Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Diplomová práce

Návrh datové sítě se zaměřením na přenosy L2 a L3 provozů (Ethernet) mezi vzdálenými lokalitami

Bc. Jakub Vrzák

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Jakub Vrzák

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Návrh datové sítě se zaměřením na přenosy L2 a L3 provozů (Ethernet) mezi vzdálenými lokalitami

Název anglicky

The data network design with a focus on L2 and L3 traffic (Ethernet) transmissions between remote sites

---

Cíle práce

Cílem diplomové práce je provést návrh a posouzení datové sítě mezi více provozovnami (lokalitami), které jsou schopné komunikovat na druhé vrstvě v rámci modelu OSI.
Seznámit se s problematikou struktury a tvorby datových sítí a na základě rozboru současného stavu ve vybrané firmě, resp. vybrané datové sítě, navrhnout datovou síť se zaměřením na posouzení ztrátovosti komunikace, dodržení ostatních potřebných provozních parametrů a nákladů na investici. Na základě poznatků z literatury, vlastní analýzy a měření, provést rozbor jednotlivých možností a navrhnout a doporučit vhodná opatření a řešení pro praktickou aplikaci, která budou posouzena z hlediska technického a ekonomického.

Metodika

1. Úvod
2. Cíl práce
3. Metodika práce
4. Současný stav sledované problematiky
5. Vlastní řešení
6. Výsledky a diskuse
7. Závěr a doporučení
8. Seznam použitých zdrojů
9. Přílohy

Doporučený rozsah práce

45 až 55 stran

Klíčová slova

Datová síť, počítačová síť, datová komunikace, Ethernet, Referenční model ISO/OSI

Doporučené zdroje informací

BOHÁČ, L. a BEZPALEC, P.: Datové sítě – přednášky. 1. vydání. České vysoké učení technické, Praha 2011, 204 s., ISBN 978-80-01-04694-4

Příslušné zákony, nařízení vlády, vyhlášky, ČSN, oborové předpisy a odborné časopisy

SPURNÁ, I.: Počítačové sítě – praktická příručka správce sítě. 1. vydání. Computer Media, Kralice na Hané 2010, 180 s. ISBN 978-80-7402-036-0

STALLINGS, W.: Data and Computer Communications. 10. vydání. Pearson: 2013, 912 s. ISBN-13: 978-0133506488

TRULOVE, J.: Sítě LAN – hardware, instalace a zapojení. 1. vydání. Grada, Praha: 2009, 384 s. ISBN 978-80-247-2098-2

Předběžný termín obhajoby

2022/2023 LS – TF

Vedoucí práce

doc. Ing. Petr Vaculík, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 29. 6. 2022

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 8. 2. 2023

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 01. 04. 2023

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Návrh datové sítě se zaměřením na přenosy L2 a L3 provozů (Ethernet) mezi vzdálenými lokalitami" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30. 3. 2023 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu diplomové práce, kterým byl doc. Ing. Petr Vaculík, Ph.D.

Návrh datové sítě se zaměřením na přenosy L2 a L3 provozů (Ethernet) mezi vzdálenými lokalitami

Abstrakt

Tato práce se věnuje návrhu datové sítě se zaměřením na přenos dat typu L2 a L3 pomocí ethernetu mezi vzdálenými lokalitami. Je zaměřena na uživatele, který chce bezpečně a spolehlivě přenášet svá data. Pro přenos dat byly využity směrovače od výrobce Nokia, které nejsou tak známé jako například směrovače od společnosti Cisco. Firma Nokia je zaměřena na profesionální řešení datových sítí. V rámci návrhu byly určeny dvě modelové řady směrovačů pro provoz datové sítě. Návrh datové sítě je koncipován pro rozlehlou datovou síť, která může být rozmístěna kdekoliv, kde je možné vytvářet přímá spojení mezi směrovači.

Pro vlastní komunikaci směrovačů byl zvolen směrovací protokol IS-IS. Nad tímto protokolem byla nakonfigurována přenosová vrstva pro směrovací protokol MPLS. Přenos uživatelských dat je realizován pomocí iBGP, který dokáže přenášet služby typu L3. Přenos služeb L2 je realizován pomocí několika transportních tunelů pro MPLS a Segment Routing. Pro přenos L3 provozů byla zvolena služba směrovače VPRN a pro přenos L2 provozů pak služba EPIPE.

Na konci práce bylo znázorněno chování transportních tunelů pro MPLS. Byly odzkoušeny tunely bez alternativního spojení a tunely s možností alternativního spojení pomocí směrovací tabulky.

Klíčová slova: Ethernet, přenos dat, směrovač, směrovací protokoly, transportní tunely, služby, vrstva L2 a vrstva L3

The data network design with focus on L2 and L3 traffic (Ethernet) transmissions between remote sites

Abstract

This thesis deals with the design of a data network focusing on the transmission of L2 and L3 data using Ethernet between remote sites. It is aimed at the user who wants to transfer his data securely and reliably. For data transmission, routers from Nokia, which are not as well known as, for example, Cisco routers, were used. Nokia is focused on professional data networking solutions. Two model series of routers were identified for data network operation in this design. The data network design is conceived for a large data network that can be deployed anywhere where direct connections between routers can be established.

The IS-IS routing protocol has been chosen for the actual router communication. Above this protocol, a transport layer was configured for the MPLS routing protocol. The transmission of user data is implemented using iBGP, which can transmit L3 services. The transmission of L2 services is implemented using several transport tunnels for MPLS and Segment Routing. The VPRN router service was chosen for the transmission of L3 traffic and the EPIPE service was chosen for the transmission of L2 traffic.

At the end of the paper, the behavior of the transport tunnels for MPLS was illustrated. Tunnels without alternative connection and tunnels with alternative connection using routing table were tested.

Keywords: Ethernet, data transmission, router, routing protocols, transport tunnels, services, L2 layer and L3 layer

Obsah

1 Úvod

Jako oblast zájmu diplomové práce jsem zvolil téma, které je blízké mé práci a zkušenostem z posledních let. Jako zaměstnanec statní organizace jsem součástí struktury zodpovědné za přenos uživatelských (zákaznických) dat.

Organizace zabezpečuje jak přenosové systémy, tak datové sítě. Jedná se zejména o vlastní přenosové prostředí s vlastní datovou sítí, které není závislá na přenosovém prostředí typu internet. Naše interní datová síť vzniká již od prvních náznaků datových sítí. Její počátky jsou datovány k 90. létům minulého století. Od této doby se samozřejmě požadavky na onu datovou síť diametrálně proměnily. V dnešní době již bez datové sítě jednoduše není možné fungovat. V průběhu let jsme se proto jako organizace snažili parametry datové sítě neustále zlepšovat. S rostoucím počtem uživatelů a požadavků docházelo k jejímu zvětšování, ale také k nutnosti řešit i vlastní zabezpečení přenášených dat. Od roku 2000 byla naše datová síť převáděna do dynamického směrovacího protokolu OSPF, který byl součástí až do posledních dní této sítě. V rámci rozvoje veřejného internetu muselo dojít i k implementaci služby „přístup k veřejnému internetu“ do naší datové sítě, která je od internetu oddělena. Implementace služby byla vyřešena zavedením prostředí MPLS a BGP, které dovolilo využívat více virtuálních směrovačů na jednom fyzickém směrovači.

Datová síť, kterou spravuji, prošla posledním zásadním vylepšením v roce 2017, kdy došlo k zásadní změně vendorového prostředí a k nutnosti realizace a implementace nových funkcionalit. V rámci této změny došlo k přechodu na technologii od firmy Alcatel-Lucent (Nokia). Nově vybudovaná datová síť začala řešit přenosy dat jiným, a troufnu si říci moderním, přístupem. Došlo totiž k přechodu do prostředí založeného pouze na technologii VRF, a veškeré provozy jsou již rozděleny do samostatných VRF. Pro provoz technologie VRF bylo nutné konfigurovat protokol BGP, který zabezpečuje přenos VRF pomocí tunelů. V rámci tohoto prostředí byl do podvozku datové sítě nasazen jiný směrovacího protokol IGP a MPLS. Protože jsou kladeny vysoké nároky na zálohování datové sítě, bylo potřeba začít využívat dynamické zálohování přenosových cest. Pro toto řešení bylo z počátku využito MPLS LDP, které mělo svá omezení. V rámci zlepšení zálohování datových tras mezi směrovači jsme nasadili MPLS RSVP-TE, které nám situaci podstatně vylepšilo. V rámci nejmodernějších trendů a zabezpečení redundantního připojení jsme do datové sítě

implementovali segment routing. Segment routing je v současné době nejlepším mechanizmem zálohování komunikačních linek mezi směrovači, alespoň za předpokladu, že mezi směrovači nějaká záloha existuje. Komunikace směrovačů je šifrována na každém odchozím uplinku. Komunikace uživatelů se začala oddělovat a segmentovat na velmi úzké segmenty. S každým rokem rostou požadavky uživatelů na šířku přenosového pásma a na optimalizaci datové sítě.

Priority individuální datové sítě jsou u každé organizace či firmy jiné. Pokud budu poskytovatelem připojení pro jiné sítě, bude mým hlavním zájmem zabezpečit nasmlouvanou šířku pásma objednané zákazníky. Naopak lokálního poskytovatele připojení k datové síti bude zajímat zejména jak zákazníky připojit, respektive jakou technologii zvolit.

V případě naší organizace řešíme základní otázku, jakým způsobem připojit naše směrovače mezi sebou. Zde jsou možnosti využití vlastních okruhů pomocí bezdrátového přenosu, vlastní optická vlákna či využití služeb poskytovatelů připojení, kde již při výběru záleží, jakou službu uživatel požaduje. Na tuto otázku slyšíme vždy různorodou škálu požadavků, nicméně ve většině případů službu zákazníkům dělíme na poskytnutí služby typu L2 či typu L3.

V rámci služeb typu L2 nabízíme zákazníkům přenos v prostředí ethernet, E1. V prostředí ethernet se jedná o službu ve formě tvorby tunelu skrze datovou síť organizace mezi dvěma i více nody. Další službou je poskytování virtuálního přepínače mezi více lokalitami. Přenosu prostředí E1 se snažíme co nejvíce vyhnout a nutit zákazníka provádět upgrade technologie z E1 na Ethernet. V rámci přenášení služby typu L2 E1 zabezpečujeme synchronizaci datové sítě, která je velmi náročná.

Při poskytování služeb typu L3 nabízíme zákazníkům celou škálu možností od separace provozu do vlastní VRF až po připojení do již stávajících VRF.

Při provozování služeb ať typu L2 či L3 je nutné dodržovat požadavky domluvené při vzniku služby. V rámci těchto požadavků se jedná zejména o dostupnost, spolehlivost a celistvost přenášených dat.

V diplomové práci bude ukázáno, jak může vypadat datová síť s cílem přenášet L2 a L3 provozy zákazníků. Zejména se jedná o to, jakým způsobem bude vystavěn podvozek datové sítě, který zabezpečuje přenos provozů zákazníka. Provozy jsou, jak již bylo uvedeno, typu L2 či L3.

2 Cíl práce

Cílem diplomové práce „Návrh datové sítě se zaměřením na přenosy L2 a L3 provozů (Ethernet) mezi vzdálenými lokalitami“ je nastínit specifickou problematiku vytváření datových sítí při užití konkrétní studie. Takto navržená datová síť bude postavena na výrobci Alcatel-Lucent (Nokia), který zastupuje zákazníky v oblasti telekomunikací. Jedná se o profesionální řešení na úrovni dnešních vysokých požadavků pro přenos uživatelských dat.

V rámci fungování směrovačů od firmy Nokia bude návrh samotné sítě rozdělen do dvou částí. V první části bude sestaven takzvaný „podvozek“ datové sítě. V tomto „podvozku“ bude navrženo spojení směrovačů (dále boxy) mezi sebou. Budou zvoleny směrovací protokoly pro spojení mezi boxy. Bude se jednat o dynamické protokoly, ačkoliv bude navržená síť o minimálním množství boxů. Výhoda tohoto řešení spočívá ve faktu, že v případě budoucí potřeby bude pouze stačit přidávat další boxy. Limitním počtem boxů v návrhu je plochá síť založená na směrovacím protokolu IS-IS (Intermediate System to Intermediate Systém).

V druhé části návrhu datové sítě bude třeba vytvořit prostředí pro uživatelské služby typu VPRN (Virtual Private Routed Network) a EPIPE (Ethernet Pipe). V návrhu bude řešen příklad pro jednu samostatnou L3 síť (VPRN), jedna trasa pro provoz L2 typu bod-bod (tedy EPIPE).

Poslední část již nesouvisí s návrhem „Datové sítě se zaměřením na přenosy L2 a L3 provozů (Ethernet) mezi vzdáleními lokalitami“ ale s otestováním ideálního přenosu všech

dat v datové síti. V rámci návrhu bude cílem zobrazit rozdíl ve využitých tunelech MPLS (Multiprotocol label switching) prostředí za využití přenosových tunelů LDP (Label Distribution Protocol), RSVP-TE (Resource Reservation Protocol for traffic engineering), dále RSVP a SR-ISIS (Segment Routing Intermediate System to Intermediate System).

3 Metodika

Předpokladem správně přenesených uživatelských dat z lokality A do lokality B je jejich celistvost, rychlost doručení a spolehlivost datové sítě. Pro takový přenos dat je důležité zabezpečit stabilní „Core“ datové sítě, na kterém budou provozovány různé služby. Za náplň této služby jsou považována uživatelská data v L3 režimu, kdy jsou data přenášena pomocí IP protokolu. Dále existují služby v L2 režimu, kdy je přenos uživatelských dat zabezpečen na bázi MAC adres.

V rámci teoretické přípravy se pokusím rozebrat a popsat použité protokoly v prezentovaném řešení. Bude se tedy jednat o popis vrstev L2 a L3, popis směrovacích protokolů a popis tvorby tunelů využívajících datovou síť. Pro popis vrstev L2 a L3 bude využit model OSI a model TCP/IP.

Pro návrh datové sítě bude v rámci testovacího polygonu vybudována datová síť na směrovačích Nokia. Směrovače Nokia byly vybrány, neboť se nejedná o zcela běžnou a standardně přístupnou technologii. Tento výrobce je zastoupen především u větších firem, kde vzniká potřeba zabezpečit náročné datové přenosy. Z vlastností výrobce dojde k návrhu konfigurace.

Na polygonu dojde k provedení návrhu datové sítě za využití směrovacích protokolů jako IS-IS, MPLS a BGP. V rámci polygonu bude představeno řešení, v němž pro přenos dat bude využito tunelování pomocí LDP, RSVP a Segment Routing. V rámci návrhu datové sítě bude vložen síťový diagram a realizace konfigurací.

Na polygonu dojde také k odzkoušení přenosu uživatelských dat v L3 a L2 režimu. Jedná se o soubor testů pro každý typ tunelu (LDP, RSVP-TE a SR). Testování bude realizováno pomocí aplikace iperf. Výstup testování bude shrnut do tabulky pro každý režim L2 a L3. Výstupem tabulky bude reakce uživatelského provozu (L2, L3) na druhy tunelů při přenosu dat. Testování bude zaměřeno na chování služeb při využití tří typů transportních tunelů.

4 Charakteristika sledované problematiky

4.1 Právní předpisy ve sledované oblasti

4.1.1 Zákony a vyhlášky

Při výstavbě datové sítě je třeba brát v potaz legislativu České republiky. Jedná se zejména o zákony a obecně daná pravidla pro nakládání s daty uživatelů, v případě budování datové sítě s režimem utajení přenášených dat také dodržovat pravidla NBÚ. Jedná se zejména o upřesňující podmínky a pravidla pro datové sítě sloužící pro přenos dat v rámci kritické infrastruktury České republiky.

- 181/2014 Sb. Zákon o kybernetické bezpečnosti
    - 82/2018 Sb. Vyhláška o kybernetické bezpečnosti
- 127/2005 Sb. Zákon o elektronických komunikacích
- 110/2019 Sb. Zákon o zpracování osobních údajů

4.1.2 Normy

Normy určující jakým způsobem fungují datové sítě jsou stanovovány z mezinárodní úrovně. Jedná se zejména o normy a případně standardy organizací. Jejich cílem je specifikovat prostředí a využívat technologie napříč výrobci.

