VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2021 Juraj Formánek

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

ZHODNOCENÍ MPLS JAKO WAN TECHNOLOGIE PRO DATOVÉ PŘENOSY V KRITICKÉ INFORMAČNÍ INFRASTRUKTUŘE

EVALUATION OF MPLS APPROACH AS A WAN TECHNOLOGY FOR DATA TRANSMISSIONS IN CRITICAL INFORMATION INFRASTRUCTURE

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Juraj Formánek**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Radek Fujdiak, Ph.D.**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Telekomunikační a informační systémy**

Ústav telekomunikací

Student: Juraj Formánek ***ID:*** 214072
Ročník: 3 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Zhodnocení MPLS jako WAN technologie pro datové přenosy v kritické informační infrastruktuře

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je zhodnocení techniky MPLS jako základní technologie v privátní WAN pro přenos dat v kritické informační infrastruktuře s ohledem na dostupnost, integritu a důvěrnost informací. Dílčími výstupy by měl být návrh podkladových protokolů a jejich zabezpečení, návrh topologie pro snadnou škálovatelnost a porovnání různých úrovní redundance a návrh zajištění segmentace a kvality služby pro různé typy provozů (SCADA, telefonie, ...). Očekávaným výstupem je i porovnání MPLS s jinými technikami a přístupy v oblasti WAN.

DOPORUČENÁ LITERATURA:

[1] ROSEN, E., A. VISWANATHAN a R. CALLON. RFC 3031: Multiprotocol Label Switching Architecture [online]. 2001. Dostupné z: https://tools.ietf.org/html/rfc3031

[2] TANENBAUM, Andrew a David WETHERALL. Computer networks. 5. vyd. Boston: Pearson Prentice Hall, 2011. ISBN 0-13-212695-8.

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 31.5.2021

Vedoucí práce: Ing. Radek Fujdiak, Ph.D.
Konzultant: Jan Churý (EG.D)

prof. Ing. Jiří Mišurec, CSc.
předseda rady studijního programu

ABSTRAKT

Práca sa zaoberá použitím technológie MPLS v energetickej kritickej informačnej infraštruktúre a jej porovnaním s iným moderným prístupom v oblasti spravovania WAN sietí. Pre tento účel bola vybraná SD-WAN technológia. Daná práca obsahuje teoretický popis a praktické testovanie jednotlivých MPLS technológií na WAN topológii, ktorá pripomína reálnu topológiu spoločnosti EG.D. Testy boli prevedené v emulátore GNS3 pomocou Cisco smerovačov. Praktické testovanie bolo primárne zamerané na testy dostupnosti pri výpadku liniek alebo zariadení a na výpadky route-reflectora. Záver práce obsahuje zhodnotenie vhodného prístupu pre datové prenosy v kritickej informačnej infraštruktúre, ktoré je založené na informáciách alebo praktických testoch obsiahnutých v tejto práci.

KĽÚČOVÉ SLOVÁ

kritická informačná infraštruktúra, MPLS, SD-WAN, WAN, GNS3, Cisco, dostupnosť

ABSTRACT

Thesis deals by using MPLS technology in energy critical information infrastructure and its comparison with another modern approach in the area of the WAN management. For this purpose was chosen a Software-defined Wide Area Network technology. This thesis contains theoretical description and practical tests of particular MPLS technologies on the WAN topology, which is considered as a virtual real topology of the EG.D's company. Test were simulated in GNS3 emulator, using Cisco routers. Practical test were firstly focused on availability test when link or node failure occurs and secondly on route-reflector failures. Conclusion sums up appropriate approach for data transmissions in critical information infrastructure based on informations or practical test in this thesis.

KEYWORDS

critical information infrastructure, MPLS, SD-WAN, WAN, GNS3, Cisco, availability

FORMÁNEK, Juraj. *Zhodnocení MPLS jako WAN technologie pro datové přenosy v kritické informační infrastruktuře*. Brno, 2021, 86 s. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce: Ing. Radek Fujdiak, PhD.

VYHLÁSENIE

Vyhlasujem, že svoju bakalársku prácu na tému „Zhodnocení MPLS jako WAN technologie pro datové přenosy v kritické informační infrastruktuře“ som vypracoval samostatne pod vedením vedúceho bakalárskej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora

POĎAKOVANIE

Rád bych poděkoval panu Ing. Jan Churý a vedoucímu diplomové práce panu Ing. Radek Fujdiak, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Úvod **11**

1 Kritická infraštruktúra **12**
1.1 Kritická energetická infraštruktúra 12
1.1.1 VVN a VN rozvodne 13
1.2 Kritická informačná infraštruktúra 14
1.2.1 Prenosy v KII 15
1.3 Priemyslové siete 17
1.3.1 Rozdiely medzi priemyslovými a kancelárskymi/domácimi sieťami 18
1.3.2 Porovnanie sietí z pohľadu CIA 19

2 Súčasná situácia a zmeny vo využívaní sietí **22**
2.1 Architektúra tradičnej pobočkovej WAN siete 22
2.1.1 Zabezpečenie tradičnej WAN 23
2.1.2 Požiadavky na pripojenie pobočky do WAN 24
2.1.3 Zhrnutie analýzy tradičných WAN riešení 25

