VŠB TECHNICKÁ UNIVERZITA OSTRAVA
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Virtuální privátní sítě používající protokol IPv6

Virtual Private Networks Using IPv6 Protocol

Vadim Karachentsev

Diplomová práce

Vedoucí práce: Ing. Petr Machník, Ph.D.

Ostrava, 2022

VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Vadim Karachentsev**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2601T013 Telekomunikační technika

Téma: Virtuální privátní sítě používající protokol IPv6
Virtual Private Networks Using IPv6 Protocol

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem diplomové práce je návrh, realizace a testování technologie VPN v síti založené na protokolu IPv6 v laboratorním prostředí s využitím směrovačů Cisco a Huawei.

Vypracování práce bude splňovat následující body zadání:
1. Popište různá řešení virtuálních privátních sítí v prostředí protokolu IPv6.
2. Navrhněte a v laboratorních podmínkách realizujte alespoň tři druhy virtuálních privátních sítí v prostředí protokolu IPv6. Použijte k tomu směrovače Cisco a Huawei. Ověřte funkčnost navržených řešení.
3. Ověřte kompatibilitu směrovačů Cisco a Huawei v těchto sítích.
4. Srovnejte jednotlivá řešení se sítěmi VPN v prostředí protokolu IPv4. Zhodnoťte výhody a nevýhody jejich použití.

Seznam doporučené odborné literatury:

[1] CARMOUCHE, James Henry. *IPsec Virtual Private Network Fundamentals.* Indianapolis: Cisco Press, 2006. ISBN 1-58705-207-5.
[2] DEAL, Richard. *The Complete Cisco VPN Configuration Guide.* Indianapolis: Cisco Press, 2006. ISBN 1-58705-204-0.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Petr Machník, Ph.D.**

Datum zadání: 01.09.2021

Datum odevzdání: 08.07.2022

prof. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. Ing. Jan Platoš, Ph.D.
děkan fakulty

Abstrakt

Cílem diplomové práce je návrh, realizace a testování technologie VPN v síti založené na protokolu IPv6 v laboratorním prostředí a s využitím směrovačů Huawei a Cisco. V této diplomové práci jsou zastoupeny technologie GRE VPN, IPsec VPN a MPLS L3 VPN. Práce se dále zabývá návrhem, realizací a ověřením funkčnosti těchto technologií v sítích používajících protokol IPv6, ale také zjištěním, jak se liší tato řešení VPN v internetových protokolech různých verzí, konkrétně IPv4 a IPv6.

Klíčová slova

Cisco, GRE, Huawei, IPsec, IPv6, MPLS L3 VPN, MPLS, VPN

Abstract

The aim of this thesis is to design, implement and test VPN technology in an IPv6-based network in a laboratory environment using Huawei and Cisco routers. GRE VPN, IPsec VPN and MPLS L3 VPN technologies are represented in this thesis. The thesis also looks at the design, implementation and verification of the functionality of these technologies in networks using IPv6, but also to see how these VPN solutions differ in the different internet protocols, namely IPv4 and IPv6.

Keywords

Cisco, GRE, Huawei, IPsec, IPv6, MPLS L3 VPN, MPLS, VPN

Poděkování

Velmi rád bych poděkoval vedoucímu své diplomové práce, panu Ing. Petru Machníkovi, Ph.D. za odbornou pomoc a cenné rady při tvorbě této práce.

Obsah

Seznam použitých zkratek a symbolů

AES	–	Advanced Encryption Standard
AFRINIC	–	African Network Information Centre
AH	–	Authentication Header
APNIC	–	Asia-Pacific Network Information Center
ARP	–	Address Resolution Protocol
ATM	–	Asynchronous Transfer Mode
BGP	–	Border Gateway Protocol
BS	–	Bottom of Stack
CE	–	Customer Edge
CoS	–	Class of Service
DES	–	Data Encryption Standard
DHCP	–	Dynamic Host Configuration Protocol
DMVPN	–	dynamic multipoint VPN
DNS	–	Domain Name Service
DSVPN	–	Dynamic Smart Virtual Private Network
eBGP	–	external Border Gateway Protocol
ESP	–	Encapsulating Security Payload
FP	–	Format Prefix
FEC	–	Forwarding Equivalence Class
FTN	–	Mapování paketů FEC na NHLFE
GRE	–	Generic Routing Encapsulation
IANA	–	Internet Assigned Numbers Authority
iBGP	–	internal Border Gateway Protocol
ICMP	–	Internet Control Message Protocol
ICMPv6	–	Internet Control Message Protocol version 6
ID	–	Identifier
IETF	–	Internet Engineering Task Force
IKE	–	Internet Key Exchange

IPSec	–	IP security
IPv4	–	Internet Protocol version 4
IPv6	–	Internet Protocol version 6
IPX	–	Internetwork Packet Exchange
IP	–	Internet Protocol
ISAKMP	–	Internet Security Association and Key Management Protocol
ISP	–	Internet service provider
L2TPv3	–	Layer 2 Tunnelling Protocol Version 3
LACNIC	–	Latin America and Caribbean Network Information Centre
LAN	–	Local Area Network
LDP	–	Label Distribution Protocol
LER	–	Label switch Edge Router
LFIB	–	Label Forwarding Information Base
LSP	–	Label Switched Path
LSR	–	Label-Switch Router
MAC	–	Media Access Control
MD5	–	Message-Digest algorithm 5
MPLS	–	Multiprotocol Label Switching
MTU	–	Maximum transmission unit
NAT	–	Network Address Translation
NHLFE	–	Next Hop Label Forwarding Entry
OSI	–	Open Systems Interconnection
OSPF	–	Open Shortest Path First
OSPFv3	–	Open Shortest Path First version 3
P	–	Provider
PC	–	Personal computer
PE	–	Provider Edge
PHP	–	Penultimate Hop Popping
PPTP	–	Point-to-Point Tunneling Protocol
QoS	–	Quality of Service
RC5	–	Rivest Cipher 5
RD	–	Route Distinguisher
RFC	–	Request for Comments
RIP	–	Routing Information Protocol
RIPE NCC	–	Réseaux IP Européens Network Coordination Centre
RSVP	–	Resource ReSerVation Protocol
RT	–	Router Target
RTP	–	Real-time Transport Protocol

SA	–	Security Association
SHA-1	–	Secure Hash Algorithm 1
SHA-2	–	Secure Hash Algorithm 2
SHA-3	–	Secure Hash Algorithm 3
SHIM	–	Stanza Headers and Internet Metadata
SLA	–	Service-level agreements
SN	–	Sequence Number
SNMA	–	Solicited-Node Multicast Address
SoO	–	Site of Origin
SPI	–	Security Parameter Index
TCP	–	Transmission Control Protocol
TCP/IP	–	Transmission Control Protocol/Internet Protocol
TTL	–	Time to Live
UDP	–	User Datagram Protocol
VPN	–	Virtuální privátní síť
VRF	–	Virtual routing and forwarding

Seznam obrázků

Seznam tabulek

Kapitola 1

Úvod

Protože existují velké firmy, které vyžadují propojení všech svých poboček do jedné sítě, je možné využít technologii VPN pro vytvoření zabezpečeného spojení těchto poboček. Tato práce se věnuje využití možných způsobů technologie VPN pro propojení sítí nad internetovým protokolem verze 6.

V prvních kapitolách je popsána teorie, v kapitole 2 je popsán protokol IPv6 a jeho struktura. V kapitole 3 je teoreticky popsána technologie VPN. Následuje praktická část, ve které jsou popsány některé typy řešení VPN. Mezi tyto typy patří GRE VPN (kapitola 4), IPSec VPN (kapitola 5) a následuje popis technologie MPLS, struktura jeho paketů a VPN na síťové vrstvě s použitím MPLS (kapitola 6).

Praktická část obsahuje realizaci daných řešení VPN a předvedení jejich správné funkčnosti. Na konci této práce budou představena praktická řešení problémů kompatibility zařízení od firem Cisco a Huawei, které vznikly při implementaci VPN řešení.

Kapitola 2

Internet Protokol verze 6

2.1 Typy IP verze 6 adres.

V IPv6 existují tři hlavní typy adres:

- **Unicast** — jedinečný identifikátor pro konkrétní koncový uzel nebo rozhraní směrovače. Paket odeslaný na tuto adresu je doručen konkrétnímu rozhraní, které je touto adresou identifikováno.[1]

  Existuje několik typů unicast adres:

  - **Global unicast** — podobné IPv4 veřejným adresám, které přiděluje IANA a mají prefix 2000::/3.
  - **Unique unicast** — podobné IPv4 privátním adresám, které se využívají v privátních sítích, nejsou určeny pro směrování v internetu a mají prefix FD00::/8.
  - **Link local** — IPv6 požaduje, aby tyto adresy (s prefixem FE80::/10) byly definovány na každém rozhraní, na kterém běží protokol IPv6. Slouží pro posílání paketů na konkrétním lokálním subnetu, směrovače je neposílají do jiných subnetů.

- **Multicast** — je svým účelem podobný multicastu v IPv4, tedy identifikuje skupinu rozhraní patřících různým uzlům. Paket odeslaný multicastové adrese je doručen na všechna rozhraní, která jsou touto adresou identifikována. Multicastové adresy v některých případech plní funkci broadcast adres, které nejsou přítomny v IPv6.[1]

- **Anycast** — podobně jako adresa multicastu, tak i anycast určuje skupinu rozhraní, ale na rozdíl od adresy multicastu je paket odeslaný anycast adrese doručen pouze na jedno z rozhraní skupiny. Rozhraní je obvykle vybráno jako to „nejbližší“, podle metriky používané směrovacími protokoly. Toho se dá využít například v případech, kdy směrovací protokol využívá i jiné metriky jako propustnost linky. Směrovač v takovém případě může využít jiného rozhraní v dané anycast skupině, a dojde tak k lepší škálovatelnosti.[1]

Za zmínku stojí ještě následující typy adres:

- **Nedefinovaná adresa (unspecifed address)** — Nespecifikovaná adresa 0:0:0:0:0:0:0:0 není nikdy přiřazena a neoznačuje žádnou adresu. Například všechny pakety odeslané hostitelem, který je ve stavu inicializace a ještě nemá adresu, obsahují v poli zdrojové adresy nedefinovanou adresu 128 nul, kterou nelze použít jako cílovou adresu.

- **Adresa zpětné smyčky (loopback address)** — na rozdíl od IPv4, kde je pro loopback adresy přiřazen rozsah 127.0.0.0/8, je v IPv6 pro loopback přiřazena pouze jedna adresa 0000:0000:0000:0000:0000:0000:0000:0001/128, která lze zkrátit na ::1/128. Loopback adresu používá hostitelský operační systém k odesílání paketů sám sobě, například pro ověření funkčnosti poskytované služby. Pokud by se stalo, že bude do sítě odeslán paket s loopback adresou v poli zdrojové nebo cílové adresy, tak jej směrovače zahodí.

Typ adresy je určen hodnotou nejvýznamnějších bitů adresy (tabulka 2.1), které se nazývají formát prefix (FP).

Tabulka 2.1: Rozdělení adres IPv6

Typ adresy	**Zadání prefixu v binárním formátu**	**Zadání prefixu ve formátu IPv6**
Nedefinováno	00...0 (128 bit)	::/128
Adresa zpětné smyčky	00... 1 (128 bit)	::1/128
Adresa multicast	11111111	FF00::/8
Adresa link-local	1111111010	FE80::/10
Globální adresa unicast	001	2000::/3

2.2 Typická sada adres rozhraní IPv6

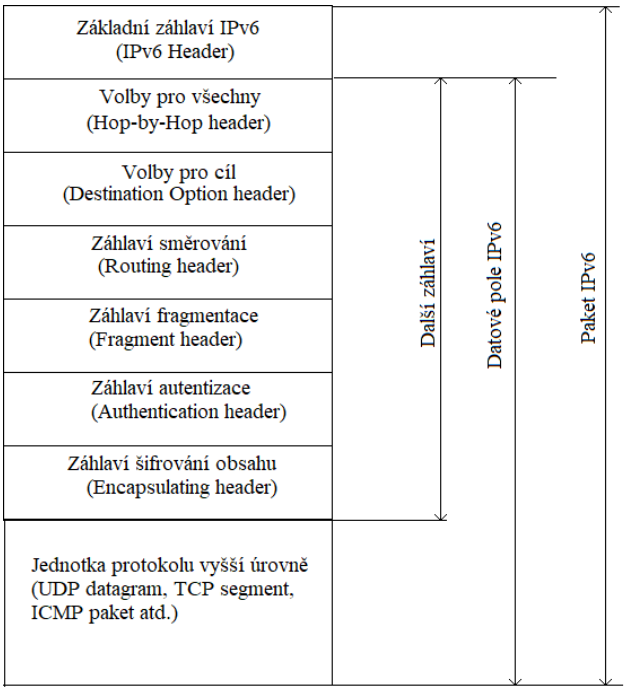
Seznam IPv6 adres, které musí být definovány na každém komunikačním uzlu podporujícím IPv6, je prezentován na obrázku 2.1. Identifikátory rozhraní jsou generovány podle RFC 7217 [2], proto se v jednotlivých podsítích mohou lišit.[3]

lokální linková	fe80::287c:7fb2:48a5:f4a3
individuální	2001:db8:a319:15:acc7:b8a8:fbe9:0b2c
individuální	2001:db8:a319:3:1fa:4dc4:78c:b9e5
lokální smyčka	::1
všechny uzly v rámci rozhraní	ff01::1
všechny uzly v rámci linky	ff02::1
vyzývaný uzel	ff02::1:ffa5:f4a3
vyzývaný uzel	ff02::1:ffe9:0b2c
vyzývaný uzel	ff02::1:ff8c:b9e5
přidělená skupinová	ff15::ac07

Obrázek 2.1: Příklad povinných adres pro počítač [3]

2.3 Formát paketů IPv6

Jedním z hlavních cílů změny formátu záhlaví protokolu IPv6 bylo snížit režii, tzn. snížit množství přenášených servisních informací v každém paketu. Za tímto účelem byly v novém protokolu IP zavedeny koncepty hlavních a doplňkových hlaviček. Hlavní záhlaví je vždy přítomno a volitelná další záhlaví jsou podle potřeby zahrnuta do paketu. Mohou obsahovat např. informace o fragmentaci paketu, úplné trasy paketu při směrování ze zdroje, informace nutné k ochraně přenášených dat a další.



Obrázek 2.2: Struktura paketů IPv6

Obrázek 2.2 ukazuje strukturu paketu IPv6, ve kterém jsou prezentována všechna dodatečná záhlaví. Ve skutečnosti mohou mít pakety IPv6 jednu, několik nebo žádné další hlavičky. Každé záhlaví v této posloupnosti označuje, které záhlaví má následovat tak, že do pole „next header“ uvede kód, který je přiřazen tomuto typu záhlaví. Například kód 0 rozšiřující hlavičky označuje, že by mělo následovat záhlaví volby pro všechny, kód 44 označuje hlavičku pro fragmentaci a kód 60 ukazuje na záhlaví volby pro cíl.