Převzaté normy:

- ČSN EN 60065 - Zvukové, obrazové a podobné elektronické přístroje – požadavky na bezpečnost
- ČSN EN IEC 61753-053 - Spojovací prvky a pasivní součástky vláknové optiky
- ČSN ETSI EN 300 132-2 V2.7.1 (872006) - Napájení stejnosměrným napětím - 48 V
- ČSN ETSI EN 300 386 V2.2.1 (872004) - Zařízení telekomunikační sítě

Organizace z mezinárodního prostředí:

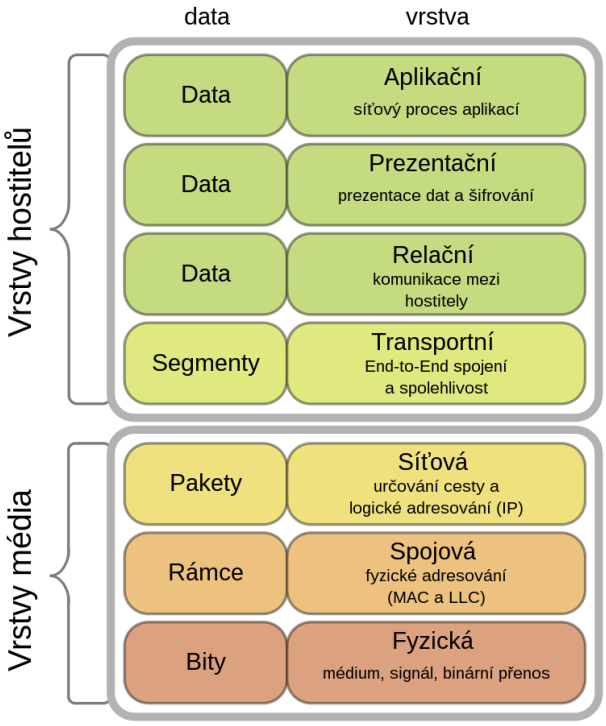
- ISO – International Organization for Standardization
- IEEE (Institute of Electrical and Electronics Engineers)
- RFC – Request For Comments (v tomto případě se nejedná o závazný standard, jako spíše o doporučení)

4.2 Základní definice a pojmy

Za účelem jednotného porozumění problematice datové komunikace bylo historicky uvedeno několik teoretických modelů pro standardizaci počítačové sítě. Jedním z prvních byl model od firmy IBM, který se nazýval SNA (Systems Network Architecture), případně model DECnet od firmy DEC (Digital Equipment Corporation). Jmenované modely byly prezentovány v 80. letech 20. století. Právě díky těmto modelům se začal utvářet svět protokolů sloužících pro datové komunikace. Od zmíněných modelů došlo postupem času až k současným nejvíce využívaným modelům pro popis počítačové sítě model ISO/OSI, který pracuje se sedmi druhy vrstev a snaží se vysvětlit, jak se otevřené systémy spojují. Díky zavedení tohoto modelu do běžného života došlo k rozšíření hardwarové základy při spojování počítačových systémů. Z modelu ISO/OSI vznik model TCP/IP, který je zjednodušen do 4 vrstev, které dokáží dále komunikovat. (1; 2)

4.2.1 Referenční model ISO/OSI

Referenční model ISO/OSI byl přijat v roce 1984 jako mezinárodní norma ISO 7498 (aktuální verze 7499-1:1994). Hlavním úkolem této normy je snaha o standardizaci pojmu „počítačové sítě“. Díky jejímu ustanovení mohla většina výrobců tehdejší doby začít spolupracovat a ubírat se jedním určitým směrem. Standard ISO/OSI bereme dnes jako běžnou věc, na jejímž základě se snažíme řešit problémy v počítačových sítích. V rámci datové sítě jsou z modelu ISO/OSI důležité vrstvy fyzická, linková, síťová a transportní.



Obrázek 1 – referenční model ISO/OSI (33)

Další tři vrstvy jsou relační, prezentační a aplikační. Poslední tři zmíněné vrstvy jsou důležité zejména pro aplikace po přenosu dat. (3)

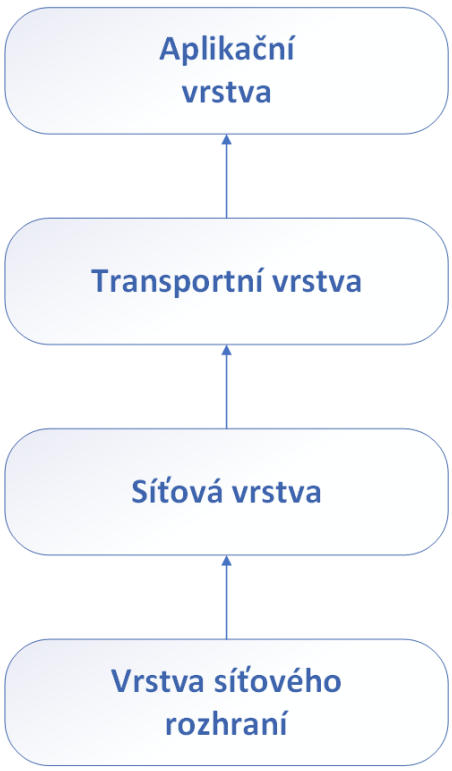
Fyzická vrstva charakterizuje a především realizuje spojení mezi systémy. Touto vrstvou jsou definovány konkrétní fyzické předpoklady pro rozhraní, definice zpracování signálu a převedení přenosu na log 0 a 1. V rámci datové komunikace na této vrstvě fungují všechna aktivní zařízení, protože potřebují realizovat fyzické spojení. Zařízení Hub (rozbočovač) funguje pouze na této vrstvě. (3)

Linková neboli spojová vrstva řadí přenášená data do tzv. rámců. Rámce jsou opatřeny údajem o svém začátku, adresováním, označením, komu rámec patří a od koho pochází a zabezpečením proti chybě přenosu dat. Rámec dokáže odhalit chybná (poškozená) data. Na této vrstvě primárně pracuje síťové zařízení Switch (přepínač). (3)

Síťová vrstva slouží k realizaci samotného směrování již vytvořeného rámce mezi datovými sítěmi. V rámci směrování je použito i adresování, které je nutné. Směrování takových dat může být statické či dynamické. Na této vrstvě pracuje v datové síti směrovač. (3)

Dále je zmíněna transportní vrstva, která zabezpečuje přenos dat v datové síti. Data jsou posílána formou packetů. V rámci přenosu mezi uzly je potřeba zabezpečit služby vyšších vrstev, jako jsou spolehlivost přenosu, celistvost přenesených dat. (3)

Poslední tři vrstvy reprezentují zpracování dat pro uživatele. V rámci datové sítě k těmto vrstvám přistupujeme spíše kvůli řešení speciálních zadání, či při řešení problémů. (3)



Obrázek 2 - model TCP/IP

4.2.2 Model TCP/IP

Model TCP/IP vznikl na základě vzešlých nedostatků modelu ISO/OSI. Hlavním nedostatkem byla především chybějící definice použitých síťových protokolů. Za protokoly TCP/IP můžeme poděkovat počítačové síti známé jako ARPANET, kterou provozovalo ministerstvo obrany USA. Model TCP/IP je soubor protokolů sloužících pro spojení v datové síti. Vrstva síťového rozhraní určuje druh přenášených dat. Jedná se o fyzické propojení, kde se může objevit technologie Ethernet, Token Ring a další. (4; 5)

Síťová vrstva je obecně známá jako hledání cesty pro data ze zdroje do cíle, bez ohledu na konkrétní způsob. Packety jsou přenášeny na základě protokolu IP. (4; 5)

Transportní vrstva realizuje přenos dat. Realizace přenosu je pomocí protokolů TCP či UDP. Takový přenos může být bezpečný a kontrolovaný v případě TCP, či nekontrolovaný v podobě UDP. Záleží na požadavcích aplikace. Transportní vrstva předává data aplikacím, které si je vyžádaly. (4; 5)

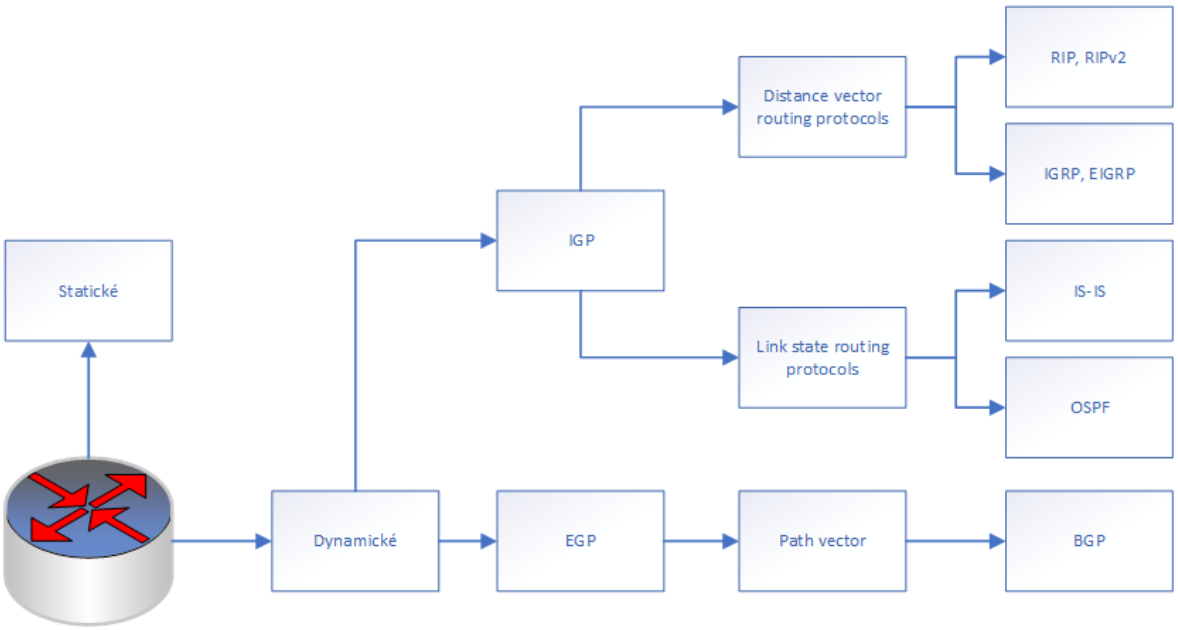
Aplikační vrstva je vrstva protokolů používající aplikace pro vzájemný přenos dat. Jedná se zejména o protokoly FTP, http, HTTPS, TELNET, SSH a WWW.

4.2.3 Směrovací protokoly

V návrhu jsou využity směrové protokoly jako ISIS, BGP, či MPLS, které spadají do různých kategorií. V rámci následujícího textu budou popsány jejich základní vlastnosti.

Směrovací protokoly je možné rozdělit na statické a dynamické. V rámci řešení problematiky moderních datových sítí je statické směrování využíváno v naprosto minimální míře ačkoliv je občas velmi účinné. Statické směrování je jednoduché, udržitelné pouze s pár směrovači a nezohledňuje dynamiku datové sítě. Statické směrování je vhodné využívat například při definici defaultní routy z datové sítě, které je nejvíce všeobecná a určuje, kam jsou směrovány data, s nimiž není obeznámena. I tuto defaultní routu lze vyrábět pomocí jiného směrování – dynamické směrování je již založeno na druhu směrovacího protokolu. Dle druhu protokolu je možné obecně stanovit jeho funkci. Existují protokoly, které jsou založeny na počtu skoků v cestě, nebo případně na základě váhy odchozí cesty. (6)

V rámci rozdělení dynamických protokolů je možné využít následující rozcestník:



Obrázek 3 - Rozdělení směrovacích protokolů

Interior gateway protocol

IGP je soubor protokolů určených pro komunikaci uvnitř podnikové sítě. Jedná se o protokoly na bázi distance-vector a link-state. Protokoly mají podrobné informace o vnitřní síti ať již v podobě vytvořené databáze, či v podrobné směrovací tabulce. (6; 7)

Exterior gateway protocol

EGP je protokol zabezpečující komunikaci mezi různými autonomními systémy. V principu se jedná o protokol, kterým jsou v dnešní době propojovány obrovské sítě mezi sebou. V rámci tohoto protokolu dochází k jasně definované výměně směrovacích informací. (7)

Distance-vector routing protocols

V případě distance-vector routing protokolu se jedná o soubor protokolů udržujících ve své směrovací tabulce informaci o „vzdálenosti“ do hledané sítě. Protokoly nicméně neznají celou topologii datové sítě za sousedními směrovači, ačkoliv směrovací tabulka disponuje vektory směru a vzdálenosti u každého záznamu. Použité protokoly jsou RIP, RIPv2, IGRP a EIGRP. Jedná se již o starší protokoly, které jsou většinou udržovány ve starých sítích, které již nelze obměnit, či změnit. (7)

Link-state routing protocols

Soubor protokolů, které si udržují stavy linek. Vyměňují si mezi sebou databázi za účelem zmapování celé sítě. Následně si z databáze vytváří nejkratší cesty k hledaným routám. V případě OSPF si mapují primárně svou areu, v případě IS-IS dochází k mapování na danému levelu. Zástupci link-state protokolů jsou OSPF a IS-IS. (6; 7)

4.2.4 Základní popis směrovacích protokolů

4.2.4.1 Protokol IS-IS

Protokol IS-IS, zkratka z anglických slov Intermediate System to Intermediate System. Protokol byl historicky vymyšlen firmou DECnet (Digital Equipment Corporation), která se v roce 1987 zabývala propojením větších sítí mezi sebou. Protokol IS-IS by měl být schopný teoreticky spojit neomezeně velké datové sítě.

Standard pro protokol IS-IS je definován normou ISO/IEC 10589:2002 a RFC1142. Protokol IS-IS patří do kategorie protokolů spadajících pod IGP. Jedná se o link-state protokol.

Na základě znalosti topologie datové sítě, v níž je směrovač s tímto protokolem, dochází k vytvoření databáze o topologii celé sítě. V tomto protokolu jsou databáze aktualizovány v okamžiku změny stavu linky určené pro přenos dat. Jakmile je databáze vytvořena, použije se Dijkstrův algoritmus k nalezení nejkratší cesty do hledané sítě. Protokol IS-IS využívá ke komunikaci linkovou vrstvu modelu ISO/OSI. Díky své univerzálnosti je vhodný pro velmi rozsáhlé datové sítě. Z historického hlediska není určen jen pro protokol IP. Protokol IS-IS je možné používat jak pro IPv4, tak pro IPv6. V protokolu rozlišujeme dvě úrovně provozů a jednu jejich kombinaci. (13; 14; 15; 16)

Protože je protokol velmi jednoduše upravitelný pro různé aplikace, došlo u něj k implementaci Traffic engineering, který je dále využíván při konstrukci definovaných cest pomocí MPLS sítě. Poslední větší úpravou bylo zavedení podpory pro Segment Routing do protokolu IS-IS. (17)

4.2.4.2 Protokol BGP

BGP je zkratkou anglických slov Border Gateway Protocol, který patří do protokolu EGP. Slouží tedy zejména pro komunikaci mezi různými autonomními systémy (AS). Jedná se o propojovací protokol v prostředí veřejného internetu. Definice BGPv4 je součástí RFC 4271. (19; 20)

Autonomním systémem je myšlena skupina sítí a směrovačů existujících pod jedním označením. Taková skupina je většinou spravována jednou organizací. V rámci této skupiny bývá využit směrovací protokol IGP, tedy OSPF či IS-IS. Čísla AS podléhají registraci, kterou řídí organizace Internet Assigned Numbers Authority (IANA). V rámci problematiky AS bylo nutno vyřešit jeho číslování a kategorizaci. Kategorizace byla vyřešena třemi kategoriemi, a to samostatný AS (Single-homed AS), redundantní AS (Multi-homed AS) a tranzitní AS (Tranzit AS). Číslování AS je určeno pomocí 16-bitového číslovacího plánu,

který obsahuje 65536 možností. Z tohoto rozsahu je několik konkrétních čísel AS určeno pro speciální užití. (21)

- Speciální účely 0, 65535, 23456
- Privátní účely 64512 – 65534
- Veřejné účely 1 – 64197

Protože se veřejný internet rozrůstá rychleji, než bylo původně zamýšleno, bylo číslování AS změněno na 32bitové. (21)

- Speciální účely 65536 – 65551
- IANA 65552 – 131071
- Privátní čísla 4200000000 – 4294967294

Směrovací protokol BGP (EBGP) své směrování určuje na hraničních směrovačích AS. Takové směrovače si vyměňují informace o svých sítích, které jsou touto cestou směřovány. Protokol podporuje beztřídní systém IPv4 a se snaží najít cestu mezi AS. V rámci svého principu dokáže zabránit směrovací smyčce na základě kontroly čísel v AS. Jakmile najde ve směrovací tabulce záznam se svým vlastním číslem AS, dojde k vyřazení takového záznamu. Při spojení několika AS je třeba velmi precizní práce administrátora daného AS, aby nedošlo k nechtěné situaci v níž se z Multi-homed AS stane Tranzit AS. V rámci spojení různých AS pomocí BGP můžeme využívat řadu atributů, kterými ovlivňujeme směrovací tabulky. (20)

Protokol BGP můžeme využít i pro vnitřní část AS, tím se z protokolu BGP stává IBGP. Taková konfigurace BGP potřebuje konfigurovat full-mesh spojení, nebo využít služeb Router Reflectoru, který předává směrovací tabulky pro iBGP.

4.2.4.3 Protokol MPLS

Protokol MPLS (Multiprotocol Label Switching) vznikl jako myšlenka, jak zjednodušit přenos dat bez nutnosti čtení dlouhých směrovacích záznamů a pro hledání jejich nejkratší a správné cesty. V době vzniku nebyl hardware připravený pro rychlé čtení směrových záznamů, vznikl proto pokus o implementaci přepínače takových informací. S touto myšlenkou přišla v roce 1994 firma Toshiba. Následně se objevilo více návrhů implementací, které vedly k založení vývojové skupiny v roce 1997. Z vývojové skupiny vznikla následně první verze nasazení MPLS na Cisco směrovačích, v roce 1998-9. (22; 23; 24)

MPLS sítě jsou dnes velmi rychlé a obecné. V rámci takové sítě je možné přenášet jak ethernet, tak i provoz E1 a další. MPLS je implementováno v rámci modelu ISO/OSI mezi vrstvu linkovou a síťovou, v rámci návrhu datové sítě je nicméně vhodné se bavit pouze o verzi pro ethernet. Protokol MPLS vychází z informací od směrovacího protokolu, který spojuje směrovače. Bez základního IGP směrovacího protokolu nelze MPLS provozovat. (22)

Protokol MPLS je tvořen MPLS hlavičkou o 32 bitech. Prvních 20 bitů reprezentuje hodnotu MPLS značky (label), další 3 bity jsou experimentální a je zde možné využít například zabezpečení priority. Další 1 bitové číslo reprezentuje konec. Posledních 8 bitů je určeno pro TTL, zaručující ukončení packetu. (22; 23; 24)

V rámci MPLS sítě jsou směrovače rozlišovány podle jejich typu, či také dle jejich funkce v MPLS síti. Jedná se o tranzitní směrovač, který v protokolu reprezentuje zkratka z anglických slov „Label Switch Router“, LSR. Dalším směrovačem v MPLS síti je směrovač označován jako LER, neboli „Label Edge Router“, v češtině často nazývaný jako hraniční nebo vstupní/výstupní směrovač. Komunikace probíhá tak, že LER směrovač přiřadí značku k přenášenému provozu, LSR směrovač obdrží packet od LER směrovače a dle směrovací MPLS tabulky rozhodne, kam daný packet pošle. Rozhodování probíhá pouze na základě značek MPLS. Vyhledávání správné cesty probíhá v MPLS databázi. Princip je založen na přidání první značky při vstupu packetu (Push), přeposlání MPLS packetu

správnou cestou, kdy původní značka je nahrazena novou (Swap). V případě doručení MPLS packetu na koncový (hraniční) směrovač dojde k odstranění značky (Pop). (22; 23; 24)

Provoz protokolu MPLS je v datové síti šířen tunely. Takové tunely mají různé funkce navíc.

