu na perimetru univerzitní sítě.
  - *Dynamické směrování* prostřednictvím směrovacího protokolu BGP – směrování síťového provozu mezi univerzitní sítí MENDELU a ISP.
- **Topologické detaily** dílčích částí univerzitní sítě, které jsou klíčové pro návrh modelu univerzitní sítě, jímž bude verifikován zpracovaný návrh integrace IPv6 do produkční počítačové sítě Mendelovy univerzity v Brně.

9 Návrh integrace IPv6 do univerzitní sítě MENDELU

V této kapitole je na základě provedených dílčích analýz zpracován návrh integrace protokolu IPv6 do univerzitní sítě MENDELU v oblasti směrování.

9.1 Metoda přechodu na IPv6

Protokol IPv6 bude do univerzitní sítě MENDELU nasazován postupně metodou Dual Stack. V období přechodu univerzitní sítě na protokol IPv6 tak bude zajištěna její stávající funkčnost.

V některých VLAN se vyskytují uzly, jimiž není protokol IPv6 vůbec podporován. Těchto VLAN se integrace IPv6 prozatím netýká.

9.2 Přidělený globální směrovací prefix

Poskytovatel internetových služeb CESNET z.s.p.o. plně podporuje protokol IPv6.

Z jeho strany byl Mendelově univerzitě v Brně přidělen globální směrovací prefix `2001:718:803::/48`. Hierarchie přidělení tohoto prefixu je znázorněna v tab. 9.

Tab. 9: Hierarchie přidělení globálního směrovacího IPv6 prefixu Mendelově univerzitě v Brně.

IANA	RIPE NCC	CESNET	MENDELU
2000::/3	2001:600::/23	2001:718::/32	**2001:718:803::/48**

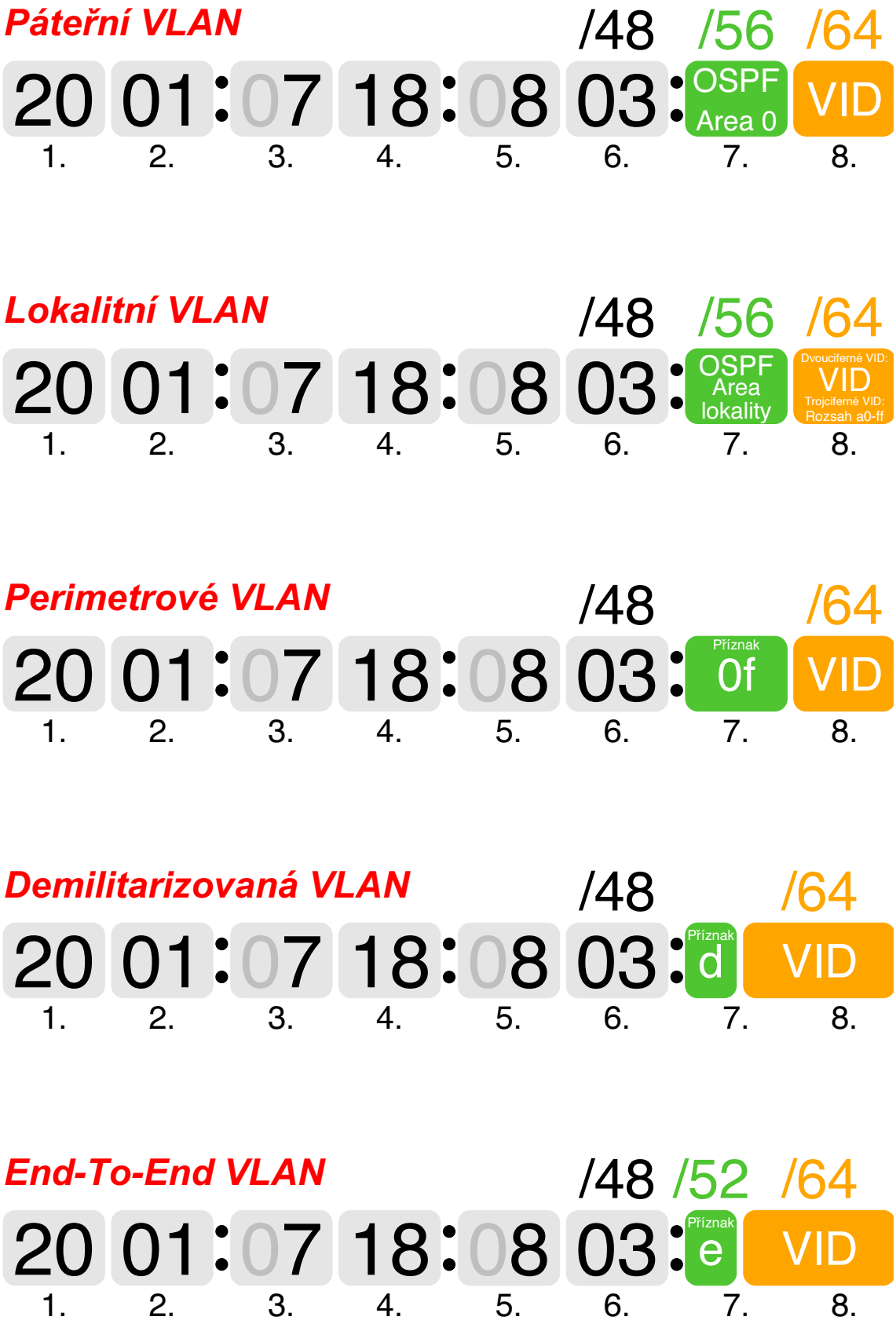
Přiděleným IPv6 prefixem lze adresovat až 65536 podsítí IPv6 prefixy s délkou prefixu 64 bitů. V celé univerzitní síti MENDELU však existuje jen několik stovek VLAN. Značný adresní prostor IPv6 poskytuje celou řadu přístupů k jejich adresování. Každý síťový uzel bude poté disponovat svojí vlastní veřejnou IPv6 adresou a nebude již zapotřebí žádných mechanismů pro přepisování IP adres (NAT).

9.3 Adresní plán IPv6

Účelem adresního plánu IPv6 je jednoznačný popis způsobu rozdělení přiděleného 48bitového globálního směrovacího prefixu jednotlivým VLAN univerzitní sítě.

Každé existující VLAN v univerzitní síti musí být přidělen IPv6 prefix délky 64 bitů. Identifikátor podsítě mezi 48. a 64. bitem (7. a 8. bajt) jednotlivých IPv6 prefixů VLAN je možné využít pro jejich smysluplný způsob adresování, protože jeho definice je plně v kompetencích administrátorů univerzitní sítě MENDELU.

V souladu s požadavky na adresní plán IPv6 (možnost sumarizace prefixů a snadná identifikace VLAN) je na obr. 17 znázorněn základní princip rozdělení globálního směrovacího IPv6 prefixu Mendelovy univerzity v Brně `2001:718:803::/48` jednotlivým typům VLAN, které byly představeny v analýze univerzitní sítě MENDELU.



Obr. 17: Adresní plán IPv6 univerzitní sítě MENDELU.

Podrobné atributy navrženého adresního plánu IPv6 jsou rozebírány v následujících sekcích.

Páteřní VLAN

Síťové prefixy *páteřních VLAN* si mezi sebou L3 prvky páteře vyměňují prostřednictvím směrovacího protokolu OSPF.

Všechna SVI *páteřních VLAN* jsou umístěna v OSPF oblasti **0**. Tento identifikátor bude promítnut v 7. bajtu 64bitových IPv6 prefixů přidělených *páteřním VLAN*. Do 8. bajtu pak budou promítnuty dvouciferné VID těchto VLAN, které jsou v rozmezí **40** až **48**. Odvozené IPv6 prefixy všech *páteřních VLAN* jsou uvedeny v tab. 10.

Tab. 10: IPv6 prefixy *páteřních VLAN* odvozené z identifikátoru OSPF oblasti páteře a VID.

OSPF oblast	*Páteřní VLAN*	Odvozený prefix
0	40	2001:718:803:40::/64
0	41	2001:718:803:41::/64
0	42	2001:718:803:42::/64
0	43	2001:718:803:43::/64
0	44	2001:718:803:44::/64
0	45	2001:718:803:45::/64
0	46	2001:718:803:46::/64
0	47	2001:718:803:47::/64
0	48	2001:718:803:48::/64

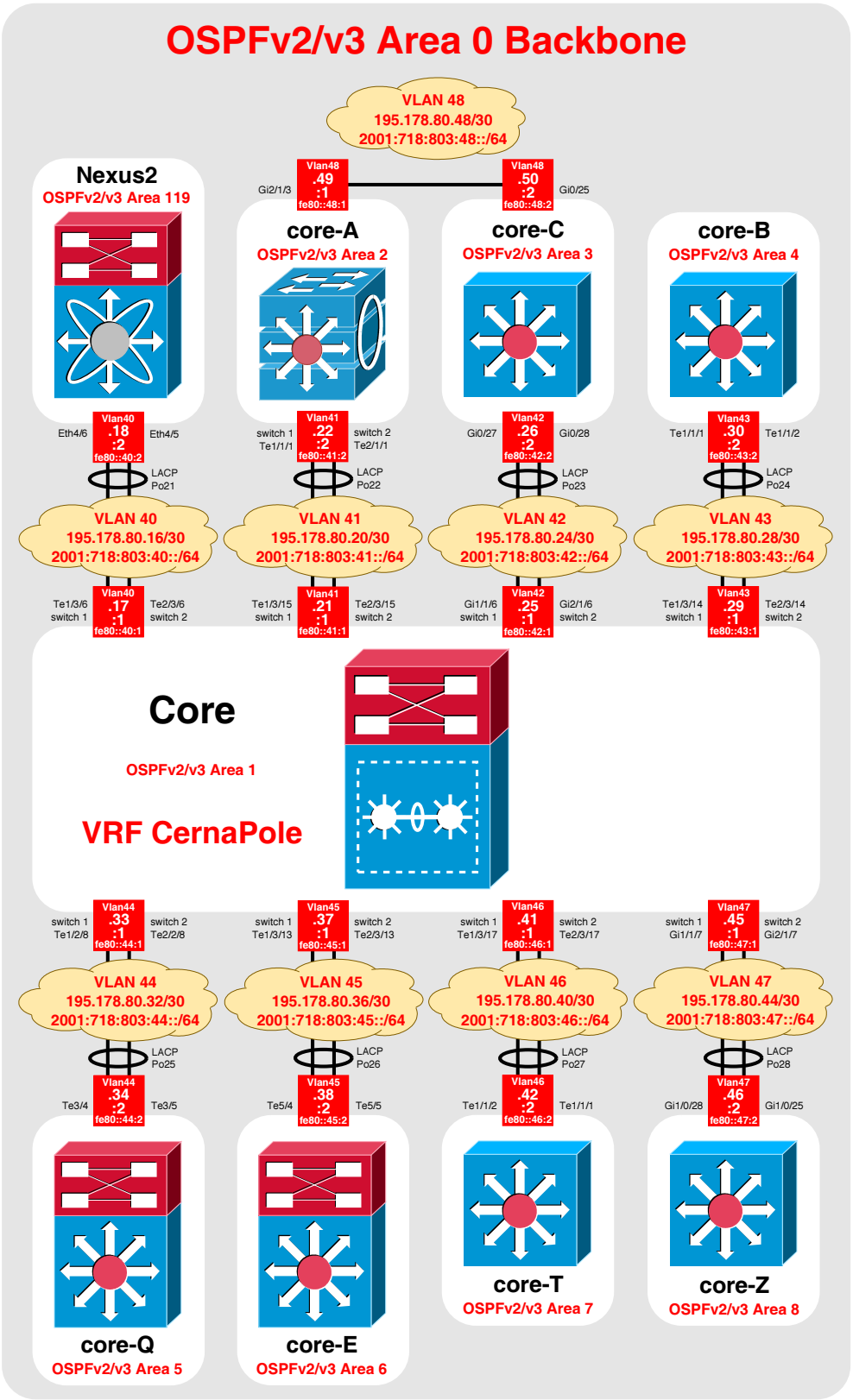
Zápis IPv6 adres umožňuje vynechání počátečních nul, takže je v každém 64bitovém IPv6 prefixu *páteřních VLAN* vždy vizuálně patrný pouze jejich VID. Při pouhém pohledu na IPv6 prefix tak lze jednoznačně identifikovat každou *páteřní VLAN*.

Výhodou tohoto způsobu adresování je možnost sumarizace všech *páteřních VLAN* pod jediný souhrnný IPv6 prefix ve tvaru `2001:718:803::/56`.

Přidělování 64bitových prefixů Point–To–Point sítím je samozřejmě nesmírné plýtvání adresním prostorem. Vzhledem k přidělenému 48bitovému globálnímu směrovacímu prefixu má však univerzitní síť MENDELU k dispozici 65536 prefixů délky 64bitů a ještě dlouhou dobu (časový horizont v desítkách let) jich bude využita jen nepatrná část.

Topologii páteře univerzitní sítě MENDELU s navrženou IPv6 adresací *páteřních VLAN* je vyobrazena na obr. 18.

Všechna SVI *páteřních VLAN* budou mít staticky konfigurované globální individuální a link–local IPv6 adresy.



Obr. 18: Návrh integrace IPv6 na páteři univerzitní sítě MENDELU.

Lokalitní VLAN

V případě adresování *lokalitních VLAN* lze uplatnit užitečný poznatek získaný z analýzy adresních plánů ostatních českých univerzit:

- Je-li konkrétní univerzitní síť rozdělena do lokalit, jsou přiřazovány síťové prefixy IPv6 nejdříve jim, a sice v délkách 52, 56 nebo 60 bitů. Teprve potom jsou koncovým podsítím v nich obsaženým přiřazeny síťové IPv6 prefixy o délce 64 bitů.
- Není-li konkrétní univerzitní síť rozdělena do žádných lokalit, jsou jednotlivým koncovým podsítím přímo přiřazeny IPv6 prefixy v délce 64 bitů.

Tab. 11: IPv6 prefixy jednotlivých lokalit univerzitní sítě MENDELU vycházející z identifikátorů jejich spádových OSPF oblastí.

Lokalita	OSPF oblast	Odvozený prefix
X	1	2001:718:803:100::/56
A	2	2001:718:803:200::/56
C	3	2001:718:803:300::/56
B	4	2001:718:803:400::/56
Q	5	2001:718:803:500::/56
E	6	2001:718:803:600::/56
T	7	2001:718:803:700::/56
Z	8	2001:718:803:800::/56
X2	119	2001:718:803:1900::/56

Univerzitní síť MENDELU je rozdělena do 9 lokalit, které zahrnují jednotlivé *lokalitní VLAN*. Z důvodu možnosti sumarizace budou nejdříve přiděleny kratší IPv6 prefixy všem lokalitám a následně 64bitové IPv6 prefixy jednotlivým *lokalitním VLAN*.

Je zapotřebí určit optimální délku IPv6 prefixu jednotlivých lokalit univerzitní sítě MENDELU. Všem lokalitám by měl být přidělen prefix stejné délky z následujících možností:

1. **52 bitů** – až *16 lokalit* a *4096 sítí* v každé z nich.
2. **56 bitů** – až *256 lokalit* a *256 sítí* v každé z nich.
3. **60 bitů** – až *4096 lokalit* a *16 sítí* v každé z nich.

Automaticky lze vyloučit poslední možnost IPv6 prefixu o délce 60 bitů, protože v některých lokalitách univerzitní sítě MENDELU existuje více než 16 *lokalitních VLAN*.

Pokud by nebyl brán zřetel na budoucí rozšiřování a vývoj univerzitní sítě MENDELU, bylo by možné jednotlivým lokalitám přidělit IPv6 prefix o délce 52 bitů. Nelze však vyloučit, že ve střednědobém časovém horizontu bude univerzitní

Tab. 12: Rozložení hodnot rozsahu 00–ff pro 8. bajt 64bitového IPv6 prefixu *lokalitních VLAN*. **00–99** pro VLAN s dvouciferným VID, **a0–ff** a **sekundární hodnoty** pro VLAN s trojciferným VID.

DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX
0	00	32	20	64	40	96	60	128	80	160	A0	192	C0	224	E0
1	01	33	21	65	41	97	61	129	81	161	A1	193	C1	225	E1
2	02	34	22	66	42	98	62	130	82	162	A2	194	C2	226	E2
3	03	35	23	67	43	99	63	131	83	163	A3	195	C3	227	E3
4	04	36	24	68	44	100	64	132	84	164	A4	196	C4	228	E4
5	05	37	25	69	45	101	65	133	85	165	A5	197	C5	229	E5
6	06	38	26	70	46	102	66	134	86	166	A6	198	C6	230	E6
7	07	39	27	71	47	103	67	135	87	167	A7	199	C7	231	E7
8	08	40	28	72	48	104	68	136	88	168	A8	200	C8	232	E8
9	09	41	29	73	49	105	69	137	89	169	A9	201	C9	233	E9
10	0A	42	2A	74	4A	106	6A	138	8A	170	AA	202	CA	234	EA
11	0B	43	2B	75	4B	107	6B	139	8B	171	AB	203	CB	235	EB
12	0C	44	2C	76	4C	108	6C	140	8C	172	AC	204	CC	236	EC
13	0D	45	2D	77	4D	109	6D	141	8D	173	AD	205	CD	237	ED
14	0E	46	2E	78	4E	110	6E	142	8E	174	AE	206	CE	238	EE
15	0F	47	2F	79	4F	111	6F	143	8F	175	AF	207	CF	239	EF
16	10	48	30	80	50	112	70	144	90	176	B0	208	D0	240	F0
17	11	49	31	81	51	113	71	145	91	177	B1	209	D1	241	F1
18	12	50	32	82	52	114	72	146	92	178	B2	210	D2	242	F2
19	13	51	33	83	53	115	73	147	93	179	B3	211	D3	243	F3
20	14	52	34	84	54	116	74	148	94	180	B4	212	D4	244	F4
21	15	53	35	85	55	117	75	149	95	181	B5	213	D5	245	F5
22	16	54	36	86	56	118	76	150	96	182	B6	214	D6	246	F6
23	17	55	37	87	57	119	77	151	97	183	B7	215	D7	247	F7
24	18	56	38	88	58	120	78	152	98	184	B8	216	D8	248	F8
25	19	57	39	89	59	121	79	153	99	185	B9	217	D9	249	F9
26	1A	58	3A	90	5A	122	7A	154	9A	186	BA	218	DA	250	FA
27	1B	59	3B	91	5B	123	7B	155	9B	187	BB	219	DB	251	FB
28	1C	60	3C	92	5C	124	7C	156	9C	188	BC	220	DC	252	FC
29	1D	61	3D	93	5D	125	7D	157	9D	189	BD	221	DD	253	FD
30	1E	62	3E	94	5E	126	7E	158	9E	190	BE	222	DE	254	FE
31	1F	63	3F	95	5F	127	7F	159	9F	191	BF	223	DF	255	FF

síť MENDELU rozšířena o další lokality. Mohlo by tak dojít k situaci, kdy by pro adresování nových lokalit již nezbyl adresní prostor, zatímco prostor pro jednotlivé *lokalitní VLAN* by nebyl zdaleka využitý. Z tohoto důvodu je optimální stanovit délku IPv6 prefixu všech lokalit na **56 bitů**.

Do 7. bajtu 56bitových IPv6 prefixů jednotlivých lokalit budou promítnuty identifikátory jejich spádových OSPF oblastí, jako je to znázorněno v tab. 11.

Pozornost vyžadují případné trojciferné identifikátory OSPF oblastí. V případě univerzitní sítě se jedná o OSPF oblast 119. Do IPv6 prefixu je totiž nutné jej převést do dvouciferné podoby, aby nezasahoval do jeho 8. bajtu. Je velmi nepravděpodobné, že by se v blízké budoucnosti v univerzitní síti MENDELU vyskytovalo více než 100 OSPF oblastí. V uvedeném případě byly do IPv6 prefixu promítnuty poslední dvě číslice dané OSPF oblasti, tedy 19.

Po definici způsobu adresování lokalit je možné přistoupit k adresování jednotlivých *lokalitních VLAN*, které se v nich vyskytují a je zapotřebí jim přiřadit prefixy délky 64 bitů.

Do 7. bajtu 64bitových IPv6 prefixů *lokalitních VLAN* je již umístěn identifikátor lokality odvozený z její spádové OSPF oblasti, takže pro rozlišení jednotlivých

lokalitních VLAN je možné využít pouze 8. bajt v IPv6 prefixu.

Nejlepší možností pro rozlišení *lokalitních VLAN* a potažmo jejich přímou identifikaci je promítnutí jejich VID do IPv6 prefixu. Jedná se tak o zcela totožný princip adresování, jako v případě *páteřních VLAN*. U *lokalitních VLAN* je však situace komplikována skutečností, že některé z nich mají dvouciferný VID a některé trojciferný. S tímto problémem je nutné se vypořádat kombinací dvou způsobů adresování *lokalitních VLAN*:

1. *Lokalitní VLAN* s **dvouciferným** VID – identifikátor bude promítnut do IPv6 prefixu naprosto stejným způsobem jako v případě adresování *páteřních VLAN*. Z dostupného hexadecimálního rozsahu 00–ff pro ně bude vyhrazen dekadický „subinterval“ **00–99**.
2. *Lokalitní VLAN* s **trojciferným** VID – tyto VLAN budou adresovány zcela nezávisle na dosavadní situaci. Jejich IPv6 prefixy budou mít v 8. bajtu umístěny hodnoty z hexadecimálního intervalu **a0–ff**. V případě vyčerpání hodnot tohoto rozsahu lze ještě využít hexadecimálních hodnot, které byly vynechány v dekadickém rozsahu 00–99 (například **1c**, **3d**, **5e** apod.).