3 Cisco SD-WAN **26**
3.1 Transformácia z tradičnej WAN na SD-WAN 26
3.2 Dôvody nasadzovania SD-WAN sietí 27
3.3 Roviny SD-WAN siete 29
3.3.1 Kompomenty Cisco SD-WAN 30
3.4 Funkcie zabezpečujúce užívateľskú skúsenosť 32
3.4.1 Application-aware routing 32
3.4.2 Samo-opravné kódovanie FEC 33
3.4.3 Software as a service (SaaS) 33
3.4.4 Infrastructure as a service (IaaS) 34
3.4.5 Duplikácia paketov 34
3.5 Segmentácia SD-WAN 34
3.6 Zapezpečenie Cisco SD-WAN 35
3.7 Zhrnutie použitia Cisco SD-WAN 36

4 Testovacie prostredie a testovacie scenáre **38**
4.1 Požiadavky na RAM a CPU 39
4.2 Testovacie scenáre pre testovanie 41
4.3 Testy dostupnosti 41

5 MPLS **44**
5.1 Popis MPLS 45
5.2 L3 MPLS VPN 48
5.2.1 Popis L3 MPLS VPN 49
5.2.2 Testy dostupnosti pre L3VPN spojenie 50
5.3 VPLS 58
5.3.1 Popis VPLS 58
5.3.2 Testy dostupnosti VPLS spojenia 60
5.4 MPLS QoS 65
5.4.1 Implementácia MPLS QoS 66
5.4.2 Meranie MPLS QoS 69
5.5 MPLS-TE 72
5.6 MPLS-TE FRR 75
5.7 Route-reflector 76

Závěr **78**

Literatúra **80**

Zoznam symbolov, veličín a skratiek **83**

Zoznam obrázkov

1 Optická sieť EG.D 11
1.1 Vyznačenie územnej pôsobnosti distribučných spoločností [7] 13
2.1 Bottleneck siete 23
3.1 Lacnejšia konektivita 28
3.2 Guest WiFi 29
3.3 Roviny Cisco SD-WAN 30
3.4 Application-aware routing 33
3.5 Bezpečnosť SD-WAN siete 36
4.1 Fyzické zapojenie topológie 38
4.2 Graf zaberania RAM 39
5.1 MPLS paket 45
5.2 Operácie s návestím 46
5.3 Príklad LSP 47
5.4 Výpadok na trase 50
5.5 Wireshark na linke 077-075 52
5.6 Wireshark na linke 077-079 53
5.7 Wireshark na koncovom zariadení 53
5.8 Vypnutie smerovača 54
5.9 Koncové zariadenie 55
5.10 MPLS sieť z pohľadu pobočky 58
5.11 Aktuálna topológia 60
5.12 Výpadok VPLS spojenia - MPLS-TE FRR 62
5.13 Výpadok VPLS - MPLS-TE FRR 63
5.14 Topológia pre testovanie MPLS QoS 66
5.15 Nastavenie značkovania DSCP v aplikácii 67
5.16 Stratovosť PC1 69
5.17 Stratovosť PC2 69
5.18 Graf priebehu bez QoS 70
5.19 Stratovosť s QoS 71
5.20 Graf priebehu s QoS 72
5.21 Aktuálna topológia 75

Zoznam tabuliek

4.1 Tabuľka nameraných hodnôt zaberania RAM 40
4.2 5 s odstup 42
4.3 10 µs odstup 43
5.1 Mapovanie IP - MPLS 65
5.2 Testy dostupnosti L3VPN spojenia 78
5.3 Testy dostupnosti VPLS spojenia 78

Zoznam výpisov

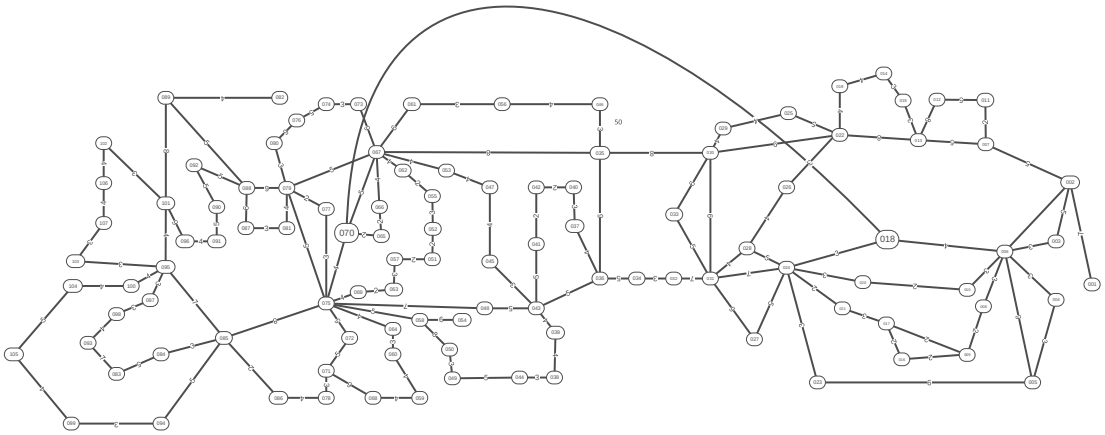
5.1 LFIB 47
5.2 Nadviazanie susedstva na CE smerovačoch 48
5.3 Prenášanie ciest VRF instancie customer_A 48
5.4 Cesty smerovača CE1-A 49
5.5 Výpadok linky 51
5.6 Zachytávanie pomocou Tshark 51
5.7 Tshark na koncovom zariadení 55
5.8 Výpadok reštartovaním smerovacích protokolov 56
5.9 Výpadok príkazom reload 57
5.10 Debugovacie správy pri načítavaní smerovača 57
5.11 Popis nakonfigurovaného VPLS spojenia na PE1-070 59
5.12 Prehľad VFI instacií 59
5.13 Výpadok linky 077-075 61
5.14 Výpadok VPLS spojenia pri výpadku smerovača 62
5.15 Výpadok RR pre VPLS spojenie 64
5.16 Výpadok RR príkazom `reload` 64
5.17 Debugovacie výpisy RR CSR1000V 65
5.18 Nastavenie DSCP v smerovači 66
5.19 Nastavenie QoS vnútri MPLS domény 68
5.20 Alokácia šírky pásma 73
5.21 Prehľad vytvorených tunelov 74
5.22 Master tunel 74
5.23 Zoznam tunelov pre MPLS-TE FRR 76
5.24 Explicitné cesty 76
5.25 Smerovacia BGP L3VPN tabuľka 77