4.2.5 Transportní tunely

Tunel typu LDP (Label Distribution Protocol) je jedním z typů tunelů používaných v síti MPLS. LDP tunely jsou využívány k přenášení datového provozu mezi směrovači v MPLS síti. LDP tunel je založen na konceptu přidělování štítků (labelů) datovému provozu. Každý štítek je přiřazen konkrétnímu datovému toku, který bude následně tunelován přes síť. Štítky jsou využívány pro směrování datového provozu přes různé síťové prvky, což umožňuje efektivní a rychlý přenos dat. LDP tunely mohou být využity k přenosu různých typů provozu, neboť nehledí na druh přenášené informace, pouze jí ukážou cestu přenosu. Vytvoření LDP tunelu může být složité a vyžaduje pečlivé plánování a konfiguraci, ale v případě fungujícího MPLS směrování se jedná již o relativně jednoduchou záležitost. Protože tunely jsou vytvářeny mezi různými síťovými prvky, je důležité zajistit správnou konfiguraci každého prvku a ověřit, že tunel je správně navázán.

V závěru lze říci, že LDP tunely jsou užitečným nástrojem pro efektivní a rychlý přenos datového provozu v síti MPLS. Díky přidělování štítků umožňují optimalizaci směrování datového provozu a lepší využití dostupných síťových zdrojů. Nicméně, vytvoření LDP tunelu může být složité a vyžaduje pečlivou konfiguraci a správné plánování. LDP tunel je základním tunelem v MPLS síti. (27)

Tunel typu RSVP-TE (Resource Reservation Protocol – Traffic Engineering) je dalším z typů tunelů používaných v síti MPLS. RSVP-TE tunely jsou využívány k přenášení datového provozu mezi směrovači v MPLS síti. RSVP-TE tunel je založen na protokolu RSVP, který umožňuje rezervovat síťové zdroje pro specifické datové toky. Protokol RSVP-TE je rozšířením tohoto základního protokolu a umožňuje rezervovat síťové zdroje pro specifické trasy a služby. Vytvoření tunelu typu RSVP-TE je složitější, než vytvoření tunelu

typu LDP. Pro vytvoření tunelu RSVP-TE musí být nejprve specifikována trasa, kterou bude tunel procházet. Tato konfigurace je prováděna ručně, za pomoci udržování informace o datové sítě v policy statement a jejich prefixů. Následně se v MPLS pro vytváření takových tunelů využívá LSP. RSVP-TE tunely mohou být využity k přenosu různých typů provozů. Tunel nehledí na druh přenášené informace, pouze jí ukážou cestu přenosu. Přenos informace je stejný, jako v případě tunelu LDP. Výhodou tunelu RSVP-TE je možnost jejího využití jakožto redundantního spojení. Tunel je vytvářen na protější bod, ale zároveň je v případě možnosti vytvořen záložní tunel, který zabezpečuje okamžité využití v případě výpadku prvního tunelu. (22; 27; 28)

Posledním typem tunelu použitým v této diplomové práci je SR-ISIS (Segment Routing - ISIS). Jedná se o tunel využívající prostředí MPLS, ale vytvářený v IGP protokolu. Segment Routing (SR) je nový koncept směrování v síti, využívající existující protokoly směrování, jako je například ISIS nebo OSPF. SR-ISIS tunely jsou založeny na tomto konceptu a umožňují směrování datového provozu přes předem definované cesty v síti.

Při vytváření tunelu typu SR-ISIS je nutné nejprve specifikovat cestu, kterou bude tunel procházet. Poté je tunel identifikován unikátním identifikátorem, který se nazývá Segment ID. Segment ID je založen na jasné definici směrovače v datové síti. Díky této jasné identifikaci je možné plánovat kompletní přenos dat. Tunel využívá výhod segment routingu (a to zejména zálohy směrovačů) při jejich výpadcích, pokud to topologie sítě umožňuje. (30; 31)

4.2.6 Ethernet

Pojem Ethernet je v této práci zmíněn mnohokrát. Jedná se o technologii, která spatřila světlo světa v roce 1973 v kooperaci firem Digital Equipment Corporation, Intel a Xerox (DIX). Díky otevření patentu došlo ke standardizaci pomocí IEEE 802.3 společnosti Institute of Electrical and Electronics Engineers (IEEE). (12)

V rámci historie standardu 802.3 došlo k mnoha úpravám, od úprav 802.3a – koaxiální kabel a rychlost 10Mbps po normu 802.3ba, která udává rychlost 40-100Gbps,

nebo 802.3cg, která upravuje parametry pro průmyslové prostředí. Jednou z posledních norem 802.3bs je přenos rychlosti 400Gbps po technologii Ethernet. Nejběžněji se zkratkou 802.3xx můžeme setkat při řešení problematiky Wi-Fi. (12)

V dnešní době je Ethernet nejčastěji přenášen za pomocí sady 4x kroucené dvoulinky, známé jako UTP a jeho variant, optických kabelů a případně bezdrátově pomocí technologie Wi-Fi. V rámci návrhu datové sítě budou použity UTP kabely a optická vlákna. Variace UTP kabelů dnes dovolují navrhovat datové sítě s rychlostmi až do 40Gbps (při Cat8 s omezením vzdálenosti 30m). Pro vyšší rychlosti je třeba využívat optická vlákna, u nichž je v návrhu datové sítě maximum kolem 100Gbps (při využití navrhovaného HW). (12)

Při komunikaci pomocí Ethernetu dochází k přenosu paketů, které jsou tvořeny ethernetovým rámcem, preambulí a oddělovačem.

Layer	Preambule	Oddělovač začátku rámce	MAC cíle	MAC zdroje	802.1Q tag (volitelný)	Délka/Typ	Datové pole	Kontrolní posloupnost rámce (32bitový CRC)	Mezera mezi pakety
	7 oktetů	1 oktet	6 oktetů	6 oktetů	(4 oktety)	2 oktety	46(42)[3]–1500 oktetů	4 oktety	12 oktetů
Ethernetový rámec (linková vrstva)			← 64–1518(1522) oktetů →						
Ethernetový paket (fyzická vrstva)	← 72–1526(1530) oktetů →								

Obrázek 4 - ethernetový rámec (34)

V datové sítí jsou zajímavé hodnoty obsažené v datovém rámci. Z těchto hodnot je možné řídit, kam který packet patří, jakou přenáší informaci, jak je důležitý a zdali je v pořádku přenesen. V případě potřeby je možné datové rámce odchytávat a provádět jejich diagnostiku například pomocí aplikace WireShark, nebo pomocí specializovaných měřících serverů. (12)

V rámci technologie Ethernet a datové sítě jsou primárně řešeny následující parametry:

- Rychlost (10/100/1000/10000 Mbps)
- Duplex – druh komunikace na rozhraní, nejběžněji full duplex

- Velikost MTU (jeho hodnota má velký význam při šifrování dat)
- Zakončení konektoru (metalické, optické)

4.2.7 MAC adresa

MAC je zkratka z anglických slov Media Access Control. Jedná se o jedinečnou identifikaci zařízení na základě výrobcem definované adresy, která je „vypálena“ do zařízení. V dnešní době toto tvrzení již docela neplatí, neboť se ustoupilo požadavkům bezpečnosti a MAC adresu je již možné měnit. V mnoha případech se jedná o vynucenou změnu s každým využitím.

MAC adresa je jedním z původních standardů z rodiny standardů IEEE 802. Jedná se o součást použitou v modelu ISO/OSI na druhé vrstvě. Skládá se ze 48 bitů, kde prvních 24 z nich je určeno pro identifikaci výrobce síťového rozhraní využívajícího standard MAC. Případný výrobce musí požádat autoritu IEEE o přidělení vendorské části MAC adresy. Druhých 24 bitů je jedinečná kombinace, přičemž za její kýženou jedinečnost odpovídá výrobce daného zařízení. (10)

MAC adresy jsou rozdělovány na tři skupiny: (10; 11)

- Unicast
    - Jedná se o jedinečnou kombinaci udanou autoritativní organizací IEEE a výrobcem
- Broadcast
    - Jedná se o adresu, se kterou budou komunikovat všechna zařízení v datové síti
- Multicast
    - Adresa, která určuje cílovou skupinu, která ji poslouchá

MAC adresa se využívá například k identifikaci v datové síti na úrovni L2, kde je jedinečným identifikátorem daného zařízení. (10)

- Switch
- Wi-fi
- Bluetooth
- FiberChnnel

4.2.8 Rozdělení IP adresního prostoru

Pro návrh datové sítě je zcela nutné stanovit IP adresní plán, který bude plně respektován. Definice IP adresy verze 4 se řídí dle RFC 791. V rámci návrhu IP adresního plánu se bude práce soustředit výhradně na IP adresaci ve verzi 4. (8)

IP adresaci IPv4 rozdělují organizace pod názvy ICANN a IANA. Tyto organizace mají na starost rozdělení veřejných částí adresace IPv4. V rámci návrhu se vychází z možností, které je možné využít ve vnitřní síti. Tyto adresy definuje RFC 1918. Bloky pro privátní užití specifikuje následující tabulka. (9)

Tabulka 1 - Privátní adresy IPv4

Adresa sítě	**Maska sítě**	**Adresní prostor**	**Počet adres**
10.0.0.0	/8	10.0.0.0 – 10.255.255.255	16 777 216
172.16.0.0	/12	172.16.0.0 - 172.31.255.255	1 048 576
192.168.0.0	/16	192.168.0.0 - 192.168.255.255	65 536

Při práci s adresními rozsahy uvnitř organizace je zaváděna funkce správce adresního prostoru, který je zodpovědný za distribuci privátních, ale i veřejných adresních prostorů (ať se jedná o IP adresaci ve verzi IPv4 či IPv6). Tento správce disponuje mnoha nástroji, s nimiž může správu provádět. Jedná se například o excelové tabulky či nástroj IPAM.

V tomto projektu bude správa využitých adresních rozsahů provedena pomocí excelové tabulky. Při návrhu datové sítě bude využit IP adresní plán z rozsahu 10.20.0.0/16, který bude určen pro podvozek a zprovoznění směrování. Zákaznické služby typu L3 budou využívat rozsah 10.21.0.0/16. Zákaznický provoz typu L2 nevyužívá IP adresaci pro přenos v datové síti a komunikace tak zůstává na druhé vrstvě dle modelu ISO/OSI.

4.2.9 High Level Design

High level design (HLD) zahrnuje podrobnější návrh datové sítě na základě hlavních parametrů, jakými jsou přenosové rychlosti, datové propustnosti, bezpečnostní opatření a mnoho dalších variant, které sděluje zadavatel.

V HLD je obvykle stanovena základní topologie sítě a jsou zde také definovány základní komponenty, jimiž jsou směrovače, přepínače a přístupové body, spolu s potřebnými funkcemi, jako jsou zabezpečení, kvalita služeb (QoS), správa sítě a další. HLD také definuje základní parametry sítě, jako jsou rychlost přenosu dat a požadavky na šířku datového pásma. HLD se často používá jako vstup pro vytvoření detailního návrhu sítě (Low Level Design, LLD), který se zaměřuje na konkrétní komponenty a technologie využité v síti. HLD je možné navrhovat jak po stránce datové sítě, tak i po stránce zabezpečení služeb, které požaduje zadavatel.

Výstup HLD je celistvá dokumentace, která definuje a shrnuje veškeré nároky zadavatele datové sítě.

4.2.10 Low Level Design

Low Level Design (LLD) v oblasti datových sítí zahrnuje celkový zámysl navrhované datové sítě. Jedná se o rozšíření High Level Designu o přesné informace a postupy. Návrh definuje celkovou architekturu datové sítě, a to včetně její topologie, využité technologie a použitých protokolů. Low level design slouží jako plán pro vytvoření datové sítě, který zohledňuje požadavky na propustnost, bezpečnost, dostupnost a škálovatelnost.

Klíčové prvky low level designu datových sítí zahrnují:

1) Topologii datové sítě
2) Návrh typu sítě dle distribuce a použitých síťových protokolů
3) Definice využitých zařízení jako směrovače, přepínače a další.
4) Definice bezpečnostních prvků, jimiž jsou bezpečnostní brány, nárazové filtry a tapy.

5) Definice software pro dohled datové sítě.

Celkově lze říci, že Low Level Design v oblasti datových sítí slouží jako plán pro realizaci navržené datové sítě, která bude schopna plnit požadavky zadavatele datové sítě. Výstupem LLD je podrobná dokumentace, jakým způsobem bude daná datová síť implementována. V dokumentaci by měla být pokryta veškerá konfigurační část všech zařízení, které jsou součástí datové sítě.

5 Vlastní řešení

5.1 Popis návrhu datové sítě

Navrhovaná datová síť bude reflektovat zadání diplomové práce. Jedná se tedy o návrh datové sítě se zaměřením na přenosy L2 a L3 provozů (Ethernet) mezi vzdálenými lokalitami. Navržená datová síť bude založena na 10Gbps linkách, které budou spojovat jednotlivé páteřní směrovače. Cílem sítě je uživatelům zabezpečit bezchybnou komunikaci pro přenos jejich dat a také co nejrychlejší reakci na změny v datové síti.

Navržená datová síť bude postavena na polygonu reprezentujícím vzorek osazené technologie a použitého řešení. Daný vzorek je bezproblémově rozšiřitelný až do několikanásobné velikosti. V rámci návrhu budou použity směrovače od firmy Nokia. Pro páteřní část datové sítě bude využito výkonných modelů typu P, konkrétně se jedná o modelovou řadu 7750. Pro přístupovou část datové sítě bude využito menších, obecnějších modelů typu PE, modelová řada 7705.

Základním směrovacím protokolem pro datovou síť je protokol IS-IS. Jedná se o protokol typu Link-State, který patří do protokolů typu IGP. Tento protokol je určen pro komunikace vnitřních částí datové sítě. Navržená síť bude pro zjednodušení plochá, bude tedy využívat pouze jednu úroveň v protokolu IS-IS. Komunikace v protokolu IS-IS se bude odehrávat na levelu-2.

Základní protokol IS-IS, který zabezpečí komunikaci mezi směrovači, poslouží jako „podvozek“ pro protokol MPLS, čímž se zajistí rychlé odbavení komunikace mezi směrovači pomocí labelů. V rámci protokolu MPLS budou využívány různé druhy transportních tunelů. Mezi těmito tunely jsou rozdíly, jejichž individuální popis bude v průběhu řešení návrhu specifikován. Tyto transportní tunely budou využity pro transport informací přenášených pomocí BGP, ale i pro informace přenášené pomocí L2 služeb.

Pomocí interního BGP protokolu bude realizována vnitřní komunikace pro uživatelská data. Toto BGP bude sloužit výhradně pro interní komunikace mezi směrovači. Díky tomuto protokolu bude docházet k výměně informací mezi jednotlivými VPRN (VRF). Pomocí

daného protokolu dojde k přenosu uživatelských dat v režimu L3, který je definován v zadání a popsán v teoretickém rozboru této práce.

Software pro směrovače je u typu P verze 20.5.R2, typ PE verze 20.4.R3. Testovací notebooky jsou s Windows 11 Pro a programem Colasoft PingTool.

5.2 Popis použité technologie

Použitá technologie je od výrobce Nokia. Někdy je možné na zařízeních vidět i název firmy Alcatel-Lucent, který byl producentem zařízení v minulosti.

5.2.1 Páteřní směrovač, typu P

Páteřní směrovač Nokia 7750 SR-a4:

Obrázek 5 - Směrovač Nokia 7750 SR-a4 (25)

Výkonný směrovač, který je vybaven procesorem FP3, díky němuž dokáže odbavovat rychlosti od 200Gbps do 400Gbps (dle režimu komunikace a HW kombinace). Omezení jsou tvořena dle osazené konfigurace daného směrovače. Směrovač je řízen pomocí řídící karty, která zabezpečuje jeho dohlížení a řízení. Dále může být vybaven mnoha druhy

rozšiřujících karet, které zabezpečují komunikaci. Zejména se jedná o karty typu Ethernet, které jsou tvořeny SFP šachtami pro osazení SFP moduly. (25)

Směrovač je o velikosti 5 RU a hloubce 300 mm. Napájení pro směrovač je řešeno pomocí DC 48 V nebo AC 230 V. Součástí směrovače je ventilátorová jednotka, která zabezpečuje chlazení zařízení. (25)

Směrovač podporuje unicast routing (IS-IS, OSPF, RIP), multicast routing (IGMP, MLD) a MPLS směrování.