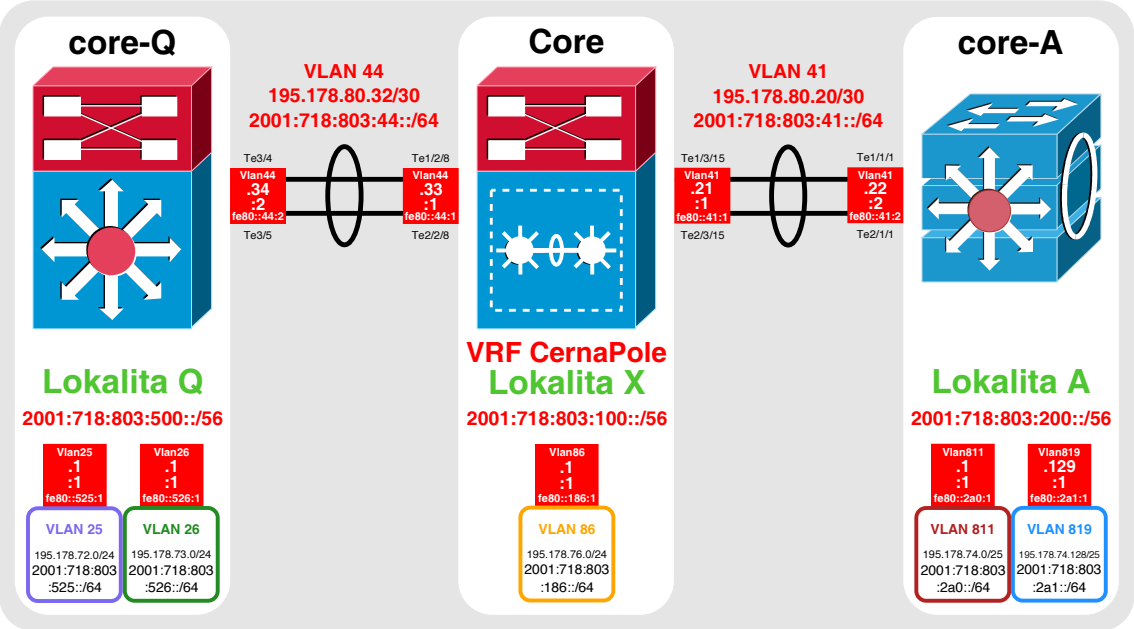
Popisovaný způsob přidělování hodnot 8. bajtu 64bitových IPv6 prefixů *lokalitních VLAN* je znázorněn v tab. 12.

Příklady modelových *lokalitních VLAN* s přiřazenými IPv6 prefixy uvádí tab. 13. Z této tabulky je patrné, že pohledem na IPv6 prefix je možné jednoznačně identifikovat *lokalitní VLAN* s dvouciferným VID. *Lokalitní VLAN* s trojciferným VID lze při pohledu na jejich IPv6 prefix pouze přiřadit ke konkrétní lokalitě univerzitní sítě. Ze všech VLAN existujících v univerzitní síti MENDELU se však jedná o poměrně nízký počet podsítí, které jsou touto nevýhodou postiženy. Řešením by mohlo být například přečíslování VLAN s trojciferným identifikátorem na dvouciferný. Je však otázkou, zda by toto vynaložené úsilí přineslo podstatný užitek. Obecně není přečíslování VLAN v jakékoli síti jednoduchou záležitostí, protože se de facto jedná o nahrazení stávajících VLAN novými.

Tab. 13: Příklady IPv6 prefixů vybraných *lokalitních VLAN* odvozených z identifikátoru jejich spádové OSPF oblasti a VID.

Lokalita	**OSPF oblast**	***Lokalitní VLAN***	**Odvozený prefix**
X	1	86	2001:718:803:186::/64
A	2	811	2001:718:803:2a0::/64
A	2	819	2001:718:803:2a1::/64
B	4	92	2001:718:803:492::/64
B	4	729	2001:718:803:4a0::/64
Q	5	25	2001:718:803:525::/64
X2	119	85	2001:718:803:1985::/64
X2	119	187	2001:718:803:19a0::/64

Princip integrace protokolu IPv6 na příkladu 3 vybraných lokalit univerzitní sítě MENDELU je znázorněn na obr. 19.



Obr. 19: Znázornění principu integrace protokolu IPv6 u vybraných lokalit univerzitní sítě.

Všechna SVI *lokalitních VLAN* (výchozí brány) budou mít staticky konfigurované globální individuální a link–local IPv6 adresy, jejichž hodnota v poslední čtveřici identifikátoru rozhraní bude `:1`.

Teoreticky by bylo možné některé *lokalitní VLAN* s trojciferným VID adresovat tak, že by měly v 8. bajtu prefixu promítnuty své identifikátory převedené z dekadické soustavy do hexadecimální. Toto by však bylo možné provést pouze u malého množství VLAN tohoto typu. Navíc nemá tento princip žádný významný přínos, protože ani tak nelze při pouhém pohledu na IPv6 prefix identifikovat konkrétní *lokalitní VLAN*. U identifikátorů nižších hodnot by navíc docházelo ke kolizím mezi jejich desítkovou a hexadecimální podobou. Například identifikátor VLAN 120 by byl v prefixu zakódován jako 78, čímž by se dostal do kolize s dvouciferným identifikátorem VLAN 78. Tento způsob je tak přímo kontraproduktivní a je tedy rozumné jej úplně zavrhnout.

Perimetrové VLAN

Perimetrové VLAN jsou v univerzitní síti MENDELU právě 2 a jejich VID jsou **21** a **22**. Jedná se o jediné VLAN, které jsou přímo připojeny k *Firewallu*.

Rozlišovacím příznakem umístěným do 7. bajtu 64bitových IPv6 prefixů *perimetrových VLAN* bude hexadecimální hodnota **0f**. Jedná se o uměle zvolený rozlišovací

příznak, protože zde není k dispozici žádný přirozený identifikátor (například číslo OSPF oblasti), který by bylo možné pro odlišení IPv6 prefixů těchto VLAN použít.

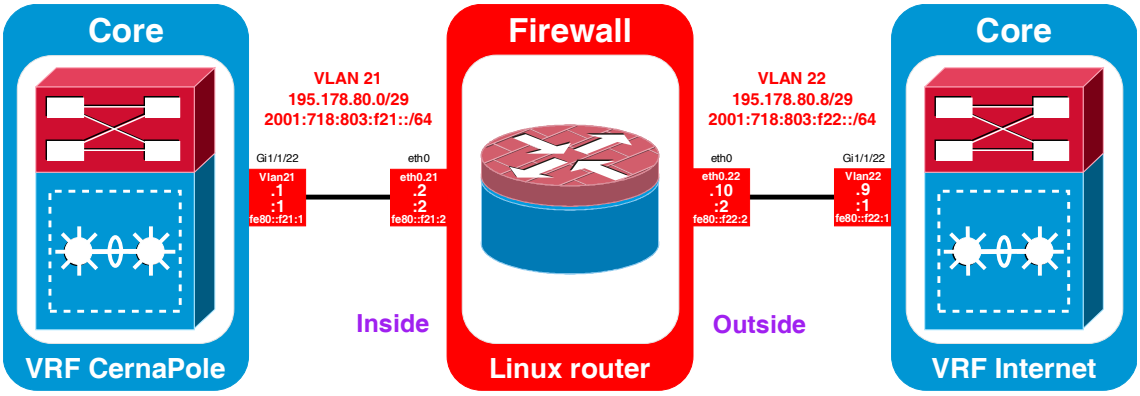
Do 8. bajtu jejich 64bitových IPv6 prefixů lze bez komplikací promítnout jejich dvouciferné VID. Tento způsob adresování *perimetrových VLAN* je znázorněn v tab. 14.

Tab. 14: IPv6 prefixy *perimetrových VLAN* odvozené ze zvoleného příznaku a VID.

Příznak	*Perimetrová VLAN*	Odvozený prefix
0f	21	2001:718:803:f21::/64
0f	22	2001:718:803:f22::/64

Vzhledem ke zvolenému přístupu adresování lze pouhým pohledem na IPv6 prefix jednoznačně identifikovat *perimetrové VLAN*.

Topologie perimetru univerzitní sítě s navrženou IPv6 adresací *perimetrových VLAN* je vyobrazena na obr. 20.



Obr. 20: Návrh integrace IPv6 na perimetru univerzitní sítě MENDELU.

Všechna SVI *perimetrových VLAN* budou mít staticky konfigurované globální individuální a link–local IPv6 adresy.

U obou typů IPv6 adres bude platit, že hodnota `:1` v poslední čtveřici identifikátoru rozhraní bude náležet směrovačům *VRF CernaPole* a *VRF Internet* a hodnota `:2` rozhraním *Firewallu*.

Demilitarizovaná VLAN

Tento typ VLAN je v univerzitní síti MENDELU zastoupen právě jedním exemplářem. *Demilitarizovaná VLAN* je specifická tím, že je umístěna před *Firewallem*, tudíž uzly v ní zahrnuté jsou přímo připojeny do veřejného Internetu.

Demilitarizovaná VLAN má trojciferný VID **222**. Ten bude v jejím 64bitovém IPv6 prefixu umístěn mezi 52. a 64. bit, takže kromě 8. bajtu IPv6 prefixu zasahuje i do druhé poloviny 7. bajtu.

Mezi 48. a 52. bit (první polovina 7. bajtu) IPv6 prefixu této VLAN bude umístěn umělý příznak **d**, kterým bude *demilitarizovaná VLAN* odlišena od ostatních typů podsítí. 64bitový IPv6 prefix přidělený *demilitarizované VLAN* získaný popsaným způsobem je uveden v tab. 14.

Tab. 15: IPv6 prefix *demilitarizované VLAN* odvozený ze zvoleného příznaku a VID.

Příznak	***Demilitarizovaná VLAN***	**Odvozený prefix**
d	222	2001:718:803:d222::/64

Zde se projevuje určitá nevýhoda VLAN s trojciferným VID v kombinaci se zvoleným způsobem adresování. Při zachování přesné podoby VID musí být totiž zvolený příznak **d** umístěn mezi 48. a 52. bit v IPv6 prefixu. To znamená, že jediná VLAN spotřebuje celý IPv6 prefix 2001:718:803:d000::/52, jímž by mohlo být adresováno dalších 4095 podsítí.

Je zřejmé, že v současné době není nutné tento problém řešit, protože adresní prostor vyplívající z 48bitového globálního směrovacího prefixu je dostatečně naddimenzovaný. Avšak v budoucnu by to mohla být nepříjemná komplikace.

V zásadě existují dvě možná řešení: jiný přístup adresování nebo změna VID *demilitarizované VLAN* na dvouciferné číslo.

V každém případě lze *demilitarizovanou VLAN* jednoznačně identifikovat pouhým pohledem na její IPv6 prefix.

End–To–End VLAN

Všechny *End–To–End VLAN* mají trojciferné VID, které budou promítnuty v jejich 64bitových IPv6 prefixech mezi 52. a 64. bitem.

Prostor mezi 48. a 52. bitem IPv6 prefixů *End–To–End VLAN* bude využit umělým příznakem **e**. Příklad *End–To–End VLAN* s IPv6 prefixem uvádí tab. 16.

Tab. 16: Příklad IPv6 prefixu *End–To–End VLAN* odvozený ze zvoleného příznaku a VID.

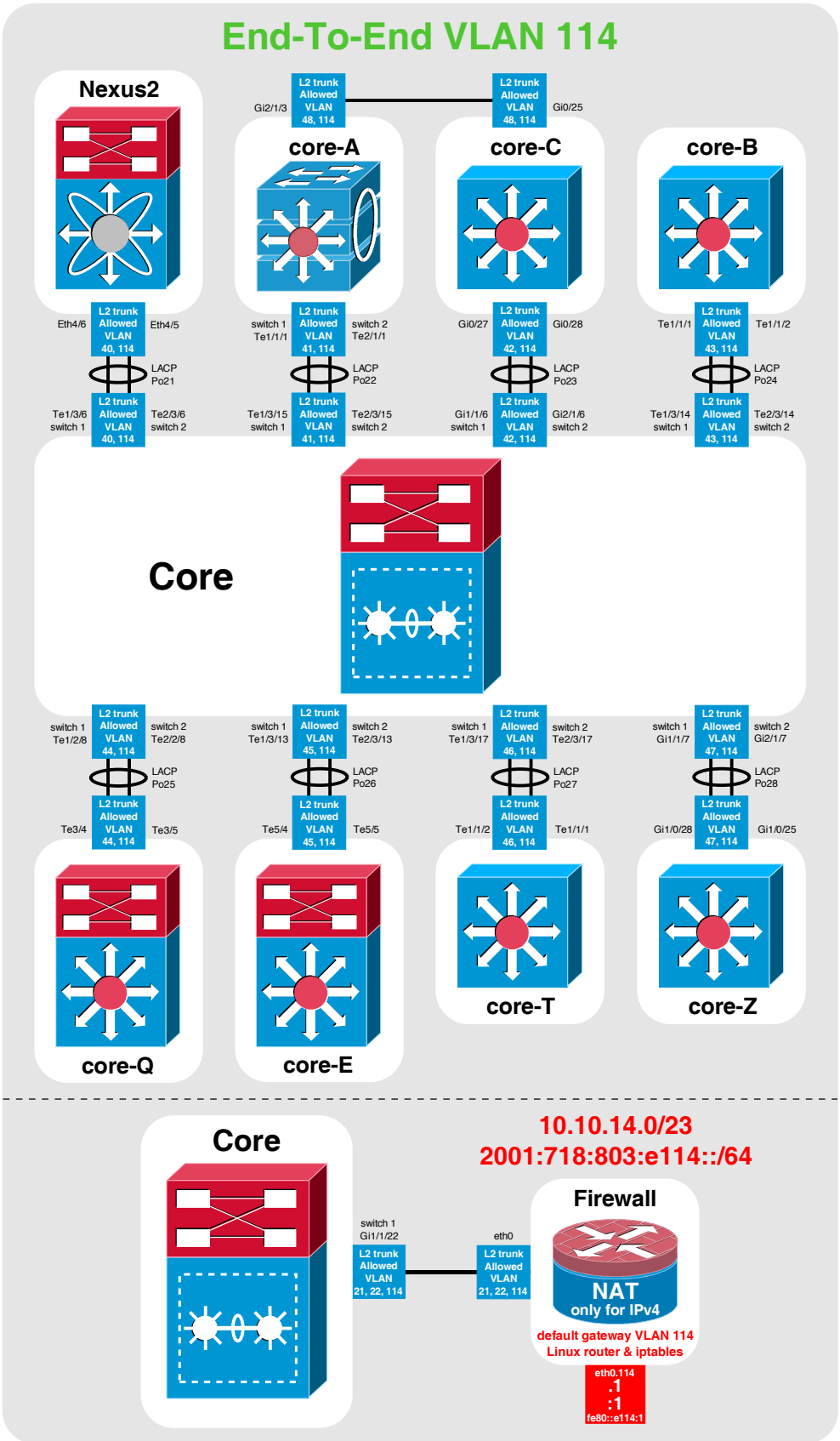
Příznak	***End–To–End VLAN***	**Odvozený prefix**
e	114	2001:718:803:e114::/64

Všechny *End–To–End VLAN* je tak možné sumarizovat pod jediný souhrnný IPv6 prefix 2001:718:803:e000::/52.

Princip integrace protokolu IPv6 do univerzitních *End–To–End VLAN* je demonstrován na obr. 21 prostřednictvím příkladové *End–To–End VLAN* **114**.

Všechna SVI *End–To–End VLAN* (výchozí brány) umístěné na *Firewallu* budou mít staticky konfigurované globální individuální a link–local IPv6 adresy, jejichž hodnota v poslední čtveřici identifikátoru rozhraní bude :1.

V prostředí protokolu IPv6 nebude zapotřebí mechanismu NAT, protože koncové uzly *End–To–End VLAN* budou v Internetu vystupovat pod svými veřejnými IPv6 adresami.



Obr. 21: Návrh integrace protokolu IPv6 v případě ukázkové *End–To–End VLAN* 114.

Správní VLAN

Správní VLAN **171** je s ohledem na bezpečnost zcela izolována od ostatních VLAN.

V prostředí IPv4 se prefix *správní VLAN* nachází ve směrovacích tabulkách páteřních L3 prvků, protože každý z nich má konfigurováno SVI této VLAN. V prostředí protokolu IPv6 nebude tento bezpečnostní problém vůbec existovat, protože je možné adresovat jednotlivé uzly ve *správní VLAN* pouze pomocí link–local adres, které mají platnost pouze v dané lokální síti. Tato VLAN tak nebude mít přiřazen žádný 64bitový globální prefix, který by se vyskytoval v jakékoli směrovací tabulce.

V link–local adresách uzlů *správní VLAN* bude promítnut umělý příznak **e** vyjadřující podobnost s *End–To–End VLAN*, VID *správní VLAN* a číslo uzlu daného zařízení převzaté z jeho IPv4 adresy spadající do této VLAN. Příklady odvozených link–local adres *správní VLAN* uvádí tab. 17.

Tab. 17: Příklady link–local adres *správní VLAN* odvozených ze zvoleného příznaku, VID a čísla uzlu v IPv4 adrese.

Příznak	*Správní VLAN*	IPv4 adresa	Odvozená IPv6 LL adresa
e	171	10.7.1.1	fe80::e171:1
e	171	10.7.1.20	fe80::e171:20
e	171	10.7.1.254	fe80::e171:254

Z ústředního linuxového stroje pro správu bude poté možné se k jednotlivým prvkům připojit přes SSH příkazem `ssh fe80::e171:x%eth0.171 -l <username>`.

Spojovací VLAN

Do adresního plánu IPv6 nemá smysl *spojovací VLAN* zahrnovat, protože jejich IPv6 prefixy budou přiděleny ze strany ISP a rozhodnutí o podobě jejich identifikátorů podsítě nespadá do kompetencí administrátorů univerzitní sítě MENDELU.

Statické link–local adresy

Aktivní síťové prvky společnosti Cisco ve výchozí konfiguraci přiřazují všem L3 rozhraním, na nichž je povolen protokol IPv6, link–local adresy s automaticky generovaným identifikátorem uzlu podle modifikovaného EUI–64.

Vzhledem ke skutečnosti, že tento typ IPv6 adres je využíván směrovacími protokoly, jsou uváděny ve směrovacích tabulkách jako rozhraní dalších přeskoků a v neposlední řadě je využívají automaticky konfigurované koncové uzly jako výchozí brány, je vhodné je pro přehlednost konfigurovat staticky.

Do předposlední čtveřice identifikátoru rozhraní link–local adres bude promítnut odlišovací znak daného typu VLAN a VID konkrétní VLAN. Příklady statických link–local adres uvádí tab. 18.

Tab. 18: Příklady vybraných statických link–local adres odvozených z příznaku nebo OSPF oblasti, VID a čísla uzlu.

Typ VLAN	Příznak, OSPF oblast	VID	Číslo uzlu	Odvozená LL adresa
Perimetrové	0f	21	1	fe80::f21:1
Demilitarizovaná	d	222	1	fe80::d222:1
Páteřní	0	40	1	fe80::40:1
Lokalitní	1	25	1	fe80::125:1
End–To–End	e	114	1	fe80::e114:1

9.4 Obecná příprava L3 prvků na provoz IPv6

V současné době nemá žádný L3 přepínač páteře univerzitní sítě MENDELU aktivován proces protokolu IPv6. To stejné platí i pro *Firewall*. Nejdříve je tedy nutné zpracovávání protokolu IPv6 na každém z těchto L3 prvků povolit.

Ústřední logický L3 přepínač *Core*

Počáteční příprava provozu protokolu IPv6 na ústředním logickém L3 přepínači *Core* zahrnuje následující kroky:

1. Aktivace podpory protokolu IPv6 pro virtuální směrovače VRF, protože ve výchozím stavu lze provozovat virtuální směrování a předávání pouze s protokolem IPv4.
2. Rozšíření konfigurací virtuálních směrovačů *VRF CernaPole* a *VRF Internet* o adresovou rodinu IPv6.
3. Povolení směrování IPv6 paketů.

Ostatní L3 přepínače páteře

Inicializace provozu protokolu IPv6 na páteřních L3 prvcích *core–A*, *core–C*, *core–B*, *core–Q*, *core–E*, *core–T*, *core–Z* a *Nexus2* zahrnuje následující kroky:

1. V případě L3 přepínačů *Cisco Catalyst 3560* a *3750* je nutné nejdříve aktivovat SDM šablonu umožňující souběžný provoz protokolů IPv4 a IPv6 s názvem *dual–ipv4–and–ipv6*.
2. Povolení směrování IPv6 paketů.

Firewall

V linuxové distribuci CentOS se globální inicializace protokolu IPv6 provede prostřednictvím konfiguračního souboru *network*, který se nachází v adresáři */etc/sysconfig*. V tomto souboru je zapotřebí povolit směrování IPv6 paketů a globálně zakázat automatickou konfiguraci L3 rozhraní.

9.5 Základní konfigurace protokolu IPv6 na L3 rozhraních

Po obecné přípravě aktivních L3 prvků páteře univerzitní sítě a *Firewallu* na provoz protokolu IPv6 musí následovat další důležitá procedura, která se týká konfigurace všech zainteresovaných L3 rozhraní, jimiž jsou SVI všech analyzovaných typů VLAN.

Přiřazení globálních individuálních a link–local adres

Základní konfigurace všech SVI spočívá v rozšíření jejich stávající konfigurace IPv4, která však zůstane zachována beze změn, o atributy IPv6. Jedná se především o statické přiřazení globálních individuálních a link–local adres v souladu s navrženým adresním plánem IPv6.

Zprávy ohlášení směrovače (RA)

Konfigurace IPv6 adres na rozhraních L3 přepínačů Cisco u nich způsobí aktivaci periodického posílání zpráv ohlášení směrovače (RA). Mimo jiné z bezpečnostních důvodů je rozumné automatické posílání těchto zpráv RA u SVI *páteřních*, *perimetrových*, *spojovacích*, *správní* a *demilitarizované VLAN* zakázat.

Posílání zpráv RA je nezbytné pouze v případě SVI *End–To–End* a *lokalitních VLAN*, protože se v nich vyskytují automaticky konfigurované koncové uzly. Podrobnostmi konfigurace voleb ohlášení směrovače, zejména způsob automatické konfigurace, se ve své bakalářské práci s názvem *Řešení dynamické konfigurace IPv6 klientů v počítačové síti Mendelovy univerzity v Brně* zabývá autorka Barbora Chumlenová.