Úvod

Kritická informačná infraštruktúra potrebuje špecifické požiadavky pre správne riadenie siete. Tradičné IP princípy sú pre kritickú infraštruktúru považované za nedostatočné. Topológia, na ktorej je demonštrovaná MPLS technológia pre správne riadenie siete je zobrazená na obr. 1. Systém je tvorený dvomi dispečerskými miestami, z čoho je jedno umiestnené v Českých Budejoviciach a druhé v Brne. Dokopy obsahuje sieť 107 prvkov, z čoho je 105 VVN rozvodní, ktoré musia neustále komunikovať s dispečerským centrom. V prípade výpadku jedného dispečerského centra musí byť prevzaté núdzové riadenie z druhého dispečerského centra naprieč oboch napäťových hladín 110 a 22 kV. Z tohto dôvodu je potrebné, aby dáta v takto navrhnutej sieti boli vzájomne synchronizované a zabezpečené. Neoprávnené vniknutie do siete by mohlo mať fatálne dôsledky, čím by mohlo dôjsť ku značným materiálnym škodám a v horšom prípade aj k ujme na zdraví.

V skutočnosti sa jedná o územie ČR, zobrazené na obr. 1.1. V oblasti južnej Moravy a južných Čechách má spoločnosť EG.D (E.ON) okolo stovky 100 kV rozvodní, ktoré komunikujú na zobrazených dispečingoch. Rozvodne sú navzájom prepojené po VVN vedeniach a upnuté na kombinovaných ochranných zemniacich lanách (KZL). KZL primárne chránia fázové vodiče vonkajšieho vedenia pred úderom blesku a sekundárne prenášajú dáta optickými vláknami uloženými v jadre KZL. Takýto optický kábel uložený v jadre KZL je typicky 48-vláknový, čo predstavuje v súčasnosti najrýchlejší a najspoľahlivejší spôsob pre zaistenie komunikácie [1].

Výstupom práce bude zhodnotenie výsledkov testovania jednotlivých MPLS technológií pre kritickú infraštruktúru, so zameraním na testy dostupnosti pri výpadku spojenia, porovnanie s tradičným a nepostačujúcim IP princípom a porovnanie s SD-WAN prístupom v oblasti spravovania WAN kritickej infraštruktúry.



Obr. 1: Optická sieť EG.D

1 Kritická infraštruktúra

Pre správne pochopenie toho, na akú oblasť sa práca sústreďuje, je vhodné definovať pojmy kritická infraštruktúra (KI), kritická energetická infraštruktúra (KEI) a kritická informačná infraštruktúra (KII). KII obsluhuje KEI, pričom KII spolu s KEI patria do oblasti kritických infraštruktúr.

Kritická infraštruktúra je popísaná zákonom č. 240/2000 Sb.:

- kritickou infraštruktúrou je prvok kritickej infraštruktúry alebo systém prvkov kritickej infraštruktúry, ktorého narušenie funkčnosti by malo závažný dopad na bezpečnosť štátu [2], zabezpečenie základných životných potrieb obyvateľstva, zdravia osôb alebo ekonomiku štátu [3].
- Zákon [3] ďalej definuje prvky kritickej infraštruktúry ako: stavby, zariadenia, prostriedky alebo verejnú infraštruktúru [4], určenú podla prierezových a odvetvových kritérií.
- Prierezovými kritériami je súbor hľadísk pre posudzovanie závažnosti vplyvu narušenia funkcie prvku kritickej infraštruktúry s hraničnými hodnotami, ktoré zahrnujú rozsah strát na živote, dopad na zdravie osôb, mimoriadne vážny ekonomický dopad alebo dopad na verejnosť v dôsledku rozsiahleho omedzenia poskytovania nevyhnutných služieb alebo iného závažného zásahu do každodenného života [3].
- Odvetvové kritéria sú technické alebo prevádzkové hodnoty k určovaniu prvku kritickej infraštruktúry v odvetviach energetika, vodné hospodárstvo, potravinárstvo a poľnohospodárstvo, zdravotníctvo, doprava, komunikačné a informačné systémy, finančný trh a mena, núdzové služby a verejná správa [3].

KI sa musí stále adaptovať na potenciálne hrozby. Tomu musia odpovedať aj východiská, metódy a nástroje a postupy ochrany KI, vrátane využitia metód a prostriedkov ekonometrie a operačného výskumu k optimalizácii priebehov procesov v tejto oblasti z hľadiska času a potrebných materiálnych a nemateriálnych zdrojov [5]. Bezpečnosť KI sa bude v tejto práci venovať z pohľadu útoku do privátnej WAN siete KII, ktorú v tejto práci prestavuje energetická sieť spoločnosti EG.D. Útok alebo porucha na KI by mohla mať fatálne následky, pričom bezpečnosť bude v menšej miere témou tejto práce, okrem hlavného zamerania sa na testy dostupnosti pri výpadku spojenia.