2.3.1 Zásadní záhlaví IPv6 paketů

Zásadní záhlaví má pevnou délku 40 bajtů a obsahuje následující pole (viz tabulku 2.2):

Tabulka 2.2: Hlavička IPv6 paketu [4]

<table>
<tr><th rowspan="2">Byty</th><th colspan="2">0</th><th colspan="2">1</th><th colspan="2">2</th><th colspan="2">3</th></tr>
<tr><td colspan="8"></td></tr>
<tr><td>0–3</td><td colspan="2">Verze</td><td colspan="2">Třída provozu</td><td colspan="4">Značka toku</td></tr>
<tr><td>4–7</td><td colspan="4">Délka dat</td><td colspan="2">Další hlavička</td><td>Max. skoků</td></tr>
<tr><td>8–11</td><td colspan="8" rowspan="4">Zdrojová adresa</td></tr>
<tr><td>12–15</td></tr>
<tr><td>16–19</td></tr>
<tr><td>20–23</td></tr>
<tr><td>24–27</td><td colspan="8" rowspan="4">Cílová adresa</td></tr>
<tr><td>28–31</td></tr>
<tr><td>32–35</td></tr>
<tr><td>36–39</td></tr>
</table>

- **Verze (version, 4 bity)** — v dnešní době je nejrozšířenější verze 4., ale kvůli nedostatku adres se přechází na verzi 6.
- **Třída provozu (traffic class, 8 bitů)** — toto pole je podobné poli Type of Service v IPv4 a lze jej použít k rozdělení provozu do malého počtu agregovaných tříd služeb s různými úrovněmi QoS.
- **Značka toku (flow label, 20 bitů)** — ukazuje na příslušnost paketu k danému toku. Pole značka toku, které chybí v protokolu IPv4, umožňuje vyčlenit z celkového provozu individuální toky a obsluhovat je způsobem odlišným od ostatních paketů. Rozdíl může spočívat v zajištění individuální úrovně QoS nebo v individuálním směru toku.
- **Délka dat (payload length, 16 bitů)** — Číslo obsažené v tomto poli určuje počet bajtů, které zabírají všechny další záhlaví. Maximální hodnota tohoto pole je 65 535. IPv6 umožňuje

existenci paketů s delším datovým polem, takzvaných supervelkých datagramů neboli jumbogramů (jumbograms). V tomto případě se k určení délky použije pole „volby pro všechny“.

- **Další hlavička (next header, 8 bitů)** — obsahuje kód, který určuje typ hlavičky, která následuje za aktuální hlavičkou. Každá následující hlavička také obsahuje pole následující hlavičky. Pokud IPv6 paket neobsahuje další hlavičky, pak toto pole bude mít hodnotu přiřazenou TCP, UDP, RIP, OSPF.
- **Maximální počet skoků (hop limit, 8 bitů)** — toto pole je s malou výjimkou stejné jako u TTL protokolu IPv4: při průchodu paketu směrovačem se od hodnoty tohoto pole odečte jednička. Pokud toto pole dosáhne hodnoty 0, směrovač odešle ICMP zprávu o překročení maximálního počtu skoků. Maximální hodnota pole je 255.
- **Zdrojová/cílová adresa (2x128 bitů)**

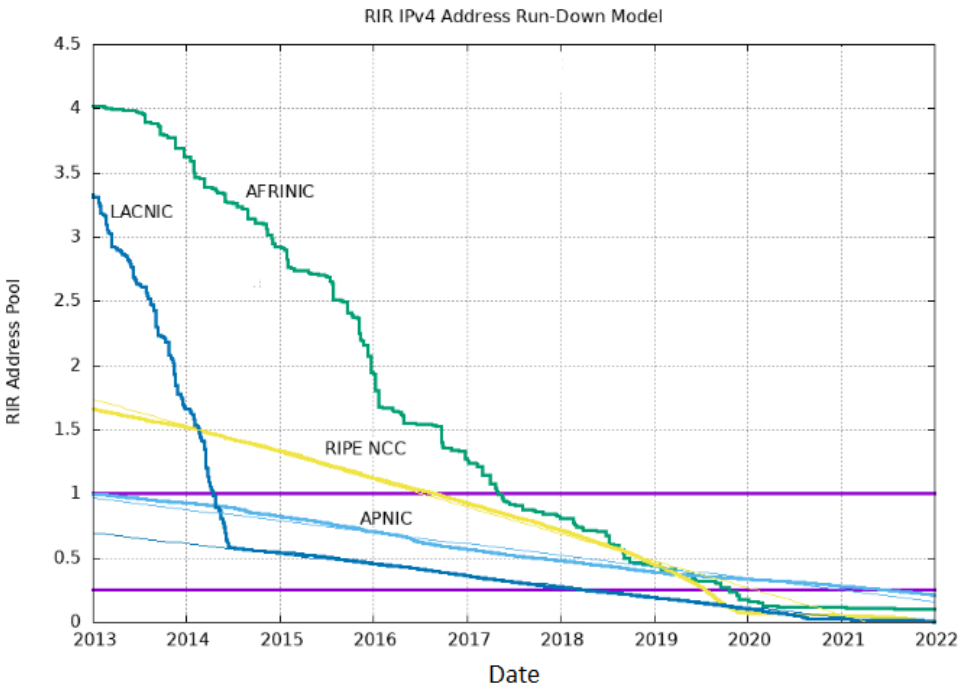
Pokud směrovač obdrží paket s nenulovou, avšak neznámou značkou toku, tak tento paket zpracovává stejně jako pakety s nulovou značkou toku. Prohlíží si všechny pole záhlaví paketu a na základě získaných informací vykonává požadované činnosti. Například jako cílovou adresu určí směrovač adresu dalšího směrovače, na základě analýzy pole třídy provozu rozhoduje, do které prioritní fronty zařadit paket. Na základě nařízené politiky se pak směrovač rozhodne, zda obsluhuje stejně všechny pakety se stejnou značkou. Pokud ano, směrovač vytvoří v cache (mezipaměti) záznam obsahující informace o zpracování tohoto paketu, které umožňují zpracování následujících paketů se stejnou značkou zrychleným způsobem. Zápis je indexován hodnotou značky a adresou zdroje. Když další paket toku přijde na směrovač, z cache se vyjme příslušný záznam a pro paket se provede zrychlený postup zpracování, při kterém se například místo hledání adresy následujícího směrovače v tabulce jednoduše vyjme z cache a místo další analýzy paketu je paket směrován do stejné prioritní řady jako první paket toku. Čas záznamu v cache je omezen na několik sekund, pak se záznam vymaže, značka se opět stane neznámou a celý postup se opakuje od začátku.

2.4 Způsoby soužití sítí IPv4 a IPv6

V případě paralelní existence protokolů IPv6 a IPv4 jsou možné tyto strategie:

- Nic neměnit, zachovat homogenní IPv4 okolí.
- Vybudovat „čistou“ síť IPv6.
- Přejít na IPv6 s částečným zachováním IPv4.

Začněme první strategií —- nic neměnit. Není skutečně nic, co by takovou strategii zásadně vylučovalo. Mezi první požadavky na IPv6 vývojáři označovali možnost sítí IPv4 koexistovat s IPv6



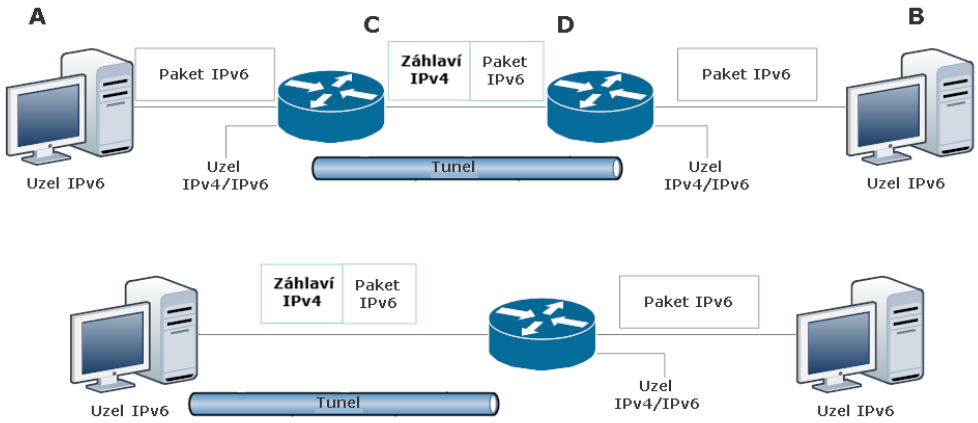
Obrázek 2.3: Model vyčerpání centrálně distribuovaných adres IPv4 [5]

neurčitě dlouhou dobu. Problém nedostatku adres je ale objektivní realitou a časem nemizí, ale jen se stupňuje. Na obrázku 2.3 jsou prezentovány údaje o vyčerpání centrálně distribuovaných adres IPv4. Jak je z obrázku patrné, od poloviny roku 2017 již žádná z organizací nedisponuje ani rozsahem /8. Za takových okolností musí správci sítí IPv4 spoléhat na technologii překladu adres pomocí NAT a nebo na stále menší počet dostupných adres IPv4. Kromě toho by měly být připraveny na nevyhnutelný nástup problémů při přístupu k cizím uzlům, které jsou identifikovány pouze pomocí IPv6 adres.

Další, přesně opačnou strategií je vybudování čisté IPv6 sítě. Přestože je tato síť konečným cílem mnoha organizací, v současnosti je takových sítí relativně málo, neboť k jejich vybudování je potřeba značných dodatečných nákladů na modernizaci nekompatibilních zařízení a aplikací s IPv6. Ideální cestou k síti využívající pouze IPv6 je pak začít s čistým štítem a budovat síť od začátku s modernějším vybavením a aplikacemi, které takovou síť podporují.

2.4.1 Tunelování přes IPv4

Existuje široká škála různých metod soužití, ale my se zastavíme u tunelování, které může být použito v případech, kdy je třeba dvě IPv6 sítě propojit přes tranzitní síť IPv4 (nebo naopak). Tuto metodu často používají velké firmy, které nechtějí ztrácet příliš mnoho času a prostředků, aby kompletně převedly své velké sítě na IPv6, nebo podporovat směrování obou protokolů ve všech



Obrázek 2.4: Typy tunelů

uzlech sítě. Tunelování se však může rychle stát těžkopádnou a nákladnou metodou, pokud roste počet sítí, které je třeba pomocí tunelování propojit.

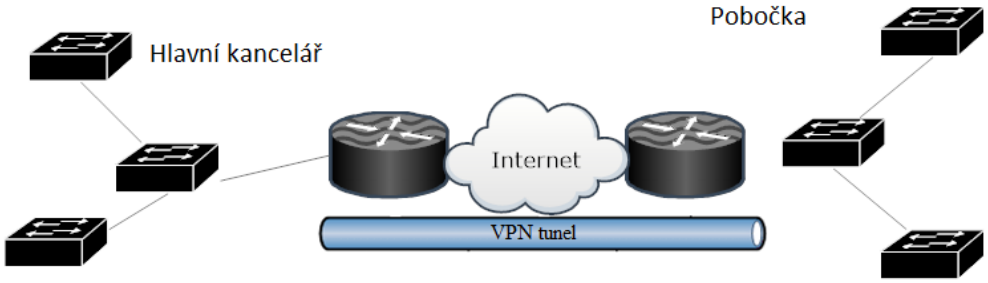
Na obrázku 2.4 je zobrazeno schéma dvou typů tunelů: Směrovač – směrovač a host – směrovač. V prvním případě uzel s IPv6 adresou A pošle paket jinému uzlu IPv6, který má adresu B. Tento paket je směrován směrovači ze sítě IPv6 do sítě IPv6 přes sítě IPv4, za použití tunelování. Směrovač C pro tunelování vytváří záhlaví IPv4 paketu, v jehož datovém poli je obsažen původní IPv6 paket. V záhlaví IPv4 je zdrojová adresa směrovače C a cílová adresa směrovače D. Na základě cílové adresy D se paket IPv4, který nese paket IPv6, směruje přes síť IPv4 naprosto stejným způsobem jako všechny ostatní pakety této IPv4 sítě, dokud nedosáhne cílové adresy D – druhého hraničního směrovače. Směrovač, který obdrží paket, analyzuje jeho hlavičku a určí, zda v poli „další hlavička“ obsahuje hodnotu 41, která ukazuje, že v datovém poli tohoto paketu se nachází paket IPv6. V takovém případě hraniční směrovač extrahuje původní IPv6 paket a směruje jej beze změny obvyklým způsobem na základě IPv6 cílové adresy B.

Různé varianty tunelů se liší způsobem, jak je konfigurovat. Například metoda **GRE** (Generic Routing Encapsulation) využívá manuální konfiguraci hraničních zařízení tunelu.

Kapitola 3

Virtuální privátní síť

Technologie virtuálních privátních sítí (Virtual Private Network, VPN) vznikla jako úspornější alternativa ke směrování pomocí vyhrazených kanálů používaných při propojování privátních počítačových sítí. Jednotlivé VPN jsou stejně jako vyhrazené kanály propojeny do jediné izolované sítě. Na rozdíl od vyhrazených kanálů používající techniky přepojování okruhů, které disponují pevnou propustností, jsou ale pakety ve VPN směrovány pomocí přepínání paketů: IP, MPLS nebo Ethernet. Úspornost služby VPN je důsledkem efektivnějšího rozdělení zdrojů sítě při přepojování paketů oproti přepojování kanálů realizovaných v rámci budování privátní sítě. Na obrázku 3.1 je uveden příklad budování firemní sítě klienta pomocí technologie VPN.



Obrázek 3.1: Standardní VPN

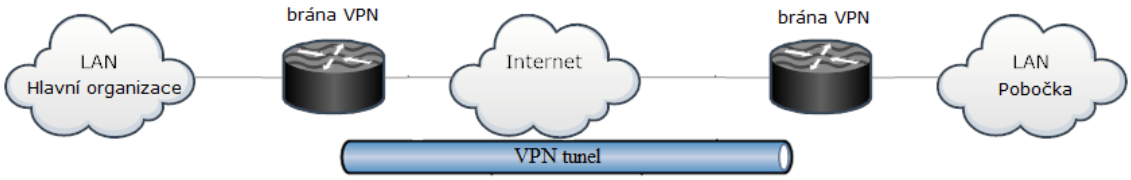
Dá se říci, že VPN napodobuje některé vlastnosti privátní sítě plynoucí z její izolovanosti a že k tomu využívá jiné technologie. Pro provozovatele VPN sítí jsou nejdůležitější tyto vlastnosti privátních sítí:

- **Omezování přístupu k síti na transportní vrstvy modelů OSI** —- pouze uzly sítě mají technickou možnost posílat své pakety navzájem. Pro technologii VPN je zabezpečení této vlastnosti velmi těžké, protože pakety uživatelů VPN procházejí stejnými komunikačními zařízeními a kanály jako pakety externích uživatelů.

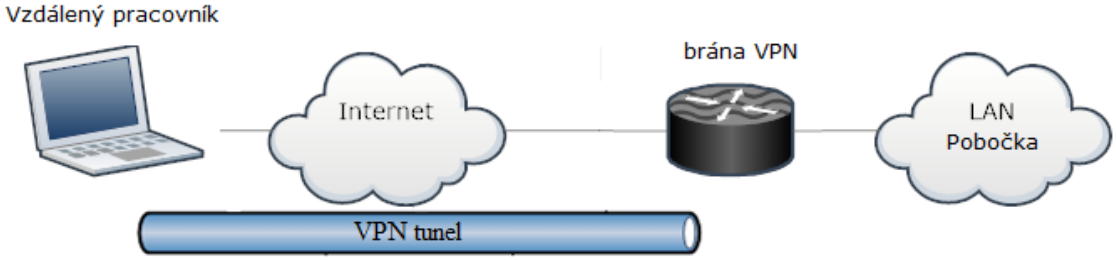
- **Nezávislý systém adresování** —- v privátních sítích není omezení pro výběr adres – mohou být libovolné. Aby byla tato vlastnost zachována, musí síť VPN umožňovat adresování uzlů z celého rozsahu IP adres, včetně privátních (doporučených pouze pro autonomní použití).
- **Maximální možné zabezpečení** —- absence spojení s okolním světem chrání privátní síť před útoky zvenčí a podstatně snižuje pravděpodobnost zachycení provozu při sledování paketů. VPN omezuje přístup externích uživatelů, což znamená, že zabraňuje možnosti útoků zvenčí, a pro ochranu před zachycením lze aplikovat šifrování.