9.6 Směrování IPv6 ve vnitřní části univerzitní sítě

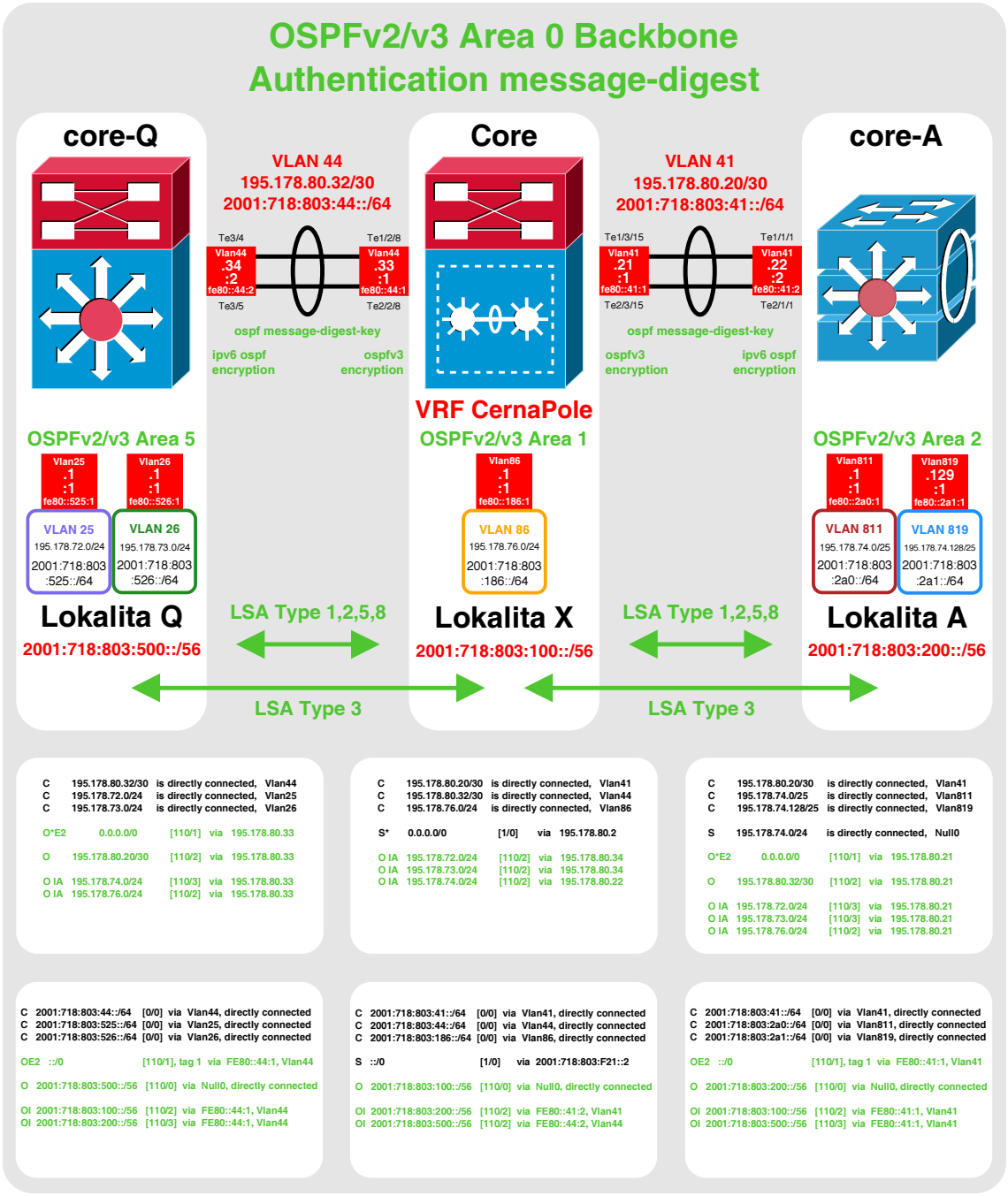
Návrh řešení dynamického směrování protokolů IPv4 a IPv6 prostřednictvím souběžného provozu směrovacích protokolů OSPFv2 a OSPFv3 ve vnitřní části univerzitní sítě MENDELU je znázorněn na obr. 22.

Na všech L3 prvcích páteře univerzitní sítě MENDELU je nutné aktivovat vedle stávajícího procesu OSPFv2 také proces OSPFv3. Procesy obou verzí směrovacího protokolu OSPF budou na L3 prvcích páteře fungovat zcela nezávisle na sobě. Budou pouze sdílet systémové prostředky páteřních L3 prvků. Na žádném L3 prvku páteře univerzitní sítě MENDELU není při implementaci protokolu OSPFv3 zapotřebí jakýmkoli způsobem zasahovat do stávající konfigurace atributů protokolu OSPFv2.

Hodnoty ID směrovačů (Router ID) budou ve směrovacím protokolu OSPFv3 totožné jako v OSPFv2.

Jediná aktivní rozhraní budou stejně jako v OSPFv2 pouze SVI *páteřních VLAN*, jejichž prostřednictvím si budou L3 prvky páteře vyměňovat směrovací informace.

IPv6 prefixy v délce 56 bitů, které byly přiděleny jednotlivým lokalitám, budou zahrnuty do svých spádových OSPFv3 oblastí. Tímto budou všechny *lokalitní*



Obr. 22: Návrh dynamického směrování protokolů IPv4 a IPv6 ve vnitřní části univerzitní sítě MENDELU prostřednictvím OSPFv2/v3 včetně očekávaných záznamů ve směrovacích tabulkách páteřních L3 prvků.

VLAN ve směrovacích tabulkách reprezentovány pouze jediným souhrnným záznamem, a sice 56bitovým prefixem svých spádových lokalit. Budou tak ušetřeny desítky záznamů ve směrovacích tabulkách L3 prvků páteře, čímž je optimalizována rychlost procesu směrování paketů IPv6 a ušetřena kapacita paměti. Rovněž bude do směrovacích tabulek automaticky vložen discard route pro 56bitový IPv6 prefix lokality na daném L3 prvku páteře. Jeho účelem je zamezení bloudění IPv6 paketů směrovaných do nevyužitých částí 56bitového IPv6 prefixu dané lokality.

Seznam lokalit a jejich spádových OSPFv3 oblastí je uveden v tab. 19.

Tab. 19: Seznam lokalit a jejich spádových OSPFv3 oblastí.

Lokalita	OSPFv3 Area
X	1
A	2
C	3
B	4
Q	5
E	6
T	7
Z	8
X2	119

Ústředním L3 prvkem *Core*, potažmo směrovačem *VRF CernaPole* bude rovněž prostřednictvím protokolu OSPFv3 propagována všem ostatním L3 prvkům páteře výchozí trasa (default route) pro směrování síťového provozu do DMZ nebo do Internetu.

Všechna SVI *páteřních VLAN* budou na L3 prvcích páteře umístěna do OSPFv3 oblasti 0 a všechna SVI *lokalitních VLAN* do svých spádových OSPFv3 oblastí. Tímto způsobem integrace směrovacího protokolu OSPFv3 je zajištěno, že oblasti se stejným identifikátorem budou v rámci obou protokolů OSPFv2 a OSPFv3 zahrnovat zcela totožná L3 rozhraní. Z toho plyne, že i v případě protokolu OSPFv3 budou všechny L3 prvky páteře vystupovat jako hraniční směrovače oblasti (ABR).

Autentizace OSPFv3

Na základě analýzy podpory protokolu IPv6 na stávajících L3 prvcích univerzitní sítě MENDELU bylo zjištěno, že prozatím není možné mechanismus autentizace OSPFv3 implementovat. Avšak po odstranění překážek znemožňujících integraci autentizace OSPFv3 v univerzitní síti MENDELU bude možné tuto funkci aktivovat na všech SVI *páteřních VLAN*, jako tomu je v současnosti v OSPFv2.

Na rozdíl od OSPFv2 nemá protokol OSPFv3 autentizační volbu v záhlaví svých zpráv LSA. OSPFv3 se místo podpory nativního autentizačního mechanismu spoléhá na IPsec, což je podle Lammle (2013, s. 944) oborový standard sady protokolů a algoritmů, které slouží k zabezpečeným přenosům dat v sítích založených na protokolu

IP a pracují na L3. IPsec umožňuje kromě autentizace zpráv také jejich šifrování. Autentizace dat a hlavičky IP paketu je zprostředkováno protokolem AH (Authentication Header), který využívá jednosměrné hešovací funkce. Šifrování IP paketů je pak umožněno protokolem ESP (Encapsulating Security Payload).

To znamená, že při implementaci autentizace OSPFv3 v univerzitní síti MENDELU může být volitelně nastaveno i šifrování této komunikace.

V rámci konfigurace SVI *páteřních VLAN* bude možné příkazem `ipv6 ospf authentication` povolit pouze autentizaci OSPFv3 prostřednictvím protokolu AH. Příkazem `ipv6 ospf encryption` může být pak provedena aktivace autentizace a zároveň šifrování OSPFv3 komunikace přes protokol ESP.

9.7 Směrování IPv6 na perimetru univerzitní sítě

Směrovače na perimetru univerzitní sítě budou směrovat síťový provoz IPv6 staticky, tak jako v prostředí IPv4. Návrh statického směrování je znázorněn na obr. 23.

VRF CernaPole

Do směrovací tabulky ústředního směrovače vnitřní části univerzitní sítě *VRF CernaPole* je nutné staticky vložit pouze IPv6 záznam výchozí trasy (default route), jejímž prostřednictvím bude směrován veškerý síťový provoz IPv6 z vnitřní části univerzitní sítě určený uzlům v DMZ nebo v Internetu.

Rozhraním dalšího přeskoku výchozí trasy bude inside rozhraní `eth0.21` na *Firewallu*.

VRF Internet

Do směrovací tabulky hraničního směrovače *VRF Internet* je nutné vložit statické záznamy souhrnných IPv6 prefixů *páteřních*, *lokalitních* a *End–To–End VLAN*.

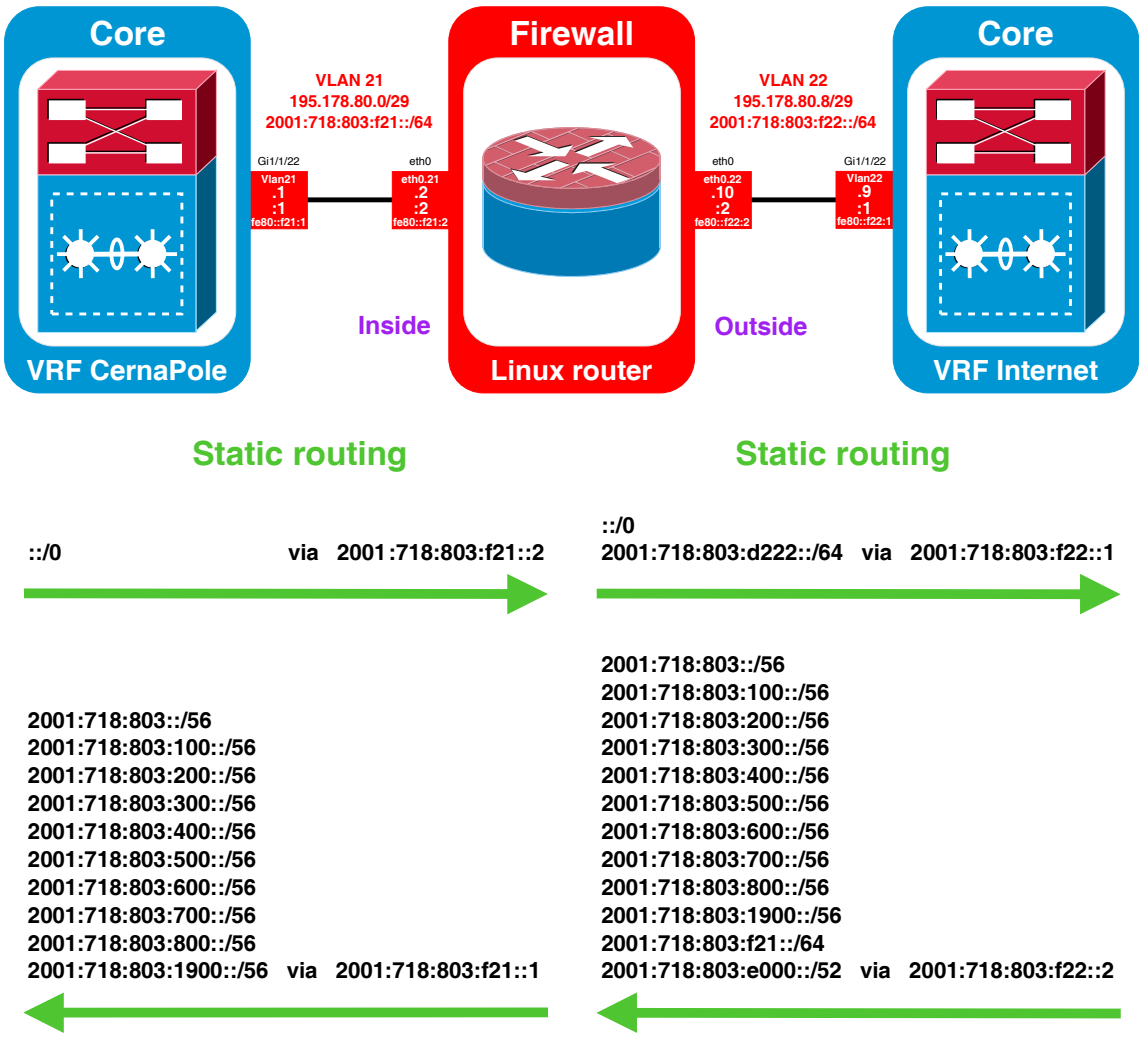
Rovněž je nutné do ní zahrnout statickou trasu do *perimetrové VLAN* 21, která se nachází na straně inside *Firewallu*.

Rozhraním dalšího přeskoku těchto statických záznamů bude outside rozhraní `eth0.22` na *Firewallu*, protože pakety s cílovou IPv6 adresou spadající do některého z uvedených IPv6 prefixů jsou určeny některému síťovému uzlu v univerzitní síti MENDELU.

Firewall

Firewall je v logické topologii perimetru univerzitní sítě umístěn mezi směrovači *VRF Internet* a *VRF CernaPole*.

Pro směrování síťového provozu IPv6 určeného uzlům umístěných ve vnitřní části univerzitní sítě je zapotřebí, aby směrovací tabulka *Firewallu* obsahovala statické záznamy se souhrnnými prefixy *páteřních* a *lokalitních VLAN*. Rozhraním dalšího přeskoku těchto statických záznamů bude SVI `Vlan21` na směrovači *VRF CernaPole*.



Obr. 23: Návrh statického směrování IPv6 na perimetru univerzitní sítě MENDELU.

Pro směrování síťového provozu IPv6 určeného uzlům v DMZ nebo v Internetu je nezbytné, aby směrovací tabulka *Firewallu* obsahovala statické záznamy s prefixem výchozí trasy a *demilitarizované VLAN*. Rozhraním dalšího přeskoku těchto statických záznamů bude tentokrát SVI `Vlan22` na směrovači *VRF Internet*.

9.8 Připojení univerzitní sítě MENDELU k ISP přes IPv6

Jak již bylo zmíněno, poskytovatel internetových služeb CESNET z.s.p.o. plně podporuje protokol IPv6.

K logickému připojení univerzitní sítě MENDELU k ISP je tak zapotřebí, aby Mendelově univerzitě v Brně byly z jeho strany kromě představeného 48bitového prefixu přiděleny další dva IPv6 prefixy, kterými budou adresovány *spojovací VLAN*

910 a 911. Tyto prefixy již nemusí mít délku 48 bitů. Pravděpodobně se bude jednat o dva 64bitové prefixy.

Aby bylo možné v této diplomové práci se *spojovacími VLAN* pracovat, budou jim přiděleny dva fiktivní 64bitové prefixy:

- VLAN 910 – `2001:718:800:3a::/64` (Primární spoj)
- VLAN 911 – `2001:718:800:3b::/64` (Záložní spoj)

Po přidělení IPv6 prefixů pro *spojovací VLAN* bude následně možné staticky přiřadit oběma SVI těchto VLAN, které se nachází na ústředním logickém L3 přepínači *Core*, potažmo na hraničním směrovači *VRF Internet*, globální individuální IPv6 adresy:

- SVI `Vlan910` – `2001:718:800:3a::2/64`
- SVI `Vlan911` – `2001:718:800:3b::2/64`

Na styčných směrovačích ISP *R142* a *R121* budou s největší pravděpodobností konfigurovány IPv6 adresy s identifikátory uzlu `:1`. Popisovaná situace je znázorněna na obr. 24.

Dále je vhodné na těchto SVI vedle globálních individuálních IPv6 adres staticky definovat i link–local adresy, které mohou mít například následující podoby:

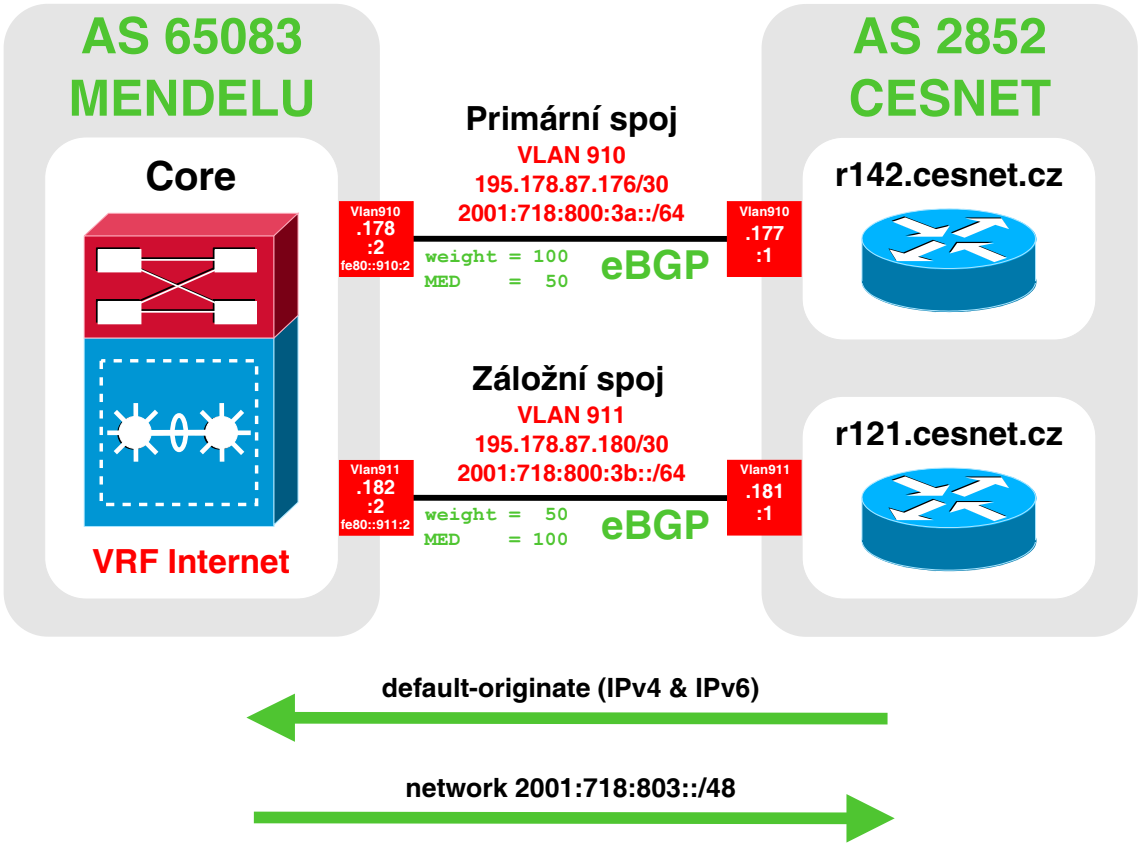
- SVI `Vlan910` – `fe80::910:2` nebo `fe80::800:3a:2`
- SVI `Vlan911` – `fe80::911:2` nebo `fe80::800:3b:2`

První zmíněný způsob odvození link–local adres vychází z VID *spojovacích VLAN*. Ve druhém přístupu jsou pak promítnuty *identifikátory podsítě* jejich IPv6 prefixů. Výběr libovolného přístupu přiřazení link–local adres je plně v kompetencích administrátorů univerzitní sítě MENDELU.

Dále je nezbytné vložit do směrovací tabulky hraničního směrovače *VRF Internet* statický **discard route** pro přidělený 48bitový globální směrovací prefix. Tento krok je nutný ze dvou důvodů:

1. Zamezení bloudění IPv6 paketů směrovaných do nevyužitých částí 48bitového globálního směrovacího prefixu Mendelovy univerzity v Brně, které tak budou hraničním směrovačem *VRF Internet* ihned zlikvidovány. Bez tohoto opatření by si směrovače *VRF Internet* a *R142* vzájemně přeposílaly tyto pakety tak dlouho, dokud by v jejich záhlaví nebyla vynulována hodnota Hop Limit.
2. Uvedením přiděleného globálního směrovacího prefixu univerzitní sítě MENDELU `2001:718:803::/48` do směrovací tabulky směrovače *VRF Internet* v této přesné podobě bude následně umožněno jeho zahrnutí do zpráv BGP Update.

Posledním krokem ke zprovoznění komunikace přes protokol IPv6 mezi univerzitní sítí MENDELU a ISP je rozšíření stávajícího procesu směrovacího protokolu



Obr. 24: Návrh připojení univerzitní sítě MENDELU k ISP přes protokol IPv6.

BGP na ústředním logickém L3 přepínači *Core* o IPv6 (MP–BGP). Tento krok zahrnuje přidání adresové rodiny *ipv6 unicast* k BGP procesu náležícímu hraničnímu směrovači *VRF Internet*. Zde se budou nacházet sousední styčné směrovače ISP *R142* a *R121* se svými globálními individuálními IPv6 adresami, které budou mít konfigurovány v rámci *spojovacích VLAN*.

Následně bude sousednímu směrovači *R142* nastaven BGP atribut weight na hodnotu 100 a sousednímu směrovači *R121* na hodnotu 50.

BGP atribut MED bude oběma sousedním směrovačům přidělen totožným způsobem jako v IPv4 prostřednictvím přiřazení identických route–map. Není zapotřebí vytvářet nové.

Tento návrh rozšíření atributů BGP zcela kopíruje dosavadní konfiguraci procesu BGP pro protokol IPv4.

Posledním krokem je zahrnutí globálního směrovacího prefixu univerzitní sítě MENDELU `2001:718:803::/48` do zpráv BGP Update posílaných ze strany hraničního směrovače *VRF Internet* sousedním směrovačům ISP *R142* a *R121*.

Ze strany ISP je zapotřebí stejná procedura rozšíření procesů BGP na směrovačích *R142* a *R121*. Podstatná je zejména propagace výchozí trasy IPv6 (`::/0`) hraničnímu směrovači univerzitní sítě *VRF Internet*.