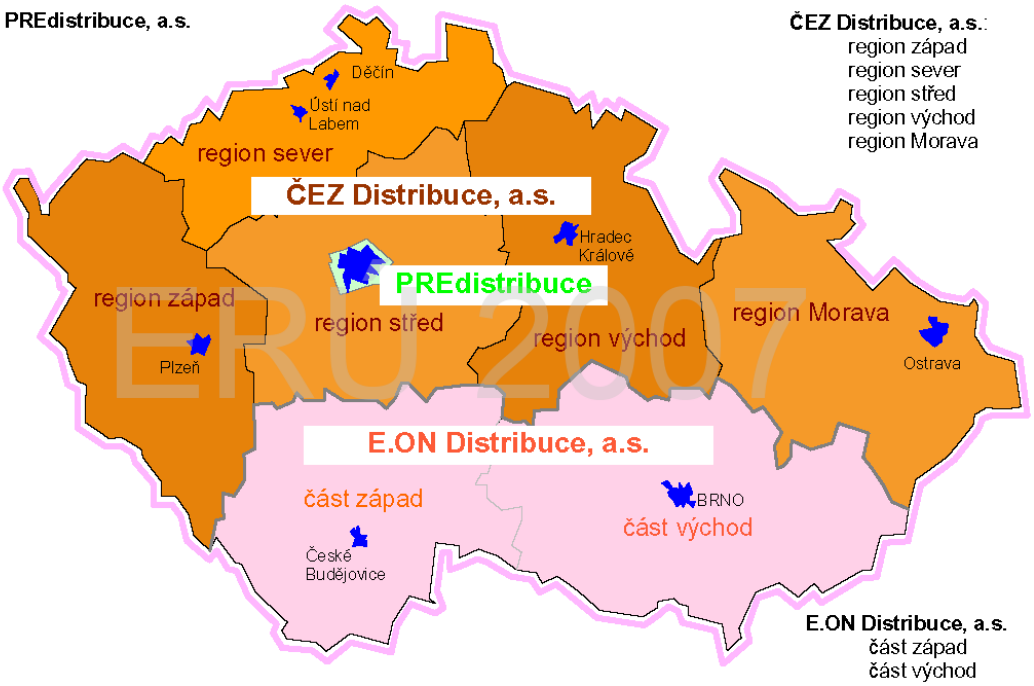
1.1 Kritická energetická infraštruktúra

Kritická energetická infraštruktúra (KEI) je riadená prostredníctvom kritickej informačnej infraštruktúry (KII). Pre zaistenie správnej funkčnosti KEI je nutná funkčnosť KII, ktorá musí pružne reagovať na zmeny sieti (výpadky, poruchy). Pri poruche

v KEI vplyvom prírodných (búrka, povodne) alebo mechanických faktorov (ľudská činnosť) musí práve KII určiť nasledujúce postupy pre správnu funkčnosť KEI. KEI tvoria:

- výrobné časti produkujúce elektrinu v rôznych zdrojov,
- prenosové sústavy vedenia a zariadení (rozvodní a transformovní), 400 kV, 220 kV a vybraných vedení a zariadení 110 kV,
- distribučné sústavy vysokého napätia 3 kV, 6 kV, 10 kV, 22 kV, 35 kV a 110 kV,
- distribučné sústavy nízkeho napätia 0,4/0,23 kV,
- technické dispečingy hierarchicky usporiadané k riadeniu celej sústavy [6].

Na obr. 1.1 je zobrazené geografické územie ČR (E.ON Distribuce, a.s.), ktorého sa práca týka. V ďalšej podkapitole nasleduje stručný popis VVN a VN rozvodní, ktorých je na zobrazenej mape dokopy okolo 6000. Všetky tieto rozvodne tvoria KEI a zároveň sú alebo budú súčasťou siete, za účelom monitorovania a ovládania z dvoch dispečingových ústrední.



Obr. 1.1: Vyznačenie územnej pôsobnosti distribučných spoločností [7]

1.1.1 VVN a VN rozvodne

V tejto práci sa bude jednať o simuláciu KII postavenej na KZL na VVN a VN rozvodniach. Skratkou VVN a VN sa označuje normalizované napätie, ktoré sa používa v ČR v prenosovej trojfázovej sústave. VVN označuje elektrické napätie v intervale od 110 kV do 400 kV. Pre VN sa používajú hodnoty 6 kV, 10 kV, 22 kV a 35 kV. Táto práca sa z hľadiska rozdelenia elektrickej sústavy bude zameriavať len na distribučné

a transformačné stanice (VVN rozvodne). Ostatné typy nie sú predmetom tejto práce. Súčasťou týchto staníc sú rôzne zariadenia zaisťujúce správnu prevádzku. Pre prehľadnosť bol vložený stručný zoznam zariadení, ktoré sú ovládateľné prostredníctvom KII na zaistenie správnej prevádzky KEI. K týmto zariadeniam patria zariadenia umožňujúce:

- istenie elektrických obvodov proti preťaženiu, skratu, prepätiu (vypínače, odpínače),
- meranie a kontrolu elektrických prístrojov (prístrojové transformátory),
- spínanie a prepínanie elektrických obvodov (spínače),
- zaistenie bezpečnosti zariadení (CCTV, detektory),
- meracie a signalizačné zariadenia [8].