VPN lze použít k řešení různých požadavků, které v sobě zahrnují potřebu bezpečně komunikovat přes veřejnou síť a jež lze kategorizovat následovně:[6]

- Propojení geograficky distribuovaných pobočkových intranetů (site-to-site nebo LAN-to-LAN, viz obrázek 3.2) —- do jednoho velkého podnikového intranetu. Tyto VPN mohou být kvůli statické adresaci snadnou kořistí útočníků, proto je třeba dbát na autentizaci jednotlivých poboček (pro každé propojení zvlášť, aby při útoku nedošlo k průniku do celé sítě) spíše než jednotlivých uživatelů.[6]
- Vzdálený přístup (remote access, viz obrázek 3.3) — připojení vzdáleného uživatele (mobilního nebo domácího pracovníka, teleworker/telecommuter) k podnikovému intranetu, kdy brána VPN musí vykonávat ještě funkce DHCP a DNS. VPN pro vzdálený přístup kladou nároky na řešení autentizace klientů, protože se uživatelé mohou připojovat opravdu odkudkoli a kdykoli.[6]



Obrázek 3.2: VPN pro propojení pobočkových LAN



Obrázek 3.3: VPN pro vzdálený přístup

V rámci této práce jsou popsány následující VPN technologie, které jsou rovněž konfigurovány v praktické části práce:

- **GRE VPN**
- **IPsec VPN**
- **MPLS L3 VPN**

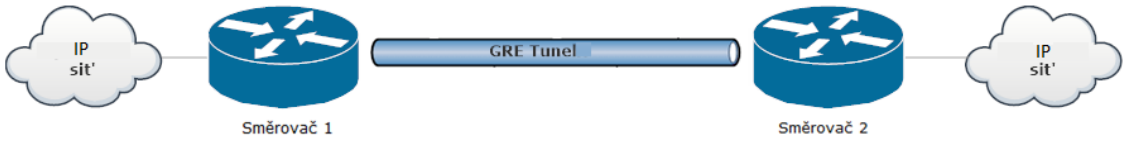
3.1 GRE VPN

Generic Routing Encapsulation (GRE) je protokol, který zapouzdřuje pakety některých protokolů síťové vrstvy, jako je IPv6. Zapouzdřené pakety pak mohou být odeslány přes jiný protokol síťové vrstvy, jako je IPv4. Jako technologie tunelování vrstvy 3 GRE zapouzdřuje pakety jednoho protokolu do paketů jiného protokolu a transparentně přenáší pakety přes tunely GRE.[7]

Výhody GRE:

- Snadno se implementuje a jen mírně zvyšuje zatížení zařízení na obou koncích tunelu.
- Vytváří tunely v síti IPv4 pro propojení sítí s různými protokoly pomocí původní struktury sítě a snížení nákladů.
- Rozšiřuje rozsah síťových protokolů, které podporují omezený počet skoků, a poskytuje flexibilní topologii v podnikových sítích.
- Dokáže zapouzdřit multicastová data a pracovat s IPSec pro zabezpečení multicastových služeb, jako jsou hlasové a video služby.
- Může pracovat s Label Distribution Protocol (LDP), s Multiprotocol Label Switching (MPLS).
- Přemosťuje různorodé podsítě a nastavuje VPN pro zajištění spojení mezi centrálou podniku a pobočkami.

Pakety přenášené přes GRE tunel procházejí procesy zapouzdření (encapsulation) a rozbalení (decapsulation). Jak je znázorněno na obrázku 3.4, směrovač 1 předá pakety pomocí GRE tunelu směrovači 2, směrovač 1 pakety zapouzdří a směrovač 2 pakety rozbalí. Tunel GRE je cesta, po níž jsou přenášeny zapouzdřené pakety.



Obrázek 3.4: Přenos paketů IP přes tunel GRE [7]

Cesta paketu tunelem:

1. Po přijetí paketu IP z rozhraní připojeného k síti IP, směrovač 1 odešle do sítě IP, která je připojena ke směrovači 2.

2. Směrovač 1 kontroluje cílovou adresu v hlavičce paketu a hledá odchozí rozhraní ve směrovací tabulce nebo v tabulce přepínání. Pokud je odchozí rozhraní tunelové rozhraní GRE, směrovač 1 přidá do paketu hlavičku GRE.

3. Směrovač 1 přidá do paketu hlavičku IP, protože páteřní síť používá protokol IP. Zdrojová adresa v hlavičce IP je zdrojová adresa tunelu a cílová adresa v hlavičce IP je cílová adresa tunelu.

4. Směrovač 1 vyhledá odchozí rozhraní ve směrovací tabulce IP na základě cílové adresy v hlavičce IP (cílová adresa tunelu) a předá paket přes páteřní síť IP.

5. Po přijetí paketu z rozhraní tunelu GRE směrovač 2 prozkoumá hlavičku IP v paketu a zjistí, že je cílem tohoto paketu. Směrovač 2 poté odstraní hlavičku IP a doručí paket ke zpracování do GRE.

6. Protokol GRE odstraní hlavičku GRE a doručí paket do sítě IP.

3.2 IPsec VPN

Zde je popsán sada protokolů IPsec, který může pomoct zajistit bezpečnost dat odesílaných v rámci privátní sítě.

IPSec je ucelený soubor otevřených standardů, který má dnes dobře definované jádro, které lze zároveň celkem jednoduše doplňovat o nové funkce a protokoly.

Jádro IPSec se skládá ze tří protokolů:

- **AH** (Authentication Header) —- jenž zaručuje integritu a autentičnost dat.
- **ESP** (Encapsulating Security Payload) —- který šifruje přenášená data, poskytuje důvěrnost, může také podporovat autentizaci a integritu dat.
- **IKE** (Internet Key Exchange) —- který řeší pomocné úkoly, jako automaticky poskytovat koncovým bodům zabezpečení kanálu tajných klíčů nezbytných pro provoz ověřovacích protokolů a šifrování dat.

Částečná duplikace ochranných funkcí protokoly AH a ESP je spojena s praxí uplatňovanou v mnoha zemích omezováním exportu a/nebo importu prostředků, které zajišťují důvěrnost dat pomocí šifrování. Každý z těchto protokolů lze používat jak samostatně, tak současně s tím druhým, takže v případech, kdy nelze použít šifrování z důvodu stávajících omezení, lze systém dodat pouze s

protokolem AH. Tato ochrana dat je přirozeně v mnoha případech nedostatečná. Přijímající strana má pouze možnost zkontrolovat, zda byla data odeslána uzlem, ze kterého jsou očekávána, a zda dorazila ve formě, v jaké byla odeslána. Protokol AH však nemůže chránit před neoprávněným prohlížením dat na cestě sítí, protože je nešifruje —- k šifrování dat je vyžadován protokol ESP.

3.2.1 Bezpečnostní asociace

Aby protokoly AH a ESP vykonávaly svou práci při ochraně přenášených dat, protokol IKE vytváří logické spojení mezi dvěma koncovými body, které se ve standardech IPSec nazývá bezpečnostní asociace (Security Association, SA).

Standardy IPSec umožňují koncovým bodům zabezpečeného kanálu buď používat jediné bezpečnostní asociace k přenášení provozu všech hostitelů komunikujících tímto kanálem, nebo pro tento účel vytvářet libovolný počet bezpečnostních asociací, například jednu na připojení TCP. To umožňuje vybrat požadovaný počet bezpečnostních asociací – od jedné pro provoz z mnoha koncových bodů až po individuálně nakonfigurovaný počet bezpečnostních asociací pro ochranu každé aplikace.

Bezpečnostní asociace v protokolu IPSec je jednosměrné (simplexní) logické připojení, takže pokud chcete poskytnout obousměrnou zabezpečenou komunikaci, musí být vytvořena dvě bezpečnostní asociace. Tyto asociace mohou mít obecně různé charakteristiky, například při odesílání požadavků do databáze postačí pouze autentizace a pro data odpovědí, která nesou cenné informace, může být také nutné zajistit jejich důvěrnost.

Navázání bezpečného spojení začíná vzájemnou autentizací stran, protože všechna bezpečnostní opatření ztratí smysl, pokud jsou data odeslána nebo přijata nesprávnou osobou nebo od nesprávné osoby. Parametry SA, které jsou dále vybrány, určují, který ze dvou protokolů, zda AH nebo ESP, bude použit k ochraně dat, které funkce spustí protokol (lze například provádět pouze ověřování a kontroly integrity, nebo lze také poskytnout důvěrnost). Vysoce důležitými parametry bezpečnostní asociace jsou také tajné klíče používané při provozu protokolů AH a ESP.

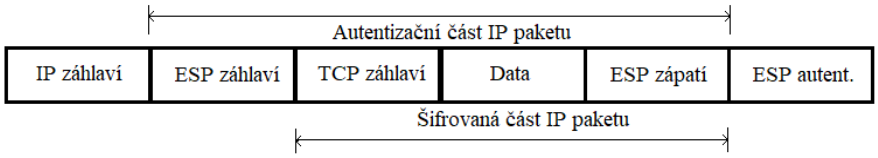
Protokol IPsec umožňuje automatické i manuální navázání bezpečného spojení. Při manuální metodě správce konfiguruje koncové uzly tak, aby podporovaly vyjednané parametry přidružení, včetně tajných klíčů. V proceduře automatického vytvoření SA si protokoly IKE pracující na opačných stranách kanálu vybírají parametry během procesu vyjednávání. Pro každý úkol řešený protokoly AH a ESP je navrženo několik autentizačních a šifrovacích schémat. Díky tomu je protokol IPSec velmi flexibilní.

Pro zajištění kompatibility definuje standardní verze IPSec určitou povinnou sadu „nástrojů“, zejména k autentizaci dat lze vždy použít některou ze standardních funkcí SHA-2 nebo SHA-3. Výrobci produktů využívajících IPSec mohou protokol záměrně rozšířit o další ověřovací algoritmy a symetrické šifrování, což se jim daří. Například mnoho implementací IPSec podporuje populární šifrovací algoritmus Triple DES a také algoritmy: Blowfish, Cast, Idea, RC5, AES.

Protokoly AH a ESP mohou chránit data ve dvou režimech: transport a tunel. V transportním režimu je přenos IP paketu po síti prováděn pomocí jeho původní hlavičky, zatímco v tunelovém režimu je původní paket umístěn do nového IP paketu a přenos dat po síti je prováděn na základě záhlaví nového IP paketu.

3.2.2 Protokol ESP

Protokol ESP řeší dvě skupiny problémů. První zahrnuje úkoly zajištění autentizace a integrity dat podobně jako úkoly protokolu AH, druhý představuje ochranu přenášených dat jejich šifrováním před neoprávněným zobrazením. Jak je vidět na obrázku 3.5, je záhlaví rozděleno na dvě části oddělené datovým polem. První část, nazývaná samotná hlavička ESP, je tvořena poli SPI a SN, jejichž účel je podobný stejnojmenným polím protokolu AH a je umístěn před datovým polem.



Obrázek 3.5: Struktura IP paketu zpracovávaného protokolem ESP v transportním režimu

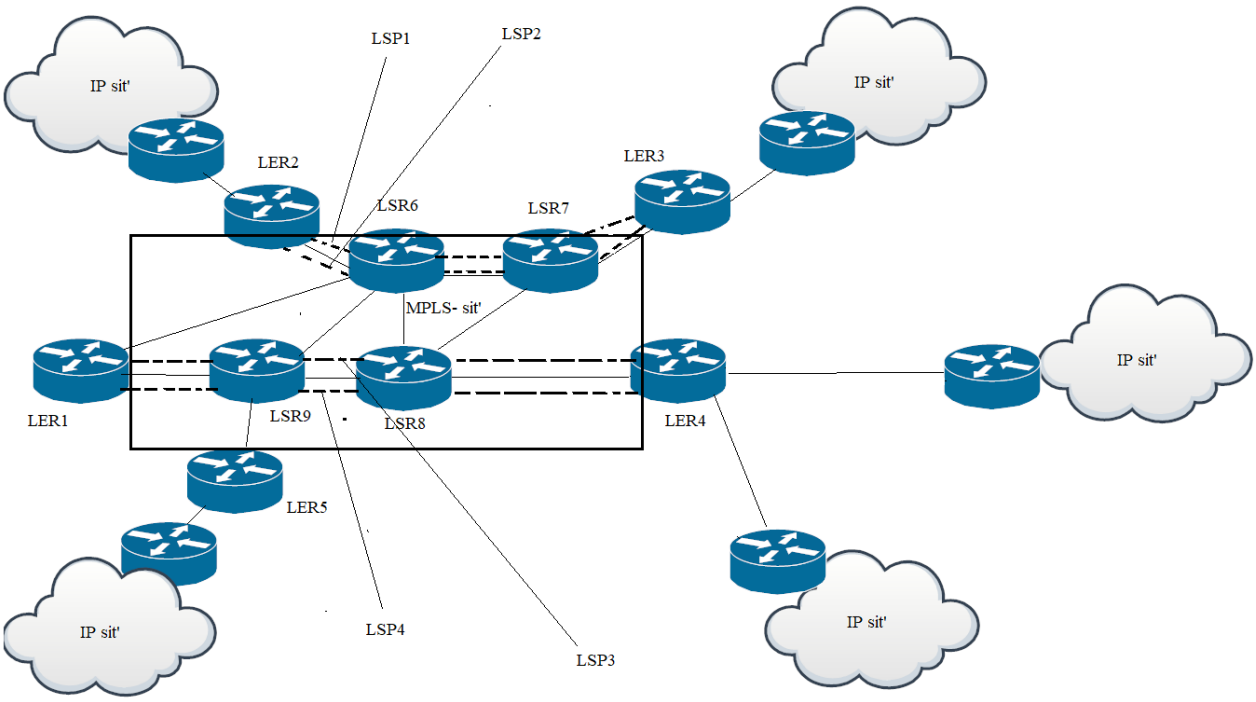
Na obrázku 3.5 je ukázáno rozložení polí hlavičky ESP v transportním režimu, v němž nešifruje hlavičku původního IP paketu, jinak směrovač nebude schopen číst pole hlavičky a správně přeposílat paket mezi sítěmi. Šifrovaná pole také nezahrnují pole SPI a SN, která musí být přenášena v čistém textu, aby bylo možné přicházející paket přiřadit ke konkrétní bezpečnostní asociaci.

3.3 MPLS L3 VPN

Multiprotokolová komunikační technologie (MultiProtocol Label Switching, MPLS) je považována za jednu z nejslibnějších transportních technologií, které spojují techniku virtuálních kanálů s funkčností TCP/IP. Hlavní přednost MPLS je ve schopnosti poskytovat rozmanité přepravní služby v IP sítích, primárně služby virtuálních soukromých sítí. Tyto služby se liší rozmanitostí, mohou být poskytovány jak na síťové, tak na linkové vrstvě. MPLS navíc doplňuje datagramové IP sítě tak důležitou vlastností, jako je přenos provozu v souladu s technikou virtuálních kanálů, což umožňuje volit potřebný režim přenosu provozu podle požadavků služby.

Vezměme si cestu LSP na příkladu sítě znázorněné na obrázku 3.6. Tato MPLS síť komunikuje přes několik IP sítí, které nemusí podporovat technologii MPLS.

Na obrázku vidíme zařízení LER. Toto zařízení, které je funkčně náročnější, přijímá provoz od ostatních sítí ve formě standardních IP paketů a poté přidá ke každému paketu značku a nasměruje podél příslušné cesty k výstupnímu zařízení LER přes několik přechodných zařízení LSR. Paket se přitom nesměruje na základě cílové IP adresy, ale na základě značky. Stejně jako v jiných



Obrázek 3.6: MPLS síť

technologiích využívajících techniku virtuálních kanálů má značka lokální význam v rámci každého zařízení LER nebo LSR, to znamená, že když je paket přenášen ze vstupního rozhraní do výstupního rozhraní, hodnota značky se změní.

Při rozhodování o výběru příštího směrovače se využívá LFIB tabulka a podobá se obdobným tabulkám jiných technologií založených na technice virtuálních kanálů (viz tabulka 3.1).

Tabulka 3.1: Příklad LFIB tabulky v technologii MPLS

Vstupní rozhraní	**Značka**	**Další rozhraní**	**Akce**
K0	243	K1	255
K0	33	K2	46
...	....	.....	...