10 Implementace navrženého řešení integrace IPv6

Navržené řešení integrace protokolu IPv6 bylo implementováno do fyzického modelu univerzitní sítě MENDELU, jehož atributy vychází z produkční sítě. Model ve všech aspektech obsahuje protokoly IPv4 i IPv6 – Dual Stack.

10.1 Použité technické prostředky

Model byl zkonstruován prostřednictvím technických prostředků Laboratoře síťových technologií Ústavu Informatiky PEF MENDELU. Základní specifikace použitých síťových prvků uvádí tab. 20.

Tab. 20: Souhrn aktivních L3 prvků zahrnutých do modelů univerzitní sítě MENDELU a sítě ISP.

Hostname	**Model Cisco**	**Cisco IOS Image**
6509–Core	Catalyst 6509	[illegible]
3560–core–A	Catalyst 3560	`c3560-ipbasek9-mz.150-1.SE2.bin`
3560–core–C	Catalyst 3560	`c3560-ipbasek9-mz.150-1.SE2.bin`
3560–core–Q	Catalyst 3560	`c3560-ipbasek9-mz.150-1.SE2.bin`
R10	Cisco 2811	`c2800-advipsercicek9-mz.124-15.T7.bin`
SW9	Catalyst 3750	`c3750-ipservicesk9-mz.122-55.SE5.bin`
SW10	Catalyst 3750	`c3750-ipservicesk9-mz.122-55.SE5.bin`
Firewall	Dell OptiPlex 390	`CentOS 6.5`

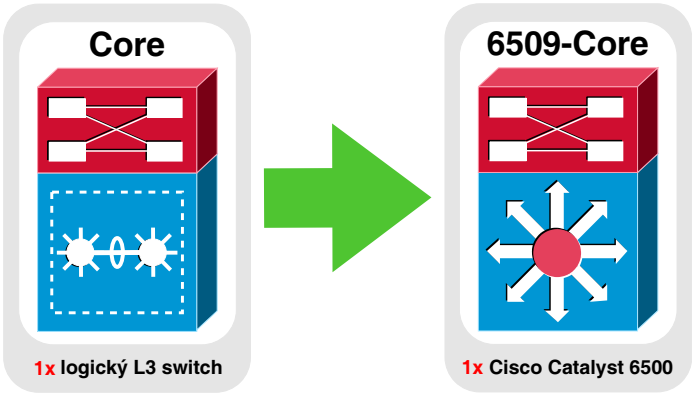
Podle nástroje *Cisco Feature Navigator* podporují téměř všechny zmíněné prvky Cisco požadované funkce protokolu IPv6. Avšak kromě L3 přepínače *6509–Core* žádný z uvedených prvků nepodporuje autentizaci protokolu OSPFv3. Tuto funkci tak nebylo možné v modelu implementovat.

10.2 Modelový ústřední L3 přepínač *6509–Core*

Jak znázorňuje obr. 25, pro modelovou reprezentaci produkčního ústředního L3 přepínače *Core* byl k dispozici pouze jediný L3 přepínač *Cisco Catalyst 6500*, tudíž do modelu nebyla zahrnuta technologie VSS. Tato technologie je z hlediska L3 transparentní.

10.3 Obecná příprava L3 prvků na provoz IPv6

Následující kroky přípravy aktivních L3 prvků Cisco na provoz protokolu IPv6 vychází z oficiálních dokumentací Cisco Systems, Inc. (2014 a 2015).



Obr. 25: Modelová reprezentace ústředního logického L3 přepínače *Core* jediným fyzickým L3 přepínačem s názvem *6509–Core*.

Podpora protokolu IPv6 pro Virtual Routing and Forwarding

Do modelu univerzitní sítě MENDELU byly prostřednictvím technologie VRF–lite zahrnuty oba virtuální směrovače *VRF CernaPole* a *VRF Internet*, které byly zprovozněny na modelovém ústředním L3 přepínači *6509–Core*.

Prvním krokem konfigurace VRF je globální aktivace podpory protokolu IPv6 pro tuto technologii, která se provádí příkazem:

- `ipv6 mls vrf`

Následně je možné definovat jednotlivé virtuální směrovače VRF příkazem:

- `vrf definition <název VRF instance>`

Na úrovni konfigurace jednotlivých VRF instancí je nutné jim přiřadit adresové rodiny IPv4 a IPv6:

- `address-family ipv4`
- `address-family ipv6`

Kompletní konfigurace VRF v modelu univerzitní sítě MENDELU je uvedena v příloze A.

SDM šablona pro souběžný provoz protokolů IPv4 a IPv6

Inicializace provozu protokolu IPv6 vyžaduje na L3 přepínačích *Cisco Catalyst 3560* a *3750* aktivaci SDM šablony pro souběžný provoz protokolů IPv4 a IPv6 příkazem:

- `sdm prefer dual-ipv4-and-ipv6 default`

Po změně SDM šablony je u zmíněných L3 přepínačů nutné potvrdit změnu konfigurace a provést restart.

Aktivace směrování protokolu IPv6

Na všech L3 prvcích Cisco je po předchozích přípravných procedurách nutné již jen povolit směrování IPv6 paketů prostřednictvím příkazu:

- `ipv6 unicast-routing`

V linuxové distribuci CentOS se globální inicializace protokolu IPv6 provádí v konfiguračním souboru sítě, který se nazývá *network* a nachází se v adresáři */etc/sysconfig*. V tomto souboru je zapotřebí povolit směrování IPv6 paketů a globálně zakázat automatickou konfiguraci L3 rozhraní a tunelování přidáním následujících řádků:

- `IPV6FORWARDING=yes`
- `IPV6_AUTOCONF=no`
- `IPV6_AUTOTUNNEL=no`

Kompletní konfigurace sítě na modelovém *Firewallu* je uvedena v příloze B.

10.4 Implementace protokolu IPv6 na L3 rozhraních

Implementace protokolu IPv6 na L3 rozhraních zahrnuje především statické přiřazení globálních individuálních a link–local IPv6 adres.

Na všech L3 prvcích Cisco se provádí statické přiřazení obou typů IPv6 adres na úrovni konfigurace jednotlivých L3 rozhraní příkazy:

- `ipv6 address <`*`IPv6 adresa`*`>/<`*`Délka prefixu`*`>`
- `ipv6 address fe80::<`*`Identifikátor rozhraní`*`> link-local`

V linuxové distribuci CentOS se persistentní statická konfigurace jednotlivých L3 rozhraní provádí prostřednictvím jejich konfiguračních souborů, které se nachází v adresáři */etc/sysconfig/network-scripts/* a mají názvy ve tvaru `ifcfg-<`*`Název rozhraní`*`>`. V těchto souborech je pro statické přiřazení IPv6 adres zapotřebí uvést následující řádky:

- `IPV6INIT=yes`
- `IPV6ADDR=<`*`IPv6 adresa`*`>/<`*`Délka prefixu`*`>`
- `IPV6ADDR_SECONDARIES=fe80::<`*`Identifikátor rozhraní`*`>/<`*`Délka prefixu`*`>`
- `IPV6_AUTOCONF=no`

V linuxové distribuci CentOS nenahrazují statické link–local adresy automaticky generované adresy, které lze ze všech L3 rozhraní odebrat ručně, ale není to nezbytné nutné.

Zprávy ohlášení směrovače (RA)

Na L3 prvcích Cisco způsobí povolení směrování protokolu IPv6 periodické odesílání zpráv ohlášení směrovače (RA) ze všech L3 rozhraní, která mají aktivovaný proces protokolu IPv6 (mají přiřazené IPv6 adresy). Mimo jiné z bezpečnostních důvodů je rozumné toto automatické odesílání zpráv RA v případě SVI *páteřních*, *perimetrových*, *spojovacích*, *správní* a *demilitarizované VLAN* zakázat příkazem:

- `ipv6 nd ra suppress`

Odesílání zpráv RA je nezbytné pouze v případě SVI *End–To–End* a *lokalitních VLAN*, protože se v nich vyskytují automaticky konfigurované koncové uzly.

10.5 Popis modelu univerzitní sítě MENDELU

Model univerzitní sítě MENDELU zahrnuje její páteř, vybrané lokality a perimetr.

Topologie páteře

Logická topologie modelové páteře univerzitní sítě MENDELU je vyobrazena na obr. 26 a zahrnuje čtyři páteřní L3 prvky.

V tab. 21 jsou uvedeny názvy páteřních L3 přepínačů produkční univerzitní sítě MENDELU a názvy modelových L3 přepínačů, kterými jsou reprezentovány.

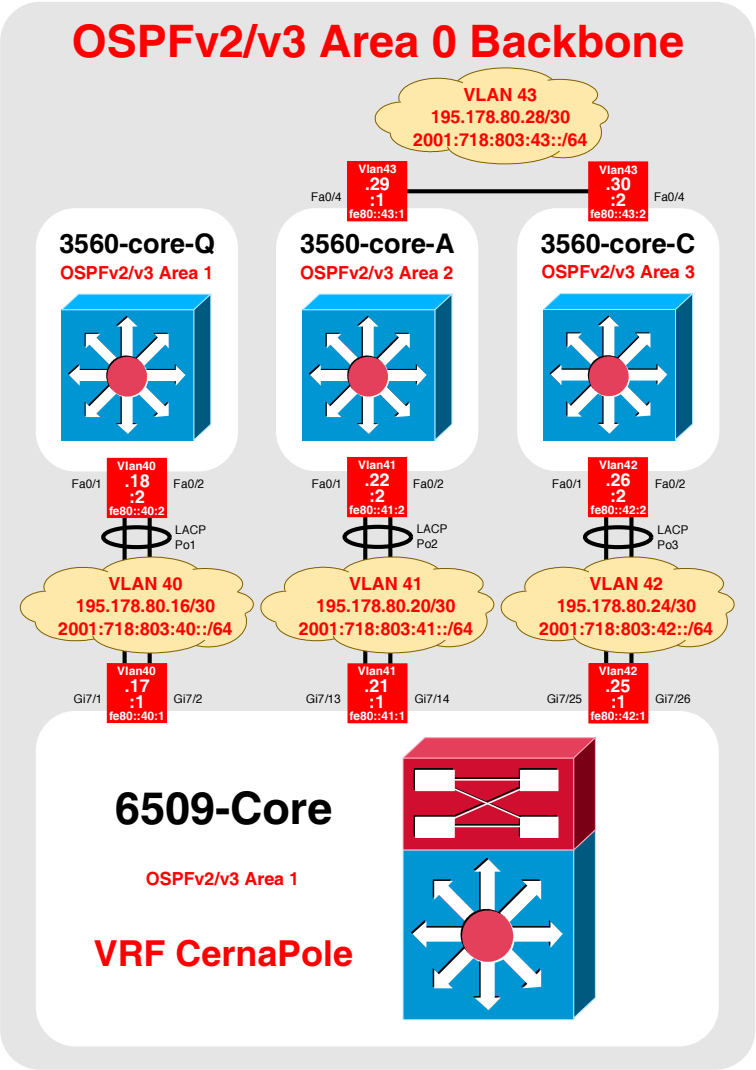
Tab. 21: Názvy L3 přepínačů v produkční univerzitní síti MENDELU a názvy použité v jejím modelu.

Hostname v produkční síti	**Hostname v modelu**
Core	*6509–Core*
core–Q	*3560–core–Q*
core–A	*3560–core–A*
core–C	*3560–core–C*

Všechny modelové páteřní L3 přepínače jsou připojeny na ústřední L3 přepínač *6509–Core* prostřednictvím spojů typu EtherChannel pracujícím na standardním protokolu LACP. Na každém páteřním L3 přepínači je do EtherChannelu zahrnuta dvojice fyzických rozhraní na každý páteřní spoj. Každá dvojice agregovaných fyzických rozhraní vytváří logické rozhraní nazývané PortChannel (Po). Tato logická rozhraní jsou konfigurována jako L2 trunky.

Do modelu byl také zahrnut přímý spoj mezi L3 přepínači *3560–core–A* a *3560–core–C*. Fyzická rozhraní tohoto spoje jsou rovněž konfigurována jako L2 trunky.

Na zmíněných L2 trunk rozhraních je povolen provoz modelových *páteřních VLAN*, jejichž účelem je logické propojení všech L3 prvků v modelu páteře univerzitní sítě. Do modelu byly zahrnuty celkem čtyři *páteřní VLAN* a jejich VID jsou v intervalu **40** až **43**.



Obr. 26: Logická topologie modelu páteře univerzitní sítě MENDELU.

Ústředním L3 prvkem modelu páteře univerzitní sítě je virtuální směrovač *VRF CernaPole*, který je zprovozněný na modelovém ústředním L3 přepínači *6509–Core*.

Kompletní konfigurace L3 atributů všech SVI modelových *páteřních VLAN* je uvedena v příloze C.

Je patrné, že topologie páteře produkční sítě MENDELU a topologie modelové páteře se od sebe liší pouze v počtu L3 prvků. Toto zjednodušení nemá žádný vliv na principy směrování. Ve směrovacích tabulkách bude sice méně záznamů, ale jejich typy zůstanou nedotčeny.

Vybrané lokality

Množstvím L3 prvků umístěných na modelovou páteř univerzitní sítě je zároveň stanoven i počet modelových lokalit, které jsou také čtyři. Jejich přehled uvádí tab. 22.

Tab. 22: Seznam vybraných lokalit zahrnutých do modelu univerzitní sítě MENDELU.

Modelový L3 prvek páteře	Připojená lokalita
VRF CernaPole	**X**
3560–core–A	**A**
3560–core–C	**C**
3560–core–Q	**Q**

V modelu je zahrnuto šest *lokalitních VLAN* s VID **25**, **26**, **84**, **86**, **811** a **819**. Každý exemplář tohoto typu VLAN se vyskytuje pouze v rámci jediné modelové lokality. Všechny páteřní L3 prvky mají pro připojené *lokalitní VLAN* vždy konfigurováno právě jedno SVI, které pro každou z nich slouží jako výchozí brána.

Do modelu univerzitní sítě byl v podobě VLAN 86 zahrnut i zvláštní typ *lokalitní VLAN*, která se sice vyskytuje pouze v rámci lokality X, protože na L3 prvku *6509–Core*, potažmo na *VRF CernaPole*, má své SVI sloužící jako výchozí brána, ale je protažena po L2 trunk rozhraních páteřního spoje na sousední páteřní L3 prvek *3560–core–C*. S tímto typem VLAN lze zacházet totožným způsobem jako s jakoukoli standardní *lokalitní VLAN*.

Topologie vybraných lokalit s modelovými *lokalitními VLAN* je vyobrazena na obr. 27.

Kompletní konfigurace L3 atributů všech SVI modelových *lokalitních VLAN* je uvedena v příloze D.

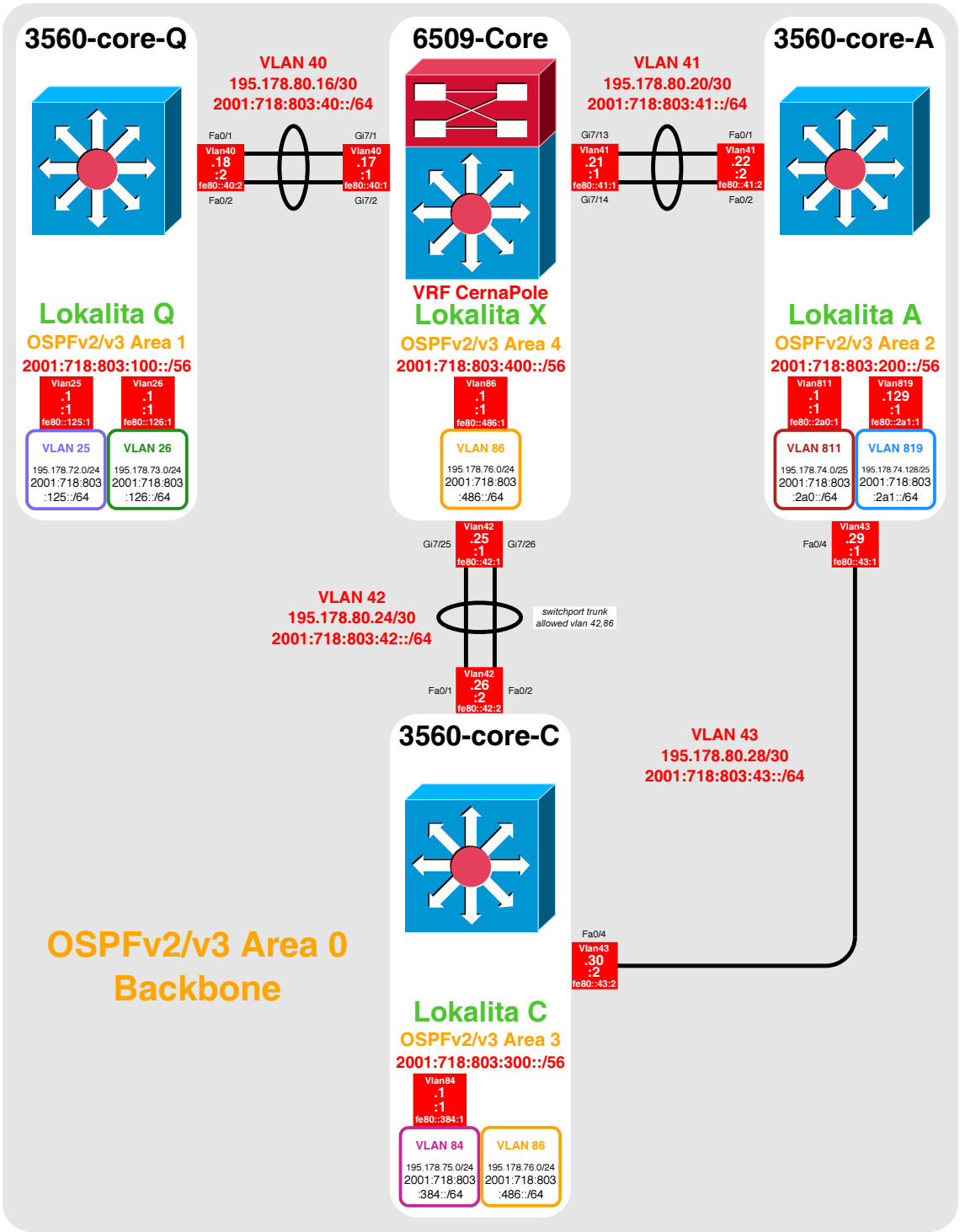
Implementace protokolu OSPFv3

V současné době existují na L3 prvcích Cisco dva způsoby aktivace procesu OSPFv3:

1. **Tradiční způsob** prostřednictvím příkazu:
   - `ipv6 router ospf <Identifikátor procesu>`
2. Nový způsob pomocí **adresových rodin** prostřednictvím příkazu:
   - `router ospfv3 <Identifikátor procesu>`

V souvislosti se zmíněnými způsoby aktivace OSPFv3 procesu platí následující důležitá pravidla:

- V případě aktivace směrovacího protokolu OSPF novým způsobem pomocí adresových rodin je možné provozovat na daném L3 prvku jediný OSPF proces pro protokoly IPv4 i IPv6. Oba protokoly tak sdílí jedinou společnou topologickou databázi LSDB.



Obr. 27: Topologie modelu vnitřní části univerzitní sítě MENDELU s vybranými *lokalitními VLAN*.

- L3 prvek, u nějž byl aktivován proces OPSFv3 novým způsobem prostřednictvím adresové rodiny IPv6, může navázat vztah sousedství s jiným L3 prvkem, u nějž byl aktivován proces OPSFv3 tradičním způsobem.
- L3 prvek, u nějž byl aktivován proces OPSFv2 novým způsobem prostřednictvím adresové rodiny IPv4, nemůže navázat vztah sousedství s jiným L3 prvkem, u nějž byl aktivován proces OPSFv2 tradičním způsobem příkazem `router ospf <Identifikátor procesu>`.
- Proces OSPFv3 lze přiřadit k virtuální směrovací instanci VRF pouze v případě, že je aktivován novým způsobem prostřednictvím adresové rodiny IPv6. Tradiční způsob aktivace procesu OSPFv3 není s VRF vůbec kompatibilní a dokáže pracovat výhradně s globální směrovací tabulkou.
- Nový způsob nasazení OSPFv3 prostřednictvím adresových rodin je podporován pouze L3 přepínači *Cisco Catalyst* řad *4500*, *6500* a *6800* a tato funkce se nazývá *OSPFv3 Address Families*.

Aktivaci procesu OSPFv3 je tedy nezbytné na modelovém ústředním L3 přepínači *6509–Core* provést novým způsobem přes adresové rodiny, protože je následně zapotřebí tento proces přiřadit k virtuálnímu směrovači *VRF CernaPole* příkazem:

- `address-family ipv6 unicast vrf CernaPole`

Na ostatních modelových L3 přepínačích je proces OSPFv3 bez komplikací aktivován tradičním způsobem.

Hodnoty ID směrovačů (Router ID) jsou definovány staticky příkazem:

- `router-id <IPv4 adresa>`

Aktivní rozhraní jsou pouze SVI *páteřních VLAN*, jejichž prostřednictvím si L3 prvky páteře vyměňují směrovací informace:

- `passive-interface default`
- `no passive-interface <SVI páteřní VLAN>`

Souhrnné 56bitové IPv6 prefixy, které byly přiděleny jednotlivým lokalitám, jsou pak přiřazeny do svých spádových OSPFv3 oblastí:

- `area <Identifikátor oblasti> range <IPv6 prefix lokality>::/56`

Tímto jsou všechny *lokalitní VLAN* ve směrovacích tabulkách reprezentovány pouze jediným souhrnným záznamem, a sice 56bitovým IPv6 prefixem svých spádových lokalit.

Seznam lokalit a jejich spádových OSPFv3 oblastí je uveden v tab. 23.

Modelovým ústředním L3 prvkem *6509–Core*, potažmo směrovačem *VRF CernaPole*, je rovněž prostřednictvím protokolu OSPFv3 propagována všem ostatním modelovým L3 prvkům páteře výchozí trasa (default route):

Tab. 23: Seznam modelových lokalit a jejich spádových OSPFv3 oblastí.