5.2.2 Přístupový směrovač typu PE

Přístupový směrovač Nokia 7705 SAR-8 a 18

Obrázek 6 - Směrovač Nokia 7705 SAR-8 (26)

Jedná se o agregační směrovač, který je vhodný jako hraniční směrovač IP/MPLS datové sítě. Zobrazený model je velmi rozmanitý z pohledu možnosti využitelných rozhraní. Dokáže přenášet služby na bázi Ethernet, ale i časově náročné aplikace jako protokol E1.

Směrovač je vybaven dvěma řídícími kartami, které se vzájemně zálohují. Řídící moduly dokáží odbavit provoz až do 30Gbps, který přichází z karet. Rozšiřující karty mohou být 10Gbps nebo 1Gbps. Rozšiřující karty mohou mít na vstupu/výstupu rozhraní jako SFP, metalický Ethernet, T1, E1, STM-1, DS3, E3, VT a SDI. (26)

Zařízení jako takové potřebuje v 19“ datovém rozvaděči prostor 3U. Napájení je realizováno DC 24 nebo 48 V. Součástí zařízení je ventilátorová jednotka, která zabezpečuje jeho chlazení. Zvláštností zařízení je pak rozmezí teplot, v němž je směrovač schopen fungovat, a to – 40 °C až +65 °C. (26)

5.3 Jmenná konvence a adresní plán datové sítě

Jmenná konvence pro realizaci návrhu datové sítě nepodléhá žádným pravidlům, ani zákonům. V případě realizace datové sítě u většího podniku či státní správy může dojít k vnitro podnikovým omezením vlivem vlastních nařízení. Jmenná konvence by měla být stanovena před realizací datové sítě, neboť její následné změny mohou být náročné ať již kvůli administrativním zásahům v dokumentaci, nebo v konfiguraci. Jmenná konvence slouží k identifikaci zařízení, a může skrývat jak název zařízení, tak například i jeho umístění. Jmenná konvence by měla dávat smysl zejména administrátorům datové sítě, kteří tuto síť spravují.

V rámci vlastního návrhu konkrétní datové sítě bude použita jmenná konvence, v níž testovací polygon pro návrh využívá název PAPOLY, a je následně rozšířen o číslo budovy, kde je prováděno testování. Jako poslední údaj je ve jmenné konvenci uvedeno, zdali se jedná o směrovač typu P či PE a jeho identifikační číslo.

Se jmennou konvencí je velmi úzce spojen IP adresní plán, který je z mnoha úhlů pohledu nejdůležitějším administrativním dokumentem datové sítě. Díky tomuto dokumentu by mělo být jednoznačně určeno, kde se jaká vnitřní IP adresace nachází. IP adresní plán je možné spravovat mnoha způsoby. Jedná se o správu pomocí aplikací jako InfoBlox, IPAM, či MS Excel. IP adresní plán musí mít svého určeného správce, který vede administrativu přidělování IP adres, vracení IP adres a případně provádí její kontrolu vůči směrovací tabulce. V případě nedodržení adresního plánu může dojít v datové sítě ke směrovacím smyčkám, a tím i k neschopnosti bezpečně a celistvě doručovat uživatelská data.

Součástí IP adresního plánu by měly být následující údaje:

- verze IP adresy,
- název směrovače,
- IP adresa směrovače,
- přidělená síť s její maskou,
- číslo VPRN pro kterou je přidělená síť.

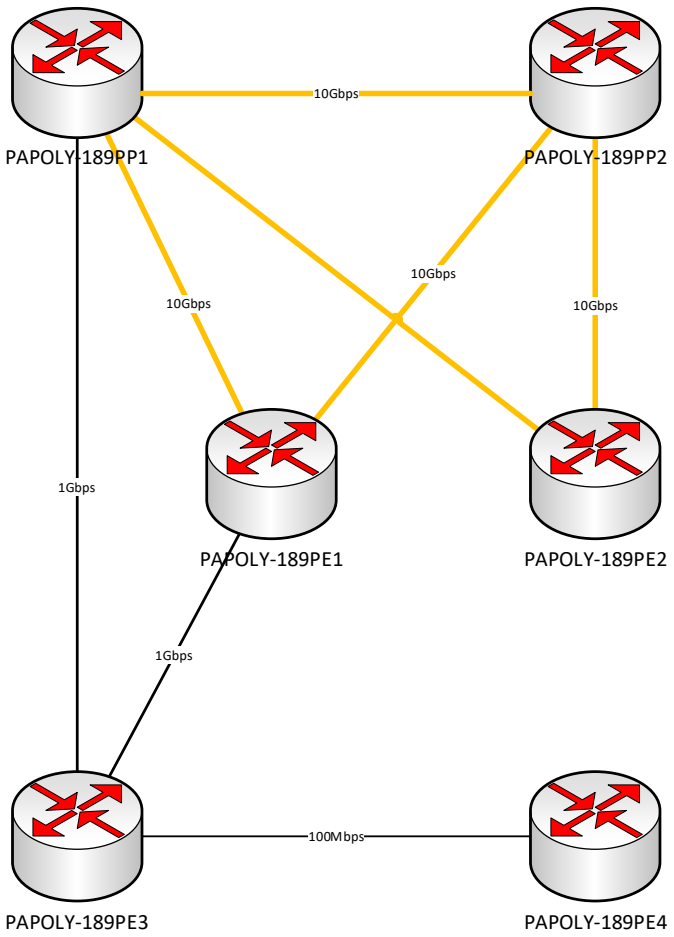
Tabulka pro IP adresní plán:

Tabulka 2 - Adresní plán pro testování

IPv4 adresní plán datové sítě						
Síť	**Maska /**	**VPRN**	**Směrovač**			**Poznámka**
			IP adresa	**Hostname**	**Lokalita**	
10.20.7.189	32	-	10.20.7.189	PAPOLY-189PP1	189	
10.20.8.189	32	-	10.20.8.189	PAPOLY-189PP2	189	
10.20.1.189	32	-	10.20.1.189	PAPOLY-189PE1	189	
10.20.2.189	32	-	10.20.2.189	PAPOLY-189PE2	189	
10.20.3.189	32	-	10.20.3.189	PAPOLY-189PE3	189	
10.20.11.252	30	-	10.20.11.253	PAPOLY-189PE3	189	
			10.20.11.254	PAPOLY-189PE4	189	
10.20.11.224	30	-	10.20.11.225	PAPOLY-189PP1	189	
			10.20.11.226	PAPOLY-189PE2	189	
10.20.11.228	30	-	10.20.11.229	PAPOLY-189PP1	189	
			10.20.11.230	PAPOLY-189PE3	189	
10.20.11.232	30	-	10.20.11.233	PAPOLY-189PP2	189	
			10.20.11.234	PAPOLY-189PE2	189	
10.20.11.236	30	-	10.20.11.237	PAPOLY-189PP1	189	
			10.20.11.238	PAPOLY-189PP2	189	
10.20.11.240	30	-	10.20.11.241	PAPOLY-189PP2	189	
			10.20.11.242	PAPOLY-189PE1	189	
10.20.11.244	30	-	10.20.11.245	PAPOLY-189PP1	189	
			10.20.11.246	PAPOLY-189PE1	189	

IPv4 adresní plán datové sítě						
Síť	Maska /	VPRN	Směrovač			Poznámka
			IP adresa	Hostname	Lokalita	
10.20.11.248	30	-	10.20.11.249	PAPOLY-189PE1	189	
			10.20.11.250	PAPOLY-189PE3	189	
10.21.189.0	26	10	10.21.189.1	PAPOLY-189PE1	189	
10.21.189.64	26	10	10.21.189.65	PAPOLY-189PE2	189	
10.21.189.128	26	10	10.21.189.129	PAPOLY-189PE3	189	
10.21.189.192	26	10	10.21.189.193	PAPOLY-189PE4	189	
192.168.0.0	30	-	192.168.0.1	NB1	189	EPIPE, IPERF server
			192.168.0.2	NB2	189	EPIPE, IPERF client

5.4 Schématické zobrazení datové sítě



Obrázek 7 - Síťový diagram

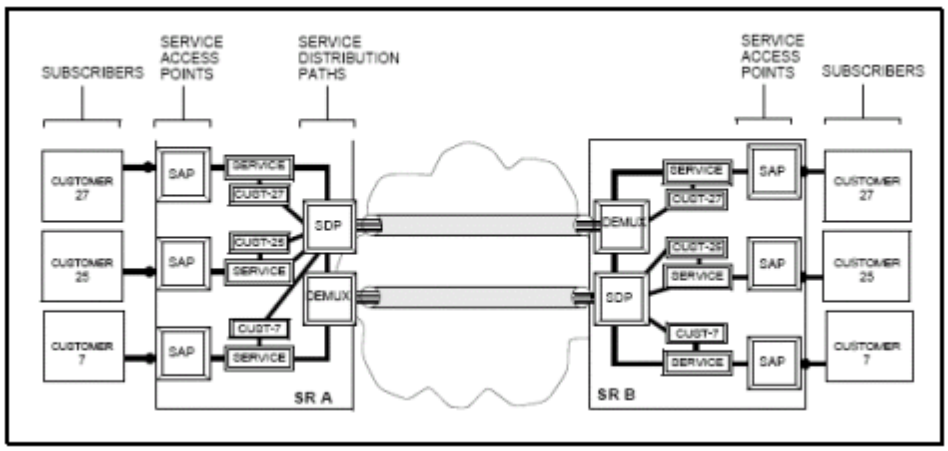
5.5 Řešení „podvozku“ datové sítě

Směrovače od firmy Nokia jsou koncipovány ve dvou konfiguračně rozdílných částech. Jedná se o část směrovací a část určenou pro tvorbu služeb. V rámci směrovací části, jak již sám název napovídá, dochází ke spojení jednotlivých směrovačů mezi sebou. Pro toto spojení bude využit IGP protokol, přesněji protokol IS-IS. V rámci protokolu IS-IS je potřeba definovat jeho základní konfiguraci a konfiguraci interface, na kterých bude možné dohledat sousední směrovače. Směrovače mezi sebou komunikují vždy přes tzv. „spojovku“, tedy síť o dvou použitelných adresách. (29)

Směrovače Nokia využívají takzvaný servisně orientovaný koncept, který byl již rámcově nastíněn výše. To výrazně zjednodušuje správu celého systému a jasně odděluje konfigurace související s jádrem sítě, a konfiguraci jednotlivých služeb. (29)

Základní logické konstrukce tohoto modelu jsou:

- Zákazník – Customer
- Služba – Service
- Přístupový port služby – Service Access Points (SAPs)
- Distribuční cesta služby, tunel přes MPLS síť – Service Distribution Paths (SDPs)



Obrázek 8 - Komponenty servisního modulu (29)

5.5.1 Konfigurace IGP protokolu

Jako směrovací protokol na úrovni IGP je použit IS-IS v level 2. Ve směrovači bude nakonfigurován IP fast reroute, umožňující nainstalovat do směrovacích informací i záložní IP cesty, pokud to fyzická topologie umožňuje. Protokol IS-IS vyniká rychlou konvergencí dat, takže ve výsledku budou vnitřní stavy protokolů velmi rychle interpretovány v databázi směrovacího protokolu. Směrovače budou konfigurovány jako Point-To-Point. V rámci dalších rozšiřujících parametrů protokolu IS-IS bude využit Traffic engineering, který poslouží při provozování MPLS a jeho transportních tunelů. Jako referenční šířka pásma bude využita hodnota 100 Gbps. V rámci konfigurace dojde k upravení hodnot spf-wait 2000 (maximální čas v ms mezi vyhledávanými SPF), spf-initial-wait 50 (vyhledávání SPF po 50ms) spf-second-wait 100 (určující, po jaké době se opět vyhledává SPF). (13; 15; 29)

Níže je uvedena konfigurace protokolu IS-IS, která je distribuována na směrovače v návrhu datové sítě. Konfigurace na ostatních směrovačích je velmi podobná. Budou se zde lišit hodnoty u konfigurace interface, kde je potřeba zohlednit adresu loopbacku, názvy a adresy vůči sousedním směrovačům. Hodnoty pro směrování IS-IS jsou ponechány defaultní, tedy hodnoty definované síťovým rozhraním fyzických portů. (13; 15)

Protokol ISIS využívá nadefinované interface v router Base. Zde je potřeba provést konfiguraci všech možných odchozích interface vůči sousedním směrovačům. V rámci definice interface je provedeno přidělení názvu interface, adresy IPv4 a odchozího portu. Konfigurace interface pro P i PE může vypadat takto:

```
router Base
    interface "system"
        address 10.20.1.189/32
        no shutdown
    exit
    interface "toPAPOLY-189PE3"
        address 10.20.11.249/30
        port 1/2/4
        no shutdown
    exit
```

Konfigurace IGP pro směrovač typu PP:

```
isis 0
        level-capability level-2
        area-id 49.00
        traffic-engineering
        reference-bandwidth 100000000
        advertise-router-capability as
        loopfree-alternates
           ti-lfa
              node-protect
           exit
        exit
        timers
           spf-wait 2000 spf-initial-wait 50 spf-second-wait 100
        exit
        level 2
           wide-metrics-only
        exit
        segment-routing
           micro-loop-avoidance
           prefix-sid-range global
           no shutdown
        exit
        interface "system"
           level-capability level-2
           ipv4-node-sid index 7189
           passive
           no shutdown
        exit
        interface "toPAPOLY-189PE2"
           level-capability level-2
           interface-type point-to-point
           no shutdown
        exit
exit
```

Konfigurace IGP pro směrovače typu PE:

```
isis 0
        level-capability level-2
        area-id 49.00
        traffic-engineering
        reference-bandwidth 100000000
        advertise-router-capability as
        loopfree-alternate ti-lfa
```

```
        timers
            spf-wait 2000 spf-initial-wait 50 spf-second-wait 100
        exit
        level 2
            wide-metrics-only
        exit
        interface "system"
            level-capability level-2
            ipv4-node-sid index 1189
            passive
            no shutdown
        exit
        interface "toPAPOLY-189PP1"
            level-capability level-2
            interface-type point-to-point
            no shutdown
        exit
exit
```

5.5.2 Konfigurace MPLS protokolu

Návrh MPLS vycházel z problematiky popsané v teoretické části, kdy bylo stanoveno, který směrovač plní úlohy typu P a který plní úlohy pro PE/CE. Základní MPLS funkcionalita bude rozšířena použitím MPLS-TE rozšíření. Díky rozšířené funkci TE budou využívány SPF z IGP, které zároveň umožní použití MPLS-FRR (Fast Re-Route) funkcionality, která pomocí předpřipravených, automaticky kalkulovaných záložních tunelů v každém redundantním bodě sítě dokáže stlačit rychlost konvergence datové sítě (definice z časovačů z IGP). To je umožněno rychlou detekcí samotného výpadku a nasazením okamžité opravy v místě samotného výpadku. Není tedy nutno čekat na rozšíření informace o výpadku přes celou síť, jako je tomu v případě interního směrovacího protokolu. Pro signalizaci MPLS značek se předpokládá využití kombinace obou hlavních protokolů: LDP (Label Distribution Protocol) pro přístupovou část sítě bez redundance, a RSVP-TE z důvodu použití MPLS-FRR v redundantních částech sítě. (22; 29)

Konfigurace MPLS:

```
mpls
        resignal-timer 30
        interface "system"
            no shutdown
```

```
        exit
        interface "toPAPOLY-189PP1"
           no shutdown
        exit
exit
```

5.5.3 Konfigurace transportních tunelů

Pro přenos dat v MPLS je potřeba definovat transportní tunely. Tunely jsou díky vlastnosti TLDP schopny obsluhovat i provozy na úrovni L2 služeb. Jedná se zejména o tunely LDP a RSVP-TE, které přenášejí MPLS značky. Třetím možným tunelem je tunel segment routingu, který také přenáší značku (ta již ale musí být pevně dána). Nejedná se o standartní provoz MPLS. Konfiguračně má nejlepší prioritu tunel RSVP-TE, následuje jej LDP a nejhorší prioritu má tunel SR-ISIS, který je z výše zmíněných nejmladší. Pro tunel RSVP-TE se využije full-mesh redundantních tunelů pomocí LSP mezi směrovači, které touto vlastností disponují (za předpokladu, že mají více odchozích uplinků). Všechny LSP budou konfigurované s Facility FRR backup zálohou, která umožňuje znovu použít stejné záložní tunely pro více procházejících LSP a šetří tak zdroje směrovače. Takové LSP bude využívat definovaný template s prefixlistem, v němž je seznam směrovačů podporujících a kompatibilních s RSVP-TE. (22; 27; 28; 29; 30; 31)

Konfigurace tunelu LDP:

```
ldp
        fast-reroute
        interface-parameters
           interface "toPAPOLY-189PP1" dual-stack
              shutdown
              ipv4
                 no shutdown
              exit
           exit
        exit
        targeted-session
        exit
        no shutdown
     exit
```

Konfigurace RSVP-TE:

```
rsvp
    shutdown
    interface "system"
        no shutdown
    exit
    interface "toPAPOLY-189PP1"
        shutdown
    exit
exit
```

5.5.4 Konfigurace interního BGP protokolu

BGP protokol bude obsluhovat veškerý provoz L3 služeb uživatelů. Jedná se o signalizaci dosažitelnosti VPNv4 adres. VPNv4 je zde kvůli omezení na IP adresní plán verze 4. Směrovací informace budou vyměňovány mezi všemi směrovači v datové síti pomocí MP-BGP, přičemž pro správnou funkci BGP je potřeba definovat číslo autonomního systému (AS). Toto číslo je zvoleno z rozsahu určeného pro interní systémy. Jedná se o číslo AS 65432. (29)

V rámci ulehčení administrativní zátěže bude při konfiguraci BGP využito služeb router reflectoru, který nahrazuje podstatné full-mesh spojení v rámci interního BGP. V každém případě je potřeba definovat nejméně dva router reflectory, které poskytnou zálohu v případě možné závady jednoho z nich. V případě nedostupnosti žádného router reflectoru jsou následky pro provoz VPRN (VRF) fatální – nebude docházet ke změnám ve směrovací tabulce. Pouze router reflector zabezpečuje výměny prefixů v rámci VPRN ke všem jeho sousedům. Sousední směrovače jsou vždy připojeny na každý router reflector v daném AS. (29)

Příklad konfigurace BGP pro router reflector:

```
bgp
        min-route-advertisement 1
        rapid-withdrawal
        rapid-update mvpn-ipv4
        group "ibgp"
```

```
        family vpn-ipv4 vpn-ipv6 mvpn-ipv4
        type internal
        cluster 10.20.7.189
        neighbor 10.20.1.189
        exit
      exit
      no shutdown
    exit
```

Příklad konfigurace BGP pro non router reflector:

```
bgp
      min-route-advertisement 1
      rapid-withdrawal
      group "ibgp"
        family vpn-ipv4 vpn-ipv6 mvpn-ipv4
        peer-as 65432
        neighbor 10.20.7.189
        exit
        neighbor 10.20.8.189
        exit
      exit
      no shutdown
    exit
```

Za účelem nastolení co nejrychlejší reakce na změny v datové síti je upravena hodnota min-route-advertisement na 1. Tímto by mělo být dosaženo 1s výpadku v rámci VPNv4, tedy L3 služeb.