Témou práce je práve zaistenie správnej funkcie meracích a signalizačných zariadení, pretože práve tie spracovávajú údaje z prístrojových transformátorov a monitorujú prevádzkový stav jednotlivých zariadení [8]. Na základe obdržaných údajov môže pracovník zo vzdialeného dispečingu rozhodovať manuálne alebo automatickou konfiguráciou u riadení energetickej siete. Primárnym cieľom práce je sieť na VVN rozvodniach (transformačných staniciach) a v budúcnosti bude sieť pri úspešnom nasadení na VVN rozvodne rozšírená na VN rozvodne (distribučné stanice). Pre sprehľadnenie rozdielu VVN a VN rozvodní je v nasledujúcich riadkoch vložená stručná charakteristika transformačných a distribučných staníc.

1. **Transformačné stanice** - slúžia na spojenie prenosových sústav s rôznym napätím (400/220 kV) a na transformáciu 400/110 kV a 220/110 kV. Často sú spájané s uzlovými stanicami do jednej elektrickej stanice [8]. V tejto práci sú zobrazené monitorované transformačné stanice na obr. 1, ktorých počet je okolo 100.
2. **Distribučné stanice** - prenášajú elektrickú energiu buď od primárnych zdrojov (elektráreň) alebo od sekundárnych zdrojov (transformačná stanica) na určené miesta, t.j. do rozvodní nižšej sústavy alebo ku spotrebiteľovi (distribučné siete) [9]. Distribučné stanice mimo vyššie spomenutých funkcií zároveň transformujú elektrické napätie (VVN/VN). Pri úspešnom nasadení optickej trasy na transformačné stanice sa počíta s rozšírením na VN linky do týchto distribučným staníc, ktorých je na zobrazenom území na obr. 1.1 okolo 6000.

1.2 Kritická informačná infraštruktúra

Tak, ako je definovaná KI v zákone č. 240/2000 Sb., tak je aj definovaná KII v zákone č. 181/2014 Sb. o kybernetickej bezpečnosti. Pojem KII tvorí:

- digitálne prostredie umožňujúce vznik, spracovanie a výmenu informácií, tvorené informačnými systémami, službami a sieťami elektronických komuniká-

cií [10],

- prvok alebo systém prvkov kritickej infraštruktúry v odvetví komunikačné a informačné systémy v oblasti kybernetickej bezpečnosti [11],
- bezpečnosť informácií, zaistenie dôvernosti, integrity a dostupnosti informácií a dát,
- informačný systém, na ktorého fungovaní je závislé poskytovanie základnej služby,
- služby, ktorých poskytovanie je závislé na sieťach elektronických komunikácií [12] alebo informačných systémoch, ktorých narušenie by mohlo mať významný dopad na zabezpečenie spoločenských alebo ekonomických činností (odvetvie energetika) [13].

1.2.1 Prenosy v KII

V nasledujúcich riadkoch sú hierarchicky usporiadané podľa dôležitosti jednotlivé typy prevádzok týkajúce sa prevádzky v sieti KII, ktorou disponuje spoločnosť EG.D.

1. **SCADA systémy** - dátovo nenáročná komunikácia v desiatkach kb/s. V tejto práci je táto komunikácia kľúčová a je k nej priradená najväčšia priorita z hľadiska celkovej prevádzky. Umožňuje dispečerské riadenie a zber dát. Zbieraním dát v reálnom čase a ich následnou grafickou interpretáciou umožňujú operátorom výroby včasnejšie korekcie pre optimalizáciu produkcie [14]. SCADA systémy využívajú napr. PLC automaty, senzory, čítače pre prenos a zber dát. Predovšetkým dôležitá je dôvernosť obdržaných dát. Pri možnom útoku môže útočník porušiť dôvernosť dát, prípadne na diaľku ovládať činnosť PLC. Pre prenos dát sa využíva svetová sieť internet, prípadne iné priemyslové linky v priemyselnej sieti. Zozbierané dáta sú ukladané na lokálnom úložisku, alebo na databázach typu SQL. Súčasťou SCADA systémov je HMI softvér, čo je softvér typicky s grafickým užívateľským prostredím, ktorý zobrazuje operátorovi informácie o stave procesu a zároveň umožňuje zadávať operátorské povely (príkazy). Obvykle sa zobrazujú grafické priebehy (trendy) vybraných veličín [15].
2. **HDO** - hromadné diaľkové ovládanie, pre potreby regulácie odberu elektrickej energie na diaľku. Cez HDO prepína distribučná spoločnosť na diaľku stav elektromera z vysokej hladiny na nízku a opačne [16]. Ďalšie využitie nájdeme napr. v prípade, kedy pri výrobe elektrickej energie v malých elektrárňach (vodné elektrárne) je nadbytok energie, tak jednoduchým signálom z distribučnej spoločnosti sa zastaví produkcia, do doby než to bude situácia znovu vyžadovať. Pri havarijných stavoch rovnako dochádza k využívaniu HDO systému

na predchádzanie nepriaznivých scenárov (ekonomické straty, straty na životoch). V ČR sa používajú 3 povely na ovládanie HDO prijímača u zákazníka:

- K1 pre prepínanie vysokého (VT) a nízkeho tarifu (NT),
- K2 pre zapínanie a vypínanie ovládaného elektrického spotrebiča (vytápanie, bojler),
- K3 pre zapínanie a vypínanie ďalšieho ovládaného spotrebiča (bojleru pre ohrev teplej vody u sadzieb pre priamotopné topenie) [17].

HDO je dátovo nenáročný protokol v jednotkách/desiatkach kb/s, náchylný na opozdenie a výpadky.