Lokalita	OSPFv3 Area
Q	1
A	2
C	3
X	4

- `default-information originate always`

Všechna SVI *páteřních VLAN* jsou na modelovém ústředním L3 prvku *6509–Core*, potažmo na směrovači *VRF CernaPole*, umístěna do páteřní OSPFv3 oblasti 0 novým příkazem:

- `ospfv3 <Identifikátor procesu> ipv6 area 0`

Na ostatních L3 prvcích páteře je stejná akce provedena tradičním příkazem:

- `ipv6 ospf <Identifikátor procesu> area 0`

Všechna SVI *lokalitních VLAN* jsou na modelovém ústředním L3 prvku *6509–Core*, potažmo na směrovači *VRF CernaPole*, umístěna do svých spádových OSPFv3 oblastí novým příkazem:

- `ospfv3 <Identifikátor procesu> ipv6 area <Identifikátor spádové OSPFv3 oblasti dané lokality>`

Na ostatních L3 prvcích páteře je stejná akce provedena tradičním příkazem:

- `ipv6 ospf <Identifikátor procesu> area <Identifikátor spádové OSPFv3 oblasti dané lokality>`

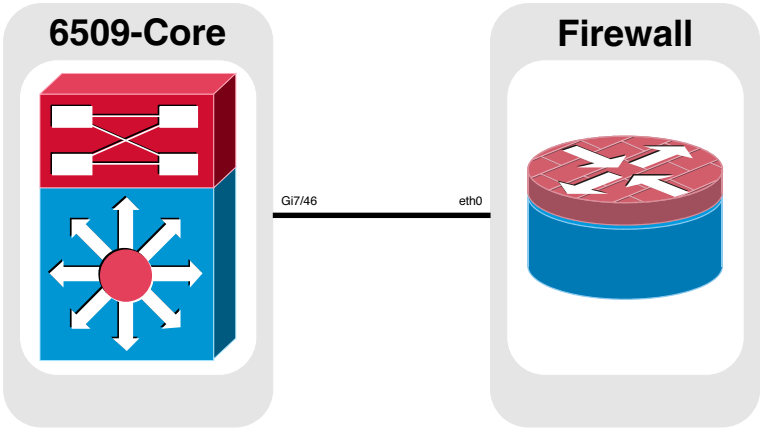
Konkrétní konfigurace protokolu OSPFv3 jsou ke všem zainteresovaným L3 prvkům uvedeny v příloze K.

Perimetr

Fyzická topologie perimetru v modelu univerzitní sítě MENDELU je znázorněna na obr. 28. Jednoduchým spojem jsou propojeny L3 prvky *6509–Core* a *Firewall*.

Logická topologie perimetru v modelu univerzitní sítě je tvořena virtuálními směrovači VRF *CernaPole* a VRF *Internet*, které jsou zprovozněny na modelovém ústředním L3 přepínači *6509–Core*, a *Firewallem*, který se nachází mezi nimi. Logická topologie perimetru univerzitní sítě MENDELU je znázorněna na obr. 29.

Všechny tři uvedené aktivní L3 prvky perimetru v modelu univerzitní sítě jsou propojeny prostřednictvím dvou *perimetrových VLAN* s identifikátory **21** a **22**. Logická topologie perimetru v modelu univerzitní sítě MENDELU tak zcela odpovídá skutečnosti.



Obr. 28: Fyzická topologie perimetru v modelu univerzitní sítě MENDELU.

Kompletní konfigurace L3 atributů všech SVI modelových *perimetrových VLAN* je uvedena v příloze E.

Na základě navrženého řešení integrace IPv6 byly do směrovacích tabulek L3 prvků na perimetru v modelu univerzitní sítě staticky vloženy následující IPv6 záznamy:

- **VRF CernaPole**
  - IPv6 prefix *výchozí trasy* (default route):

    ```
    ipv6 route vrf CernaPole ::/0 2001:718:803:f21::2
    ```

- **VRF Internet**
  - Souhrnný 56bitový IPv6 prefix všech *páteřních VLAN*:

    ```
    ipv6 route vrf Internet 2001:718:803::/56 2001:718:803:f22::2
    ```

  - Všechny souhrnné 56bitové IPv6 prefixy *lokalitních VLAN*:

    ```
    ipv6 route vrf Internet <IPv6 prefix lokality>::/56 2001:718:803:f22::2
    ```

  - Souhrnný 52bitový IPv6 prefix všech *End–To–End VLAN*:

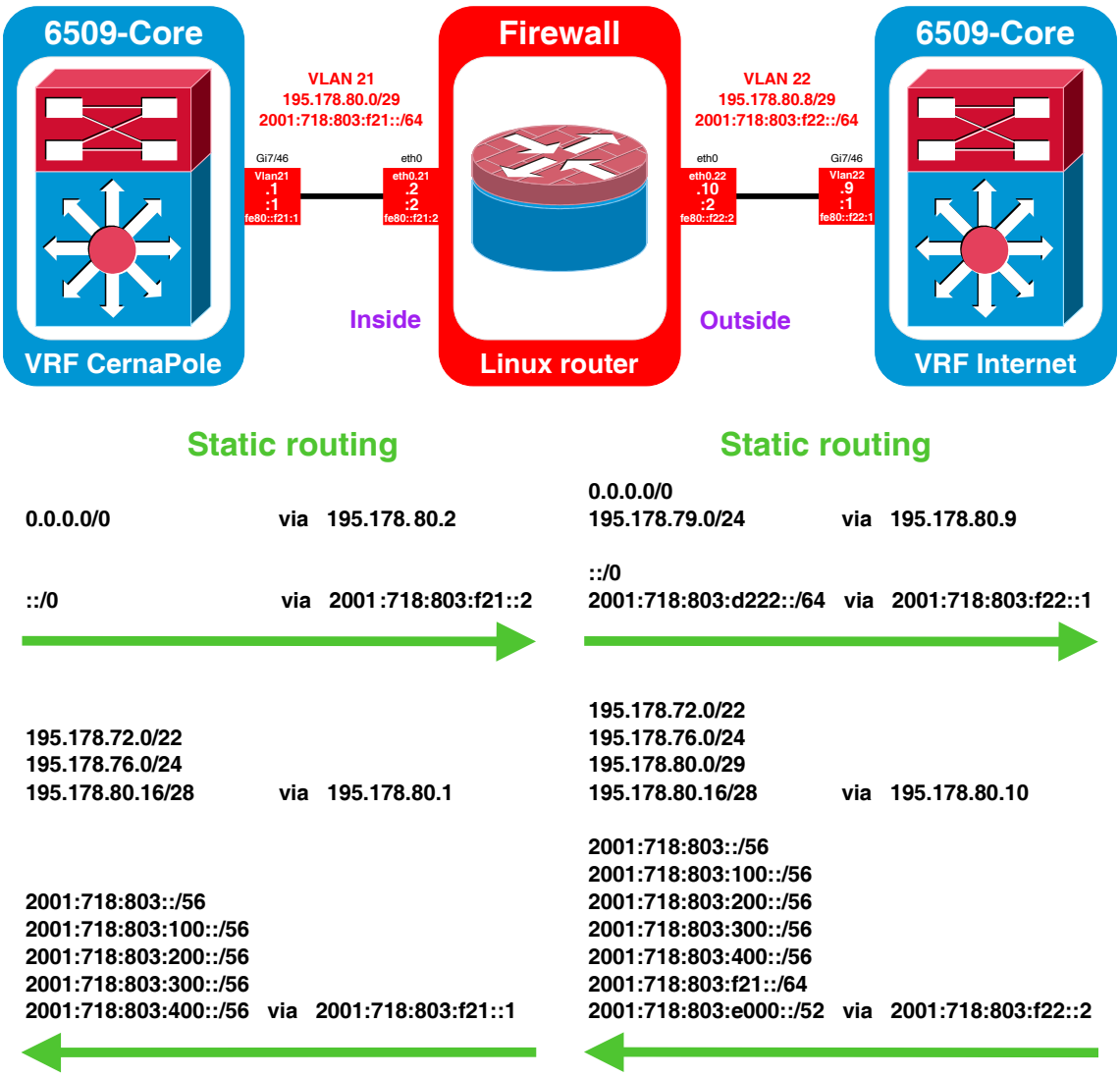
    ```
    ipv6 route vrf Internet 2001:718:803:e000::/52 2001:718:803:f22::2
    ```

  - 64bitový IPv6 prefix odlehlé *perimetrové VLAN* 21:

    ```
    ipv6 route vrf Internet 2001:718:803:f21::/64 2001:718:803:f22::2
    ```

- **Firewall**
  - **inside** – souhrnné IPv6 prefixy *páteřních* a *lokalitních VLAN*:

    ```
    ip -6 route add 2001:718:803::/56 via 2001:718:803:f21::1
    ```



Obr. 29: Logická topologie a statické směrování perimetru v modelu sítě MENDELU.

```
ip -6 route add <IPv6 prefix lokality>::/56 via 2001:718:803:f21::1
```

– **outside** – IPv6 prefix *výchozí trasy* a *demilitarizované VLAN*:

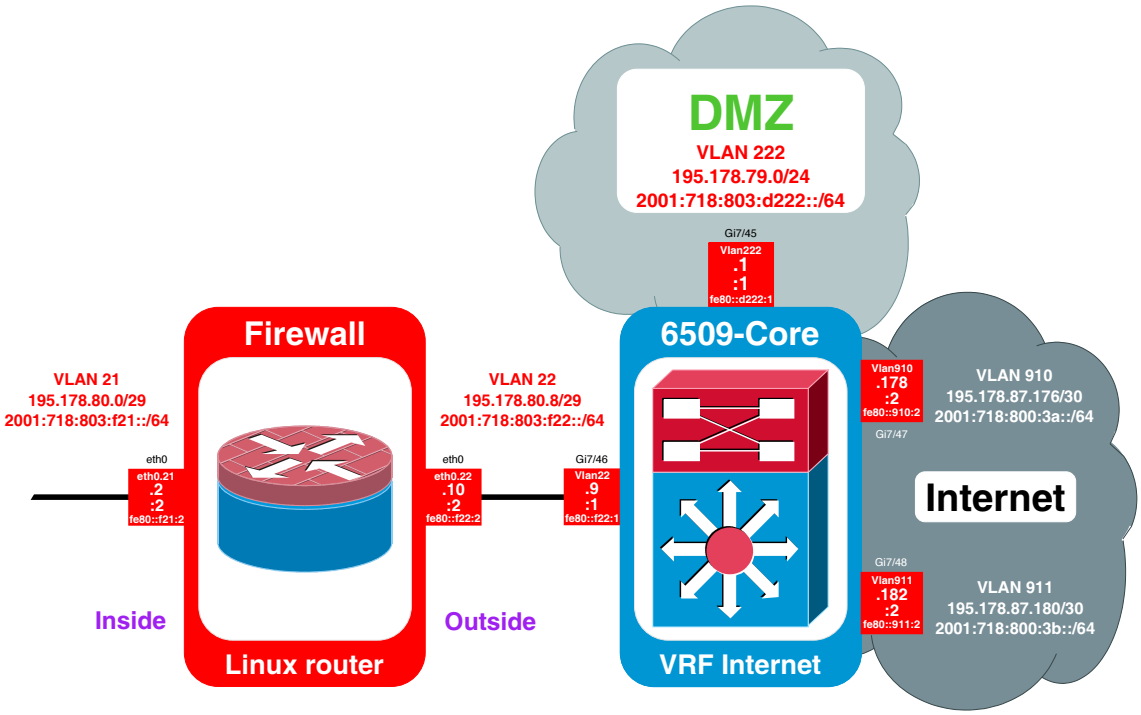
```
ip -6 route add default via 2001:718:803:f22::1
```

```
ip -6 route add 2001:718:803:d222::/64 via 2001:718:803:f22::1
```

Demilitarizovaná zóna

DMZ je reprezentována modelovou *demilitarizovanou VLAN* **222**, která je přímo připojena prostřednictvím SVI `Vlan222` k modelovému hraničnímu směrovači *VRF*

Internet a nachází se tak na straně outside *Firewallu*. Umístění DMZ v topologii modelu univerzitní sítě znázorňuje obr. 30 a přesně odpovídá skutečnosti.



Obr. 30: Demilitarizovaná zóna v topologii modelu univerzitní sítě MENDELU.

Kompletní konfigurace L3 atributů SVI modelové *demilitarizované VLAN* je uvedena v příloze F.

End–To–End VLAN

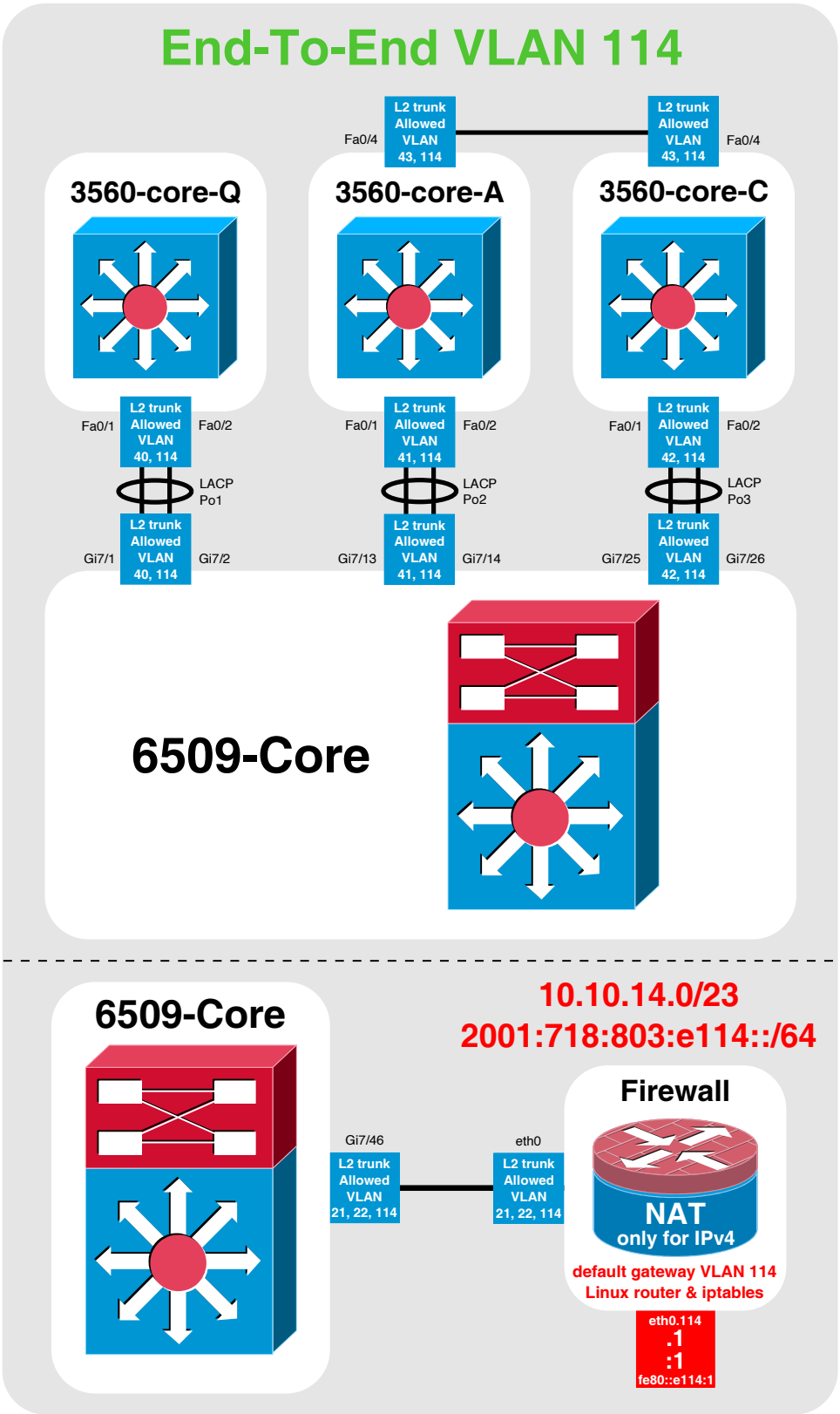
Do modelu univerzitní sítě MENDELU byla zahrnuta příkladová *End–To–End VLAN* **114**, která je prostřednictvím L2 trunků rozprostřena po všech modelových lokalitách a perimetru (stejná L2 trunk rozhraní jako *páteřní*, *lokalitní* a *perimetrové VLAN*). Topologii této modelové *End–To–End VLAN* znázorňuje obr. 31.

Výchozí bránou této modelové *End–To–End VLAN* je SVI `eth0.114` na *Firewallu*. Kompletní konfigurace L3 atributů tohoto SVI je uvedena v příloze G.

Dále je na *Firewallu* pro tuto VLAN zároveň zprovozněn NAT, resp. varianta PAT prostřednictvím příkazu:

- `iptables -t nat -A POSTROUTING -o eth0.22 -s 10.10.14.0/23 -j MASQUERADE`

Všem odchozím paketům protokolu IPv4 určeným síťovým uzlům v DMZ nebo v Internetu jsou tak přepisovány zdrojové privátní IPv4 adresy na veřejnou IPv4 adresu outside rozhraní *Firewallu* `eth0.22`, která je stanovena na `195.178.80.10`.

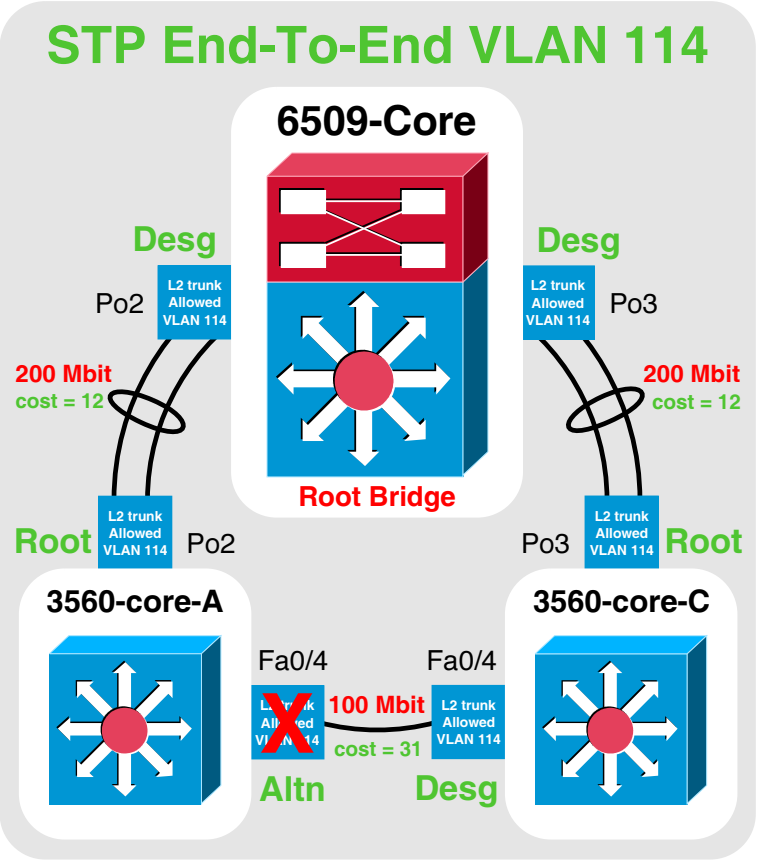


Obr. 31: Topologie modelové *End–To–End VLAN* 114.

Do modelu univerzitní sítě MENDELU byla zahrnuta L2 smyčka způsobená přímým spojením L3 prvků *3560–core–A* a *3560–core–C*. Tuto L2 smyčku je nutné eliminovat zejména v případě modelové *End–To–End VLAN* 114, kde se mohou projevit její negativní dopady na celou síť v případě všesměrové bouře. Modelový ústřední L3 přepínač *6509–Core* byl zvolen jako kořenový most protokolu STP pro *End–To–End VLAN* 114 nastavením atributu *priority* pod prahovou hodnotu 32768 následujícím příkazem:

- `spanning-tree vlan 114 priority 8192`

Výsledek eliminace L2 smyčky prostřednictvím protokolu STP v modelu univerzitní sítě je znázorněn na obr. 32. Zásluhou činnosti STP došlo k zablokování rozhraní `Fa0/4` na L3 přepínači *3560–core–A*, čímž byla L2 smyčka přerušena.



Obr. 32: Eliminace L2 smyčky na modelové páteři univerzitní sítě MENDELU prostřednictvím STP.

Přístupová vrstva

Součástí modelu univerzitní sítě MENDELU je také přístupová vrstva tvořená třemi L2 přepínači *Cisco Catalyst 2960* připojenými prostřednictvím L2 trunků k modelovým páteřním L3 přepínačům *3560–core–Q*, *3560–core–A* a *3560–core–C*.

Verze operačního systému Cisco IOS jsou na těchto L2 přepínačích natolik zastaralé, že nemají ani minimální podporu protokolu IPv6. Jejich přínos v modelu však v současnosti spočívá především v možnosti testování automatické konfigurace protokolu IPv6 u koncových uzlů ve vybraných modelových *lokalitních* a *End–To–End VLAN*. Model univerzitní sítě MENDELU byl záměrně zkonstruován tak, aby mohl být využíván nejen v rámci této diplomové práce.

Přístupová vrstva není v popisu modelu univerzitní sítě MENDELU zahrnuta, protože je z hlediska protokolu IPv6 a zásad jeho směrování zcela bezvýznamná.

10.6 Popis modelu sítě ISP

Pro účely verifikace směrování mezi univerzitní sítí MENDELU a ISP byl zkonstruován jednoduchý model sítě ISP, jehož topologie je vyobrazena na obr. 33. Ve všech aspektech obsahuje protokoly IPv4 i IPv6 – Dual Stack.

Modelové L3 přepínače **SW9** a **SW10** simulují reálné hraniční směrovače *R142* a *R121* skutečného ISP Mendelovy univerzity v Brně – CESNET z.s.p.o. Směrovač **R10** pak simuluje vnitřní L3 prvek modelové sítě ISP.

Z důvodu zjednodušení modelu ISP byly atributy L3 konfigurovány přímo na fyzická rozhraní modelových L3 prvků *SW9*, *SW10* a *R10*. Nenacházejí se zde žádné atributy VLAN.