5.5.5 Konfigurace Segment-Routing:

Segment-routing je velmi mladá záležitost vzhledem ke stáří ostatních protokolů, neboť za rok jejího vzniku je označován rok 2013. Byla vymyšlena pracovní skupinou organizace Internet Engineering Task Force (IETF).

Základním předpokladem je zjednodušení MPLS, v němž nebude potřeba tvořit transportní tunely nad IGP. Segment-routing využívá IGP pro přenos MPLS tunelů, IGP je tedy nutné mít na směrovačích zkonfigurované a funkční. Nabízí se tedy otázka, proč nevyužít již funkční databázi k přenosu MPLS značek. Není zde potřeba žádný signalizační protokol jako LDP. Jakákoliv topologie bude zálohována (pokud je to fyzicky možné) bez

nutnosti konfigurace. Zálohou je myšleno jak zálohovaní linek mezi směrovači, tak směrovačů samotných. (29)

Datová síť vyžívající segment-routing je rozdělena na segmenty dvou druhů. Prvním druhem je definovaný segment, administrátorsky určený pomocí označení NODE-SID, jehož označení je globální. Druhý typ segmentu je označován ADJ-SID (Adjacency SID), který má pouze lokální funkci a jeho značka je tedy přepisována, (29)

Jak již bylo zmíněno výše, NODE-SID je globálním označení směrovače. Takových označení může být teoreticky více, ale z důvodu přehlednosti to v praxi není doporučováno. K označení dochází pomocí labelů z MPLS, proto je potřeba tyto labely vyčlenit pro segment-routing. (29)

Určení labelů pro segment-routing:

```
mpls-labels
        sr-labels start 20000 end 30000
exit
```

Definice NODE-SID je tvořena na základě rezervovaných značek pro segment – routing a identifikátoru v datové síti. Jako identifikátor byly určeny poslední 4 číslice z IP adresy Loopbacku ve směrovacím protokolu ISIS. (29)

```
isis 0
        ...
        loopfree-alternates                     //určeno pro 7750
                ti-lfa
                node-protect
        loopfree-alternate ti-lfa               //určeno pro 7705
        exit
        exit
        interface "system"
                ipv4-node-sid index 1189
                no shutdown
         exit
        segment-routing
                micro-loop-avoidance            //pouze pro 7750
```

```
        prefix-sid-range global
        no shutdown
    exit
```

5.6 Konfigurace přenosu datových služeb typu L3

Konfigurace přenosu služeb typu L3 je prováděna ve směrovačích v sekci „Service“, kde je možné vybírat z celého portfolia služeb. Oddělením konfiguračních prostředí ve směrovači je dosaženo minimalizace poškození chybnou konfigurací na úrovni směrování. Směrování je upravováno minimálně a pouze po velmi přesných krocích. Konfigurace služeb může být svěřena do péče i méně zkušeným administrátorům. V případě konfigurační chyby u služby je omezena pouze služba, které se daná konfigurace týká, nikoliv celý směrovač. (29)

Služby na směrovačích Nokia jsou určovány pomocí vytváření VPRN (obdoba VRF). Každá VPRN má vlastní identifikátor, může být omezována pomocí politiky a také zálohována mezi více směrovači. VPRN spolu komunikují na základě funkční komunikace vnitřního BGP protokolu, který obstarává přenos dat pomocí svých tunelů. Tunely jsou různých typů, a proto je potřeba rozlišovat, přes který tunel budou data posílána. V případě definice všech typů transportních tunelů do rozlišovacího filtru je potřeba mít na paměti hodnoty priority tunelu. (29)

Vytváření služeb ve směrovači je spojeno s definicí zákazníka, pro nějž je služba realizována. V tomto konkrétním návrhu si zadavatel „vystačí“ s Customer 1. Konfigurace samotné VPRN pro L3 služby je založena na unikátním čísle pro VPRN (VRF), čísle autonomního systému, identifikaci route-distinguisher a interface se zvolenou adresací pro danou VPRN. (29)

Konfigurace na směrovačích typu PE je stejná. Dochází jen k logickým změnám v route-distinguisher a interface s použitou IPv4 adresou z adresního plánu. V rámci realizace konfigurace nesmí dojít ke shodě na více směrovačích, v tomto případě by nebylo možné doručit řádně požadovanou informaci od uživatele. Konfigurace na páteřních

směrovačích typu P není potřeba, neboť tyto směrovače jsou primárně určeny pro jiné funkce. (29)

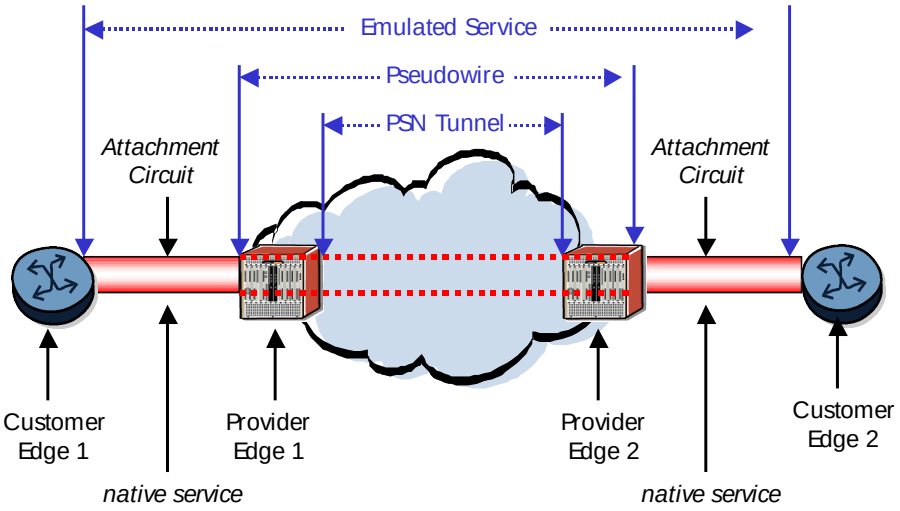
Konfigurace VPRN 10:

```
vprn 10 customer 1 create                    //vytvoření VPRN
  description "TEST"
  autonomous-system 65432                    //číslo AS
  route-distinguisher 10.20.1.189:10         //definovaná hodnota IP:Service
  auto-bind-tunnel
    resolution-filter                        //druhy tunelu pro přenos dat
      ldp
      rsvp
      sr-isis
    exit
    resolution filter
  exit
  interface "IPEKO" create                   //vytvořený interface
    address 10.21.189.1/26                   //adresace
    sap 1/1/1 create                         //fyzické rozhraní služby
    exit
  exit
  no shutdown
exit
```

Službu VPRN lze zakončit na fyzickém portu směrovače v různých konfiguracích. Zejména se jedná o tagování či netagování datového provozu na interface připojených ve VPRN. Další možností je službu zakončit do virtuálního switche (VPLS) - díky tomuto zakončení je možné v rámci směrovače vytvořit virtuální switch, který dokáže komunikovat s rozhraním ve VPRN a několika fyzickými porty na směrovači. Další zajímavou možností je záloha výchozí brány, a to adresací z VPRN mezi několika boxy. Jedná se zejména o vytváření zálohy výchozí brány pro různé druhy provozů. Využívá se technologie VRRP pro interface ve VPRN. (29)

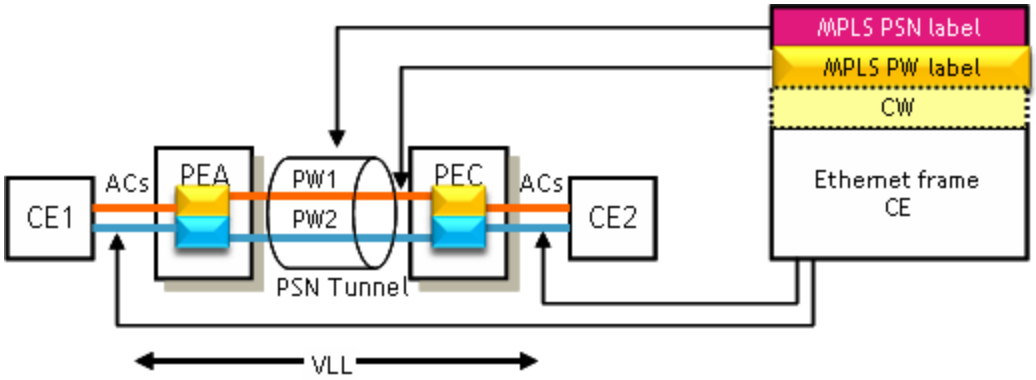
5.7 Konfigurace přenosu datových služeb L2

Služba byla definována IETF pracovní skupinou Pseudo Wire Emulation Edge-to-Edge (PWE3), zodpovědnou za vývoj standardů pro emulaci různých druhů služeb přes obecnou paketovou síť PSN (Paket Switched Network). Referenční model takové služby je zobrazen na následujícím obrázku. (29)



Obrázek 9 - Referenční model PWE3 (29)

Zákaznické směrovače nebo přepínače (CE) jsou připojeny ke směrovačům poskytovatele (PE) přes připojený okruh (AC). PE směrovače mají mezi sebou vytvořeny virtuální tunely přes datovou síť, aby bylo možné přenášet komunikace stejně, jako kdyby bylo spojení realizováno fyzickým připojením přímo mezi zákazníky. Veškerý provoz z CE (zařízení zákazníka) je zapouzdřen do MPLS tunelu, který je definován při konfiguraci PWE. Aby nemusela páteřní síť spravovat status mnoha virtuálních okruhů PWE, jsou jednotlivé rámce v PWE označovány značkou (Pseudowire Label), identifikující konkrétní PWE/službu, která je použita jako demultiplexor paketů na cílovém PE směrovači. Protokol používaný na signalizaci PWE značky je určen dle druhu použitého tunelu. (23; 29)



Obrázek 10 - VLL servis (29)

Na směrovačích typu PE je PWE3 služba označována jako Virtual Leased Line (VLL) nebo epipe (Ethernet-pipe). Služba pro L2 provoz je nazývána VLL a při jejím vytváření je třeba definovat spojení Bod-Bod, tedy směrovač A se směrovačem B. Mezi těmito směrovači je vytvořen servisní tunel, označovaný jako SDP. Pro servisní tunel SDP je nutno definovat cílovou adresu a jakým protokolem budou přenášeny informace. Na základě znalosti SDP je potřeba definovat službu EPIPE, kde je potřeba zohlednit vstupní/výstupní port služby (zákaznická data) vytvořené SDP na cílové místo. Veškeré níže zobrazené konfigurace jsou konfigurace „Service“. Služba EPIPE bude konfigurována mezi PE1 a PE3. (29)

Konfigurace služby EPIPE je uvedena v porovnávací tabulce pro směrovač A, B.

Tabulka 3 - Konfigurace Epipe

Směrovač PE2	Směrovač PE3
EPIPE	
sdp 1003 create far-end 10.20.3.189 ldp keep-alive shutdown exit no shutdown exit epipe 2002003 customer 1 create Description TEST_EPIPE Service-Name EPIPE_TEST sap 1/1/1create no shutdown exit spoke-sdp 1003:2002003 create no shutdown exit no shutdown exit	sdp 1002 create far-end 10.20.2.189 ldp keep-alive shutdown exit no shutdown exit epipe 2002003 customer 1 create Description TEST_EPIPE Service-Name EPIPE_TEST sap 1/1/4 create no shutdown exit spoke-sdp 1002:2002003 create no shutdown exit no shutdown exit

Z uvedeného výpisu konfigurace je vidět definice servisního tunelu SDP. V rámci změny tunelu, který je využíván pro přenos v MPLS, lze vyžít RSVP a SR-ISIS. Následně je ve výpisu uvedena konfigurace EPIPE, kde jsou vidět již dříve zmíněné závislosti na SDP a rozhraní připojeného do EPIPE.

Výhodou služby EPIPE oproti službě VPLS je napodobení chování jako při fyzickém propojení zařízení. Směrovače přenášející data z EPIPE (na vstupu a výstupu) nepotřebují znát MAC adresu připojených zařízení. Takže můžeme říci, že služba EPIPE je bez zásahu do uživatelské komunikace určené k přenosu.

5.8 Testování datové sítě

Testování navržené a nakonfigurované datové sítě bude probíhat pomocí scénářů. Scénáře budou podobné pro oba druhy datového provozu v rámci zadání diplomové práce. V rámci funkční a ustálené konfigurace bude navíc simulována závada na datovém okruhu pomocí jeho administrativního přerušení. Tímto přerušením dojde k přepočítání směrovacích cest a k jejich novému ustálení. V rámci testování funkčnosti dojde k přerušení na trase pro každý scénář celkem dvakrát, a to s cílem otestovat všechny transportní tunely, které byly zmíněny v teoretické části diplomové práce. Datová síť je tvořena pro rychlou konvergenci, a proto je zde předpoklad, že k výpadkům bude docházet v minimálním množství. Mezi konfigurační změnou volby transportního tunelu dojde k oživení přerušené linky do původního stavu, čímž budou zachovány podmínky pro všechny testy. Měření doby výpadku bude realizováno pomocí aplikace iperf v 3.9, která bude vždy na každém z notebooků, které budou součástí testování. Pro testování datového provozu typu L3 budou notebooky komunikovat pomocí adresace z VPRN 10, která je na každém směrovači jedinečná. Testování datového provozu typu L2 bude realizováno taktéž pomocí dvou notebooků, které budou označeny adresou IPv4 z jednoho subnetu, viz adresní plán IPv4.

Cílem testování nakonfigurované datové sítě je ověření splnění zadání diplomové práce, tedy funkčního přenosu dat mezi lokalitami pro druhy L2 a L3. Dále budou v rámci testování ověřeny typy transportních tunelů a jejich chování při přerušení topologie. Pro ověření výše zmíněných parametrů byly zvoleny směrovače PE2 a PE3. Tyto směrovače jsou vzájemně propojeny pomocí páteřních směrovačů typu P.

Před samotným testováním jsem provedl úpravu směrování pomocí vhodně zvolené metriky (level 2, metric 10000). Cílem této úpravy je dosažení stavu, kdy směrovače v trase PE3 – PE2, budou nuceny při výpadku portu na směrovači PE3 otočit trasu toku dat (nebude docházet pouze k lokální opravě na směrovači PE3). Na směrovači PP1 byla ponížena kvalita linek ve prospěch linky směřující na směrovač PE3. Testování bude prováděno pomocí administrativních zásahů ve směrovači s označením PE3, který má redundantní připojení ke zbytku datové sítě. Komunikace proti směrovači PE2 je primárně směrována na port 1/1/8, záložním portem je port 1/2/8. Přerušován bude port 1/1/8. Ověření dostupnosti

služby bude realizováno pomocí aplikace iperf v 3.9. Při testování datového provozu L3 bude využita sada notebooků, které budou připojeny ke směrovači PE3 a PE2 do VPRN 10 jako koncový uživatelé. Testování pro L3 bude tedy z notebooku ve VPRN 10, směrovač PE3 oproti notebooku ve VRPN10, směrovače PE2. Testování pro L2 bude provedeno na službě EPIPE, s označením 2002003, která vytváří virtuální spojení mezi definovanými porty směrovačů PE2 a PE3. Testování bude realizováno pomocí dvou notebooků, přičemž každý z nich bude připojen na jeden ze směrovačů. Protože se jedná o L2 službu, budou notebooky adresovány ze stejného subnetu. Komunikace bude tedy probíhat přímo mezi těmito notebooky.