3. Protokoly typu **HTTPS, RDP, SSH, Syslog, NTP**. Tieto protokoly nevyžadujú veľkú kapacitu, ale pri zahltení linky môže ich nefunkčnosť výrazne narušiť KII a je teda potrebné ich priorizovať pred ostatnými prevádzkami.
4. **Prenos hlasu** - ide o poskytnutie telefónneho spojenia prostredníctvom VoIP, pre ktoré platia štandardné parametre:
   - opozdenie $\leq$ 400 ms, pri prekročení tejto hodnoty je hovor nekvalitný a môže dôjsť ku strate synchronizácie a výpadku spojenia,
   - stratovosť paketov $\leq 2\,\%$, pri prekročení stratovosti 2 % (2-5 %) dochádza k narastajúcej nezrozumiteľnosti hovoru a pri 5-10 % je zrozumiteľnosť nízka a kvalita hlasu je výrazne znehodnotená.
5. **Kamerový systém** - z hľadiska trvalej prevádzky patria tieto prenosy k najobjemnejším prenosom v KII v rade desiatok Mb/s. Použitý protokol je UDP a je náchylný na opozdenie a výpadky. Význam kamerového systému nájdeme najmä pri zabezpečení kritickej infraštruktúry, kde by vniknutie neoprávnenej osoby do strážanej oblasti mohlo privodiť neželané scenáre. Kamerové systémy slúžia na detekciu vniknutia neoprávnenej osoby do nejakej strážanej oblasti (obvykle miestnosti, budovy, alebo areálu) [18]. Kamerový systém je spravidla doplnený rôznymi detektormi, ktoré s kombináciou s kamerovým systémom poskytujú dostatočnú fyzickú ochranu kritickej infraštruktúry. Pre prevádzku kamerového systému na základe streamovania videa platí:
   - stratovosť paketov $\leq 5\,\%$,
   - opozdenie $\leq$ 400 ms.
6. **Jednorázové operácie** - týmito operáciami sa rozumie zálohovanie, migrácia, aktualizácie a podobne cielené prenosy, ktoré môžu bez dodatočnej konfigurácie výrazne zaťažiť sieť. Môžu vyžadovať prevádzku v rade desiatok až stoviek Mb/s. Nie sú náchylné na opozdenie a výpadky. Pridáva sa im zostávajúca priepustnosť liniek. Tieto operácie majú jedinú podmienku, a to aby boli prenesené bez chýb. Z tohoto dôvodu sa využíva protokol TCP, kedy pri prípadnom chybnom doručení je prenos daného segmentu opakovaný.

Pre tieto druhy prevádzok je vyžadovaná dodatočná konfigurácia siete tak, aby

vyhovovala požiadavkám KII. Táto dodatočná konfigurácia bude v neskorších kapitolách prakticky otestovaná prostredníctvom MPLS technológie, a to konkrétne technológií MPLS-TE, MPLS-TE FRR a MPLS QoS, ktoré sú bližšie popísane v piatej kapitole.

1.3 Priemyslové siete

KII je možné zaradiť do odvetvia priemyselných sietí, kde táto sieť vyžaduje špecifický spôsob použitia. Pre KII a priemyselné siete sa dá nájsť množstvo spoločných prvkov, nakoľko KII sa dá zaradiť do podmnožiny priemyselných sietí. Priemyslové siete sú definované kľúčovými parametrami a pojmami, pomocou ktorých sú popísané protokoly používané v priemyslovom prostredí. Pre potreby priemyselných sietí sú kľúčové nasledovné parametre:

- **Doba odozvy systému** - resp. garancia odozvy do predom definovanej doby. V priemyslových protokoloch sa v praxi používa výraz Timeline. Pre potreby KII je vyžadovaný neustály čas dostupnosti, kde by pre potreby kritických prenosov nemala doba odozvy prekračovať stanovený čas.
- **Synchronizácia** - akcia jednotlivých entít s určitou presnosťou v čase, na základe čoho sú definované požiadavky na kolísanie opozdenia (jitter). V priemyselnom prostredí nájdeme veľké množstvo údajov, ktoré musia byť naraz v jednom čase vyhodnocované. V prípade KEI sa môže jednať napr. o infraštruktúru typu AMI, kde koncové zariadenia u zákazníka odosielajú namerané dáta distribučnej spoločnosti a zároveň vďaka obojsmernej komunikácii môže koncové zariadenie u zákazníka prijímať rôzne aktualizácie (tarify). Podľa aktuálnych vyhlášok si môže zákazník zobraziť informácie o spotrebe napätia a prúdu v jednotlivých fázach za jeden deň/týždeň/mesiac a i. Zákazník tak môže sledovať svoju spotrebu a zmeny spotreby v čase.
- **Hard realtime** - v prípade nedodržania časových parametrov nastáva nefunkčnosť systému. Pre KEI by pri výpadku spojenia a nerealizovania vopred určených akcií na určitej trase mohli nastať neželané scenáre.
- **Dobra trvania cyklu** - na prenášanie dát v definovanom časovom rastri sú dáta prenášané v cykloch. Je to doba, počas ktorej sa určite obdrží správa (cycletime). V praxi arbiter komunikácie (master) posiela zhluk rámcov, ktoré predstavujú dáta v jednom cykle.
- **Priepustnosť a jitter** - v závislosti od veľkosti prenášaných dát konkrétneho protokolu. Pre KII musí byť napr. splnená podmienka komunikácie medzi jednotlivými rozvodňami vo vhodnom časovom úseku (VOIP, kamerový systém).