L3 prvky *SW9* a *R10* jsou propojeny spojovací sítí s prefixy:

- IPv4 – `195.113.156.4/30`
- IPv6 – `2001:718:1:40::/64`

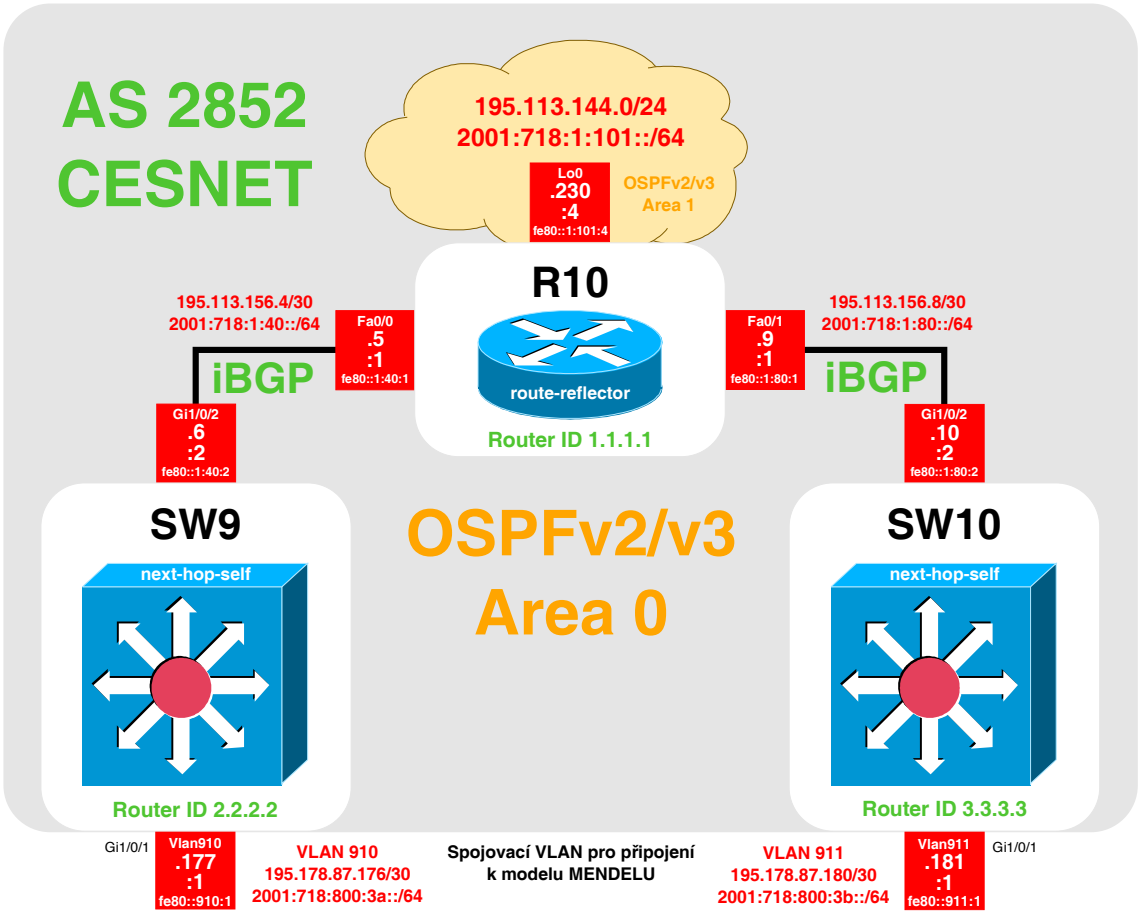
L3 prvky *SW10* a *R10* jsou propojeny spojovací sítí s prefixy:

- IPv4 – `195.113.156.8/30`
- IPv6 – `2001:718:1:80::/64`

Všechna L3 rozhraní uvedených spojovacích sítí spadají do OSPFv2/v3 oblasti 0, takže se obě tyto sítě vyskytují ve směrovacích tabulkách všech L3 prvků modelového ISP, čímž je mezi nimi zajištěna úplná konektivita.

Na směrovači *R10* bylo dále konfigurováno zpětnovazební rozhraní `Lo0`, jehož účelem je simulace koncové sítě ISP s prefixy:

- IPv4 – `195.113.144.0/24`
- IPv6 – `2001:718:1:101::/64`



Obr. 33: Jednoduchý model sítě ISP.

Toto zpětnovazební rozhraní spadá do OSPFv2/v3 oblasti 1, tudíž je *R10* hraničním směrovačem oblasti (ABR) a zmíněnou koncovou síť propaguje L3 přepínačům *SW9* a *SW10* přes OSPFv2/v3 zprávy LSA Type 3 (Inter–Area).

Všechny tyto L3 prvky spadají do modelového autonomního systému 2852.

L3 přepínač *SW9* a směrovač *R10* jsou sousedy typu iBGP. Rovněž L3 přepínač *SW10* a směrovač *R10* jsou sousedy typu iBGP.

Směrovač *R10* je pro sousední směrovače *SW9* a *SW10* konfigurován jako *Route Reflector*, tudíž není zapotřebí vytvářet full mesh topologii protokolu BGP. Směrovač *R10* přeposílá Route Reflector klientům síťové prefixy, které sám prostřednictvím protokolu BGP obdrží.

Hraniční L3 přepínače *SW9* a *SW10* mají v rámci konfigurace BGP pro sousední směrovač *R10* aktivovánu funkci *next–hop–self*. Oba hraniční L3 přepínače tak upravují u síťových prefixů, které přeposílají směrovači *R10*, původní adresy rozhraní dalšího přeskoku na adresy svých vlastních L3 rozhraní přiléhající ke směrovači *R10*, který tak nemusí mít ve směrovací tabulce záznamy *spojovacích VLAN* 910 a 911, aby si mohl uložit síťové prefixy pocházející od směrovače *VRF Internet*.

11 Verifikace navrženého řešení integrace IPv6

Na základě výstupů z různých příkazů výpisů získaných ze všech aktivních prvků modelů sítí MENDELU a ISP bude rozhodnuto o správnosti navrženého řešení integrace IPv6 do univerzitní sítě MENDELU.

11.1 Test 1: Směrování ve vnitřní části modelu sítě MENDELU

Účelem tohoto verifikačního testu je ověření navržené implementace protokolu OSPFv3 na modelu univerzitní sítě MENDELU.

Očekávaným výsledkem tohoto testu je přítomnost záznamů všech *páteřních* a *lokalitních VLAN* ve směrovacích tabulkách L3 prvků *VRF CernaPole*, *3560–core–Q*, *3560–core–A* a *3560–core–C*.

Okolnosti verifikačního testu

Pracovní topologie pro tento verifikační test je vyobrazena na obr. 27 na straně 85.

Kompletní modelová konfigurace protokolu OSPFv3 je ke všem zainteresovaným L3 prvkům uvedena v příloze K.

Výsledek verifikačního testu

Modelová implementace protokolu OSPFv3 zajistila, že výsledné směrovací tabulky IPv6 modelových páteřních L3 prvků obsahovaly záznamy:

- všech *páteřních VLAN* – záznamy typu `O`,
- všech *lokalitních VLAN* – záznamy typu `OI`,
- výchozí trasy – záznamy typu `OE2`.

```
6509-Core#show ipv6 route vrf CernaPole ospf

O   2001:718:803:43::/64    [110/16385]   via FE80::41:2, Vlan41
                                          via FE80::42:2, Vlan42
OI  2001:718:803:100::/56   [110/2]       via FE80::40:2, Vlan40
OI  2001:718:803:200::/56   [110/2]       via FE80::41:2, Vlan41
OI  2001:718:803:300::/56   [110/2]       via FE80::42:2, Vlan42
O   2001:718:803:400::/56   [110/1]       via Null0, directly connected

3560-core-Q#show ipv6 route ospf

OE2 ::/0                    [110/1]       via FE80::40:1, Vlan40
O   2001:718:803:41::/64    [110/2]       via FE80::40:1, Vlan40
O   2001:718:803:42::/64    [110/2]       via FE80::40:1, Vlan40
O   2001:718:803:43::/64    [110/16386]   via FE80::40:1, Vlan40
O   2001:718:803:100::/56   [110/0]       via Null0, directly connected
OI  2001:718:803:200::/56   [110/3]       via FE80::40:1, Vlan40
OI  2001:718:803:300::/56   [110/3]       via FE80::40:1, Vlan40
```

```
OI  2001:718:803:400::/56   [110/2]       via FE80::40:1, Vlan40

3560-core-A#show ipv6 route ospf

OE2 ::/0                    [110/1]   via FE80::41:1, Vlan41
O   2001:718:803:40::/64    [110/2]   via FE80::41:1, Vlan41
O   2001:718:803:42::/64    [110/2]   via FE80::41:1, Vlan41
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
OI  2001:718:803:300::/56   [110/3]   via FE80::41:1, Vlan41
OI  2001:718:803:400::/56   [110/2]   via FE80::41:1, Vlan41

3560-core-C#show ipv6 route ospf

OE2 ::/0                    [110/1]   via FE80::42:1, Vlan42
O   2001:718:803:40::/64    [110/2]   via FE80::42:1, Vlan42
O   2001:718:803:41::/64    [110/2]   via FE80::42:1, Vlan42
OI  2001:718:803:100::/56   [110/3]   via FE80::42:1, Vlan42
OI  2001:718:803:200::/56   [110/3]   via FE80::42:1, Vlan42
O   2001:718:803:300::/56   [110/0]   via Null0, directly connected
OI  2001:718:803:400::/56   [110/2]   via FE80::42:1, Vlan42
```

Z toho vyplývá, že zásluhou činnosti protokolu OSPFv3 byla ve vnitřní části modelu univerzitní sítě MENDELU zprovozněna konektivita mezi všemi koncovými VLAN. Implementace protokolu OSPFv3 byla provedena na základě navrženého řešení integrace protokolu IPv6 do univerzitní sítě. Lze tedy vyvodit závěr, že navržené řešení směrování IPv6 ve vnitřní části univerzitní sítě MENDELU prostřednictvím protokolu OSPFv3 bylo úspěšně verifikováno.

11.2 Test 2: Směrování na perimetru modelu sítě MENDELU

Účelem tohoto verifikačního testu je ověření navržené implementace statického směrování IPv6 na perimetru modelu univerzitní sítě MENDELU.

Očekávaným výsledkem tohoto testu je přítomnost požadovaných statických záznamů ve směrovacích tabulkách L3 prvků *VRF CernaPole*, *VRF Internet* a *Firewall*.

Okolnosti verifikačního testu

Pracovní topologie pro tento verifikační test je vyobrazena na obr. 29 na straně 89.

Výsledek verifikačního testu

```
6509-Core#show ipv6 route vrf CernaPole static

S   ::/0                    [1/0]    via 2001:718:803:F21::2

6509-Core#show ipv6 route vrf Internet static

S   2001:718:803::/48       [1/0]    via Null0, directly connected
S   2001:718:803::/56       [1/0]    via 2001:718:803:F22::2
S   2001:718:803:100::/56   [1/0]    via 2001:718:803:F22::2
S   2001:718:803:200::/56   [1/0]    via 2001:718:803:F22::2
S   2001:718:803:300::/56   [1/0]    via 2001:718:803:F22::2
S   2001:718:803:400::/56   [1/0]    via 2001:718:803:F22::2
S   2001:718:803:F21::/64   [1/0]    via 2001:718:803:F22::2
S   2001:718:803:E000::/52  [1/0]    via 2001:718:803:F22::2

[root@firewall _Lab]# ip -6 route show

2001:718:803::/56                   via 2001:718:803:f21::1 dev eth0.21  metric 1024
2001:718:803:100::/56               via 2001:718:803:f21::1 dev eth0.21  metric 1024
2001:718:803:200::/56               via 2001:718:803:f21::1 dev eth0.21  metric 1024
2001:718:803:300::/56               via 2001:718:803:f21::1 dev eth0.21  metric 1024
2001:718:803:400::/56               via 2001:718:803:f21::1 dev eth0.21  metric 1024
2001:718:803:d222::/64              via 2001:718:803:f22::1 dev eth0.22  metric 1024
default                             via 2001:718:803:f22::1 dev eth0.22  metric 1024
```

Výsledné statické záznamy ve směrovacích tabulkách L3 prvků na perimetru v modelu univerzitní sítě přesně odpovídají požadovanému stavu.

11.3 Test 3: Směrování mezi modely sítí MENDELU a ISP

Účelem tohoto verifikačního testu je ověření navržené implementace protokolu BGP na propojených modelech univerzitní sítě MENDELU a ISP.

Očekávaným výsledkem tohoto verifikačního testu je:

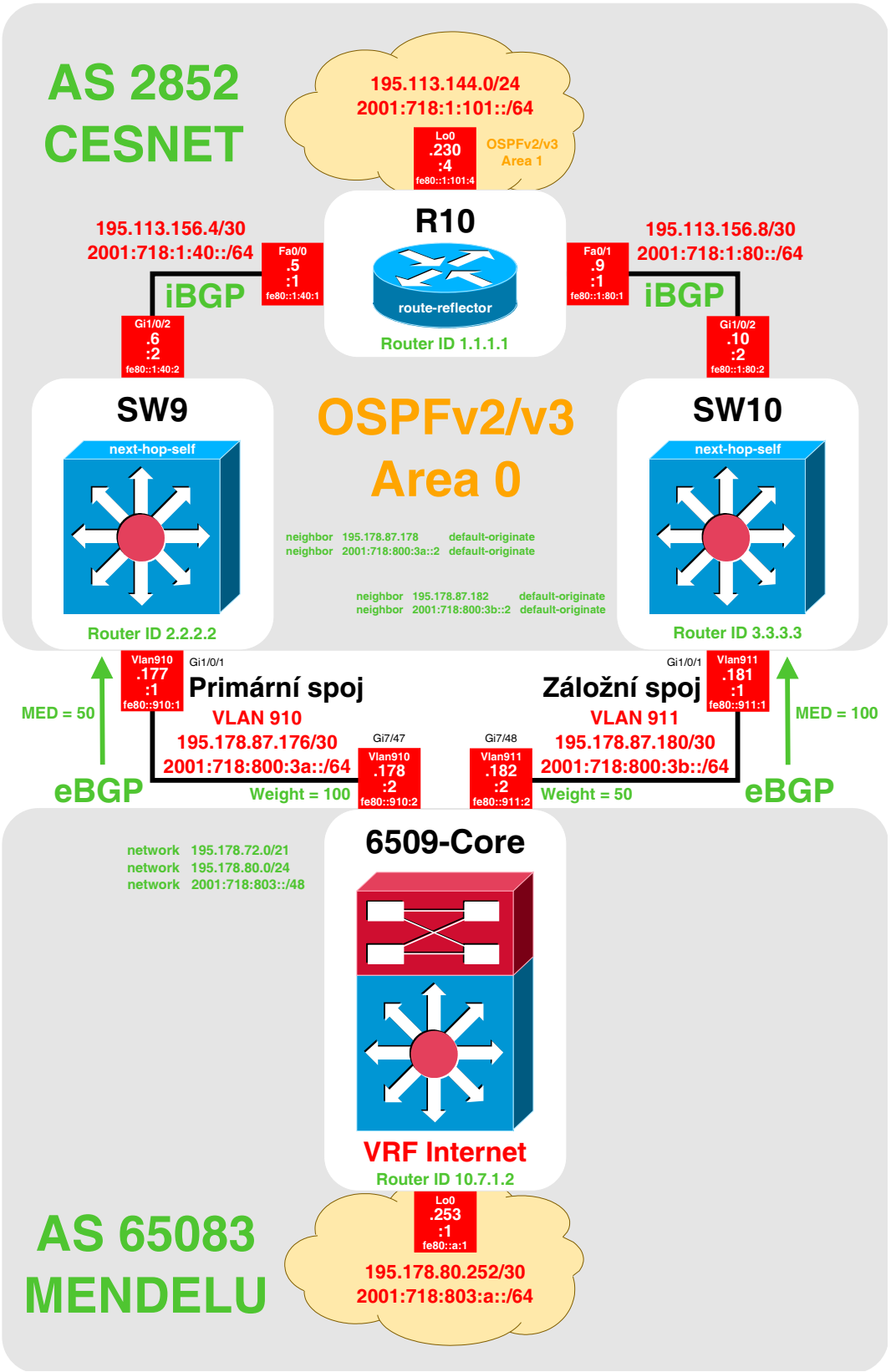
1. Přítomnost IPv6 prefixu výchozí trasy (`::/0`) ve směrovací tabulce hraničního směrovače modelu univerzitní sítě MENDELU *VRF Internet* získaného prostřednictvím směrovacího protokolu BGP.
2. Přítomnost 48bitového globálního směrovacího IPv6 prefixu Mendelovy univerzity v Brně (`2001:718:803::/48`) ve směrovací tabulce vnitřního směrovače modelu ISP *R10* rovněž získaného prostřednictvím směrovacího protokolu BGP.

Okolnosti verifikačního testu

Pracovní topologii tohoto verifikačního testu znázorňuje obr. 34.

Kompletní modelové konfigurace SVI *spojovacích VLAN* a protokolu BGP jsou ke všem zainteresovaným L3 prvkům uvedeny v přílohách I a L.

Znázorněná topologie a konfigurace směrovacího protokolu BGP zcela přesně odráží skutečnou situaci mezi produkční univerzitní sítí MENDELU a ISP.



Obr. 34: Topologie připojení hraničního L3 prvku modelu univerzitní sítě k modelu ISP.

Výsledek verifikačního testu

```
6509-Core#show bgp vpnv6 unicast vrf Internet summary

BGP router identifier 10.7.1.2, local AS number 65083

Neighbor             V           AS   State/PfxRcd
2001:718:800:3A::1   4         2852          1
2001:718:800:3B::1   4         2852          1
```

Hraniční směrovač modelu univerzitní sítě MENDELU *VRF Internet* obdržel od sousedních hraničních L3 přepínačů modelu ISP *SW9* a *SW10* zprávy BGP Update obsahující IPv6 prefix výchozí trasy `::/0`.

```
6509-Core#show bgp vpnv6 unicast vrf Internet

local router ID is 10.7.1.2
Status codes: * valid, > best

     Network             Next Hop            Metric   LocPrf   Weight   Path

 *>  ::/0                2001:718:800:3A::1       0              100   2852 i
 *                       2001:718:800:3B::1       0               50   2852 i
 *>  2001:718:803::/48   ::                       0            32768   i
```

Vzhledem ke konfigurovanému atributu BGP weight upřednostňuje hraniční směrovač modelu univerzitní sítě MENDELU *VRF Internet* směrovací informace obdržené od hraničního L3 přepínače modelu sítě ISP *SW9*, který je pro něho sousedem na primárním spoji (VLAN 910).

```
6509-Core#show ipv6 route vrf Internet bgp

B     ::/0     [20/0]     via FE80::910:1, Vlan910
```

Hraniční směrovač modelu univerzitní sítě MENDELU *VRF Internet* si propagovaný IPv6 prefix výchozí trasy `::/0` uložil do své směrovací tabulky s IPv6 adresou rozhraní dalšího přeskoku `fe80::910:1`, které se nachází přímo na hraničním L3 přepínači *SW9*. Jedná se o sousedství typu eBGP, tudíž je administrativní vzdálenost záznamu rovna 20.

```
R10#show ipv6 route bgp

B     2001:718:803::/48     [200/50]     via 2001:718:1:40::2
```

Vnitřní směrovač modelu sítě ISP *R10* si do směrovací tabulky uložil 48bitový globální směrovací prefix univerzitní sítě MENDELU. Získal jej od svého iBGP souseda *SW9* (administrativní vzdálenost záznamu je 200, metrika 50), který tento prefix získal od hraničního směrovače modelu univerzitní sítě MENDELU *VRF Internet*

a vzhledem k povolené funkci *next–hop–self* jej propaguje směrovači *R10* s vlastní IPv6 adresou rozhraní dalšího přeskoku.

Hraniční L3 prvky modelů univerzitní sítě MENDELU a sítě ISP tak byly schopny zprostředkovávat komunikaci mezi oběma subjekty, protože ve svých směrovacích tabulkách měly potřebné informace o směrování. Dosažené výsledky se tak plně shodují s očekávanými. Z toho plyne, že navržené řešení směrování IPv6 mezi univerzitní sítí MENDELU a ISP prostřednictvím směrovacího protokolu BGP bylo úspěšně verifikováno.

11.4 Test 4: Selhání primárního spoje mezi MENDELU a ISP

Účelem tohoto verifikačního testu je ověření reakce směrovacího protokolu BGP na selhání primárního spoje mezi modely univerzitní sítě MENDELU a sítě ISP.

Očekávaným výsledkem tohoto verifikačního testu je:

1. Úprava rozhraní dalšího přeskoku u IPv6 prefixu výchozí trasy (`::/0`) ve směrovací tabulce hraničního směrovače modelu univerzitní sítě MENDELU *VRF Internet* získaného prostřednictvím směrovacího protokolu BGP.
2. Úprava rozhraní dalšího přeskoku u 48bitového globálního směrovacího IPv6 prefixu Mendelovy univerzity v Brně (`2001:718:803::/48`) ve směrovací tabulce vnitřního směrovače modelu ISP *R10* získaného prostřednictvím směrovacího protokolu BGP.

Podstatný je také čas, za který je schopen směrovací protokol BGP automatickou konvergenci provést.

Okolnosti verifikačního testu

Pracovní topologii tohoto verifikačního testu opět znázorňuje obr. 34, protože se od předchozího verifikačního testu neliší.

Také konfigurace zainteresovaných modelových L3 prvků zůstala nezměněna.

Výsledek verifikačního testu

Verifikační test byl započat spuštěním příkazu ping na hraničním směrovači modelu univerzitní sítě *VRF Internet*:

- `ping vrf Internet 2001:718:1:101::4 source lo0 repeat 20000`

Tímto příkazem byl proveden test konektivity mezi fiktivními koncovými sítěmi v modelech sítí MENDELU a ISP. Koncové sítě byly v obou případech simulované zpětnovazebními rozhraními `Lo0`, které se v případě modelu sítě MENDELU nacházelo na hraničním směrovači *VRF Internet* a v případě sítě ISP na vnitřním směrovači *R10*. Celkem bylo odesláno 20000 testovacích paketů.