5.8.1 Testování datové provozu typu L2

Testování provozu pro režim L2 je možné znázornit na službě EPIPE, která vytváří pseudowire tunel mezi danými porty směrovačů. Konfigurace tunelu EPIPE je ovlivněna pomocí konfigurace zvolené transportní metody v SDP. Před samotným testováním dochází k ověření stavu služby EPIPE pomocí příkazu „show service id 2002003 base“, kde je potvrzena funkčnost L2 tunelu.

```
*A:PAPOLY-189PE3# show service id 2002003 base

===============================================================================
Service Basic Information
===============================================================================
Service Id        : 2002003
Service Type      : Epipe
Name              : EPIPE_TEST
Description       : TEST_EPIPE
Customer Id       : 1                   Creation Origin   : manual
Last Status Change: 03/24/2023 12:58:21
Last Mgmt Change  : 03/24/2023 12:41:16
Admin State       : Up                  Oper State        : Up
MTU               : 1514
Vc Switching      : False
SAP Count         : 1                   SDP Bind Count    : 1
Per Svc Hashing   : Disabled
TEID Hashing      : Disabled            L4 Hashing        : Disabled
Force QTag Fwd    : Disabled

-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                            Type         AdmMTU  OprMTU  Adm   Opr
-------------------------------------------------------------------------------
sap:1/1/4                             null         1514    1514    Up    Up
sdp:1002:2002003 S(10.20.2.189)       Spok         0       1770    Up    Up
===============================================================================
```

Obrázek 11 - Služba Epipe

Samotné testování bylo realizováno pro EPIPE 2002003 s parametrem transportního tunelu v SDP pro LDP a SR-ISIS. Pro každý tunel bylo prováděno testování pomocí aplikace iperf v3.9 s nastavením:

NB1: iperf3 -s

NB2: iperf3 -c 192.168.0.1 -u -b 20M -t 300s -i 0.1s --logfile EPIPE_LDP

NB2: iperf3 -c 192.168.0.1 -u -b 20M -t 300s -i 0.1s --logfile EPIPE_SR-ISIS

Z výše uvedených parametrů aplikace ipref vyplívá, provedení testování pomocí UDP provozu, datový tok 20 Mbps, doba testování 300 sekund a interval mezi vzorky.

```
===============================================================================
Service Destination Point (Sdp Id : 1003) Details
===============================================================================
-------------------------------------------------------------------------------
 Sdp Id 1003  -10.20.3.189
-------------------------------------------------------------------------------
Description          : (Not Specified)
SDP Id               : 1003                  SDP Source         : manual
Admin Path MTU       : 0                     Oper Path MTU      : 1770
Delivery             : MPLS
Far End              : 10.20.3.189
Tunnel Far End       : n/a                   LSP Types          : SR-ISIS

Admin State          : Up                    Oper State         : Up
Signaling            : TLDP                  Metric             : 0
Last Status Change   : 03/27/2023 16:47:46   Adv. MTU Over.     : No
Last Mgmt Change     : 03/27/2023 16:47:46   VLAN VC Etype      : 0x8100
Flags                : None
```

Obrázek 12 - Směrovač PE2, type SR-ISIS

```
===============================================================================
Service Destination Point (Sdp Id : 1002) Details
===============================================================================
-------------------------------------------------------------------------------
 Sdp Id 1002  -10.20.2.189
-------------------------------------------------------------------------------
Description          : (Not Specified)
SDP Id               : 1002                  SDP Source         : manual
Admin Path MTU       : 0                     Oper Path MTU      : 1770
Delivery             : MPLS
Far End              : 10.20.2.189
Tunnel Far End       : n/a                   LSP Types          : SR-ISIS

Admin State          : Up                    Oper State         : Up
Signaling            : TLDP                  Metric             : 0
Last Status Change   : 03/27/2023 16:42:33   Adv. MTU Over.     : No
Last Mgmt Change     : 03/27/2023 16:42:33   VLAN VC Etype      : 0x8100
Flags                : None

Mixed LSP Mode Information :
Mixed LSP Mode       : Disabled              Active LSP Type    : SR-ISIS
```

Obrázek 13 - Směrovač PE3, type SR-ISIS

Testování bylo provedeno celkem dvakrát, kdy jedno měření proběhlo pro tunel LDP a druhé pro SR-ISIS. Níže jsou zobrazeny výsledky z aplikace iperf. Po dobu každého měření byl simulován výpadek primární linky spojení (směrovač PE3, port 1/1/8). Tento výpadek byl realizován po 40 s, k obnovení provozu primárním portem došlo během dalších 40 s. Takto byl výpadek simulován třikrát.

Tabulka 4 – L2 měření s LDP

[ID]	Interval [s]	Transfer [MBytes]	Bitrate [Mbps]	Jitter [ms]	Lost/Total Datagrams		Směr
[1]	0.00-300.00	715	20.0	0.000	0/513678	0%	sender
[1]	0.00-300.05	712	19.9	0.243	2445/513674	0.48%	receiver

Tabulka 5 – L2 měření s SR-ISIS

[ID]	Interval [s]	Transfer [MBytes]	Bitrate [Mbps]	Jitter [ms]	Lost/Total Datagrams		Směr
[2]	0.00-300.00	715	20.0	0.000	0/513686	0%	sender
[2]	0.00-300.05	715	20.0	0.143	161/513686	0.031%	receiver

Z výsledků měření pomocí aplikace iperf, je patrné, k jaké docházelo ztrátě dat při změně ve směrovacích tabulkách. Transportní tunel LDP zahazoval největší množství dat. Transportní tunel SR-ISIS využil možnosti alternativních tras a minimalizoval množství ztracených dat. Z měření vychází jako nejlepší varianta pro přenos dat typu L2 tunel SR-ISIS.

5.8.2 Testování datového provozu typu L3

Ověření správné konfigurace pro režim L3, tedy využití služby VPRN, bylo provedeno dle výpisu směrovací tabulky. Směrovací tabulka zohledňuje informace o dostupných prefixech a použité transportní tunely. Na obrázcích pod tímto textem jsou uvedeny směrovací tabulky směrovače PE2, služba VPRN. V pořadí pro použité transportní tunely LDP, RSVP a SR-ISIS.

```
===============================================================================
Route Table (Service: 10)
===============================================================================
Dest Prefix[Flags]                              Type    Proto     Age        Pref
      Next Hop[Interface Name]                                    Metric
-------------------------------------------------------------------------------
10.21.189.0/26                                  Remote  BGP VPN   01h06m04s  170
       10.20.1.189 (tunneled)                                       0
10.21.189.64/26                                 Local   Local     80d01h33m  0
       IPEKO                                                        0
10.21.189.128/26                                Remote  BGP VPN   00h08m06s  170
       10.20.3.189 (tunneled)                                       0
10.229.191.0/24                                 Remote  BGP VPN   00h08m06s  170
       10.20.3.189 (tunneled)                                       0
192.168.189.0/30                                Remote  BGP VPN   01h06m04s  170
       10.20.1.189 (tunneled)                                       0
-------------------------------------------------------------------------------
```

Obrázek 14 - Směrovač PE2, VRPN 10 LDP

```
===============================================================================
Route Table (Service: 10)
===============================================================================
Dest Prefix[Flags]                              Type    Proto     Age        Pref
      Next Hop[Interface Name]                                    Metric
-------------------------------------------------------------------------------
10.21.189.0/26                                  Remote  BGP VPN   00h00m03s  170
       10.20.1.189 (tunneled:SR-ISIS:0)                             0
10.21.189.64/26                                 Local   Local     80d02h04m  0
       IPEKO                                                        0
10.21.189.128/26                                Remote  BGP VPN   00h00m03s  170
       10.20.3.189 (tunneled:SR-ISIS:0)                             0
10.21.189.192/26                                Remote  BGP VPN   00h00m03s  170
       10.20.4.189 (tunneled:SR-ISIS:0)                             0
10.229.189.96/27                                Remote  BGP VPN   00h00m03s  170
       10.20.4.189 (tunneled:SR-ISIS:0)                             0
10.229.191.0/24                                 Remote  BGP VPN   00h00m03s  170
       10.20.3.189 (tunneled:SR-ISIS:0)                             0
192.168.189.0/30                                Remote  BGP VPN   00h00m03s  170
       10.20.1.189 (tunneled:SR-ISIS:0)                             0
-------------------------------------------------------------------------------
```

Obrázek 15 - Směrovač PE2, VPRN 10 RSVP

Ověření komunikace notebooků mezi sebou proběhlo po kontrole směrovacích tabulek služby VPRN. Ověření spojení bylo provedeno pomocí příkazové řádky a služby PING. Notebook 1 byl připojen na směrovač PE3 s IPv4 adresou 10.21.189.140/26, notebook 2 byl připojen na směrovač PE2 s IPv4 adresou 10.21.189.80/26.

```
===============================================================================
Route Table (Service: 10)
===============================================================================
Dest Prefix[Flags]                              Type    Proto     Age        Pref
     Next Hop[Interface Name]                                       Metric
-------------------------------------------------------------------------------
10.21.189.0/26                                  Remote  BGP VPN   00h00m05s  170
       10.20.1.189 (tunneled:RSVP:61441)                            0
10.21.189.64/26                                 Local   Local     80d01h57m  0
       IPEKO                                                        0
10.21.189.128/26                                Remote  BGP VPN   00h00m05s  170
       10.20.3.189 (tunneled:RSVP:61442)                            0
10.229.191.0/24                                 Remote  BGP VPN   00h00m05s  170
       10.20.3.189 (tunneled:RSVP:61442)                            0
192.168.189.0/30                                Remote  BGP VPN   00h00m05s  170
       10.20.1.189 (tunneled:RSVP:61441)                            0
-------------------------------------------------------------------------------
```

Obrázek 16 - Směrovač PE2, VPRN 10 SR-ISIS

Pro měření byla použita aplikace iperf v3.9. v režimu klient-server. V rámci aplikace byla provedena specifikace parametrů. Jedná se o parametry UDP provoz, datový tok 20 Mbps, doba testování 300 sekund a interval mezi vzorky. Pro testováni byly použity následující příkazy:

NB1: iperf3 -s
NB2: iperf3 -c 10.21.189.140 -u -b 20M -t 300s -i 0.1s --logfile VPRN_LDP
NB2: iperf3 -c 10.21.189.140 -u -b 20M -t 300s -i 0.1s --logfile VPRN_RSVP
NB2: iperf3 -c 10.21.189.140 -u -b 20M -t 300s -i 0.1s --logfile VPRN_SR-ISIS

Testování bylo provedeno celkem třikrát, kdy jedno měření proběhlo pro tunel LDP, druhé pro RSVP a poslední pro SR-ISIS. Níže jsou zobrazeny výsledky z aplikace iperf. Po dobu každého měření byl simulován výpadek primární linky spojení (směrovač PE3, port 1/1/8). Tento výpadek byl realizován po 40 s, k obnovení provozu primárním portem došlo během dalších 40 s. Takto byl výpadek simulován třikrát u každého měření.

Tabulka 6 – L3 měření s LDP

[ID]	Interval [s]	Transfer [MBytes]	Bitrate [Mbps]	Jitter [ms]	Lost/Total Datagrams		Směr
[3]	0.00-300.00	715	20.0	0.000	0/513694	0%	sender
[3]	0.00-300.04	714	20.0	0.215	908/513684	0.18%	receiver

Tabulka 7 - Měření s RSVP

[ID]	Interval [s]	Transfer [MBytes]	Bitrate [Mbps]	Jitter [ms]	Lost/Total Datagrams		Směr
[4]	0.00-300.01	715	20.0	0.000	0/513684	0%	sender
[4]	0.00-300.05	715	20.0	0.225	17/513684	0.0033%	receiver

Tabulka 8 - Měření s SR-ISIS

[ID]	Interval [s]	Transfer [MBytes]	Bitrate [Mbps]	Jitter [ms]	Lost/Total Datagrams		Směr
[5]	0.00-300.00	715	20.0	0.000	0/513682	0	sender
[5]	0.00-300.04	715	20.0	0.116	360/513682	0.07%	receiver

Z výsledků měření pro přenos dat v režimu L3 je patrné, že nejlépe dopadl přenos dat pomocí tunelu RSVP. V případě porovnání výsledků s ostatními tunely a porovnání s časovou náročností daných konfigurací, vychází nejlépe využití tunelu SR-ISIS.

6 Závěr

Při realizaci návrhu datové sítě se zaměřením na přenosy L2 a L3 provozů (Ethernet) mezi vzdálenými lokalitami došlo k nastínění komplexní problematiky takového návrhu. Návrh datové sítě se odvíjí od požadavků na konkrétní síť, tedy High Level Design (HLD), který udává cílovou činnost datové sítě. Až pokud je správně nastaven HLD, může začít vznikat Low Level Design, který je pomyslnou kuchařkou pro implementaci komplexního řešení. Pro návrh datové sítě byly zvoleny parametry spolehlivosti pro doručení a rychlost reakcí na změny v síti. Rychlou změnu v rámci datové sítě je možné zvolit s co nejrychlejšími parametry, protože se jedná o interní uzavřenou síť, která nepotřebuje reagovat na obsáhlé směrovací záznamy z veřejného internetu.

V rámci návrhu došlo k zaměření na primární oblasti konfigurace, jako byla konfigurace vnitřního směrovacího protokolu, sestavení funkčního prostředí MPLS a vnitřního BGP za účelem přenosu VRPN sítí. V rámci návrhu nebyly blíže rozepisovány konfigurace směrovačů v oblasti zabezpečení, komunikace vůči dohledovým nástrojům, nastavení NTP a logování. Veškeré tyto informace jsou dostupné v přílohách č.1 a č. 2. Při konfiguraci došlo k úmyslnému vynechání bezpečností aplikace pro směrovací protokol IS-IS, RSVP. Návrh datové sítě by byl o něco komplikovanější, protože by bylo nutné rozebrat jakým způsobem funguje proprietární dohledový nástroj od výrobce Nokia, pomocí nějž je možné spravovat mnoho bezpečnostních prvků na směrovačích.

Pro přenos dat v režimu L3 byla využita služba VPRN, která je obdobou VRF. Jedná se o vytvoření ploché datové sítě, která komunikuje pomocí BGP a následuje topologii IGP (alespoň pokud není provedeno administrativní upravení topologie). V rámci VPRN 10 byla pomocí směrovacích tabulek při každé změně transportního tunelu ověřena funkčnost VPRN. Měření spolehlivosti přenosové trasy proběhlo pomocí aplikace iperf mezi dvěma notebooky, které simulovali uživatelský provoz. Transportní tunely fungovaly dle očekávání, kdy nejhorším, respektive nejméně spolehlivým tunelem se ukázal být LDP tunel, který při výpadku primárná linky z testovaného směrovače byl nucen provést přepočet jiné cesty. Při těchto změnách docházelo ke ztrátě dat. Při testování dalších transportních tunelů byly výsledky velmi podobné. Nejspolehlivějším tunel při měření přenosu dat v L3 režimu byl tunel RVPS-TE, který si nejlépe poradil se zálohou primární trasy. Při porovnání

administrativní náročnosti údržby RSVP-TE oproti SR-ISIS je efektivnější využívání SR-ISIS, který konfiguračně jednodušší. Předpokladem funkčnosti SR-ISIS je plná podpora tohoto řešení.

Pro přenos dat v režimu L2 byla využita služba z části VLL, přesně EPIPE. Jedná se o vytvoření virtuálního datového okruhu mezi dvěma směrovači. Výhodou služby EPIPE je její chování, které simuluje fyzické propojení daných zařízení (v konkrétním případě této diplomové práce pak propojení dvou notebooků). V rámci přenosu dat L2 pro EPIPE byla ověřena realizace služby a její funkčnosti na základě ICMP mezi danými notebooky. Služba byla vždy v pořádku spojena. V rámci otestování transportních tunelů dané služby byly využity tunely LDP a SR-ISIS. Měřením bylo dosaženo výsledků, kdy transport pomocí LDP byl velmi náchylný na změnu v přenosové trase. Druhé měření pro tunel SR-ISIS byl téměř bez chybný. Pro uživatele je nejvhodnější provoz pomocí tunelu SR-ISIS.

Organizace, v níž se zabývám přenosem datových služeb zákazníků (uživatelů), se potýkala se značnými problémy při přenosu L2 služeb pomocí datové sítě Ethernet. Dříve byl využíván protokol LDP, který je velmi jednoduše konfigurovatelný a není potřeba vynaložit mnoho lidského času při jeho používání. Bohužel protokol LDP se v praxi neosvědčil zejména pro přenos L2 služeb, kdy docházelo k rozpadání spojení. Vylepšením V současnosti jako nejlepší přenosové tunely pro provozy typu L2 využíváme segment routingu, který poskytuje výhodu zálohováni nodu. Díky segmentu routingu není potřeba pro každou záložní datovou linku nic upravovat či definovat, vše se odehrává na základě IGP a zvolených metrik.