Ve většině případů zpracování MPLS rámců se tato pole používají stejným způsobem jako odpovídající pole zobecněné přepínací tabulky. To znamená, že hodnota pole dalšího skoku je hodnota rozhraní, do kterého má být rámec odeslán, a hodnota pole akce je hodnota nové značky. V některých případech ale tato pole mohou sloužit jiným účelům. Tabulky jsou pro každé zařízení LSR tvořeny signalizačním protokolem. MPLS používá dva různé signalizační protokoly: Label Distribution Protocol (LDP) a modifikaci protokolu RSVP. Při tvorbě LFIB tabulky na zařízeních LSR

signalizační protokol prokládá přes síť virtuální trasy, které se v technologii MPLS označují jako cesty přepojování po značkách (Label Switching Path, LSP).

V případě, že jsou značky vloženy v LFIB tabulkách pomocí protokolu LDP, jsou trasy virtuálních cest LSP shodné s trasami IP, protože jsou vybírány běžnými protokoly směrování.

LSP je jednosměrný virtuální kanál, takže pro přenos provozu mezi dvěma zařízeními LER musí být nastaveny alespoň dvě komunikační cesty po značkách – jedna v každém směru. Na obrázku 3.6 jsou dva páry komunikačních cest, které spojují zařízení LER2 s LER3 a LER1 s LER4. LER pak plní důležitou funkci, jako je směrování provozu po jedné z cest LSP. Pro implementaci této funkce je v MPLS zaveden pojem Forwarding Equivalence Class (FEC).

Příchozí paket je řazen do dané třídy na základě některých znaků. Zde je několik příkladů klasifikace:

- **Na základě cílové IP adresy** — nejblíže principům fungování IP sítí je přístup, který spočívá v tom, že pro každý prefix cílové sítě, který je k dispozici v LFIB tabulce směrování LER, vzniká samostatná třída FEC. Protokol LDP, který dále zvažujeme, plně automatizuje proces vytváření tříd FEC podle tohoto způsobu.
- **V souladu s požadavky filtrování paketů** — třídy jsou vybírány tak, aby bylo dosaženo vyváženého využití síťových kanálů.
- **Podle požadavků VPN** — pro konkrétní virtuální soukromou síť klienta vzniká samostatná třída FEC.
- **Podle typů aplikace** — například provoz IP telefonie (RTP) představuje jednu třídu FEC a webový provoz představuje jinou třídu FEC.
- **Podle rozhraní** — rozhraní, ze kterého je přijat paket.
- **Podle cílové MAC adresy** — pokud se jedná o ethernetový rámec.

Jak je vidět z příkladů, při klasifikaci provozu v MPLS mohou být použity parametry nejen převzaté z hlavičky IP paketu, ale i mnohé další, včetně informací z linkové (MAC) a z fyzické (rozhraní) úrovně.

Po rozhodnutí, zda paket patří do určité třídy FEC, musí být přidružen k existující cestě LSP. Pro tuto operaci používá LER tabulku FTN (FEC Then Next hop – mapování třídy FEC na další skok). Tabulka 3.2 je příkladem FTN.

Tabulka 3.2: Příklad tabulky FTN

Parametry FEC	**Značka**
110.19.0.0/16; 183.99.0.0/16	41
188.81.30.0/24; eth23	42

Na základě tabulky FTN je každému příchozímu paketu přiřazena příslušná značka, poté se tento paket stává nerozeznatelným v doméně MPLS od ostatních paketů stejné třídy FEC, všechny se posunují stejnou cestou uvnitř domény. Správce sítě má k dispozici možnost sestavovat tabulky FEC, případně je korigovat, pokud se tvoří automaticky. Konfigurace jsou prováděny pouze v LER a všechna přechodová zařízení LSR dělají jednoduchou práci tím, že paket směrují v souladu s technikou virtuálního kanálu. Výstupní zařízení LER odstraňuje značku a přenáší paket do další sítě již ve standardní podobě IP paketu. Technologie MPLS tak zůstává transparentní pro ostatní IP sítě.

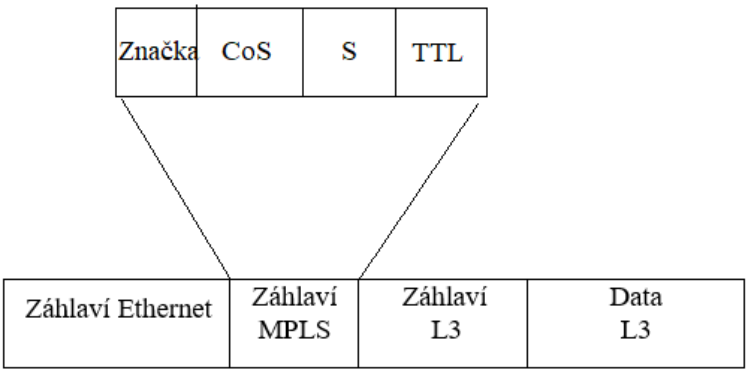
V MPLS sítích se obvykle používá vylepšený algoritmus pro zpracování paketů. Vylepšení spočívá v tom, že odstranění značky neřeší poslední zařízení na cestě, ale předposlední. Po zjištění předposledního zařízení na základě významu značky další skok již značka v MPLS rámce není nutná, protože poslední zařízení, tedy výstupní zařízení LER musí posuzovat paket na základě významu IP adresy. Tato malá změna algoritmu propagace rámců umožňuje ušetřit jednu operaci nad MPLS rámcem. V opačném případě by poslední zařízení podél cesty muselo odstranit značku a až poté provést náhled do směrovací tabulky. Tato technika byla pojmenována po technice odstranění značky na předposledním skoku (Penultimate Hop popping, PHP).

Záhlaví MPLS se skládá z několika polí (viz obrázek 3.7):

- **Značka** — Používá se pro výběr vhodné LSP.
- **Doba života** — Toto pole, které zabírá 8 bitů, se podobá obdobnému poli IP paketu. Je nutné proto, aby zařízení LSR mohlo zahazovat „zbloudilé“ pakety pouze na základě informací obsažených v hlavičce MPLS, aniž by muselo kontrolovat hlavičku IP.
- **Třída služeb** — Pole CoS, které zabírá tři bity, bylo původně rezervováno pro rozvoj technologie, ale v poslední době se používá hlavně pro uvedení třídy provozu, která vyžaduje určitou úroveň QoS.
- **Bottom of Stack (BS)** — Tento znak (S) zabírá 1 bit a určuje dno zásobníku.

Pro objasnění mechanismu interakce MPLS s technologiemi linkové úrovně zvážíme situaci, kdy záhlaví MPLS zahrnuje pouze jednu značku. V rámci linkové vrstvy je záhlaví MPLS umístěno mezi původní záhlaví a záhlaví paketu síťové vrstvy. Na obrázku 3.7 je způsob, jak umístit značku do ethernetového rámce. Standardy MPLS definují také způsob, jak umístit značku do rámce Frame Relay nebo také ATM. Vzhledem k tomu, že hlavička MPLS se vejde mezi záhlaví linkové vrstvy a záhlaví IP, říká se ji SHIM Header.

Pokud je tedy v MPLS použit ethernetový rámec, pak se zdrojové a přijímací adresy MAC, i když jsou přítomny v odpovídajících polích ethernetového rámce, nepoužívají k předávání rámců v ethernetových připojeních typu point-to-point. Výjimkou je případ, kdy existuje síť ethernetových přepínačů mezi dvěma sousedními LSR zařízeními: Cílová MAC adresa rámce MPLS bude vyžadována, aby bylo možné paket dostat k dalšímu zařízení LSR, a bude jej propagovat na základě značky.



Obrázek 3.7: Struktura MPLS záhlaví

Nalezení MAC adresy dalšího LSR pak bude provedeno standardním způsobem pomocí protokolu ARP (Address Resolution Protocol) přes IP adresu LSR.

Výskyt zásobníků značek je jednou z originálních vlastností MPLS. Systém agregovaných cest LSP umožňuje vytvoření takového systému, který obsahuje libovolný počet úrovní hierarchie. Pro udržení této funkce musí MPLS rámec, který se pohybuje podél hierarchicky organizované cesty, zahrnovat tolik záhlaví MPLS, kolik má systém úrovní hierarchie. Posloupnost záhlaví je organizována jako zásobník, kde rozlišujeme značku na vrcholu a na konci zásobníku, přičemž za poslední značkou následuje příznak S = 1. Nad značkami se provádějí následující operace zadávané v LFIB tabulce:

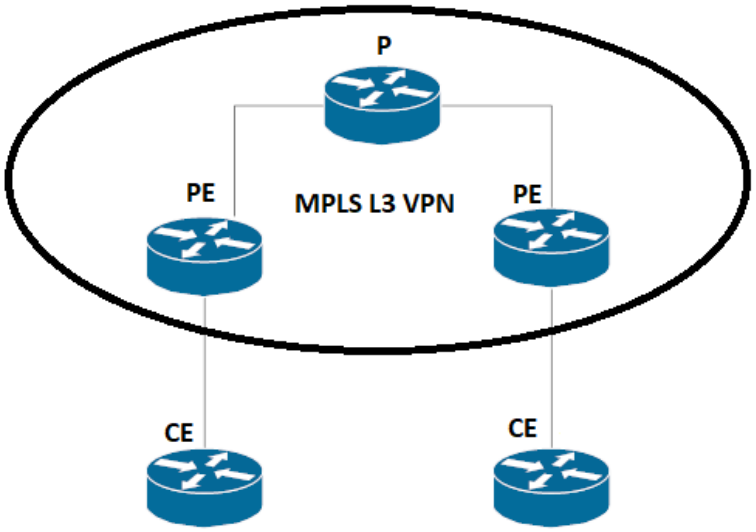
- **Push** — Vloží značku do zásobníku. V případě prázdného zásobníku tato operace znamená jednoduché přiřazení značky k paketu. Pokud jsou již na zásobníku jiné značky, pak v důsledku této operace nová značka posune „starší“ značky hlouběji do zásobníku a sama se umístí na vrchol.

- **Swap** — Nahradí současnou značku novou značkou.

- **Pop** — Vyjmutí (odstranění) horní značky, čímž se všechny ostatní značky zásobníku posunou o jednu úroveň výše.

Průběh MPLS paketu vždy probíhá na základě značky umístěné v dané chvíli na vrcholu zásobníku. Hierarchie značek nejčastěji nachází své uplatnění v sítích rozdělených do několika domén. Uvnitř domény dochází k postupu paketů na základě značek jedné z úrovní zásobníku a mezi doménami na základě značek jiné úrovně. Tento přístup umožňuje nezávisle na sobě zařídit vnitrodoménové a mezidoménové směrování paketů, což se v mnoha případech ukazuje jako užitečné. Zde lze provést analogii s využitím MAC adres pro přenos rámce uvnitř IP podsítě a IP adres pro přenos paketů mezi IP podsítěmi. Zásobník značek se také ukazuje jako užitečný při organizaci technologie **VPN**.

Virtuální privátní sítě MPLS jsou založeny na přepojování datagramů přes MPLS, zatímco informace o směrování se šíří přes BGP, který je také zodpovědný za přenos informací o členství ve VPN. Hierarchie komponent MPLS L3 VPN je uvedena na obrázku 3.8, na němž je zobrazena oblast působnosti operátora oproti oblasti působení klienta. VPN se dělí na síť provozovanou poskytovatelem P a síť klienta C. V síti operátora jsou z hlediska VPN nejdůležitější směrovače na okrajích sítě – PE. Tam se odehrává celé řízení MPLS VPN. Uvnitř sítě jsou centrální směrovače P, které propojují hraniční směrovače, nemají informace o VPN a fungují pouze jako výkonné směrovače na základě značek MPLS.[6]



Obrázek 3.8: Příklad MPLS L3 VPN sítě

Klienti připojují své sítě přes směrovače Customer Edge (CE), které se mohou připojit k jednomu, nebo více hraničním směrovačům PE. Klientský směrovač CE je rovnocenným partnerem periferního směrovače operátora PE. CE poskytuje informace o směrování PE pro privátní síť. Každý hraniční směrovač PE musí udržovat globální směrovací tabulku (na základě interního směrovacího protokolu nebo BGP) a jednotlivé směrovací tabulky virtuální směrování a posílání (VRF) pro každou VPN, aby bylo možné realizovat přeposílání paketů po cestách s přepojováním po značkách (LSP). LSP je definován pro tok paketů s podobnými charakteristikami (FEC, Forwarding Equivalence Class) na základě různých filtrů (podle adres, typů aplikačních protokolů). VRF umožňuje propojit síť MPLS operátora s rozšířeným protokolem MBGP a síť klienta, který využívá protokol vnitřního směrování nebo statické trasy. Z pohledu BGP jsou PE a CE partneři v externím eBGP a PE jsou partneři ve vnitřním iBGP (interní směrovací protokol běží v síti poskytovatele, např. RIP). Rozšíření BGP umožňuje koexistenci tras VPN s běžnými trasami v síti operátora, a to i trasami VPN, které se překrývají z hlediska používaných soukromých adres.[6]

Každá VPN má svou vlastní adresu, která identifikuje všechny uživatele, kteří tuto VPN používají. Route Distinguisher (RD) je osmibitová hodnota přidávaná k prefixu IPv4 adresy. To vytváří

nový typ prefixu VPN v prostředí IPv4: Prefix RD + IPv4. Rozlišovač cesty může obsahovat číslo autonomního systému operátora sítě MPLS plus identifikátor VPN, přiřazený provozovatelem. Použití rozlišovače cesty nevyžaduje žádnou modifikaci BGP.[6]

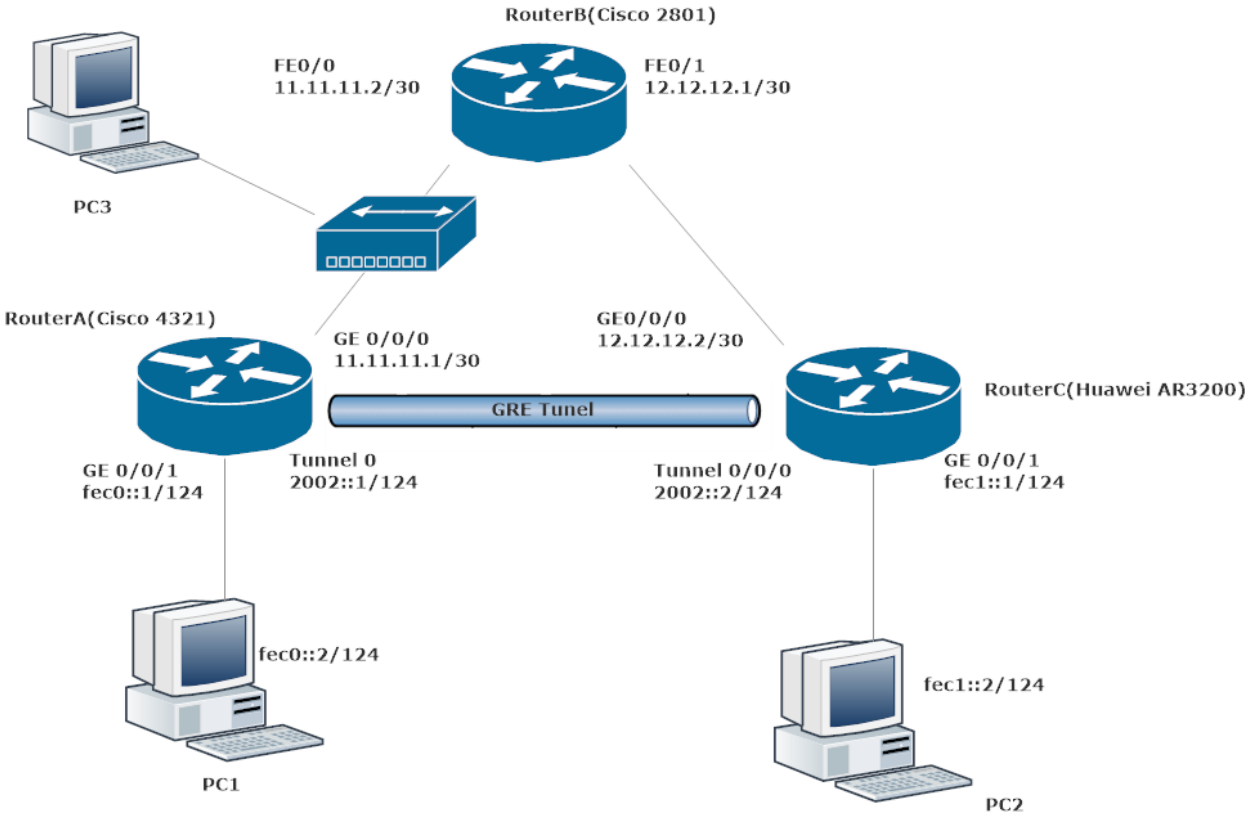
Hostitelské PE by mělo vědět, odkud cesta vede a do jaké tabulky VRF má být umístěna a také jak rozlišovat opakující se adresy. Hraniční směrovač u vstupu do sítě by tedy měl „převést“ informace o směrování z IPv4 do konceptu VPN: Přiřazuje RD, místo původu (SoO, Site of Origin) a cíl exportu trasy (RT, Router Target). Přepíše také atribut následujícího směrovače (next hop) na rozhraní oblasti PE. Přiřazuje značku VPN a posílá aktualizace všem sousedům iBGP. Přijímací PE překládá adresy VPN do IPv4.[6]

Značka VPN se používá pro správné směrování dat do VPN, obsahuje informace o příslušné VRF, jinak se nemění během přenosu přes páteř MPLS. Uvnitř páteře se používá značka interniho protokolu, která je přiřazena vstupnímu hraničnímu směrovači PE a mění se v každém páteřním LSR P.[6]

Kapitola 4

Konfigurace GRE VPN

Topologie mezi zařízeními Cisco a Huawei pomocí tří směrovačů byla vytvořena za účelem testování funkčnosti technologie GRE VPN. Dva směrovače jsou umístěny po stranách a mezi mini je vytvořen GRE tunel. Centrální směrovač (Router B) emuluje poskytovatele IPv4.