V průběhu posílání testovacích paketů byl z fyzického rozhraní `Gi7/47`, které se nachází na hraničním směrovači modelu univerzitní sítě *VRF Internet*, vypojen síťový kabel. Došlo tak k přerušení primárního spoje mezi hraničním směrovačem *VRF Internet* a hraničním L3 přepínačem modelu sítě ISP *SW9*.

```
Success rate is 99 percent (19999/20000), round-trip min/avg/max = 0/0/84 ms
```

Automatická konvergence směrovacího protokolu BGP trvala méně než jednu sekundu a byl ztracen jediný testovací paket, což je výborný výsledek.

```
6509-Core#show bgp vpnv6 unicast vrf Internet summary

BGP router identifier 10.7.1.2, local AS number 65083

Neighbor             V           AS   State/PfxRcd
2001:718:800:3A::1   4         2852   Idle
2001:718:800:3B::1   4         2852          1
```

Po selhání primárního spoje byl pro hraniční směrovač modelu univerzitní sítě *VRF Internet* logicky nedostupný sousední L3 přepínač *SW9* s IPv6 adresou `2001:718:800:3A::1`. IPv6 prefix výchozí trasy `::/0` tak v danou chvíli propagoval pouze L3 přepínač *SW10* nacházející se na záložním spoji.

```
6509-Core#show bgp vpnv6 unicast vrf Internet

local router ID is 10.7.1.2
Status codes: * valid, > best

     Network             Next Hop            Metric   LocPrf   Weight   Path

 *>  ::/0                2001:718:800:3B::1       0               50   2852 i
 *>  2001:718:803::/48   ::                       0            32768   i
```

IPv6 prefix výchozí trasy `::/0` byl tak při selhání primárního spoje nedostupný se standardním rozhraním dalšího přeskoku s IPv6 adresou `2001:718:800:3A::1` a s hodnotou atributu BGP weight 100. Při selhání primárního spoje byl tento prefix k dispozici pouze s rozhraním dalšího přeskoku s IPv6 adresou `2001:718:800:3B::1` nacházející se na záložním spoji s nižší hodnotou atributu BGP weight 50.

```
6509-Core#show ipv6 route vrf Internet bgp

B     ::/0     [20/0]     via FE80::911:1, Vlan911
```

Důležitá je ovšem skutečnost, že ve směrovací tabulce hraničního směrovače modelu univerzitní sítě *VRF Internet* došlo u IPv6 prefixu výchozí trasy `::/0` pouze k úpravě rozhraní dalšího přeskoku, nikoli k úplnému odstranění tohoto záznamu ze směrovací tabulky. Konektivita na model sítě ISP tak byla i po selhání primárního spoje nadále dostupná.

```
R10#show ipv6 route bgp

B     2001:718:803::/48     [200/100]     via 2001:718:1:80::2
```

Také ve směrovací tabulce vnitřního směrovače modelu ISP *R10* došlo pouze k úpravě rozhraní dalšího přeskoku u 48bitového globálního směrovacího IPv6 prefixu univerzitní sítě MENDELU, který jej při výpadku získával od sousedního L3 přepínače *SW10* s horší metrikou 100. Avšak i zde byla nadále dostupná konektivita směrem do modelu univerzitní sítě MENDELU.

Zásluhou automatické konvergence směrovacího protokolu BGP tak byla v plném rozsahu zachována konektivita mezi modely sítí MENDELU a ISP, přičemž síťový provoz byl automaticky přeřazen na záložní spoj.

Verifikační test konektivity v případě selhání primárního spoje mezi sítěmi MENDELU a ISP tak dopadl opět úspěšně.

12 Závěr

V rámci této diplomové práce byl pro produkční univerzitní síť MENDELU zpracován komplexní návrh integrace protokolu IPv6 v oblasti směrování.

Nejdůležitějšími složkami vytvořeného návrhu pro nasazení protokolu IPv6 jsou:

- Zvolený přechodový mechanismus Dual Stack pro souběžný provoz protokolů IPv4 a IPv6.
- Navržený adresní plán IPv6, jehož výhodami jsou snadná identifikace jednotlivých VLAN v univerzitní síti, optimalizace procesu směrování IPv6 zásluhou sumarizace a prostor pro další rozšiřování univerzitní sítě MENDELU.
- Návrh implementace směrovacího protokolu OSPFv3 pro směrování síťového provozu IPv6 na páteři a mezi jednotlivými lokalitami univerzitní sítě.
- Návrh implementace statického směrování síťového provozu IPv6 na perimetru univerzitní sítě.
- Návrh implementace směrovacího protokolu BGP, respektive jeho aktualizace MP–BGP, za účelem směrování síťového provozu IPv6 mezi univerzitní sítí Mendelovy univerzity v Brně a jejím poskytovatelem internetových služeb CESNET z.s.p.o.

V prostředí Laboratoře síťových technologií ÚI PEF MENDELU se s využitím dostupných technických prostředků podařilo na zkonstruovaných fyzických modelech univerzitní sítě MENDELU a jednoduché sítě ISP prostřednictvím verifikačních testů ověřit:

- Návrh implementace směrovacího protokolu OSPFv3.
- Návrh implementace směrovacího protokolu BGP, respektive jeho aktualizace MP–BGP.
- Automatickou konvergenci směrovacího protokolu BGP s ohledem na protokol IPv6 v případě selhání primárního spoje mezi univerzitní sítí MENDELU a jejím poskytovatelem internetových služeb CESNET z.s.p.o.

Z výše uvedených skutečností vyplývá, že bylo dosaženo cíle této diplomové práce.

Vzhledem k neaktuálním verzím operačního systému Cisco IOS na síťových zařízeních dostupných v laboratoři síťových technologií ÚI PEF MENDELU nebylo možné provést implementaci autentizace směrovacího protokolu OSPFv3 na SVI *páteřních VLAN* v modelu univerzitní sítě MENDELU. Z důvodu zabezpečení je však velmi záhodno odstranit veškeré překážky bránící implementaci této funkce v produkční univerzitní síti MENDELU, což může vyžadovat určité finanční náklady ze strany Mendelovy univerzity v Brně.

Dalšími nezbytnými kroky v kontextu s postupným nasazením protokolu IPv6 do univerzitní sítě MENDELU by měly být návrhy řešení v oblastech zabezpečení a síťových služeb (nasazení iptables6, DNS, webové služby, univerzitní pošta apod.).

Po dosažení nezbytné míry zabezpečení univerzitní sítě MENDELU v souvislosti s protokolem IPv6 bude možné postupně umožnit síťovou konektivitu přes nový protokol i koncovým uzlům.

Nakonec by měla následovat integrace protokolu IPv6 i do geograficky vzdálených oblastí univerzitní sítě MENDELU, jimiž jsou Zahradnická fakulta a koleje Jana Amose Komenského (JAK) a koleje Josefa Taufera (TAK).

13 Literatura

BRUNO, A. *CCDA 640-864 Official Cert Guide*. Indianapolis, IN 46240 USA: Cisco Press, 2011, 721 s. ISBN 978-1-58714-257-4.

Cisco.com. *How To Configure InterVLAN Routing on Layer 3 Switches* [online]. 2014 [cit. 2015-03-07]. Dostupné z: <http://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html#proc>.

Cisco Systems, Inc. *OSPFv3 VRF-Lite/PE-CE* [online]. 2015 [cit. 2015-01-17]. Dostupné z: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-15-sy-book.pdf>.

Cisco Systems, Inc. *Cisco IOS IPv6 Command Reference* [online]. 2014 [cit. 2015-03-19]. Dostupné z: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/command/ipv6-cr-book.pdf>.

EMPSON, S. *CCNP Routing and Switching Portable Command Guide*. Indianapolis, IN 46240 USA: Cisco Press, 2014, 391 s. ISBN 978-1-58714-434-9.

HAKL, J. *Návrh integrace protokolu IPv6 ve firmě Z-Ware*. Brno, 2013. Bakalářská práce. Mendelova univerzita v Brně.

HRACHOVSKÝ, J. *Přechod počítačových sítí z IPv4 na IPv6*. Zlín, 2012. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně.

HUCABY, D. *CCNP Routing and Switching SWITCH 300-115 Official Cert Guide*. Indianapolis, IN 46240 USA: Cisco Press, 2015, 527 s. ISBN 978-1-58720-560-6.

IETF. *RFC 2328*. 1998. Dostupné z: <http://tools.ietf.org/html/rfc2328>.

IETF. *RFC 2460*. 2007. Dostupné z: <http://tools.ietf.org/html/rfc2460>.

IETF. *RFC 4213*. 2005. Dostupné z: <http://tools.ietf.org/html/rfc4213>.

IETF. *RFC 4271*. 2006. Dostupné z: <http://tools.ietf.org/html/rfc4271>.

IETF. *RFC 4760*. 2007. Dostupné z: <http://tools.ietf.org/html/rfc4760>.

IETF. *RFC 4861*. 2007. Dostupné z: <http://tools.ietf.org/html/rfc4861>.

IETF. *RFC 5340*. 2008. Dostupné z: <http://tools.ietf.org/html/rfc5340>.

KOCHARIANS, N. *CCIE Routing and Switching v5.0 Official Cert Guide, Volume 1*. 5th Edition. Indianapolis, IN 46240 USA: Cisco Press, 2014, 742 s. ISBN 978-1-58714-396-0.

KOSTĚNEC, M. *IPv6 na ZČU v Plzni – aktuální stav* [online]. 2010 [cit. 2015-01-17]. Dostupné z: <http://archiv.cesnet.cz/ipv6/wg/p/zcu-ipv6.pdf>.

KOUTECKÝ, T. *Implementace IPv6 v BIVŠ*. Praha, 2014. Diplomová práce. Bankovní institut vysoká škola Praha.

LACOSTE, R. *CCNP Routing and Switching TSHOOT 300-135 Official Cert Guide*. Indianapolis, IN 46240 USA: Cisco Press, 2014, 988 s. ISBN 978-1-58720-561-3.

LAMMLE, T. *CCNA Routing and Switching Study Guide*. Indianapolis, IN 46256 USA: John Wiley Sons, Inc., 2013, 1100 s. ISBN 978-1-118-74961-6.

LAMPA, P. *Pravidla přidělování IPv6 adres na VUT* [online]. 2009 [cit. 2015-01-17]. Dostupné z: <http://www.fit.vutbr.cz/CVT/ipv6/lib/exe/fetch.php?media=intro:pravidlaipv6doc.pdf>.

MACURA, L. *Implementace IPV6 na OPF SU* [online]. 2010 [cit. 2015-01-17]. Dostupné z: <http://archiv.cesnet.cz/ipv6/wg/p/su-ipv6.pdf>.

MCFARLAND, S. *IPv6 for Enterprise Networks: The practical guide to deploying IPv6 in campus, WAN/branch, data center, and virtualized environments*. Indianapolis, IN 46240 USA: Cisco Press, 2011, 372 s. ISBN 978-1-58714-227-7.

ODOM, W. *Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide*. Indianapolis, IN 46240 USA: Cisco Press, 2013, 808 s. ISBN 978-1-58714-485-1.

PETLACH, J. *Problematika realizace přechodu na IPv6 v podnikových sítích*. Brno, 2006. Diplomová práce. Mendelova zemědělská a lesnická univerzita v Brně.

PUSTKA, M. *Přehled stavu IPv6 v síti VŠB TUO* [online]. 2010 [cit. 2015-01-17]. Dostupné z: <http://archiv.cesnet.cz/ipv6/wg/p/vsb-ipv6.pdf>.

ROHLEDER, D. *Univerzitní síť – leden 2012* [online]. 2012 [cit. 2015-01-17]. Dostupné z: <cit.ukb.muni.cz/kurzy/files/HiTech/HiTechSite.pdf>.

SATRAPA, P. *IPv6: Internetový protokol verze 6*. 3. aktualizované a doplněné vydání. Praha: CZ.NIC, 2011, 407 s. ISBN 978-80-904248-4-5.

SATRAPA, P. *IPv6 na TU v Liberci* [online]. 2010 [cit. 2015-01-17]. Dostupné z: <http://archiv.cesnet.cz/ipv6/wg/p/tul-ipv6.pdf>.

TISO, J. *Designing Cisco Network Service Architectures (ARCH) Foundation Learning Guide: (CCDP ARCH 642-874)*. 3rd ed. Indianapolis, IN 46240 USA: Cisco Press, 2011, 698 s. ISBN 978-1-58714-288-8.

VANĚK, F. *IPv6 – Areál Karlova náměstí (FEL ČVUT)* [online]. 2010 [cit. 2015-01-17]. Dostupné z: <http://archiv.cesnet.cz/ipv6/wg/p/fel-ipv6.pdf>.

VIKLICKÝ, M. *Implementace protokolu IPv6 do firemní sítě společnosti Znovín Znojmo, a.s. se sídlem v Šatově*. Brno, 2015. Bakalářská práce. Mendelova univerzita v Brně.

WALLACE, K. *CCNP Routing and Switching ROUTE 300-101 Official Cert Guide*. Indianapolis, IN 46240 USA: Cisco Press, 2015, 840 s. ISBN 978-1-58720-559-0.

Přílohy

A Modelová konfigurace VRF na L3 prvku *6509–Core*

```
mls ipv6 vrf
!
vrf definition CernaPole
 rd 21:1
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition Internet
 rd 22:2
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
```

B Modelová konfigurace sítě na *Firewallu*

```
[root@firewall _Lab]# cat /etc/sysconfig/network

NETWORKING=yes
NETWORKING_IPV6=yes
FORWARD_IPV4=yes
IPV6FORWARDING=yes
IPV6_AUTOCONF=no
IPV6_AUTOTUNNEL=no
HOSTNAME=firewall.mendelu.cz



[root@firewall _Lab]# cat /etc/sysconfig/network-scripts/ifcfg-eth0

# L2 Trunk interface

DEVICE=eth0
HWADDR=00:1B:21:C8:40:C2
TYPE=Ethernet
NM_CONTROLLED=no
ONBOOT=yes
USERCTL=no

BOOTPROTO=none

IPV6INIT=no
IPV6_AUTOCONF=no
IPV6_ROUTER=no
IPV6TO4INIT=no



[root@firewall _Lab]# ip addr show dev eth0

2:  eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP
    link/ether 00:1b:21:c8:40:c2 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::21b:21ff:fec8:40c2/64 scope link
```

C Modelová konfigurace SVI *páteřních VLAN*

L3 přepínač *6509–Core*, *VRF CernaPole*

```
interface Vlan40
 vrf forwarding CernaPole
 ip address 195.178.80.17 255.255.255.252
 ipv6 address FE80::40:1 link-local
 ipv6 address 2001:718:803:40::1/64
 ipv6 nd ra suppress
!
interface Vlan41
 vrf forwarding CernaPole
 ip address 195.178.80.21 255.255.255.252
 ipv6 address FE80::41:1 link-local
 ipv6 address 2001:718:803:41::1/64
 ipv6 nd ra suppress
!
interface Vlan42
 vrf forwarding CernaPole
 ip address 195.178.80.25 255.255.255.252
 ipv6 address FE80::42:1 link-local
 ipv6 address 2001:718:803:42::1/64
 ipv6 nd ra suppress
!
```

L3 přepínač *3560–core–Q*

```
interface Vlan40
 ip address 195.178.80.18 255.255.255.252
 ipv6 address FE80::40:2 link-local
 ipv6 address 2001:718:803:40::2/64
 ipv6 nd ra suppress
!
```

L3 přepínač *3560–core–A*

```
interface Vlan41
 ip address 195.178.80.22 255.255.255.252
 ipv6 address FE80::41:2 link-local
 ipv6 address 2001:718:803:41::2/64
 ipv6 nd ra suppress
!
interface Vlan43
 ip address 195.178.80.29 255.255.255.252
 ipv6 address FE80::43:1 link-local
 ipv6 address 2001:718:803:43::1/64
 ipv6 nd ra suppress
!
```

L3 přepínač *3560–core–C*

```
interface Vlan42
 ip address 195.178.80.26 255.255.255.252
 ipv6 address FE80::42:2 link-local
 ipv6 address 2001:718:803:42::2/64
 ipv6 nd ra suppress
!
interface Vlan43
 ip address 195.178.80.30 255.255.255.252
 ipv6 address FE80::43:2 link-local
 ipv6 address 2001:718:803:43::2/64
 ipv6 nd ra suppress
!
```

D Modelová konfigurace SVI *lokalitních VLAN*

L3 přepínač *6509–Core, VRF CernaPole*

```
interface Vlan86
 vrf forwarding CernaPole
 ip address 195.178.76.1 255.255.255.0
 ipv6 address FE80::486:1 link-local
 ipv6 address 2001:718:803:486::1/64
 ipv6 nd prefix 2001:718:803:486::/64
!
```

L3 přepínač *3560–core–Q*

```
interface Vlan25
 ip address 195.178.72.1 255.255.255.0
 ipv6 address FE80::125:1 link-local
 ipv6 address 2001:718:803:125::1/64
 ipv6 nd prefix 2001:718:803:125::/64
!
interface Vlan26
 ip address 195.178.73.1 255.255.255.0
 ipv6 address FE80::126:1 link-local
 ipv6 address 2001:718:803:126::1/64
 ipv6 nd prefix 2001:718:803:126::/64
!
```

L3 přepínač *3560–core–A*

```
interface Vlan811
 ip address 195.178.74.1 255.255.255.128
 ipv6 address FE80::2A0:1 link-local
 ipv6 address 2001:718:803:2A0::1/64
 ipv6 nd prefix 2001:718:803:2A0::/64
!
interface Vlan819
 ip address 195.178.74.129 255.255.255.128
 ipv6 address FE80::2A1:1 link-local
 ipv6 address 2001:718:803:2A1::1/64
 ipv6 nd prefix 2001:718:803:2A1::/64
!
```

L3 přepínač *3560–core–C*

```
interface Vlan84
 ip address 195.178.75.1 255.255.255.0
 ipv6 address FE80::384:1 link-local
 ipv6 address 2001:718:803:384::1/64
 ipv6 nd prefix 2001:718:803:384::/64
!
```

E Modelová konfigurace SVI *perimetrových VLAN*

L3 přepínač *6509–Core*, *VRF CernaPole*

```
interface Vlan21
 vrf forwarding CernaPole
 ip address 195.178.80.1 255.255.255.248
 ipv6 address FE80::F21:1 link-local
 ipv6 address 2001:718:803:F21::1/64
 ipv6 nd ra suppress
!
```

L3 přepínač *6509–Core*, *VRF Internet*

```
interface Vlan22
 vrf forwarding Internet
 ip address 195.178.80.9 255.255.255.248
 ipv6 address FE80::F22:1 link-local
 ipv6 address 2001:718:803:F22::1/64
 ipv6 nd ra suppress
!
```

Firewall s OS Linux, distribuce CentOS 6.5

```
[root@firewall _Lab]# ip addr show dev eth0.21

35: eth0.21@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP
    link/ether 00:1b:21:c8:40:c2 brd ff:ff:ff:ff:ff:ff
    inet 195.178.80.2/29 brd 195.178.80.7 scope global eth0.21
    inet6 2001:718:803:f21::2/64 scope global
    inet6 fe80::f21:2/64 scope link
    inet6 fe80::21b:21ff:fec8:40c2/64 scope link

[root@firewall _Lab]# ip addr show dev eth0.22

36: eth0.22@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP
    link/ether 00:1b:21:c8:40:c2 brd ff:ff:ff:ff:ff:ff
    inet 195.178.80.10/29 brd 195.178.80.15 scope global eth0.22
    inet6 2001:718:803:f22::2/64 scope global
    inet6 fe80::f22:2/64 scope link
    inet6 fe80::21b:21ff:fec8:40c2/64 scope link
```

```
[root@firewall _Lab]# cat /etc/sysconfig/network-scripts/ifcfg-eth0.21

# SVI VLAN 21

DEVICE=eth0.21
VLAN=yes
NM_CONTROLLED=no
ONBOOT=yes
USERCTL=no

BOOTPROTO=none
IPADDR=195.178.80.2
NETMASK=255.255.255.248

IPV6INIT=yes
IPV6ADDR=2001:718:803:f21::2/64
IPV6ADDR_SECONDARIES=fe80::f21:2/64
IPV6_AUTOCONF=no
IPV6_ROUTER=no
IPV6TO4INIT=no
```

```
[root@firewall _Lab]# cat /etc/sysconfig/network-scripts/ifcfg-eth0.22

# SVI VLAN 22

DEVICE=eth0.22
VLAN=yes
NM_CONTROLLED=no
ONBOOT=yes
USERCTL=no

BOOTPROTO=none
IPADDR=195.178.80.10
NETMASK=255.255.255.248

IPV6INIT=yes
IPV6ADDR=2001:718:803:f22::2/64
IPV6ADDR_SECONDARIES=fe80::f22:2/64
IPV6_AUTOCONF=no
IPV6_ROUTER=no
IPV6TO4INIT=no
```

F Modelová konfigurace SVI *demilitarizované VLAN*

L3 přepínač *6509–Core, VRF Internet*

```
interface Vlan222
 vrf forwarding Internet
 ip address 195.178.79.1 255.255.255.0
 ipv6 address FE80::D222:1 link-local
 ipv6 address 2001:718:803:D222::1/64
 ipv6 nd ra suppress
!
```

G Modelová konfigurace SVI *End–To–End VLAN*

Firewall s OS Linux, distribuce CentOS 6.5

```
[root@firewall _Lab]# ip addr show dev eth0.114

33: eth0.114@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP
    link/ether 00:1b:21:c8:40:c2 brd ff:ff:ff:ff:ff:ff
    inet 10.10.14.1/23 brd 10.10.15.255 scope global eth0.114
    inet6 2001:718:803:e114::1/64 scope global
    inet6 fe80::e114:1/64 scope link
    inet6 fe80::21b:21ff:fec8:40c2/64 scope link



[root@firewall _Lab]# cat /etc/sysconfig/network-scripts/ifcfg-eth0.114

# SVI VLAN 114

DEVICE=eth0.114
VLAN=yes
NM_CONTROLLED=no
ONBOOT=yes
USERCTL=no

BOOTPROTO=none
IPADDR=10.10.14.1
NETMASK=255.255.254.0

IPV6INIT=yes
IPV6ADDR=2001:718:803:e114::1/64
IPV6ADDR_SECONDARIES=fe80::e114:1/64
IPV6_AUTOCONF=no
IPV6_ROUTER=no
IPV6TO4INIT=no



[root@firewall _Lab]# cat /etc/radvd.conf

interface eth0.114
{
  AdvSendAdvert on;
  prefix 2001:718:803:e114::/64 {};
};
```

H Modelová konfigurace SVI *správní VLAN*

L3 přepínač *6509–Core*

```
interface Vlan171
 ip address 10.7.1.2 255.255.255.0
 ipv6 address FE80::E171:2 link-local
 ipv6 nd ra suppress
!
```

L3 přepínač *3560–core–Q*

```
interface Vlan171
 ip address 10.7.1.3 255.255.255.0
 ipv6 address FE80::E171:3 link-local
 ipv6 nd ra suppress
!
```