1.3.1 Rozdiely medzi priemyslovými a kancelárskymi/domácimi sieťami

Pri porovnaní siete KII ako siete patriacej do podmnožiny priemyselných sietí s klasickými kancelárskymi/domácimi sieťami je možné nájsť nieľko zásadných rozdielov:

- **Determinizmus a doba doručenia dát** - pri priemyselných sieťach je dôležité poznať determinizmus siete, kým u kancelárskych sietí je to tradične iba rýchlosť siete. Aplikácie používané v kancelárskych a v priemyselných sieťach majú rôzne dĺžky dátových blokov, ktoré majú väčšinou konštantnú veľkosť. Pri riadení alebo monitorovaní udalostí s vysokou rýchlosťou musí komunikácia prebiehať v konštantnom časovom rámci. V domácich sieťach, kde sa šírka pásma pohybuje okolo 100 Mb/s nie je tento jav pozorovateľný, nakoľko napr. užívateľovi pri tlači dokumentu cez sieť nezáleží, či kancelárska tlačiareň má pri príjme dokumentu 2 s opozdenie, ale ak sa tak dlho malo čakať na odpojenie linky pod napätím, mohlo by to spôsobiť neželané scenáre [19]. Dobu doručenia dát sa v priemyslových sieťach charakterizuje na 2 oblasti:
  - Ľudské riadenie - v priemyselných sieťach, kde sa využíva práve sieť napr. na manuálne riadenie zariadení prostredníctvom ľudského riadenia a na prenos povelov je nutná doba doručenia dát okolo 100 ms, čo odpovedá rýchlosti reakcie človeka. V takomto prípade je plne vyhovujúci bežný ethernet a TCP/IP protokol. V KEI môžeme túto oblasť prirovnať napr. k odčítaniu inteligentných elektromerov, príp. rôznym úpravám tarifov, kde prenosy nespadajú do kritickej oblasti.
  - Kontrola procesov - pri procesoch v priemyselných podnikoch, akými sú napr. chladenie, zahrievanie výrobku je potrebná doba doručenia < 10 ms. Táto doba doručenia je charakteristická pre väčšinu zariadení typu PLC a riadiacich systémov založených na PC. Väčšina regulačných slučiek algoritmov počíta s rýchlym doručením dát a u procesov vyplývajúcich zo svojej fyzikálnej podstaty, ktoré majú dlhodobý charakter (ohrievanie/chladenie výrobku) je potrebné dáta dodávať v rýchlom slede, aby tieto regulátory vykazovali lepšie výsledky, než systémy riadené človekom, nakoľko človek potrebuje prirodzene dlhšiu dobu na spracovávanie údajov.

    Pre KEI ide o vopred stanovené akcie pri poruchách, akými sú prepínanie/vypínanie liniek a komunikácia rozvodní s dispečingom tak, aby sa zamedzilo nepriaznivým scenárom.
- **Prostredie** - v priemyslovom prostredí sú často potrebné odlišné prostriedky na zaistenie mechanickej a elektrickej odolnosti. Patria sem napr. veľký rozdiel teplôt, najčastejšie od -20 až $+80$°C, odolnosť voči pohyblivým častiam,

reaktívnym chemikáliám, odolnosť proti vlhkosti, vibráciám a elektromagnetickému rušeniu. Spôsob montáže sieťových prvkov je odlišný, kedy pri kancelárskych sieťach sú sieťové prvky namontované v štandardných 19-palcových rackoch. V priemyselnom prostredí sa montujú prvky napr. DIN lištu, príp. na iné dostupné miesta.

- **Široké spektrum zariadení** - v priemyslovom prostredí sa okrem stolových počítačov používa široké spektrum rôznych zariadení (PLC, aktuátory, senzory) pripojených do siete na rôzne účely, napr. riadenie motorov, čerpadiel, zapínanie/vypínanie spínačov. U klasických sietí ide iba prevažne o stolné počítače, tlačiarne a mobilné telefóny.
- **Výmena dát medzi viac než dvomi entitami** - v priemyslových sieťach je komunikačný kanál zbernicového typu. Keď kontrolér (riadiaca jednotka) odosiela dáta a tieto dáta sú doručené každej entite v danej sieti, výrazne sa tak zaťažuje sieť nepotrebnými prenosmi, čo môže mať vplyv na dobu doručenia u kritických aplikácií. Situácie, kedy každá entita v sieti prijíma takéto dáta by mali byť podla efektívnosti iba požiadavky typu DHCP a ARP. Z tohoto dôvodu boli vynájdené priemyslové protokoly, ktoré komunikujú len na adresách typu broadcast. U kancelárskych sietí je tento problém nepodstatný.

1.3.2 Porovnanie sietí z pohľadu CIA

Ďalším charakteristickým rozdielom medzi domácimi/kancelárskymi a priemyslovými sieťami je porovnanie sietí z pohľadu CIA triády (confidentiality, integrity, availability) - dôvernosť, integrita a dostupnosť. Je zrejmé, že pre domáce a priemyslové siete, zvlášť pre sieť KII v energetike budú platiť diametrálne odlišné princípy a postupy.

Jedným zo zásadných rozdielov je, že v prípade KI sa stará o zaistenie CIA triády vo väčšine prípadov štát, ktorý by mal tak vymedziť dostatočný počet prostriedkov na zaistenie bezpečnosti. Štát tak zaručí bezpečnosť KI pred teroristickými útokmi, ale aj prijme opatrenia na obmedzenie zraniteľnosti prvkov KI s dôrazom na informačné a komunikačné systémy, a na minimalizáciu negatívnych následkov útokov na ne, pričom bude pokračovať v aktivitách zameraných na bezpečnosť a integritu informačných a komunikačných systémov, zvlášť systémov nevyhnutných pre bezpečný výkon základných funkcií štátu [20]. V tejto práci predstavujú informačné a komunikačné systémy prvky v KII a KEI spoločnosti EG.D.