Obrázek 4.1: Topologie pro GRE VPN

Směrovače „Router A“ a „Router C“ jsou pobočky společnosti, mezi kterými musíme vytvořit síť VPN. IPv6 GRE tunel nám umožňuje přenášet data po síti takového poskytovatele, který neumožňuje šifrovaný provoz a pouze formát IPv4. Uvnitř tohoto tunelu je tedy provoz IPv4, ale na jeho koncích je adresa IPv4 i adresa IPv6. Pro ověření provozuschopnosti této sítě mezi „Router A“ a „Router B“ byl připojen rozbočovač, ke kterému byl připojen počítač PC3. PC3 bude shromažďovat provoz v této síti. Všechno adresování je znázorněno na obrázku 4.1. K vybudování této sítě byla použita dokumentace Cisco [8] i Huawei [9].

4.1 Konfigurace směrovače RouterA

Povolení IPv6 směrování na třetí vrstvě:

```
ipv6 unicast-routing
```

Dále nastavíme protokol směrování OSPF ve dvou verzích. Jeden protokol OSPF je používán pro dynamické směrování internetového protokolu verze 4 a druhý OSPFv3 pro dynamické směrování internetového protokolu verze 6:

```
router ospf 1
    network 11.11.11.0 0.0.0.3 area 0
ipv6 router ospf 1
    router-id 1.1.1.1
```

Dále nakonfigurujeme všechna rozhraní, která potřebujeme použít. Nakonfigurujeme IP adresy, zapneme tyto rozhraní, povolíme možnost používat adresy IPv6 a přidáme příkaz pro zapnutí OSPFv3 protokolu:

```
interface GigabitEthernet0/0/0
    ip address 11.11.11.1 255.255.255.252
interface GigabitEthernet0/0/1
    ipv6 enable
    ipv6 address FEC0::1/124
    ipv6 ospf 1 area 0
```

Poté vytvoříme GRE tunel, kterému uvedeme jeho adresu, začátek a konec:

```
interface Tunnel0
    ipv6 enable
    ipv6 address 2002::1/124
    ipv6 ospf 1 area 0
    tunnel source 11.11.11.1
    tunnel destination 12.12.12.2
```

4.2 Konfigurace směrovače RouterB

K tomuto směrovači musíme nastavit IPv4 adresy na rozhraních, aby celá síť fungovala podle patřičných pravidel, a také nastavíme protokol směrování OSPF.

```
interface FastEthernet0/0
    ip address 11.11.11.2 255.255.255.252
interface FastEthernet0/1
    ip address 12.12.12.1 255.255.255.252
router ospf 1
    network 11.11.11.0 0.0.0.3 area 0
    network 12.12.12.0 0.0.0.3 area 0
```

4.3 Konfigurace směrovače RouterC

Pro zapnutí IPv6 směrování na směrovačích Huawei je třeba následujícího příkazu:

```
ipv6
```

Dále nastavíme protokol směrování OSPF ve dvou verzích. Jeden protokol OSPF je používán pro dynamické směrování internetového protokolu verze 4 a druhý OSPFv3 pro dynamické směrování internetového protokolu verze 6:

```
ospf 1
    area 0.0.0.0
    network 12.12.12.0 0.0.0.3
ospfv3 1
    router-id 2.2.2.2
```

Dále nakonfigurujeme všechna rozhraní, která potřebujeme použít. Nakonfigurujeme IP adresy, zapneme tyto rozhraní, povolíme možnost používat adresy IPv6 a přidáme příkaz pro zapnutí OSPFv3 protokolu:

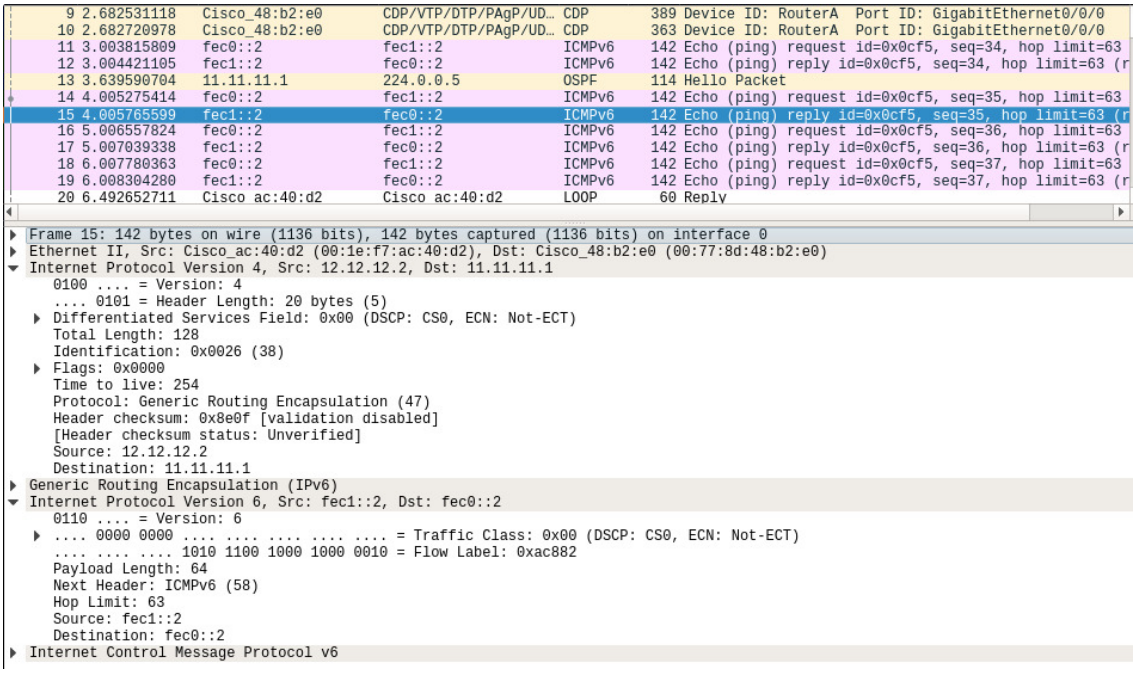
```
interface GigabitEthernet0/0/0
    ip address 12.12.12.2 255.255.255.252
interface GigabitEthernet0/0/1
    ipv6 enable
    ipv6 address FEC1::1/124
    ospfv3 1 area 0.0.0.0
```

Poté vytvoříme GRE tunel, kterému uvedeme jeho adresu, začátek a konec:

```
interface Tunnel 0/0/1
    ipv6 enable
    ipv6 address 2002::2/124
    ospfv3 1 area 0.0.0.0
    source 12.12.12.2
    destination 11.11.11.1
```

4.4 Ověření funkčnosti

Pro potvrzení fungování této technologie je v rámci této sítě použit nástroj Wireshark. Pro zachycení provozu a jeho pozdější analýzu je tedy mezi směrovače „Router A“ a „Router B“ připojen rozbočovač a k němu připojeno PC3, na kterém je nainstalován program Wireshark. Utilita ping byla použita z PC2 na PC1 a výsledky můžeme vidět na obrázku 4.2



Obrázek 4.2: Odesílání paketu IPv6 z PC2 na PC1

Z paketů zachycených na PC3 a analýzy jejich struktury lze vidět, že pakety projdou přes GRE IPv6 oběma směry, což potvrzuje správnost provozu sítě v souladu se zadáním. Níže je zobrazen výpis směrovací tabulky pro obě verze IP protokolů na obou směrovačích, kterými jsou „Router A“ a „Router C“.

```
RouterA#show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
    ia - IS-IS inter area, * - candidate default, U - per-user static route
    o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
    a - application route
    + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set

    11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   11.11.11.0/30 is directly connected, GigabitEthernet0/0/0
L   11.11.11.1/32 is directly connected, GigabitEthernet0/0/0
    12.0.0.0/30 is subnetted, 1 subnets
O   12.12.12.0 [110/11] via 11.11.11.2, 00:17:32, GigabitEthernet0/0/0

RouterA#show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
           B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
           I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
           EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
              Destination
           NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
           OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
           a - Application

C   2002::/124 [0/0]
   via Tunnel0, directly connected
L   2002::1/128 [0/0]
    via Tunnel0, receive
C   FEC0::/124 [0/0]
    via GigabitEthernet0/1, directly connected
L   FEC0::1/128 [0/0]
    via GigabitEthernet0/1, receive
O   FEC1::/124 [110/1001]
    via FE80::C0C:C02, Tunnel0
```

```
L   FF00::/8 [0/0]
    via Null0, receive

<RouterC>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
              Destinations : 8      Routes : 8
Destination/Mask  Proto   Pre  Cost      Flags NextHop         Interface
     11.11.11.0/30 OSPF   10   11          D   12.12.12.1      GigabitEthernet0/0/0
     12.12.12.0/30 Direct 0    0           D   12.12.12.2      GigabitEthernet0/0/0
     12.12.12.2/32 Direct 0    0           D   127.0.0.1       GigabitEthernet0/0/0
      127.0.0.0/8  Direct 0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32 Direct 0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32 Direct 0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32 Direct 0    0           D   127.0.0.1       InLoopBack0

<RouterC>display ipv6 routing-table
Routing Table : Public
            Destinations : 7        Routes : 7
 Destination : ::1                           PrefixLength : 128
 NextHop     : ::1                           Preference  : 0
 Cost        : 0                             Protocol    : Direct
 RelayNextHop : ::                           TunnelID    : 0x0
 Interface   : InLoopBack0                   Flags       : D

 Destination : 2002::                        PrefixLength : 124
 NextHop     : 2002::2                       Preference  : 0
 Cost        : 0                             Protocol    : Direct
 RelayNextHop : ::                           TunnelID    : 0x0
 Interface   : Tunnel0/0/0                   Flags       : D

 Destination : 2002::2                       PrefixLength : 128
 NextHop     : ::1                           Preference  : 0
 Cost        : 0                             Protocol    : Direct
 RelayNextHop : ::                           TunnelID    : 0x0
 Interface   : Tunnel0/0/0                   Flags       : D
```

```
 Destination : FE80::                        PrefixLength : 10
 NextHop     : ::                            Preference  : 0
 Cost        : 0                             Protocol    : Direct
 RelayNextHop : ::                           TunnelID    : 0x0
 Interface   : NULL0                         Flags       : D

 Destination : FEC0::                        PrefixLength : 124
 NextHop     : FE80::277:8DFF:FE48:B2E0      Preference  : 10
 Cost        : 1563                          Protocol    : OSPFv3
 RelayNextHop : ::                           TunnelID    : 0x0
 Interface   : Tunnel0/0/0                   Flags       : D

 Destination : FEC1::                        PrefixLength : 124
 NextHop     : FEC1::1                       Preference  : 0
 Cost        : 0                             Protocol    : Direct
 RelayNextHop : ::                           TunnelID    : 0x0
 Interface   : GigabitEthernet0/0/1          Flags       : D

 Destination : FEC1::1                       PrefixLength : 128
 NextHop     : ::1                           Preference  : 0
 Cost        : 0                             Protocol    : Direct
 RelayNextHop : ::                           TunnelID    : 0x0
 Interface   : GigabitEthernet0/0/1          Flags       : D


RouterA#show interfaces tunnel0
Tunnel0 is up, line protocol is up
Hardware is Tunnel
MTU 9976 bytes, BW 100 Kbit/sec, DLY 50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel linestate evaluation up
Tunnel source 11.11.11.1, destination 12.12.12.2
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
```

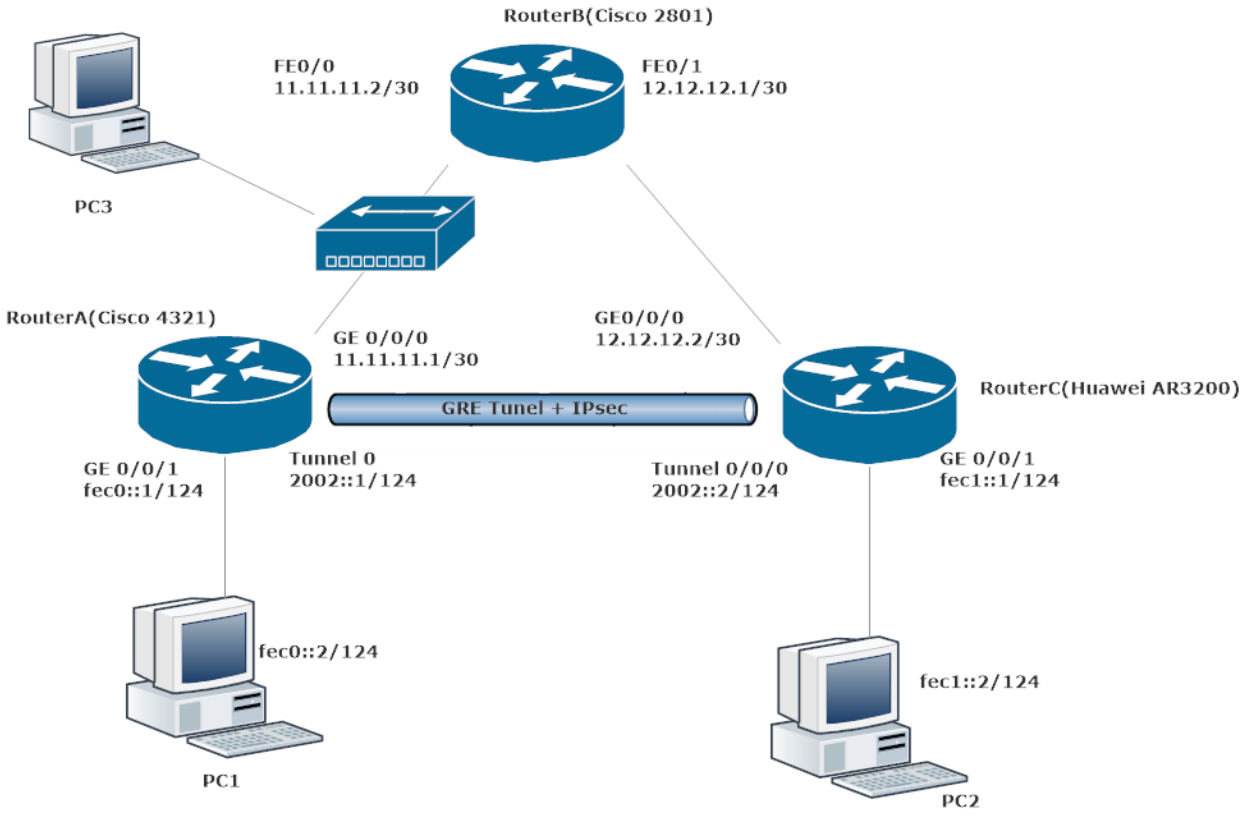
```
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:18:08
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
221 packets input, 20724 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
244 packets output, 27864 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out

<RouterC>display interface tunnel 0/0/0
Tunnel0/0/0 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Tunnel0/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 12.12.12.2 (GigabitEthernet0/0/0), destination 11.11.11.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2007-08-14 00:46:51
Last 300 seconds input rate 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate 10 bytes/sec, 0 packets/sec
Realtime 39 seconds input rate 0 bytes/sec, 0 packets/sec
Realtime 39 seconds output rate 10 bytes/sec, 0 packets/sec
0 packets input, 0 bytes, 0 drops
288 packets output, 30568 bytes, 0 drops
Input bandwidth utilization : --
```

```
Output bandwidth utilization : --
```