L3 přepínač *3560–core–A*

```
interface Vlan171
 ip address 10.7.1.4 255.255.255.0
 ipv6 address FE80::E171:4 link-local
 ipv6 nd ra suppress
!
```

L3 přepínač *3560–core–C*

```
interface Vlan171
 ip address 10.7.1.5 255.255.255.0
 ipv6 address FE80::E171:5 link-local
 ipv6 nd ra suppress
!
```

Firewall s OS Linux, distribuce CentOS 6.5

```
[root@firewall _Lab]# ip addr show dev eth0.171

34: eth0.171@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP
    link/ether 00:1b:21:c8:40:c2 brd ff:ff:ff:ff:ff:ff
    inet 10.7.1.1/24 brd 10.7.1.255 scope global eth0.171
    inet6 fe80::e171:1/64 scope link
    inet6 fe80::21b:21ff:fec8:40c2/64 scope link
```

```
[root@firewall _Lab]# cat /etc/sysconfig/network-scripts/ifcfg-eth0.171

# SVI VLAN 171

DEVICE=eth0.171
VLAN=yes
NM_CONTROLLED=no
ONBOOT=yes
USERCTL=no

BOOTPROTO=none
IPADDR=10.7.1.1
NETMASK=255.255.255.0

IPV6INIT=yes
IPV6ADDR=fe80::e171:1/64
IPV6_AUTOCONF=no
IPV6_ROUTER=no
IPV6TO4INIT=no
```

I Modelová konfigurace SVI *spojovacích VLAN*

L3 přepínač *6509–Core*, *VRF Internet*

```
interface Vlan910
 vrf forwarding Internet
 ip address 195.178.87.178 255.255.255.252
 ipv6 address FE80::910:2 link-local
 ipv6 address 2001:718:800:3A::2/64
 ipv6 nd ra suppress
!
interface Vlan911
 vrf forwarding Internet
 ip address 195.178.87.182 255.255.255.252
 ipv6 address FE80::911:2 link-local
 ipv6 address 2001:718:800:3B::2/64
 ipv6 nd ra suppress
!
```

L3 přepínač *SW9*

```
interface Vlan910
 ip address 195.178.87.177 255.255.255.252
 ipv6 address FE80::910:1 link-local
 ipv6 address 2001:718:800:3A::1/64
 ipv6 nd ra suppress
!
```

L3 přepínač *SW10*

```
interface Vlan911
 ip address 195.178.87.181 255.255.255.252
 ipv6 address FE80::911:1 link-local
 ipv6 address 2001:718:800:3B::1/64
 ipv6 nd ra suppress
!
```

J Modelová konfigurace protokolu OSPFv2

6509–Core, VRF CernaPole

```
router ospf 1 vrf CernaPole
 router-id 10.7.1.2
 log-adjacency-changes detail
 area 0 authentication message-digest
 passive-interface default
 no passive-interface Vlan40
 no passive-interface Vlan41
 no passive-interface Vlan42
 network 195.178.76.0 0.0.0.255 area 4
 network 195.178.80.16 0.0.0.3 area 0
 network 195.178.80.20 0.0.0.3 area 0
 network 195.178.80.24 0.0.0.3 area 0
 default-information originate always
!
interface Vlan40
 ip ospf message-digest-key 1 md5 7 073B204640102B0003171109071C7F
!
interface Vlan41
 ip ospf message-digest-key 1 md5 7 06320E2B42573B1C1112080E0F327E
!
interface Vlan42
 ip ospf message-digest-key 1 md5 7 133116180515362F3F213236361447
!
```

3560–core–Q

```
router ospf 1
 router-id 10.7.1.3
 log-adjacency-changes detail
 area 0 authentication message-digest
 passive-interface default
 no passive-interface Vlan40
 network 195.178.72.0 0.0.0.255 area 1
 network 195.178.73.0 0.0.0.255 area 1
 network 195.178.80.16 0.0.0.3 area 0
!
interface Vlan40
 ip ospf message-digest-key 1 md5 7 113D180F190B3909102F31212B0561
!
```

3560–core–A

```
router ospf 1
 router-id 10.7.1.4
 log-adjacency-changes detail
 area 0 authentication message-digest
 area 2 range 195.178.74.0 255.255.255.0
 passive-interface default
 no passive-interface Vlan41
 no passive-interface Vlan43
 network 195.178.74.0 0.0.0.255 area 2
 network 195.178.80.20 0.0.0.3 area 0
 network 195.178.80.28 0.0.0.3 area 0
!
interface Vlan41
 ip ospf message-digest-key 1 md5 7 0127070E5512340A3549540C1A3343
!
interface Vlan43
 ip ospf message-digest-key 1 md5 7 08154D4407003712060E1601291D70
 ip ospf cost 16384
!
```

3560–core–C

```
router ospf 1
 router-id 10.7.1.5
 log-adjacency-changes detail
 area 0 authentication message-digest
 passive-interface default
 no passive-interface Vlan42
 no passive-interface Vlan43
 network 195.178.75.0 0.0.0.255 area 3
 network 195.178.80.24 0.0.0.3 area 0
 network 195.178.80.28 0.0.0.3 area 0
!
interface Vlan42
 ip ospf message-digest-key 1 md5 7 06320E2B42573B1C1112080E0F327E
!
interface Vlan43
 ip ospf message-digest-key 1 md5 7 046F0A0C01387E4B1D1C1F12113D58
 ip ospf cost 16384
!
```

K Modelová konfigurace protokolu OSPFv3

6509–Core, VRF CernaPole

```
router ospfv3 1
 log-adjacency-changes detail
 !
 address-family ipv6 unicast vrf CernaPole
  passive-interface default
  no passive-interface Vlan40
  no passive-interface Vlan41
  no passive-interface Vlan42
  default-information originate always
  router-id 10.7.1.2
  area 4 range 2001:718:803:400::/56
 exit-address-family
!
interface Vlan40
 ospfv3 1 ipv6 area 0
!
interface Vlan41
 ospfv3 1 ipv6 area 0
!
interface Vlan42
 ospfv3 1 ipv6 area 0
!
interface Vlan86
 ospfv3 1 ipv6 area 4
!
```

3560–core–Q

```
ipv6 router ospf 1
 router-id 10.7.1.3
 log-adjacency-changes detail
 area 1 range 2001:718:803:100::/56
 passive-interface default
 no passive-interface Vlan40
!
interface Vlan40
 ipv6 ospf 1 area 0
!
interface Vlan25
 ipv6 ospf 1 area 1
!
interface Vlan26
 ipv6 ospf 1 area 1
!
```

3560–core–A

```
ipv6 router ospf 1
 router-id 10.7.1.4
 log-adjacency-changes detail
 area 2 range 2001:718:803:200::/56
 passive-interface default
 no passive-interface Vlan41
 no passive-interface Vlan43
!
interface Vlan41
 ipv6 ospf 1 area 0
!
interface Vlan43
 ipv6 ospf cost 16384
 ipv6 ospf 1 area 0
!
interface Vlan811
 ipv6 ospf 1 area 2
!
interface Vlan819
 ipv6 ospf 1 area 2
!
```

3560–core–C

```
ipv6 router ospf 1
 router-id 10.7.1.5
 log-adjacency-changes detail
 area 3 range 2001:718:803:300::/56
 passive-interface default
 no passive-interface Vlan42
 no passive-interface Vlan43
!
interface Vlan42
 ipv6 ospf 1 area 0
!
interface Vlan43
 ipv6 ospf cost 16384
 ipv6 ospf 1 area 0
!
interface Vlan84
 ipv6 ospf 1 area 3
!
```

L Modelová konfigurace protokolu MP–BGP

6509–Core, VRF Internet

```
router bgp 65083
 bgp router-id 10.7.1.2
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf Internet
  network 195.178.72.0 mask 255.255.248.0
  network 195.178.80.0
  neighbor 195.178.87.177 remote-as 2852
  neighbor 195.178.87.177 activate
  neighbor 195.178.87.177 weight 100
  neighbor 195.178.87.177 route-map SET_MED_CESNET_PRI_OUT out
  neighbor 195.178.87.181 remote-as 2852
  neighbor 195.178.87.181 activate
  neighbor 195.178.87.181 weight 50
  neighbor 195.178.87.181 route-map SET_MED_CESNET_SEC_OUT out
 exit-address-family
 !
 address-family ipv6 vrf Internet
  network 2001:718:803::/48
  neighbor 2001:718:800:3A::1 remote-as 2852
  neighbor 2001:718:800:3A::1 activate
  neighbor 2001:718:800:3A::1 weight 100
  neighbor 2001:718:800:3A::1 route-map SET_MED_CESNET_PRI_OUT out
  neighbor 2001:718:800:3B::1 remote-as 2852
  neighbor 2001:718:800:3B::1 activate
  neighbor 2001:718:800:3B::1 weight 50
  neighbor 2001:718:800:3B::1 route-map SET_MED_CESNET_SEC_OUT out
 exit-address-family
!
route-map SET_MED_CESNET_PRI_OUT permit 90
 set metric 50
!
route-map SET_MED_CESNET_SEC_OUT permit 91
 set metric 100
!
```

SW9

```
router bgp 2852
 bgp router-id 2.2.2.2
 neighbor 195.113.156.5 remote-as 2852
 neighbor 195.178.87.178 remote-as 65083
 neighbor 2001:718:1:40::1 remote-as 2852
 neighbor 2001:718:800:3A::2 remote-as 65083
 !
 address-family ipv4
  neighbor 195.113.156.5 activate
  neighbor 195.113.156.5 next-hop-self
  neighbor 195.178.87.178 activate
  neighbor 195.178.87.178 default-originate
 exit-address-family
 !
 address-family ipv6
  neighbor 2001:718:1:40::1 activate
  neighbor 2001:718:1:40::1 next-hop-self
  neighbor 2001:718:800:3A::2 activate
  neighbor 2001:718:800:3A::2 default-originate
 exit-address-family
!
```

SW10

```
router bgp 2852
 bgp router-id 3.3.3.3
 neighbor 195.113.156.9 remote-as 2852
 neighbor 195.178.87.182 remote-as 65083
 neighbor 2001:718:1:80::1 remote-as 2852
 neighbor 2001:718:800:3B::2 remote-as 65083
 !
 address-family ipv4
  neighbor 195.113.156.9 activate
  neighbor 195.113.156.9 next-hop-self
  neighbor 195.178.87.182 activate
  neighbor 195.178.87.182 default-originate
 exit-address-family
 !
 address-family ipv6
  neighbor 2001:718:1:80::1 activate
  neighbor 2001:718:1:80::1 next-hop-self
  neighbor 2001:718:800:3B::2 activate
  neighbor 2001:718:800:3B::2 default-originate
 exit-address-family
!
```

R10

```
router bgp 2852
 bgp router-id 1.1.1.1
 neighbor 195.113.156.6 remote-as 2852
 neighbor 195.113.156.10 remote-as 2852
 neighbor 2001:718:1:40::2 remote-as 2852
 neighbor 2001:718:1:80::2 remote-as 2852
 !
 address-family ipv4
  neighbor 195.113.156.6 activate
  neighbor 195.113.156.6 route-reflector-client
  neighbor 195.113.156.10 activate
  neighbor 195.113.156.10 route-reflector-client
 exit-address-family
 !
 address-family ipv6
  neighbor 2001:718:1:40::2 activate
  neighbor 2001:718:1:40::2 route-reflector-client
  neighbor 2001:718:1:80::2 activate
  neighbor 2001:718:1:80::2 route-reflector-client
 exit-address-family
!
```

M Směrovací tabulky IPv4 a IPv6 na *VRF CernaPole*

```
6509-Core#show ip route vrf CernaPole

S*    0.0.0.0/0           [1/0]         via 195.178.80.2
O IA  195.178.72.0/24     [110/2]       via 195.178.80.18, Vlan40
O IA  195.178.73.0/24     [110/2]       via 195.178.80.18, Vlan40
O IA  195.178.74.0/24     [110/2]       via 195.178.80.22, Vlan41
O IA  195.178.75.0/24     [110/2]       via 195.178.80.26, Vlan42
C     195.178.76.0/24                   is directly connected, Vlan86
C     195.178.80.0/29                   is directly connected, Vlan21
C     195.178.80.16/30                  is directly connected, Vlan40
C     195.178.80.20/30                  is directly connected, Vlan41
C     195.178.80.24/30                  is directly connected, Vlan42
O     195.178.80.28/30    [110/16385]   via 195.178.80.26, Vlan42
                          [110/16385]   via 195.178.80.22, Vlan41
```

```
6509-Core#show ipv6 route vrf CernaPole

S   ::/0                    [1/0]         via 2001:718:803:F21::2
C   2001:718:803:40::/64    [0/0]         via Vlan40, directly connected
C   2001:718:803:41::/64    [0/0]         via Vlan41, directly connected
C   2001:718:803:42::/64    [0/0]         via Vlan42, directly connected
O   2001:718:803:43::/64    [110/16385]   via FE80::41:2, Vlan41
                                          via FE80::42:2, Vlan42
OI  2001:718:803:100::/56   [110/2]       via FE80::40:2, Vlan40
OI  2001:718:803:200::/56   [110/2]       via FE80::41:2, Vlan41
OI  2001:718:803:300::/56   [110/2]       via FE80::42:2, Vlan42
O   2001:718:803:400::/56   [110/1]       via Null0, directly connected
C   2001:718:803:486::/64   [0/0]         via Vlan86, directly connected
C   2001:718:803:F21::/64   [0/0]         via Vlan21, directly connected
```

N Směrovací tabulky IPv4 a IPv6 na *3560–core–Q*

```
3560-core-Q#show ip route

O*E2  0.0.0.0/0          [110/1]       via 195.178.80.17, Vlan40
C     10.7.1.0/24                      is directly connected, Vlan171
C     195.178.72.0/24                  is directly connected, Vlan25
C     195.178.73.0/24                  is directly connected, Vlan26
O IA  195.178.74.0/24    [110/3]       via 195.178.80.17, Vlan40
O IA  195.178.75.0/24    [110/3]       via 195.178.80.17, Vlan40
O IA  195.178.76.0/24    [110/2]       via 195.178.80.17, Vlan40
C     195.178.80.16/30                 is directly connected, Vlan40
O     195.178.80.20/30   [110/2]       via 195.178.80.17, Vlan40
O     195.178.80.24/30   [110/2]       via 195.178.80.17, Vlan40
O     195.178.80.28/30   [110/16386]   via 195.178.80.17, Vlan40



3560-core-Q#show ipv6 route

OE2 ::/0                     [110/1]       via FE80::40:1, Vlan40
C   2001:718:803:40::/64     [0/0]         via Vlan40, directly connected
O   2001:718:803:41::/64     [110/2]       via FE80::40:1, Vlan40
O   2001:718:803:42::/64     [110/2]       via FE80::40:1, Vlan40
O   2001:718:803:43::/64     [110/16386]   via FE80::40:1, Vlan40
O   2001:718:803:100::/56    [110/0]       via Null0, directly connected
C   2001:718:803:125::/64    [0/0]         via Vlan25, directly connected
C   2001:718:803:126::/64    [0/0]         via Vlan26, directly connected
OI  2001:718:803:200::/56    [110/3]       via FE80::40:1, Vlan40
OI  2001:718:803:300::/56    [110/3]       via FE80::40:1, Vlan40
OI  2001:718:803:400::/56    [110/2]       via FE80::40:1, Vlan40
```

O Směrovací tabulky IPv4 a IPv6 na *3560–core–A*

```
3560-core-A#show ip route

O*E2  0.0.0.0/0           [110/1]   via 195.178.80.21, Vlan41
C     10.7.1.0/24                   is directly connected, Vlan171
O IA  195.178.72.0/24     [110/3]   via 195.178.80.21, Vlan41
O IA  195.178.73.0/24     [110/3]   via 195.178.80.21, Vlan41
S     195.178.74.0/24               is directly connected, Null0
C     195.178.74.0/25               is directly connected, Vlan811
C     195.178.74.128/25             is directly connected, Vlan819
O IA  195.178.75.0/24     [110/3]   via 195.178.80.21, Vlan41
O IA  195.178.76.0/24     [110/2]   via 195.178.80.21, Vlan41
O     195.178.80.16/30    [110/2]   via 195.178.80.21, Vlan41
C     195.178.80.20/30              is directly connected, Vlan41
O     195.178.80.24/30    [110/2]   via 195.178.80.21, Vlan41
C     195.178.80.28/30              is directly connected, Vlan43
```

```
3560-core-A#show ipv6 route

OE2 ::/0                    [110/1]   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
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
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
C   2001:718:803:2A1::/64   [0/0]     via Vlan819, directly connected
OI  2001:718:803:300::/56   [110/3]   via FE80::41:1, Vlan41
OI  2001:718:803:400::/56   [110/2]   via FE80::41:1, Vlan41
```

P Směrovací tabulky IPv4 a IPv6 na *3560–core–C*

```
3560-core-C#show ip route

O*E2  0.0.0.0/0          [110/1]   via 195.178.80.25, Vlan42
C     10.7.1.0/24                  is directly connected, Vlan171
O IA  195.178.72.0/24    [110/3]   via 195.178.80.25, Vlan42
O IA  195.178.73.0/24    [110/3]   via 195.178.80.25, Vlan42
O IA  195.178.74.0/24    [110/3]   via 195.178.80.25, Vlan42
C     195.178.75.0/24              is directly connected, Vlan84
O IA  195.178.76.0/24    [110/2]   via 195.178.80.25, Vlan42
O     195.178.80.16/30   [110/2]   via 195.178.80.25, Vlan42
O     195.178.80.20/30   [110/2]   via 195.178.80.25, Vlan42
C     195.178.80.24/30             is directly connected, Vlan42
C     195.178.80.28/30             is directly connected, Vlan43



3560-core-C#show ipv6 route

OE2 ::/0                     [110/1]   via FE80::42:1, Vlan42
O   2001:718:803:40::/64     [110/2]   via FE80::42:1, Vlan42
O   2001:718:803:41::/64     [110/2]   via FE80::42:1, Vlan42
C   2001:718:803:42::/64     [0/0]     via Vlan42, directly connected
C   2001:718:803:43::/64     [0/0]     via Vlan43, directly connected
OI  2001:718:803:100::/56    [110/3]   via FE80::42:1, Vlan42
OI  2001:718:803:200::/56    [110/3]   via FE80::42:1, Vlan42
O   2001:718:803:300::/56    [110/0]   via Null0, directly connected
C   2001:718:803:384::/64    [0/0]     via Vlan84, directly connected
OI  2001:718:803:400::/56    [110/2]   via FE80::42:1, Vlan42
```

Q Směrovací tabulky IPv4 a IPv6 na *VRF Internet*

```
6509-Core#show ip route vrf Internet

B*    0.0.0.0/0           [20/0]   via 195.178.87.177
S     195.178.72.0/21             is directly connected, Null0
S     195.178.72.0/22     [1/0]    via 195.178.80.10
S     195.178.76.0/24     [1/0]    via 195.178.80.10
C     195.178.79.0/24             is directly connected, Vlan222
S     195.178.80.0/24             is directly connected, Null0
S     195.178.80.0/29     [1/0]    via 195.178.80.10
C     195.178.80.8/29             is directly connected, Vlan22
S     195.178.80.16/28    [1/0]    via 195.178.80.10
C     195.178.80.252/30           is directly connected, Loopback0
C     195.178.87.176/30           is directly connected, Vlan910
C     195.178.87.180/30           is directly connected, Vlan911
```

```
6509-Core#show ipv6 route vrf Internet

B   ::/0                     [20/0]   via FE80::910:1, Vlan910
C   2001:718:800:3A::/64     [0/0]    via Vlan910, directly connected
C   2001:718:800:3B::/64     [0/0]    via Vlan911, directly connected
S   2001:718:803::/48        [1/0]    via Null0, directly connected
S   2001:718:803::/56        [1/0]    via 2001:718:803:F22::2
C   2001:718:803:A::/64      [0/0]    via Loopback0, directly connected
S   2001:718:803:100::/56    [1/0]    via 2001:718:803:F22::2
S   2001:718:803:200::/56    [1/0]    via 2001:718:803:F22::2
S   2001:718:803:300::/56    [1/0]    via 2001:718:803:F22::2
S   2001:718:803:400::/56    [1/0]    via 2001:718:803:F22::2
S   2001:718:803:F21::/64    [1/0]    via 2001:718:803:F22::2
C   2001:718:803:F22::/64    [0/0]    via Vlan22, directly connected
C   2001:718:803:D222::/64   [0/0]    via Vlan222, directly connected
S   2001:718:803:E000::/52   [1/0]    via 2001:718:803:F22::2
```

R Směrovací tabulky IPv4 a IPv6 na *Firewallu*

```
[root@firewall _Lab]# ip route show

195.178.80.8/29 dev eth0.22  proto kernel  scope link  src 195.178.80.10
195.178.80.0/29 dev eth0.21  proto kernel  scope link  src 195.178.80.2
195.178.80.16/28 via 195.178.80.1 dev eth0.21
195.178.76.0/24 via 195.178.80.1 dev eth0.21
195.178.79.0/24 via 195.178.80.9 dev eth0.22
10.7.1.0/24 dev eth0.171  proto kernel  scope link  src 10.7.1.1
10.10.14.0/23 dev eth0.114  proto kernel  scope link  src 10.10.14.1
195.178.72.0/22 via 195.178.80.1 dev eth0.21
default via 195.178.80.9 dev eth0.22



[root@firewall _Lab]# ip -6 route show

2001:718:803::/56 via 2001:718:803:f21::1 dev eth0.21  metric 1024
2001:718:803:100::/56 via 2001:718:803:f21::1 dev eth0.21  metric 1024
2001:718:803:200::/56 via 2001:718:803:f21::1 dev eth0.21  metric 1024
2001:718:803:300::/56 via 2001:718:803:f21::1 dev eth0.21  metric 1024
2001:718:803:400::/56 via 2001:718:803:f21::1 dev eth0.21  metric 1024
2001:718:803:f21::/64 dev eth0.21  proto kernel  metric 256
2001:718:803:f22::/64 dev eth0.22  proto kernel  metric 256
2001:718:803:d222::/64 via 2001:718:803:f22::1 dev eth0.22  metric 1024
2001:718:803:e114::/64 dev eth0.114  proto kernel  metric 256
default via 2001:718:803:f22::1 dev eth0.22  metric 1024
```