7 Seznam použitých zkratek

SNA	Systems Network Architecture
ISO	International Organization for Standardization
OSI	Open Systems Interconnection
TCP/IP	Transmission Control Protocol over Internet Protocol
ARPANET	Advanced Research Projects Agency NETwork
TCP	Transmission Control Protocol
UDP	User Datagram Protocol)
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
TELNET	Teletype Network
SSH	Secure Shell
WWW	World Wide Web
VPRN	Virtual Private Routed Network
VRF	Virtual Router
EPIPE	Ethernet Pipe
VPLS	Virtual Private LAN Service
IS-IS	Intermediate System to Intermediate System
BGP	Border Gateway Protocol
MPLS	Multi Protocol Label Switching
LDP	Label Distribution Protocol
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol – Traffic Engineering
SR-ISIS	Segment Routing - Intermediate System to Intermediate System
AS	Autonomous System
TTL	Time to Live
QOS	Quality of Service
SFP	Small Form-factor Pluggable
OSPF	Open Shortest Path First
RIP	Routing Information Protocol

IGMP	Internet Group Management Protokol
SPF	Shortest Path First
MPLS-TE	Multi Protocol Label Switching - Traffic Engineering
MPLS-FRR	Multi Protocol Label Switching - Fast Reroute
TLDP	Targeted LDP
LSP	Label Switch Path
MP-BGP	Multiprotocol Border Gateway Protocol
VRRP	Virtual Router Redundancy Protocol
SAP	Service Aggregation Point
SDP	Service Distribution Path
VLL	Virtual Leased Line
IGP	Interior Gateway Protocol
LSA	Link State Advertisement
LSP	Label Switched Path
LSR	Label Switch Router
NTP	Network Time Protocol
PE	Provider Edge
RD	Route Distinguisher
RT	Route Target
SPF	Shortest Path First

8 Seznam použitých zdrojů

(1) What is Systems Network Architecture (SNA)?. *IBM Corporation* (online). (cit. 2023-03-25). Dostupné z: https://www.ibm.com/docs/en/zos-basic-skills?topic=implementation-what-is-systems-network-architecture-sna

(2) DECnet. In: *Wikipedia: the free encyclopedia* (online). San Francisco (CA): Wikimedia Foundation, 2001- (cit. 2023-03-25). Dostupné z: https://en.wikipedia.org/wiki/DECnet

(3) ISO/IEC 7498-1:1994. *International Organization for Standardization* (online). Ženeva: ISO, 1994 (cit. 2023-03-25). Dostupné z: https://www.iso.org/standard/20269.html

(4) SOCOLOFSKY, T. a C. KALE. A TCP/IP Tutorial. *RFC Editor* (online). Edinburgh: Spider Systems Limited, 1991 (cit. 2023-03-25). Dostupné z: https://www.rfc-editor.org/rfc/rfc1180

(5) SOCHOR, Tomáš. *POČÍTAČOVÉ SÍTĚ 2*. Ostrava, 2014. Skripta. Ostravská univerzita v Ostravě.

(6) BALLUCH, Andrej. Filtrace cest z protokolů třídy distance vector. Policy routing.: 1. Protokoly třídy Distance Vector. In: *VŠB Technická Univerzita Ostrava* (online). Ostrava, 2003 (cit. 2023-03-25). Dostupné z: https://www.cs.vsb.cz/grygarek/SPS/projekty0405/RouteOptimization/dokumentace/ar01s01.html

(7) BOUŠKA, Petr. TCP/IP - Routing - směrování. *Samuraj-cz* (online). Praha, 2007 (cit. 2023-03-25). Dostupné z: https://www.samuraj-cz.com/clanek/tcpip-routing-smerovani/

(8) RFC 791. *INTERNET PROTOCOL*. California: Information Sciences Institute University of Southern California, 1981.

(9) RFC 1918. Address Allocation for Private Internets. Network Working Group: IETF, 1996.

(10) IEEE802. IEEE 802 LMSC. Piscataway: IEEE Standards Association, 2016.

(11) IEEE802.1Q. Standard Group MAC Addresses. Piscataway: IEEE Standards Association, 2014.

(12) IEEE802.3. Ethernet. Piscataway: IEEE Standards Association, 1983.

(13) 7705 SAR Routing Protocols Guide R20.4.R1. Nokia Documentation Center [online]. Espoo: Nokia, 2020, 29.2.2020 [cit. 2023-03-26]. Dostupné z: https://infocenter.nokia.com/public/7705SAR2041A/index.jsp?topic=/com.sar.routing_protocols/html/preface_routing_protocols.html

(14) ISO/IEC 10589:2002. Information technology. 2. Ženeva: International Organization for Standardization, 2002.

(15) MALAMUD, Carl. Analyzing Decnet/Osi Phase V. 1. Van Nostrand Reinhold Computer, 1991. ISBN 0442003757.

(16) RFC 1132. A Standard for the Transmission of 802.2 Packets over IPX Networks. 1. IETF, 1989.

(17) GORALSKI, Walter a Hannes GREDLER. The Complete IS-IS Routing Protocol. 1. Springer Science & Business Media, 2005. ISBN 1-85233-822-9.Traffic Engenering

(18) HECKMANN, Oliver. The Complete IS-IS Routing Protocol. 1. New York: John Wiley, 2006. ISBN 0470012935.

(19) GRYGAREK, Petr. Směrovací protokol BGP. In: VŠB Technická Univerzita Ostrava [online]. Ostrava, 2003 [cit. 2023-03-26]. Dostupné z: https://www.cs.vsb.cz/grygarek/SPS/lect/BGP/BGP.html

(20) RFC 4271. A Border Gateway Protocol 4 (BGP-4). 1. IETF, 2006.

(21) RFC 5396. Textual Representation of Autonomous System (AS) Numbers. 1. IETF, 2008.

(22) RFC 4364. BGP/MPLS IP Virtual Private Networks (VPNs). 1. IETF, 2006.

(23) PEPELNJAK, Ivan a Jim GUICHARD. MPLS and VPN Architectures. 1. Cisco Systems, 2002. ISBN 1587050811.

(24) 7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide 20.2.R1. Nokia Documentation Center [online]. Espoo: Nokia, 2020, 28.2.2020 [cit. 2023-03-26]. Dostupné z:

https://infocenter.nokia.com/public/7750SR202R1A/index.jsp?topic=/com.sr.unicast/html/getstarted.html

(25) Nokia 7750 SR-a Service Router. In: ALE [online]. Espoo: Nokia, 2022 [cit. 2023-03-26]. Dostupné z: https://www.al-enterprise.com/-/media/assets/internet/documents/ale-nokia-7750-sr-a-service-router-ip-mpls-datasheet-en.pdf

(26) Nokia 7705 Service Aggregation Router. In: Nokia Documentation Center [online]. Espoo: Nokia, 2022 [cit. 2023-03-26]. Dostupné z: https://onestore.nokia.com/asset/162833

(27) RFC 5036. LDP Specification. 1. IETF, 2007.

(28) RFC 3209. RSVP-TE: Extensions to RSVP for LSP Tunnels. 1. IETF, 2001.

(29) 7705 SERVICE AGGREGATION ROUTER | RELEASE 20.4.R1: 3HE 16307 AAAA TQZZA. In: Nokia Documentation Center [online]. Espoo: Nokia, 2020, 1 [cit. 2023-03-26]. Dostupné z: https://documentation.nokia.com/cgi-bin/dbaccessfilename.cgi/3HE16307AAAATQZZA01_V1_7705%20SAR%20Routing%20Protocols%20Guide%2020.4.R1.pdf

(30) JASEN, Arnold. How to build better IP services with segment routing. Nokia Documentation Center [online]. Espoo: Nokia, 2021, 14.10.2021 [cit. 2023-03-26]. Dostupné z: https://www.nokia.com/blog/how-to-build-better-ip-services-with-segment-routing/

(31) RFC 8402. Segment Routing Architecture. 1. IETF, 2018.

(32) RFC 9256. Segment Routing Policy Architecture. 1. IETF, 2022.

(33) OFFNFOPT. Model ISO/OSI. In: Wikipedie [online]. Praha, 2023 [cit. 2023-03-26]. Dostupné z: https://cs.wikipedia.org/wiki/Referen%C4%8Dn%C3%AD_model_ISO/OSI#/media/Soubor:OSI_Model_v1.svg

(34) Ethernetový rámec. In: Wikipedie [online]. Praha, 2022 [cit. 2023-03-26]. Dostupné z: https://cs.wikipedia.org/wiki/Ethernetov%C3%BD_r%C3%A1mec

9 Seznam obrázků

10 Seznam tabulek

11 Přílohy

11.1 Příloha č. 1 Konfigurace směrovače typu P

```
# TiMOS-C-20.5.R2 cpm/hops64 Nokia 7750 SR Copyright (c) 2000-2020 Nokia.
# All rights reserved. All use subject to applicable license agreements.
# Built on Wed Jun 17 13:12:36 PDT 2020 by builder in /builds/c/205B/R2/panos/main/sros
# Configuration format version 20.5 revision 0

# Generated WED MAR 29 07:44:10 2023 UTC

exit all
configure
#--------------------------------------------------
echo "System Configuration"
#--------------------------------------------------
    system
        name "PAPOLY-189PP1"
        snmp
            streaming
                no shutdown
            exit
            packet-size 9216
        exit
        time
            ntp
                no shutdown
            exit
            sntp
                shutdown
            exit
            dst-zone CEST
                start last sunday march 02:00
                end last sunday october 03:00
```

```
        exit
        zone CET
      exit
   exit
#------------------------------------------------
echo "System Security Configuration"
#------------------------------------------------
   system
      security
         password
            authentication-order local
         exit
         user "polygon"
            password
"XXy$10$WB0.GXPqDLOoigsEA5Cq6.BiXu6V8TTLlJj0ULq1Ahdg9WnErsxXX"
            access console snmp
            console
               member "default"
               member "administrative"
            exit
         exit
         user "dohled_snmp"
            password
"XXy$10$m/Z7MJQvHZr9WQ.LQw.RM.mlxEI.MmzVn1.1PpxEp/.8mj8oL.iXX"
            access snmp
            snmp
               authentication hash2 sha
XXhzM6SOnn6apEFONhWqutmOo5rw4CXlnLVtW9mQ1+b3VxXX privacy aes-128-
cfb-key XXrM4RHT0SCftYqOjEri/LgtT0sURwhpDcy30wLXmXX=
               group "snmp-ro"
            exit
         exit
```

```
        snmp
            access group "snmp-ro" security-model usm security-level privacy read "iso"
        exit
        ssh
            preserve-key
        exit
        per-peer-queuing
        dist-cpu-protection
            policy "_default-access-policy" create
            exit
            policy "_default-network-policy" create
            exit
        exit
    exit
#------------------------------------------------
echo "Log Configuration"
#------------------------------------------------
    log
        event-control "igmp" 2005 suppress
        event-control "vrtr" 2034 generate
        syslog 1
            description "log server"
            address 10.20.189.30
        exit
        snmp-trap-group 11
            description "dohled_snmp"
            trap-target "dohled_snmp" address 10.20.189.29 snmpv3 notify-community
"dohled_snmp" security-level privacy
        exit
        log-id 1
            description "log server"
```

```
            from main security
            to syslog 1
            no shutdown
        exit
        log-id 11
            description "dohled_snmp"
            from main security
            to snmp
            no shutdown
        exit
    exit
#--------------------------------------------------
echo "Card Configuration"
#--------------------------------------------------
    card 1
        card-type iom-a
        mda 1
            mda-type maxp10-10gb-sfp+
            sync-e
            no shutdown
        exit
        mda 2
            mda-type ma44-1gb-csfp
            sync-e
            no shutdown
        exit
        no shutdown
    exit
#--------------------------------------------------
echo "Port Configuration"
#--------------------------------------------------
    port 1/1/1
```

```
    description "toPAPOLY-189PE1"
    ethernet
        mtu 1800
        lldp
            dest-mac nearest-bridge
                admin-status tx-rx
                tx-tlvs port-desc sys-name sys-desc
            exit
        exit
        hold-time up 5
        ssm
            no shutdown
        exit
    exit
    no shutdown
exit
port 1/1/2
    description "toPAPOLY-189PE2"
    ethernet
        mtu 1800
        lldp
            dest-mac nearest-bridge
                admin-status tx-rx
                tx-tlvs port-desc sys-name sys-desc
            exit
        exit
        hold-time up 5
        ssm
            no shutdown
        exit
    exit
    no shutdown
```

```
exit
port 1/1/3
    shutdown
    ethernet
    exit
exit
port 1/1/4
    shutdown
    ethernet
    exit
exit
port 1/1/5
    description "toPAPOLY-189PP2"
    ethernet
        mtu 1800
        lldp
            dest-mac nearest-bridge
                admin-status tx-rx
                tx-tlvs port-desc sys-name sys-desc
            exit
        exit
        hold-time up 5
    exit
    no shutdown
exit
port 1/1/6
    shutdown
    ethernet
    exit
exit
port 1/1/7
    shutdown
```

```
    ethernet
    exit
exit
port 1/1/8
    shutdown
    ethernet
    exit
exit
port 1/1/9
    shutdown
    ethernet
    exit
exit
port 1/1/10
    shutdown
    ethernet
    exit
exit
port 1/2/1
    description "toPAPOLY-189PE3"
    ethernet
        mtu 1800
        lldp
            dest-mac nearest-bridge
                admin-status tx-rx
                tx-tlvs port-desc sys-name sys-desc
            exit
        exit
        hold-time up 5
    exit
    no shutdown
exit
```

```
port 1/2/2
    shutdown
    ethernet
    exit
exit
port 1/2/3
    shutdown
    ethernet
    exit
exit
port 1/2/4
    shutdown
    ethernet
    exit
exit
port 1/2/5
    shutdown
    ethernet
    exit
exit
port 1/2/6
    shutdown
    ethernet
    exit
exit
port 1/2/7
    shutdown
    ethernet
    exit
exit
port 1/2/8
    shutdown
```

```
    ethernet
    exit
exit
port 1/2/9
    shutdown
    ethernet
    exit
exit
port 1/2/10
    shutdown
    ethernet
    exit
exit
port 1/2/11
    shutdown
    ethernet
    exit
exit
port 1/2/12
    shutdown
    ethernet
    exit
exit
port 1/2/13
    shutdown
    ethernet
    exit
exit
port 1/2/14
    shutdown
    ethernet
    exit
```

```
exit
port 1/2/15
   shutdown
   ethernet
   exit
exit
port 1/2/16
   shutdown
   ethernet
   exit
exit
port 1/2/17
   shutdown
   ethernet
   exit
exit
port 1/2/18
   shutdown
   ethernet
   exit
exit
port 1/2/19
   shutdown
   ethernet
   exit
exit
port 1/2/20
   shutdown
   ethernet
   exit
exit
port 1/2/21
```

```
    shutdown
    ethernet
    exit
exit
port 1/2/22
    shutdown
    ethernet
    exit
exit
port 1/2/23
    shutdown
    ethernet
    exit
exit
port 1/2/24
    shutdown
    ethernet
    exit
exit
port 1/2/25
    shutdown
    ethernet
    exit
exit
port 1/2/26
    shutdown
    ethernet
    exit
exit
port 1/2/27
    shutdown
    ethernet
```

```
    exit
exit
port 1/2/28
    shutdown
    ethernet
    exit
exit
port 1/2/29
    shutdown
    ethernet
    exit
exit
port 1/2/30
    shutdown
    ethernet
    exit
exit
port 1/2/31
    shutdown
    ethernet
    exit
exit
port 1/2/32
    shutdown
    ethernet
    exit
exit
port 1/2/33
    shutdown
    ethernet
    exit
exit
```

```
port 1/2/34
   shutdown
   ethernet
   exit
exit
port 1/2/35
   shutdown
   ethernet
   exit
exit
port 1/2/36
   shutdown
   ethernet
   exit
exit
port 1/2/37
   shutdown
   ethernet
   exit
exit
port 1/2/38
   shutdown
   ethernet
   exit
exit
port 1/2/39
   shutdown
   ethernet
   exit
exit
port 1/2/40
   shutdown
```

```
        ethernet
        exit
    exit
    port 1/2/41
        shutdown
        ethernet
        exit
    exit
    port 1/2/42
        shutdown
        ethernet
        exit
    exit
    port 1/2/43
        shutdown
        ethernet
        exit
    exit
    port 1/2/44
        shutdown
        ethernet
        exit
    exit
#------------------------------------------------
echo "Redundancy Configuration"
#------------------------------------------------
    redundancy
        synchronize config
    exit
#------------------------------------------------
echo "Management Router Configuration"
#------------------------------------------------
```

```
    router management
    exit
#--------------------------------------------------
echo "Router (Network Side) Configuration"
#--------------------------------------------------
    router Base
        interface "system"
            address 10.20.7.189/32
            no shutdown
        exit
        interface "toPAPOLY-189PE1"
            address 10.20.11.245/30
            port 1/1/1
            bfd 10 receive 10 multiplier 3 type cpm-np
            no shutdown
        exit
        interface "toPAPOLY-189PE2"
            address 10.20.11.225/30
            port 1/1/2
            bfd 10 receive 10 multiplier 3 type cpm-np
            no shutdown
        exit
        interface "toPAPOLY-189PE3"
            address 10.20.11.229/30
            port 1/2/1
            bfd 10 receive 10 multiplier 3 type cpm-np
            no shutdown
        exit
        interface "toPAPOLY-189PP2"
            address 10.20.11.237/30
            port 1/1/5
            bfd 10 receive 10 multiplier 3 type cpm-np
```

```
        no shutdown
    exit
    autonomous-system 65432
    ip-fast-reroute
#------------------------------------------------
echo "MPLS Label Range Configuration"
#------------------------------------------------
    mpls-labels
        sr-labels start 20000 end 30000
    exit
#------------------------------------------------
echo "ISIS Configuration"
#------------------------------------------------
    isis 0
        level-capability level-2
        area-id 49.00
        authentication-key "XX333bVBBBW96Qi9Te4V34/yVQPX" hash2
        authentication-type message-digest
        traffic-engineering
        reference-bandwidth 100000000
        advertise-router-capability as
        loopfree-alternates
            ti-lfa
                node-protect
            exit
        exit
        timers
            spf-wait 2000 spf-initial-wait 50 spf-second-wait 100
        exit
        level 2
            wide-metrics-only
        exit
```

```
segment-routing
    micro-loop-avoidance
    prefix-sid-range global
    no shutdown
exit
interface "system"
    level-capability level-2
    ipv4-node-sid index 7189
    passive
    no shutdown
exit
interface "toPAPOLY-189PE2"
    level-capability level-2
    hello-authentication-key "XX333bVBBBW96Qi9Te4V39cngmN2" hash2
    hello-authentication-type message-digest
    interface-type point-to-point
    bfd-enable ipv4
    no shutdown
exit
interface "toPAPOLY-189PE1"
    level-capability level-2
    hello-authentication-key "XX333bVBBBW96Qi9Te4V318kDtvl" hash2
    hello-authentication-type message-digest
    interface-type point-to-point
    bfd-enable ipv4
    level 2
        metric 100000
    exit
    no shutdown
exit
interface "toPAPOLY-189PE3"
    level-capability level-2
```

```
            hello-authentication-key "XX333bVBBBW96Qi9Te4V3xG+y0Bs" hash2
            hello-authentication-type message-digest
            interface-type point-to-point
            bfd-enable ipv4
            no shutdown
        exit
        interface "toPAPOLY-189PP2"
            level-capability level-2
            hello-authentication-key "XX333bVBBBW96Qi9Te4V3347DF1l" hash2
            hello-authentication-type message-digest
            interface-type point-to-point
            bfd-enable ipv4
            level 2
                metric 100000
            exit
            no shutdown
        exit
        no shutdown
    exit
#--------------------------------------------------
echo "MPLS Configuration"
#--------------------------------------------------
    mpls
        resignal-timer 30
        interface "system"
            no shutdown
        exit
        interface "toPAPOLY-189PE2"
            no shutdown
        exit
        interface "toPAPOLY-189PE1"
            no shutdown
```

```
            exit
            interface "toPAPOLY-189PE3"
                no shutdown
            exit
            interface "toPAPOLY-189PP2"
                no shutdown
            exit
        exit
#--------------------------------------------------
echo "RSVP Configuration"
#--------------------------------------------------
        rsvp
            interface "system"
                no shutdown
            exit
            interface "toPAPOLY-189PE2"
                bfd-enable
                no shutdown
            exit
            interface "toPAPOLY-189PE1"
                bfd-enable
                no shutdown
            exit
            interface "toPAPOLY-189PE3"
                bfd-enable
                no shutdown
            exit
            interface "toPAPOLY-189PP2"
                bfd-enable
                no shutdown
            exit
            no shutdown
```

```
        exit
#------------------------------------------------
echo "MPLS LSP Configuration"
#------------------------------------------------
        mpls
            no shutdown
        exit
#------------------------------------------------
echo "LDP Configuration"
#------------------------------------------------
        ldp
            fast-reroute
            import-pmsi-routes
            exit
            interface-parameters
                interface "toPAPOLY-189PE2" dual-stack
                    ipv4
                        no shutdown
                    exit
                    no shutdown
                exit
                interface "toPAPOLY-189PE1" dual-stack
                    ipv4
                        no shutdown
                    exit
                    no shutdown
                exit
                interface "toPAPOLY-189PE3" dual-stack
                    ipv4
                        no shutdown
                    exit
                    no shutdown
```

```
            exit
            interface "toPAPOLY-189PP2" dual-stack
               ipv4
                  no shutdown
               exit
               no shutdown
            exit
         exit
         targeted-session
         exit
         no shutdown
      exit
   exit

#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
   service
      customer 1 name "1" create
         description "Default customer"
      exit
   exit
#--------------------------------------------------
echo "Router (Service Side) Configuration"
#--------------------------------------------------
   router Base
#--------------------------------------------------
echo "ISIS Configuration"
#--------------------------------------------------
      isis 0
         no shutdown
      exit
```

```
#-------------------------------------------------
echo "Policy Configuration"
#-------------------------------------------------
        policy-options
            begin
            commit
        exit
#-------------------------------------------------
echo "BGP Configuration"
#-------------------------------------------------
        bgp
            min-route-advertisement 1
            rapid-withdrawal
            rapid-update mvpn-ipv4
            group "ibgp"
                family vpn-ipv4 vpn-ipv6 mvpn-ipv4
                authentication-key "XXl25bVBBBW96Qi9Te4V3x954hdV" hash2
                type internal
                cluster 10.20.7.189
                neighbor 10.20.1.189
                exit
                neighbor 10.20.2.189
                exit
                neighbor 10.20.3.189
                exit
                neighbor 10.20.4.189
                exit
            exit
            no shutdown
        exit
    exit
```

```
#------------------------------------------------
echo "Source IP Address Configuration"
#------------------------------------------------
    system
        security
            source-address
                application snmptrap "system"
            exit
        exit
    exit
#------------------------------------------------
echo "Log all events for service vprn Configuration"
#------------------------------------------------
    log
    exit
#------------------------------------------------
echo "System Time NTP Configuration"
#------------------------------------------------
    system
        time
            ntp
                server 10.20.189.28
            exit
        exit
    exit

exit all
```