Kapitola 5

Konfigurace IPsec VPN

Poněvadž první metoda má značně velkou nevýhodu – nedostatečné zabezpečení přenosu dat, musíme tento problém vyřešit a k tomu můžeme použít bezpečnostní nástroje poskytované IPsec.Pro praktickou realizaci sítě byla použita literatura, kterou lze nalézt na odkazech [10][11]



Obrázek 5.1: Topologie pro IPsec VPN

Vzhledem k tomu, že konfigurace zvažovaná výše se částečně opakuje, budou zohledněny pouze

ty části konfigurace, kde byla použita technologie IPsec.Pro praktickou realizaci sítě byla použita literatura, kterou lze nalézt na odkazu

5.1 Konfigurace směrovače RouterA

Pro instalaci prvního tunelu pro bezpečnostní asociace bylo rozhodnuto použít parametry uvedené níže, protože parametry šifrování nebo hašování použité pro propojení dvou směrovačů od různých výrobců musí být totožné. Dále musíme vytvořit hlavní tunel pro přenos dat. Pro zabezpečení přenosu dat po síti je třeba vytvoření šifrovací mapy. Tato kryptomapa se musí připojit k rozhraním, aby mohla začít fungovat.

```
crypto isakmp policy 10
    encr aes
    authentication pre-share
    group 2
crypto isakmp key 123545 address 12.12.12.2
crypto ipsec transform-set RA - RC esp-aes esp-sha-hmac
    mode tunnel
ip access-list extended RA - RC - GRE
    permit gre host 11.11.11.1 host 12.12.12.2
crypto map RA - RC 10 ipsec-isakmp
    set peer 12.12.12.2
    set transform-set RA - RC
    match address RA - RC - GRE
interface GigabitEthernet0/0/0
    crypto map RA - RC
```

5.2 Konfigurace směrovače RouterC

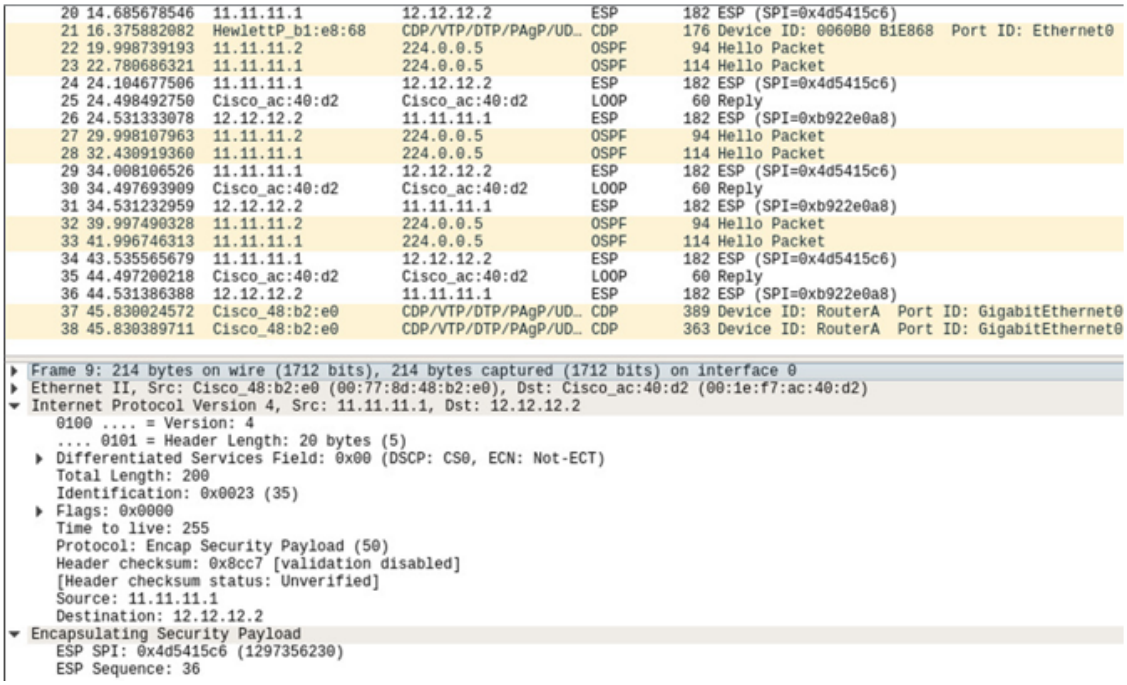
Na tomto směrovači byli provedeny podobná nastavení, jako je na směrovači RouterA:

```
ike proposal 5
    encryption-algorithm aes-cbc-128
    dh group2
ike peer RC-RA v1
    pre-shared-key simple 123545
    ike-proposal 5
    remote-address 11.11.11.1
ipsec proposal RC-RA
```

```
    esp authentication-algorithm sha1
    esp encryption-algorithm aes-128
acl number 3018
    rule 5 permit gre source 12.12.12.2 0 destination 11.11.11.1 0
ipsec policy RC-RA 1 isakmp
    security acl 3018
    ike-peer RC-RA
    proposal RC-RA
interface GigabitEthernet0/0/0
    ipsec policy RC-RA
```

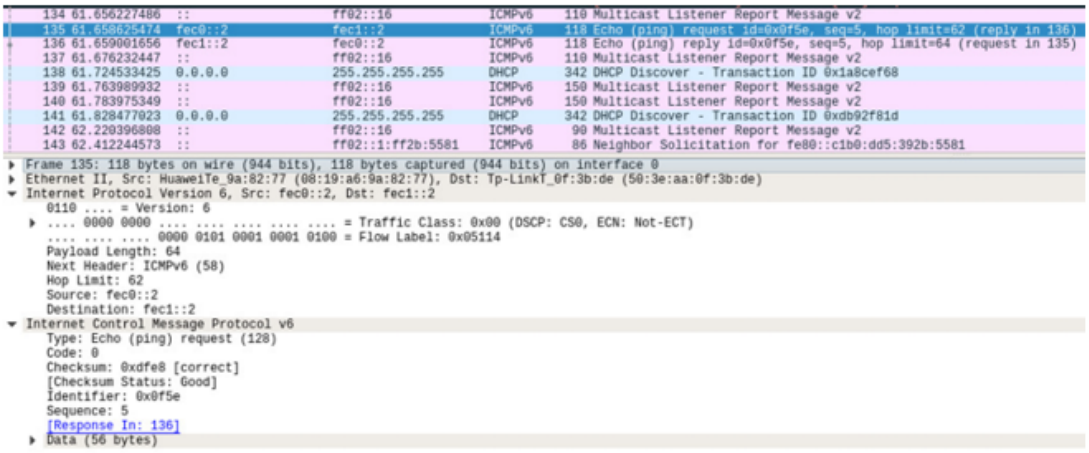
5.3 Ověření funkčnosti

Pro otestování funkčnosti protokolu IPsec je připojen PC3 pomocí rozbočovače uvnitř tunelu, výsledky jsou na obrázku 5.2.



Obrázek 5.2: Ověření funkčnosti protokolu IPsec

Na obrázku 5.2 lze vidět, že data jsou chráněna protokolem ESP, což znamená, že nastavení zabezpečení tunelu bylo provedeno správně. Která data protokol chrání, je vidět na obrázku 5.3. K tomu je na PC1 spuštěn nástroj Wireshark, ukazující data, která jsou odesílána/přijímána zabezpečeným tunelem.



Obrázek 5.3: Data před vstupem do zabezpečeného tunelu

Dále jsou uvedeny informace o fungování protokolu IPsec:

```
RouterA #show crypto ipsec sa

interface: GigabitEthernet0/0/0
Crypto map tag: RA - RC, local addr 11.11.11.1
protected vrf: (none)
local ident (addr/mask/prot/port): (11.11.11.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (12.12.12.2/255.255.255.255/47/0)
current-peer 12.12.12.2 port 500
PERMIT, flags={$origin-is-acl,$}
#pkts encaps: 177, #pkts encrypt: 177, #pkts digest: 177
#pkts decaps: 135, #pkts decrypt: 135,#pkts verify: 135
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 11.11.11.1, remote crypto endpt.: 12.12.12.2
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
current outbound spi: 0x4D5415C6(1297356230)
PFS (Y/N): N, DH group: none
inbound esp sas:
spi: 0xB922E0A8(3106070696)
transform: esp-aes esp-sha-hmac ,
```

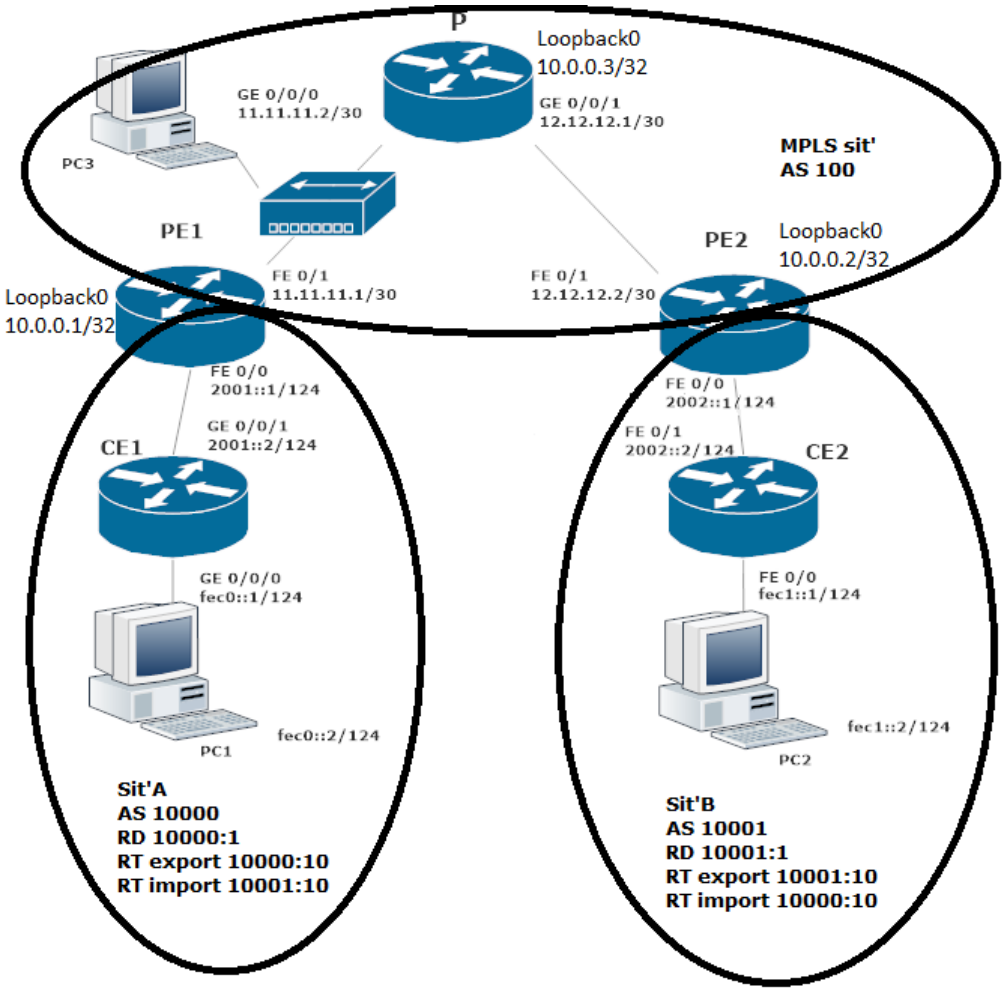
```
in use settings ={Tunnel, }
conn id: 2001, flow-id: ESG:1, sibling-flags FFFFFFFF80000048, crypto map:RA - RC
sa timing: remaining key lifetime (k/sec): (1843178/2791)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x4D5415C6(1297356230)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2002, flow-id: ESG:2, sibling-flags FFFFFFFF80000048, crypto map: RA - RC
sa timing: remaining key lifetime (k/sec): (1843180/2791)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
outbound ah sas:
outbound pcp sas:

<RouterC>display ipsec sa

==============================

Interface: GigabitEthernet0/0/0

Path MTU: 1500

==============================

------------------------------

IPSec policy name: "RC-RA"
Sequence number : 1
Acl Group : 3018
Acl rule : 5
Mode : ISAKMP
```

```
-----------------------------

Connection ID : 12
Encapsulation mode: Tunnel
Tunnel local : 12.12.12.2
Tunnel remote : 11.11.11.1
Flow source : 12.12.12.2/255.255.255.255 47/0
Flow destination : 11.11.11.1/255.255.255.255 47/0
Qos pre-classify : Disable
[Outbound ESP SAs]
SPI: 3106070696 (0xb922e0a8)
Proposal: ESP-ENCRYPT-AES-128 ESP-AUTH-SHA
SA remaining key duration (bytes/sec): 1887418264/2530
Max sent sequence-number: 162
UDP encapsulation used for NAT traversal: N
[Inbound ESP SAs]
SPI: 1297356230 (0x4d5415c6)
Proposal: ESP-ENCRYPT-AES-128 ESP-AUTH-SHA1
SA remaining key duration (bytes/sec): 1887413768/2530
Max received sequence-number: 205
Anti-replay window size: 32
UDP encapsulation used for NAT traversal: N
```

Kapitola 6

Konfigurace MPLS L3 VPN

Pro implementaci řešení MPLS L3 VPN je navržena topologie znázorněná na obrázku 6.1. V této topologii jsou dvě sítě (síť A a síť B). Pro implementaci jsou použity přístroje od Huawei AR1200 (na schématu označené jako CE1) a AR3200 (na schématu označeny jako P). Pro zbytek sítě jsou použity přístroje Cisco řady 2801. V jádru MPLS je připojen rozbočovač, k němuž je připojen počítač PC3, který je použit pro analýzu paketů. Síť na obrázku 6.1 je rozdělena na tři části. Síť v části od PE1 do PE2 je síť poskytovatele, v níž je spuštěn MPLS. V této části je použit OSPF jako směrovací protokol. Mezi hraničními směrovači PE je nakonfigurován protokol iBGP. Celá tato část se nachází v rámci autonomního systému 100. Ostatní části představují samostatné pobočky. Každá síť je připojena jako jeden z autonomních systémů 10000–10001. Pro praktickou realizaci sítě byla použita literatura, kterou lze nalézt na [7][12]



Obrázek 6.1: Topologie sítě MPLS L3 VPN

6.1 Konfigurace směrovačů

Nastavení IPv6 pro připojení jednotlivých klientů do sítě je řešeno jako první. Pokud jde o nastavení jednotlivých CE směrovačů, na všech je konfigurace stejná, liší se jen použití IPv6 adres na jednotlivých rozhraních. Proto je uvedena pouze názorná konfigurace směrovače CE1. Směrovači CE1 je nejprve povoleno používat protokol IPv6 na celém směrovači, poté jsou spuštěna rozhraní s příslušnými adresami a nastaven protokol BGP v autonomním systému 10000, kde je přiřazeno router-id souseda, identifikujícího se jako směrovač PE1, s nímž si vyměňuje směrovací informace.

```
ipv6
interface GigabitEthernet 0/0/0
    description connect-to-PC1
    ipv6 enable
```

```
    ipv6 address FEC0::1/124
interface GigabitEthernet 0/0/1
    description connect-to-PE1
    ipv6 enable
    ipv6 address 2001::2/124
bgp 10000
    router-id 1.1.1.1
    peer 2001::1 as-number 100
    ipv6 family unicast
        network 2001:: 124
        network FEC0:: 124
```

V rámci první fáze nastavení je konfigurace prováděna na hraničním směrovači PE1. Tabulka VRF je nastavena a přidána do rozhraní. Při nastavení VRF je pomocí RT uvedeno, k jakým sítím má přístup. Následně je toto rozhraní spuštěno. V autonomním systému 100 je nastaven externí BGP, kde byl směrovač CE1A označen jako soused VRF, s nímž jsou vyměňovány směrovací informace a distribuovány informace o přímo připojených sítích v VRF.

```
ipv6 unicast routing
vrf definition sit'A
    rd 10000:1
    address-family ipv6
        route-target export 10000:10
        route-target import 10001:10
interface FastEthernet0/0
    vrf forwarding sit'A
    description connect-to-CE1
    ipv6 address 2001::1/124
router bgp 100
    address-family ipv6 vrf sit'A
        neighbor 2001::2 remote-as 10000
        neighbor 2001::2 activate
```

Druhým krokem je nastavení jádra MPLS. Na PE a P směrovačích je spuštěno směrování přes OSPF a spuštěno MPLS. Funkcionalita této části konfigurace je ověřena pingem mezi jednotlivými virtuálními rozhraními a při zachytávání na počítači (připojených přes rozbočovač) je vidět, že probíhající provoz obsahuje záhlaví MPLS. Posledním krokem je nastavení iBGP mezi hraničními směrovači. Zde opět platí, že konfigurace je uvedena pouze pro směrovač PE1. Nejprve je nainstalo-

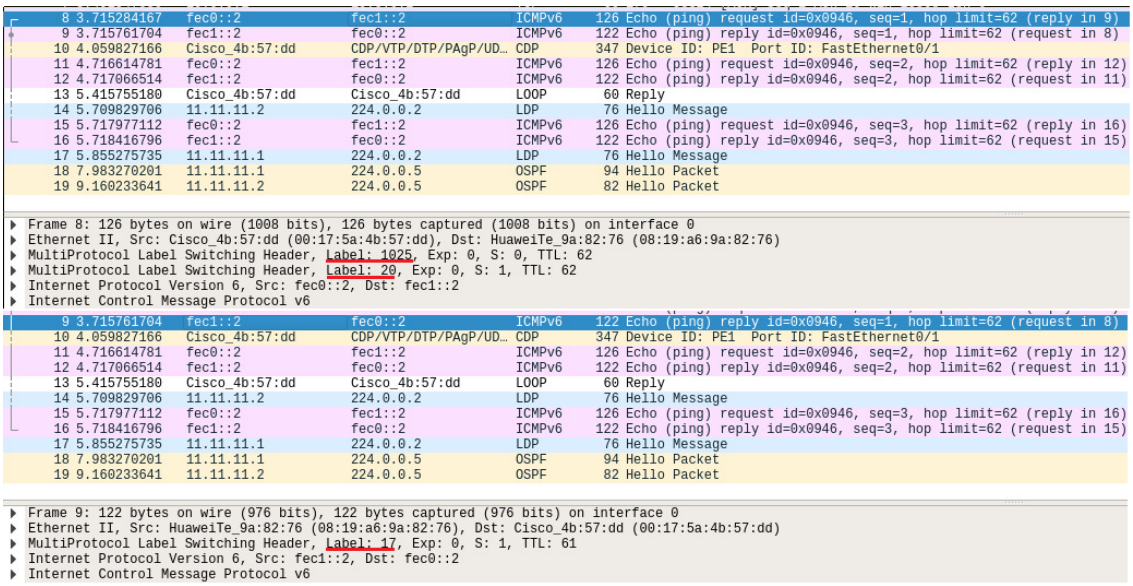
váno iBGP s druhým PE směrovačem a je stanoveno, že zprávy od něj budou přijímány na rozhraní loopback 0. Poté byla zahrnuta výměna VPNv6 prefixu mezi PE směrovači.

```
router bgp 100
    neighbor 10.0.0.2 remote-as 100
    neighbor 10.0.0.2 update-source Loopback 0
    address-family vpnv6
        neighbor 10.0.0.2 active
        neighbor 10.0.0.2 send-comunity extended
```

Tímto způsobem se vytvoří síť z obrázku 6.1, následuje kontrola tohoto řešení.

6.2 Ověření funkčnosti

Funkčnost MPLS L3 VPN se ověří pomocí služby ping. Na obrázku 6.2 jsou znázorněny jednotlivé pakety zachycené aplikací Wireshark.



Obrázek 6.2: Zobrazené informace z programu Wireshark pro ověření funkčnosti implementace technologie MPLS L3 VPN

Horní část obrázku zachycuje ping z PC1 na PC2, tzn. z adresy zdroje fec0::2 na adresu cíle fec1::2. Vidíme, že vnitřní značka je 20 a vnější 1025. To potvrzuje spojení IPv6 mezi sítěmi A a B.

V dolní části obrázku probíhá ping z PC2 na PC1, tzn. z adresy zdroje fec1::2 na adresu cíle fec0::2, dále vidíme pouze jedno záhlaví MPLS. Je to dáno tím, že paket je zachycen za směrovačem P, který je předposledním směrovačem v LSP, a je na něm zapnuta funkce PHP, takže odstraní

vnější značku a pouze vnitřní značka dorazí na hranici směrovače PE1. Takto je ověřena dostupnost mezi sítěmi A a B.

V níže uvedeném záznamu je uvedena směrovací tabulka na směrovači CE2, kde můžeme vidět přímo připojené sítě a sítě, které jsou získané z BGP, tzn. síť A.

```
CE2#show ipv6 route
IPv6 Routing Table - Default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
{B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
EX - EIGRP external
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B 2001::/124 [20/0]
via FE80::217:5AFF:FE4B:52F2, FastEthernet0/1
C 2002::/124 [0/0]
via FastEthernet0/1, directly connected
L 2002::2/128 [0/0]
via FastEthernet0/1, receive
B FEC0::/124 [20/0]
via FE80::217:5AFF:FE4B:52F2, FastEthernet0/1
C FEC1::/124 [0/0]
via FastEthernet0/0, directly connected
L FEC1::1/128 [0/0]
via FastEthernet0/0, receive
L FF00::/8 [0/0]
via Null0, receive
```

V prvním z následujících dvou výpisů lze vidět, že globální tabulka směrování IPv6 na směrovači PE1 je prázdná, a ve druhém výpisu je vidět směrovací tabulku pro VRF síť A, kde jsou správné záznamy.

```
PE1#show ipv6 route
IPv6 Routing Table - Default - 1 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
    B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
    I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
    EX - EIGRP external
    O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
    ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

```
L FF00::/8 [0/0]
via Null0, receive

PE1#show ipv6 route vrf sit'A
IPv6 Routing Table - sit'A - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

    B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
    I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
    EX - EIGRP external
    O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
    ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

C 2001::/124 [0/0]
via FastEthernet0/0, directly connected
L 2001::1/128 [0/0]
via FastEthernet0/0, receive}
B 2002::/124 [200/0]
via 10.0.0.2 Default-IP-Routing-Table, indirectly connected
B FEC0::/124 [20/0]
via 2001::2
B FEC1::/124 [200/0]
via 10.0.0.2 Default-IP-Routing-Table, indirectly connected
L FF00::/8 [0/0]
via Null0, receive
```

Můžeme také vidět interní značky jednotlivých prefixů na směrovači PE1, kde se paket dostane do sítě FEC1::/124 přes next-hop ::FFFF: 10.0.0.2 a odesílá provoz do této sítě s interní značkou 20. To odpovídá zachycenému pingu z PC1 na PC2.

```
PE1#show bgp vpnv6 unicast vrf sit'A labels
    Network Next Hop In label/Out label
Route Distinguisher: 10000:1 (sit'A)
    2001::/124 2001::2 16/nolabel
    2002::/124 ::FFFF:10.0.0.2 nolabel/19
    FEC0::/124 2001::2 17/nolabel
    FEC1::/124 ::FFFF:10.0.0.2 nolabel/20
```

Kapitola 7

Ověření kompatibility směrovačů Cisco a Huawei

Lze říci, že zařízení Cisco a Huawei jsou kompatibilní, protože výše uvedená tři řešení VPN byla implementována úspěšně. Stojí však za to zmínit některé překážky, které byly třeba při implementaci překonat.

Při implementaci metody GRE VPN i IPsec VPN bylo zjištěno, že pokud není předem nakonfigurován parametr MTU obou okrajových směrovačů, nebude protokol OSPFv3 fungovat, a oba směrovače si tak nebudou vzájemně vyměňovat informace o svých IPv6 sítích. Problém může být vyřešen následujícími způsoby. Buď je pro oba směrovače nastaven stejný parametr MTU, nebo musí být parametr MTU na obou rozhraních směrovačů tunelu ignorován. Toho lze dosáhnout na rozhraní tunelu směrovače Cisco pomocí příkazu:

```
ipv6 ospf mtu-ignore
```

Ve směrovači Huawei na rozhraní tunelu je třeba použít příkaz:

```
ospfv3 mtu-ignore
```

Pokud jde o rozdíly v nastavení řešení VPN, pokud by došlo k rozhodnutí implementovat technologii DSVPN, pak by nastaly potíže, protože ve směrovačích Huawei musí být před prací s touto technologií povolena licence. K tomu je třeba na směrovači použít následující příkazy:

```
license active accept agreement
license function dsvpn
```

Dále lze zdůraznit, že v směrovačích Cisco a Huawei jsou všechna rozhraní zpočátku vypnuta, ale rozdíl je v tom, že pokud v směrovačích Huawei přejdete do nastavení rozhraní a napíšete tam ip adresu, automaticky se zapne, což se o zařízeních Cisco říci nedá. Z tohoto důvodu je na zařízeních Cisco nutné spustit každé rozhraní, které chceme používat, příkazem:

```
no shutdown
```

Kapitola 8

Srovnání jednotlivých řešení se sítěmi VPN v prostředí protokolu IPv4

Při konfiguraci na směrovačích Cisco 2811 a Huawei řady AR bylo zjištěno, že při implementaci technologie GRE VPN tunelu nelze využít nakonfigurovaných IPv6 adres na začátku a konci tunelu, ale pokud bude tato technologie implementována pouze pomocí IPv4, pak to není problém. Ve stejném smyslu můžeme totéž říci o technologii, která se v zařízeních Cisco nazývá DMVPN a v zařízeních Huawei DSVPN. V zařízeních řady Huawei AR nelze technologii DSVPN používat v IPv6. Technologie VPN mohou pracovat ve dvou verzích protokolů, a to jak IPv4, tak IPv6, vše ale závisí na tom, jaké konkrétní zařízení je využíváno a jakou verzi operačního systému toto zařízení má.

Při pohledu na tři řešení VPN lze uvidět, že pokud je používán protokol IPv4, je nutné směrovací protokol OSPF nakonfigurovat jinak. Pro IPv4 je potřeba pouze zadat všechny sítě, ke kterým je směrovač připojen. Pokud je používán protokol IPv6, je nutné povolit protokol OSPF, zadat jeho ID a poté jej povolit na každém rozhraní.

V případě implementace dvou technologií VPN, tedy GRE VPN a IPsec VPN, zůstává konfigurace zařízení stejná, pouze se změní IP adresa na verzi 4. V případě implementace technologie MPLS L3 VPN se však nemění pouze IP adresy, ale používá se i jiný prefix. Při konfiguraci směrovačů PE je nutné používat prefix VPNv4 místo prefixu VPNv6.

Kapitola 9

Závěr

Cílem této práce bylo ukázat implementaci tří technologií VPN v prostředí IPv6 a otestovat kompatibilitu zařízení od různých firem a zjistit rozdíly, pokud by implementovaná VPN používala pouze IPv4. V teoretické části jsem popsal IPv6, konkrétně typy adres, formát paketů a další hlavičky paketů. Dále jsem popsal způsoby koexistence IPv4 a IPv6, protože v dnešní době se využívají oba protokoly současně. Následně jsem popsal technologii VPN, jaké jsou výhody použití této technologie a také jsem ukázal a popsal různé typy VPN, které jsem používal pro praktickou implementaci v laboratorním prostředí, konkrétně: GRE VPN, IPsec VPN, MPLS L3 VPN.

Pro technologie popsané v teoretické části, byly v praktické části navrženy a konfigurovány sítě, které jsem implementoval v laboratorním prostředí. V těchto sítích jsem využil směrovače od výrobců Cisco a Huawei. Následně jsem ověřil kompabilitu těchto zařízení. Poslední části, kterou jsem se zabýval, bylo srovnání jednotlivých řešení sítí VPN v prostředí IPv6 s IPv4.

Dalším rozvojem této práce by mohlo být porovnání kompatibility pro další výrobce, např. TP-Link, Mikrotik, D-Link atd. To by však vyžadovalo nákup těchto zařízení. Je také možné změnit tuto konfiguraci tak, aby vůbec nepoužívala protokol IPv4 v žádné podobě. Lze taky nakonfigurovat další řešení VPN, jako např: DMVPN, L2TPv3, PPTP.

Z mého pohledu je největším přínosem mé práce podrobný návod na konfiguraci tří různých řešení VPN a popis možných problémů, které se mohou vyskytnout při implementaci na zařízeních v různých verzích IP a od různých výrobců. Tato tři řešení obsahují konfiguraci pro vybrané směrovače Cisco i směrovače Huawei. Výhodou je, že tyto konfigurace mohou firmy využít k implementaci sítě VPN se zařízeními pouze od jedné společnosti, nebo od obou společností zároveň. Tato konfigurace je užitečná zejména pro ty firmy, jejichž sítě jsou postaveny na protokolu IPv6, ale jejichž poskytovatel internetového připojení podporuje pouze protokol IPv4. Vzhledem k tomu, že mnoho materiálů k tomuto tématu je k dispozici pouze v angličtině, může být tento materiál užitečný pro osoby, které neovládají dobře angličtinu.

Literatura

1. IETF. *RFC 4291* [online] [cit. 2022-02-06]. Dostupné z: https://datatracker.ietf.org/doc/html/rfc%204291.
2. IETF. *RFC 7217* [online] [cit. 2022-02-06]. Dostupné z: https://www.ietf.org/rfc/rfc7217.txt.
3. PAVEL, Satrapa. *IPv6: Internetový protokol verze 6*. CZ.NIC, z.s.p.o, 2019. Czech. ISBN 978-80-88168-46-1.
4. *Wikipedie: Otevřená encyklopedie: IPv6* [online] [cit. 2022-02-06]. Dostupné z: https://cs.wikipedia.org/wiki/IPv6.
5. HUSTON, Geoff. *IPv4 Address Report* [online] [cit. 2022-02-06]. Dostupné z: https://ipv4.potaroo.net/.
6. PUŽMANOVÁ, Rita. *TCP/IP v kostce. 2., upr. a rozš. vyd. České Budějovice*. Kopp, 2009. Czech. ISBN 978-80-7232-388-3.
7. CO., Huawei Technologies. *AR120, AR150, AR160, AR200, AR1200, AR2200, AR3200, and AR3600 V200R007 CLI-based Configuration Guide - VPN* [online] [cit. 2022-02-06]. Dostupné z: https://support.huawei.com/enterprise/en/doc/EDOC1000097190.
8. CISCO SYSTEMS, Inc. *IPv6 over IPv4 GRE Tunnels* [online] [cit. 2022-02-06]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-ip4-gre-tunls-xe.pdf.
9. CO., Huawei Technologies. *IPv6 over IPv4 GRE Tunnels* [online] [cit. 2022-02-06]. Dostupné z: https://support.huawei.com/enterprise/br/doc/EDOC0100585934/3b340c91/example-for-configuring-an-ipv6-over-ipv4-gre-tunnel.
10. CARMOUCHE, James Henry. *IPsec Virtual Private Network Fundamentals*. Indianapolis: Cisco Press, 2006. ISBN 1-58705-207-5.
11. CO., Huawei Technologies. *Special Topic - IPsec* [online] [cit. 2022-02-06]. Dostupné z: https://support.huawei.com/view/contentview/getFileStream?mid=SUPE_DOC&viewNid=EDOC1000122881&nid=EDOC1000122881&partNo=j004&type=htm#EN-US_TASK_0264628116.

12. CISCO SYSTEMS, Inc. *Multiprotocol BGP MPLS VPN* [online] [cit. 2022-02-06]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-s/mp-l3-vpns-15-s-book/mp-bgp-mpls-vpn.pdf.

Seznam příloh

Příloha A

Výpis kompletní konfigurace GRE VPN