11.2 Příloha č. 2 Konfigurace směrovače typu PE

```
# TiMOS-B-20.4.R3 both/hops Nokia 7705 SAR Copyright (c) 2000-2020 Nokia.
# All rights reserved. All use subject to applicable license agreements.
# Built on Tue Aug 25 10:48:37 EDT 2020 by builder in /builds/F204B/R3/panos/main

# Generated WED MAR 29 07:43:41 2023 UTC

exit all
configure
#--------------------------------------------------
echo "System Configuration"
#--------------------------------------------------
    system
        name "PAPOLY-189PE3"
        dns
        exit
        snmp
            packet-size 9216
        exit
        time
            ntp
                server 10.20.189.28
                no shutdown
            exit
            sntp
                shutdown
            exit
            dst-zone CEST
                start last sunday march 02:00
                end last sunday october 03:00
            exit
```

```
        zone CET
      exit
      thresholds
        rmon
        exit
      exit
    exit
#------------------------------------------------
echo "System Security Configuration"
#------------------------------------------------
    system
      security
        password
          authentication-order local
        exit
        user "polygon"
          password
"XXy$10$WB0.GXPqDLOoigsEA5Cq6.BiXu6V8TTLlJj0ULq1Ahdg9WnErsxXX"
          access console snmp
          console
            member "default"
            member "administrative"
          exit
        exit
        user "dohled_snmp"
          password
"XXy$10$m/Z7MJQvHZr9WQ.LQw.RM.mlxEI.MmzVn1.1PpxEp/.8mj8oL.iXX"
          access snmp
          snmp
            authentication hash2 sha
XXhzM6SOnn6apEFONhWqutmOo5rw4CXlnLVtW9mQ1+b3VxXX privacy aes-128-
cfb-key XXrM4RHT0SCftYqOjEri/LgtT0sURwhpDcy30wLXmXX=
```

```
            group "snmp-ro"
         exit
      exit
      snmp
         access group "snmp-ro" security-model usm security-level privacy read "iso"
      exit
      ssh
         preserve-key
      exit
      per-peer-queuing
      dist-cpu-protection
         policy "_default-access-policy" create
         exit
         policy "_default-network-policy" create
         exit
      exit
   exit
#------------------------------------------------
echo "Log Configuration"
#------------------------------------------------
   log
      event-control "igmp" 2005 suppress
      event-control "vrtr" 2034 generate
      syslog 1
         description "log server"
         address 10.20.189.30
      exit
      snmp-trap-group 11
         description "dohled_snmp"
         trap-target "dohled_snmp" address 10.20.189.29 snmpv3 notify-community
"dohled_snmp" security-level privacy
```

```
        exit
        log-id 1
            description "log server"
            from main security
            to syslog 1
            no shutdown
        exit
        log-id 11
            description "dohled_snmp"
            from main security
            to snmp
            no shutdown
        exit
    exit
#--------------------------------------------------
echo "System Security Cpm Hw Filters and PKI Configuration"
#--------------------------------------------------
    system
        security
        exit
    exit
#--------------------------------------------------
echo "VLAN-Filter Configuration"
#--------------------------------------------------
    filter
    exit
#--------------------------------------------------
echo "QoS Policy Configuration"
#--------------------------------------------------
    qos
        fabric-profile 2 aggregate-mode create
            description "2.5G fabric profile"
```

```
            aggregate-rate 2500000 unshaped-sap-cir 0
        exit
        fabric-profile 10 aggregate-mode create
            description "10G fabric profile"
            aggregate-rate 10000000 unshaped-sap-cir 0
        exit
    exit
#--------------------------------------------------
echo "Card Configuration"
#--------------------------------------------------
    card 1
        card-type iom-sar
        mda 1
            mda-type a8-1gb-v3-sfp
            network
                ingress
                    fabric-policy 2
                exit
            exit
            access
                ingress
                    fabric-policy 2
                exit
            exit
            no shutdown
        exit
        mda 2
            mda-type a8-1gb-v3-sfp
            network
                ingress
                    fabric-policy 2
                exit
```

```
            exit
            access
               ingress
                  fabric-policy 2
               exit
            exit
            no shutdown
         exit
         no shutdown
      exit
#------------------------------------------------
echo "Port Configuration"
#------------------------------------------------
      port 1/1/1
         shutdown
         ethernet
         exit
      exit
      port 1/1/2
         shutdown
         ethernet
         exit
      exit
      port 1/1/3
         description "TEST_EPIPE"
         ethernet
         exit
         no shutdown
      exit
      port 1/1/4
         description "TEST_VPRN"
         ethernet
```

```
    exit
    no shutdown
exit
port 1/1/5
                shutdown
    ethernet
    exit
exit
port 1/1/6
    shutdown
    ethernet
    exit
exit
port 1/1/7
    shutdown
    ethernet
    exit
exit
port 1/1/8
    description "toPAPOLY-189PP1"
    ethernet
        mode network
        mtu 1800
        lldp
            dest-mac nearest-bridge
                admin-status tx-rx
                tx-tlvs port-desc sys-name sys-desc
            exit
        exit
        hold-time up 5
    exit
    no shutdown
```

```
exit
port 1/2/1
   shutdown
   ethernet
   exit
exit
port 1/2/2
   shutdown
   ethernet
   exit
exit
port 1/2/3
   shutdown
   ethernet
   exit
exit
port 1/2/4
   shutdown
   ethernet
   exit
exit
port 1/2/5
   shutdown
   ethernet
   exit
exit
port 1/2/6
   shutdown
   ethernet
   exit
exit
port 1/2/7
```

```
        description "toPAPOLY-189PE4"
        ethernet
            mode network
            mtu 1800
            lldp
                dest-mac nearest-bridge
                    tx-tlvs port-desc sys-name sys-desc
                exit
            exit
            hold-time up 5
        exit
        no shutdown
    exit
    port 1/2/8
        description "toPAPOLY-189PE1"
        ethernet
            mode network
            mtu 1800
            lldp
                dest-mac nearest-bridge
                    admin-status tx-rx
                    tx-tlvs port-desc sys-name sys-desc
                exit
            exit
            hold-time up 5
        exit
        no shutdown
    exit
#--------------------------------------------------
echo "External Alarm Configuration"
#--------------------------------------------------
    external-alarms
```

```
    exit
#--------------------------------------------------
echo "Network Security Configuration"
#--------------------------------------------------
    security
        logging
        exit
        begin
        commit
    exit
#--------------------------------------------------
echo "Management Router Configuration"
#--------------------------------------------------
    router management
    exit

#--------------------------------------------------
echo "Router (Network Side) Configuration"
#--------------------------------------------------
    router Base
        interface "system"
            address 10.20.3.189/32
            no shutdown
        exit
        interface "toPAPOLY-189PE1"
            address 10.20.11.250/30
            port 1/2/8
            bfd 10 receive 10 multiplier 3 type np
            no shutdown
        exit
        interface "toPAPOLY-189PE4"
            address 10.20.11.253/30
```

```
            port 1/2/7
            bfd 10 receive 10 multiplier 3 type np
            no shutdown
        exit
        interface "toPAPOLY-189PP1"
            address 10.20.11.230/30
            port 1/1/8
            bfd 10 receive 10 multiplier 3 type np
            no shutdown
        exit
        autonomous-system 65432
        ip-fast-reroute
#--------------------------------------------------
echo "MPLS Label Range Configuration"
#--------------------------------------------------
        mpls-labels
            sr-labels start 20000 end 30000
        exit
#--------------------------------------------------
echo "ISIS Configuration"
#--------------------------------------------------
        isis 0
            level-capability level-2
            area-id 49.00
            authentication-key "xx333bVBBBW96Qi9Te4V34/yVQPX" hash2
            authentication-type message-digest
            traffic-engineering
            reference-bandwidth 100000000
            advertise-router-capability as
            loopfree-alternate ti-lfa
            timers
                spf-wait 2000 spf-initial-wait 50 spf-second-wait 100
```

```
exit
level 2
    wide-metrics-only
exit
interface "system"
    level-capability level-2
    ipv4-node-sid index 3189
    passive
    no shutdown
exit
interface "toPAPOLY-189PE4"
    level-capability level-2
    hello-authentication-key "xx333bVBBBW96Qi9Te4V36oguGEH" hash2
    hello-authentication-type message-digest
    interface-type point-to-point
    bfd-enable ipv4
    no shutdown
exit
interface "toPAPOLY-189PE1"
    level-capability level-2
    hello-authentication-key "xx333bVBBBW96Qi9Te4V318kDtvl" hash2
    hello-authentication-type message-digest
    interface-type point-to-point
    bfd-enable ipv4
    no shutdown
exit
interface "toPAPOLY-189PP1"
    level-capability level-2
    hello-authentication-key "xx333bVBBBW96Qi9Te4V3/BphyUa" hash2
    hello-authentication-type message-digest
    interface-type point-to-point
    bfd-enable ipv4
```

```
            no shutdown
        exit
        segment-routing
            prefix-sid-range global
            no shutdown
        exit
        no shutdown
    exit
#--------------------------------------------------
echo "MPLS Configuration"
#--------------------------------------------------
    mpls
        interface "system"
            no shutdown
        exit
        interface "toPAPOLY-189PE4"
            no shutdown
        exit
        interface "toPAPOLY-189PE1"
            no shutdown
        exit
        interface "toPAPOLY-189PP1"
            no shutdown
        exit
    exit
#--------------------------------------------------
echo "RSVP Configuration"
#--------------------------------------------------
    rsvp
        interface "system"
            no shutdown
        exit
```

```
            interface "toPAPOLY-189PE4"
                no shutdown
            exit
            interface "toPAPOLY-189PE1"
                no shutdown
            exit
            interface "toPAPOLY-189PP1"
                no shutdown
            exit
            no shutdown
        exit
#--------------------------------------------------
echo "MPLS LSP Configuration"
#--------------------------------------------------
        mpls
            path "dyn"
                no shutdown
            exit
            lsp-template "CORE-LSP" mesh-p2p
                default-path "dyn"
                cspf
                fast-reroute facility
                exit
                no shutdown
            exit
            auto-lsp lsp-template "CORE-LSP" policy "PS-CORE-LSP"
            no shutdown
        exit
#--------------------------------------------------
echo "LDP Configuration"
#--------------------------------------------------
        ldp
```

```
            fast-reroute
            interface-parameters
               interface "toPAPOLY-189PE4" dual-stack
                  ipv4
                     no shutdown
                  exit
                  no shutdown
               exit
               interface "toPAPOLY-189PE1" dual-stack
                  ipv4
                     no shutdown
                  exit
                  no shutdown
               exit
               interface "toPAPOLY-189PP1" dual-stack
                  ipv4
                     no shutdown
                  exit
                  no shutdown
               exit
            exit
            targeted-session
            exit
            no shutdown
         exit
      exit

#------------------------------------------------
echo "Service Configuration"
#------------------------------------------------
      service
         sdp 1002 create
```

```
    far-end 10.20.2.189
    sr-isis
    keep-alive
        shutdown
    exit
    no shutdown
exit
customer 1 create
    description "Default customer"
exit
vprn 10 customer 1 create
    interface "IPEKO" create
    exit
exit
vprn 10 customer 1 create
    description "IPEKO"
    autonomous-system 65432
    route-distinguisher 10.20.3.189:10
    auto-bind-tunnel
        resolution-filter
            sr-isis
        exit
        resolution filter
    exit
    interface "IPEKO" create
        address 10.21.189.129/26
        sap 1/1/4 create
        exit
    exit
    no shutdown
exit
epipe 2002003 customer 1 create
```

```
            description "TEST_EPIPE"
            service-name "EPIPE_TEST"
                                sap 1/1/3 create
                                no shutdown
                                exit
            spoke-sdp 1002:2002003 create
               no shutdown
            exit
            no shutdown
         exit
      exit
#--------------------------------------------------
echo "Router (Service Side) Configuration"
#--------------------------------------------------
      router Base
#--------------------------------------------------
echo "ISIS Configuration"
#--------------------------------------------------
         isis 0
            no shutdown
         exit
#--------------------------------------------------
echo "Policy Configuration"
#--------------------------------------------------
         policy-options
            begin
            prefix-list "CORE"
               prefix 10.20.1.189/32 exact
               prefix 10.20.2.189/32 exact
               prefix 10.20.3.189/32 exact
               prefix 10.20.7.189/32 exact
               prefix 10.20.8.189/32 exact
```

```
        exit
        policy-statement "PS-CORE-LSP"
            entry 10
                from
                    prefix-list "CORE"
                exit
                action accept
                exit
            exit
        exit
        commit
    exit
#------------------------------------------------
echo "BGP Configuration"
#------------------------------------------------
    bgp
        min-route-advertisement 1
        rapid-withdrawal
        group "ibgp"
            family vpn-ipv4 vpn-ipv6 mvpn-ipv4
            authentication-key "xx333bVBBBW96Qi9Te4V3x123hdV" hash2
            peer-as 65432
            neighbor 10.20.7.189
            exit
            neighbor 10.20.8.189
            exit
        exit
        no shutdown
    exit
#------------------------------------------------
echo "Network Security Zone Configuration"
#------------------------------------------------
```

```
    exit

#--------------------------------------------------
echo "Source IP Address Configuration"
#--------------------------------------------------
    system
        security
            source-address
                application snmptrap "system"
            exit
        exit
    exit
#--------------------------------------------------
echo "System Time Configuration"
#--------------------------------------------------
    system
        time
            ntp
            exit
        exit
    exit

exit all
```