```
RouterA

Building configuration...
Current configuration : 2355 bytes
!
!
Last configuration change at 17:16:42 UTC Mon Mar 28 2022
!
version 16.6
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
!
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
```

```
 exit-address-family
!
!
no aaa new-model
!
!
subscriber templating
!
!
!
!
!
ipv6 unicast-routing
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
license udi pid ISR4321/K9 sn FDO2304115D
license accept end user agreement
license boot level appxk9
diagnostic bootup level minimal
spanning-tree extend system-id
!
!
!
!
redundancy
 mode none
!
!
!
!
```

```
!
!
!
!
!
!
!
!
!
interface Tunnel0
 no ip address
ipv6 address 2002::1/124
ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf mtu-ignore
 tunnel source 11.11.11.1
 tunnel destination 12.12.12.2
!
interface GigabitEthernet0/0/0
 ip address 11.11.11.1 255.255.255.252
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 ipv6 address FEC0::1/124
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Serial0/1/0
 no ip address
 shutdown
!
interface Serial0/1/1
 no ip address
 shutdown
!
```

```
interface Serial0/2/0
 no ip address
 shutdown
!
interface Serial0/2/1
 no ip address
 shutdown
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
router ospf 1
 network 11.11.11.0 0.0.0.3 area 0
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
!
!
!
ipv6 router ospf 1
 router-id 1.1.1.1
!
!
!
!
!
control-plane
!
!
line con 0
 transport input none
 stopbits 1
```

```
line aux
 stopbits 1
line vty 0 4
 login
!
wsma agent exec
!
wsma agent config
!
wsma agent filesys
!
wsma agent notify
!
!
end
```

RouterB:

```
Building configuration...
Current configuration : 1014 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
```

```
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
!
!
!
!
interface FastEthernet0/0
 ip address 11.11.11.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 12.12.12.1 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 125000
!
router ospf 1
 log-adjacency-changes
 network 11.11.11.0 0.0.0.3 area 0
```

```
 network 12.12.12.0 0.0.0.3 area 0
!
ip classless
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

RouterC:

```
[V200R003C00SPC200]
#
 sysname RouterC
#
 snmp-agent local-engineid 800007DB030819A69A8275

 snmp-agent
```

```
#
cwmp
 cwmp cpe connect retry 0
#
 http timeout 3
#
 drop illegal-mac alarm
#
ipv6
#
dhcp enable
#
undo dhcp server bootp
#
#
#
#
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default-admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
ospfv3 1
 router-id 2.2.2.2
#
firewall zone Local
 priority 128
#
interface GigabitEthernet0/0/0
 ip address 12.12.12.2 255.255.255.252
#
interface GigabitEthernet0/0/1
```

```
 ipv6 enable
 ipv6 address FEC1::1/124
 ospfv3 1 area 0.0.0.0
 ospfv3 mtu-ignore
 ip address dhcp-alloc

#
interface GigabitEthernet0/0/2
#
interface Cellular0/0/0
 link-protocol ppp

#
interface Cellular0/0/1
 link-protocol ppp
#
interface NULL0
#
interface Tunnel0/0/0
 ipv6 enable
 ipv6 address 2002::2/124
 ospfv3 1 area 0.0.0.0
 ospfv3 mtu-ignore
 tunnel-protocol gre
 source 12.12.12.2
 destination 11.11.11.1

#
ospf 1
area 0.0.0.0
network 12.12.12.0 0.0.0.3
#

user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$7K}3%:ex,K6ZJ|H(PY&&,'CZr|jz2=~;+T1x]{Rd"#19'C],%$%$
user-interface vty 0 4
```

```
#
wlan ac
#
voice
#
 diagnose
#
return
```

Příloha B

Výpis kompletní konfigurace IPsec VPN

```
RouterA:
Building configuration...
Current configuration : 2355 bytes
!
! Last configuration change at 17:16:42 UTC Mon Mar 28 2022
!
version 16.6
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
```

```
!
no aaa new-model
!
!
subscriber templating
!
!
!
!
!
ipv6 unicast-routing
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
license udi pid ISR4321/K9 sn FDO2304115D
license accept end user agreement
license boot level appxk9
diagnostic bootup level minimal
spanning-tree extend system-id
!
!
!
!
redundancy
 mode none
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
```

```
crypto isakmp key 123545 address 12.12.12.2
!
!
crypto ipsec transform-set RA - RC esp-aes esp-sha-hmac
 mode tunnel
!
!
!
crypto map RA - RC 10 ipsec-isakmp
 set peer 12.12.12.2
 set transform-set RA - RC
 match address RA - RC - GRE
!
!
!
!
!
!
!
!
interface Tunnel0
 no ip address
 ipv6 address 2002::1/124
 ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf mtu-ignore
 tunnel source 11.11.11.1
 tunnel destination 12.12.12.2
!
interface GigabitEthernet0/0/0
 ip address 11.11.11.1 255.255.255.252
 negotiation auto
 crypto map RA - RC
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 ipv6 address FEC0::1/124
```

```
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface Serial0/1/0
 no ip address
 shutdown
!
interface Serial0/1/1
 no ip address
 shutdown
!
interface Serial0/2/0
 no ip address
 shutdown
!
interface Serial0/2/1
 no ip address
 shutdown
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
router ospf 1
 network 11.11.11.0 0.0.0.3 area 0
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
!
!
!
ip access-list extended RA - RC - GRE
 permit gre host 11.11.11.1 host 12.12.12.2
```

```
ipv6 router ospf 1
 router-id 1.1.1.1
!
!
!
!
!
control-plane
!
!
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line con 1
 login
!
wsma agent exec
!
wsma agent config
!
wsma agent filesys
!
wsma agent notify
!
!
end
```

```
RouterB:
Building configuration...
Current configuration : 1014 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

```
hostname RouterB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
!
!
!
!
interface FastEthernet0/0
 ip address 11.11.11.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 12.12.12.1 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/1/0
```

```
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 125000
!
router ospf 1
 log-adjacency-changes
 network 11.11.11.0 0.0.0.3 area 0
 network 12.12.12.0 0.0.0.3 area 0
!
ip classless
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
 login
```

```
!
end
```

```
RouterC:
[V200R003C00SPC200]
#
 sysname RouterC
#
 snmp-agent local-engineid 800007DB030819A69A8275
 snmp-agent
#
cwmp
 cwmp cpe connect retry 0
#
 http timeout 3
#
 drop illegal-mac alarm
#
ipv6
#
dhcp enable
#
undo dhcp server bootp
#
acl number 3018
 rule 5 permit gre source 12.12.12.2 0 destination 11.11.11.1 0
#
ipsec proposal RC-RA
 esp authentication-algorithm sha1
 esp encryption-algorithm aes-128
#
ike proposal 5
 encryption-algorithm aes-cbc-128
 dh group2w
#
ike peer RC-RA v1
 pre-shared-key simple 123545
 ike-proposal 5
```

```
 remote-address 11.11.11.1w
#
ipsec policy RC-RA 1 isakmp
 security acl 3018
 ike-peer RC-RA
 proposal RC-RA
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default-admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
ospfv3 1
 router-id 2.2.2.2
#
firewall zone Local
 priority 128
#
interface GigabitEthernet0/0/0
 ip address 12.12.12.2 255.255.255.252
 ipsec policy RC-RA
#
interface GigabitEthernet0/0/1
 ipv6 enable
 ipv6 address FEC1::1/124
 ospfv3 1 area 0.0.0.0
 ospfv3 mtu-ignore
 ip address dhcp-alloc
#
interface GigabitEthernet0/0/2
#
interface Cellular0/0/0
 link-protocol ppp
#
```

```
interface Cellular0/0/1
 link-protocol ppp
#
interface NULL0
#
interface Tunnel0/0/0
 ipv6 enable
 ipv6 address 2002::2/124
 ospfv3 1 area 0.0.0.0
 ospfv3 mtu-ignore
 tunnel-protocol gre
 source 12.12.12.2
 destination 11.11.11.1
#
ospf 1
 area 0.0.0.0
  network 12.12.12.0 0.0.0.3
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$7K}3%:ex,K6ZJ|H(PY&&,'CZr|jz2=~;+T1x]{Rd"#l9'C],%$%$
user-interface vty 0 4
#
wlan ac
#
voice
 #
 diagnose
#
return
```

Příloha C

Výpis kompletní konfigurace MPLS L3 VPN

```
CE1:
[V200R005C20SPC200]
#
 sysname CE1
#
 drop illegal-mac alarm
#
ipv6
#
dhcp enable
#
pki realm default
 enrollment self-signed
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default-admin
 local-user admin password irreversible-cipher
%@%@Z*Dz#r*\=ZDphc>OF2hXZ%>a%@-..<)^aTQ#!ULPtzy@%>dZ%@%@
 local-user admin service-type http
#
firewall zone Local
 priority 64
```

```
#
interface GigabitEthernet0/0/0
 description connect-to-PC1
 ipv6 enable
 ipv6 address FEC0::1/124
 ip address dhcp-alloc
#
interface GigabitEthernet0/0/1
 description connect-to-PE1
 ipv6 enable
 ipv6 address 2001::2/124
 ip address dhcp-alloc
#
interface GigabitEthernet0/0/2
#
interface Cellular0/0/0
#
interface Cellular0/0/1
#
interface NULL0
#
bgp 10000
 router-id 1.1.1.1
 peer 2001::1 as-number 100
 #
 ipv4-family unicast
  undo synchronization
 #
 ipv6-family unicast
  undo synchronization
  network 2001:: 124
  network FEC0:: 124
  peer 2001::1 enable
#
 snmp-agent local-engineid 800007DB030819A69B6D4D
#
user-interface con 0
 authentication-mode password
```

```
 set authentication password cipher
%@%@5<S|0,sF3)xPuoS*p|4~,"Q~/{,Y6y%-r,U;/1B|x:>7"QB,%@%@
user-interface vty 0 4
#
wlan ac
#
voice
 #
 diagnose
#
return
```

```
PE1:
Building configuration...
Current configuration : 1848 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE1
!
boot-start-marker
boot-end-marker
!
vrf definition sit'A
 rd 10000:1
 !
 address-family ipv6
 route-target export 10000:10
 route-target import 10001:10
 exit-address-family
!
logging message-counter syslog
!
no aaa new-model
dot11 syslog
```

```
ip source-route
!
!
!
!
ip cef
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
interface Loopback0
 ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet0/0
 description connect-to-CE1
 vrf forwarding sit'A
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001::1/124
 ipv6 enable
!
interface FastEthernet0/1
 description connect-to-P1
 ip address 11.11.11.1 255.255.255.252
 duplex auto
 speed auto
 mpls ip

!
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 125000
!
```

```
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 125000
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.1 0.0.0.0 area 0
 network 11.11.11.0 0.0.0.3 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.2 remote-as 100
 neighbor 10.0.0.2 update-source Loopback0
 no auto-summary
 !
 address-family vpnv6
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.2 send-community extended
 exit-address-family
 !
 address-family ipv6 vrf sit'A
  neighbor 2001::2 remote-as 10000
  neighbor 2001::2 activate
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
mpls ldp router-id Loopback0
!
control-plane
!
!
```

```
!
ccm-manager fax protocol cisco
!
mgcp fax t38 ecm
!
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```

```
P:
[V200R003C00SPC200]
#
 sysname P
#
 snmp-agent local-engineid 800007DB030819A69A8275
 snmp-agent
#
cwmp
 cwmp cpe connect retry 0
#
 http timeout 3
#
 drop illegal-mac alarm
#
mpls lsr-id 10.0.0.3
mpls
#
mpls ldp
#
#
aaa
 authentication-scheme default
 authorization-scheme default
```

```
 accounting-scheme default
 domain default
 domain default-admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
firewall zone Local
 priority 128
#
interface GigabitEthernet0/0/0
 description connect-to-PE1
 ip address 11.11.11.2 255.255.255.252
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/1
 description connect-to-PE2
 ip address 12.12.12.1 255.255.255.252
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/2
#
interface Cellular0/0/0
 link-protocol ppp
#
interface Cellular0/0/1
 link-protocol ppp
#
interface NULL0
#
interface LoopBack0
 ip address 10.0.0.3 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.0.0.3 0.0.0.0
  network 11.11.11.0 0.0.0.3
```

```
  network 12.12.12.0 0.0.0.3
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
%$%$fD+>U(‘K*@u3B80OX7’5,)Vw:MRQBQ8l#--w%mAPt4iF)Vz,%$%$
user-interface vty 0 4
#
wlan ac
#
voice
 #
 diagnose
#
return
```

```
PE2:
Building configuration...
Current configuration : 1894 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE2
!
boot-start-marker
boot-end-marker
!
vrf definition sit’B
 rd 10001:1
 !
 address-family ipv6
 route-target export 10001:10
 route-target import 10000:10
 exit-address-family
!
```

```
logging message-counter syslog
!
no aaa new-model
dot11 syslog
ip source-route
!
!
!
!
ip cef
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
voice-card 0
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.0.0.2 255.255.255.255
```

```
!
interface FastEthernet0/0
 description connect-to-CE2
 vrf forwarding sit'B
 no ip address
 duplex auto
 speed auto
 ipv6 address 2002::1/124
 ipv6 enable
!
interface FastEthernet0/1
 description connect-to-P1
 ip address 12.12.12.2 255.255.255.252
 duplex auto
 speed auto
 mpls ip
!
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 125000
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.2 0.0.0.0 area 0
 network 12.12.12.0 0.0.0.3 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.1 remote-as 100
 neighbor 10.0.0.1 update-source Loopback0
 no auto-summary
```

```
 !
 address-family vpnv6
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 send-community extended
 exit-address-family
 !
 address-family ipv6 vrf sit'B
  neighbor 2002::2 remote-as 10001
  neighbor 2002::2 activate
  redistribute connected
  no synchronization
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
mpls ldp router-id Loopback0
!
control-plane
!
!
!
ccm-manager fax protocol cisco
!
mgcp fax t38 ecm
!
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
```

```
 login
!
scheduler allocate 20000 1000
end
```

```
CE2
Building configuration...
Current configuration : 1548 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE2
!
boot-start-marker
boot system flash:c2801-advipservicesk9-mz.124-22.T.bin
boot-end-marker
!
logging message-counter syslog
!
ip source-route
!
!
!
!
ip cef
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
voice-card 0
!
```

```
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 description connect-to-PC2
 no ip address
 duplex auto
 speed auto
 ipv6 address FEC1::1/124
 ipv6 enable
!
interface FastEthernet0/1
 description connect-to-PE2
 no ip address
 duplex auto
 speed auto
 ipv6 address 2002::2/124
 ipv6 enable
!
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/1/1
```

```
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2/0
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 125000
!
router bgp 10001
 no synchronization
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 neighbor 2002::1 remote-as 100
 no auto-summary
 !
 address-family ipv6
neighbor 2002::1 activate
  network 2002::/124
  network FEC1::/124
 exit-address-family
!
ip forward-protocol nd
ip http server
no ip http secure-server
!
!
!
!
!
!
!
!
```

```
!
!
control-plane
!
!
!
ccm-manager fax protocol cisco
!
mgcp fax t38 ecm
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```