Zaistenie CIA triády je závislé od typu organizácie a veľkosti vyčlenených prostriedkov na zaistenie bezpečnosti. Niektorý z troch prvkov CIA triády tak môže prevažovať nad iným. Napr. dôvernosť je vyžadovaná v určitých štátnych odvetviach, napr. spravodajská služba, ktorá utajeným spôsobom získava informácie pre najvyš-

šie štátne orgány (polícia, bezpečnostná informačná služba, vojenské spravodajstvo). Integrita je vo zvýšenej miere vyžadovaná vo finančnom sektore, kde by napr. útočník pozmenením pár znakov (vyčlenenie 1 € namiesto 1 000 000 €) mohol spôsobiť katastrofické scenáre. Dostupnosť je vyžadovaná napr. v elektronickom obchode, kde by výpadok v ráde niekoľkých hodín mohol spôsobiť obrovské finančné straty, príp. v zdravotníckom sektore, kde by mohlo dôjsť ku stratám životom kvôli nefunkčnosti prístrojov [21]. Pre účely KI a účely tejto práce je najdôležitejšia práve dostupnosť. Pracovník dispečingu tak musí mať neustály dohľad nad aktuálnym obrazom siete tak, aby sa minimalizovalo riziko výpadku služby a pri výpadku bol prevedený tzv. havarijný plán. Z tohoto dôvodu je aj táto práca zameraná predovšetkým na testy dostupnosti.

V nasledujích riadkoch sú popísané jednotlivé zložky CIA triády, so zameraním na KII v energetike.

1. **Dôvernosť** - KII musí spĺňať všetky moderné princípy a postupy kyberbezpečnosti tak, aby nedošlo k úniku rôznych informácií, ktoré by mohol útočník zneužiť. V tomto prípade ide predovšetkým o zabezpečenie všetkých smerovačov, keďže každá rozvodňa predstavuje samostatný smerovač typu PE vo VPN modeli a každá rozvodňa zároveň potrebuje komunikovať s dispečingovými centrami prostredníctvom VPN spojenia. Jediným zraniteľným miestom je tak vstupný a výstupný smerovač, nakoľko medzi týmito smerovačmi sú dátové prenosy šifrované prostredníctvom VPN spojenia.
   K moderným princípom k zaisteniu správnej dôvernosti patrí v súčastnosti dvojfaktorová autentifikácia, prihlasovanie pomocou biometrických údajov, kedy sa pracovník KI dostáva následne do vnútra KII prostredníctvom rôznych VPN spojení.
   Medzi možné útoky na dôvernosť KEI môže patriť únik osobných informácií zákazníkov (rodné číslo, meno, priezvisko čísla účtov, heslá, email) alebo proprietárne informácie o KEI a KII. V takejto KI by malo byť zakázané akékoľvek vynášanie interných informácií - najmä nahrávanie, odpočúvanie, ukladanie správ a iné druhy zachytávania komunikácie. Pre zachovanie dôvernosti musia byť prenosy v KII dostatočne šifrované a pracovníci KII by mali používať dostatočne silné heslá pre minimalizáciu rizík pri autentizácii. Zaistenie dôvernosti zahŕňa aj obranu proti útokom typu social-engineering, kde je možná prevencia dosiahnutá vzdelávaním rizikových osôb v KI proti týmto typom útokov. KI by mala tradične obsahovať databázu osôb, ktorým je povolený autorizovaný prístup k špecifickým položkám a zároveň by mala neautorizovaným osobám tento prístup aktívne zamietnuť. Zamedzí sa tak zároveň prístup neoprávnených osôb do KI, kde by mohlo dôjsť ku krádežiam alebo poškodeniu fyzického HW, prípadne iného dôležitého objektu pre funkč-

nosť KI. K ďalším možným útokom na dôvernosť siete patria útoky typu MitM (man-in-the-midde), možný phishing, alebo eskalácia privilégií. Útočník by tak mohol získať údaje pre prístup do KI a zneužiť tajné informácie v nej obsiahnuté.

2. **Integrita** - zaisteniu integrity v KI venuje zákon č. 45/2011 o kritickej infraštruktúre, ktorý určuje primárne povinnosti prevádzkovateľov, ktorí musia na zabezpečenie v rámci stanovenej úrovne ochrany prijať všetky potrebné opatrenia pre dostatočnú ochranu prvku kritickej infraštruktúry tak, aby bola zaistená absolútna funkčnosť, kontinuita a integrita tohto prvku, zároveň však musia dbať aj na včasné odvrátenie, zmiernenie alebo neutralizáciu identifikovaných možných hrozieb a rizík [22]. Pre potreby KI môže ísť napr. o zaistenie mravnosti pracovníkov KI, ktorý musia zachovávať profesionálne dodržovanie štandardov, správne princípy a hodnoty pre úspešný chod KI. Tieto profesionálne štandardy a princípy sú najmä slovné dohody medzi pracovníkmi a vedením KI, kedy sa určujú formálne a neformálne zodpovednosti pracovníkov KI, spolu so správnymi zásadami správania v oblasti informačnej bezpečnosti [23].

   V oblasti informačných technológii je pre zaistenie integrity dôležité používanie zálohovania systému a súborov, používanie oprávnení na prístup k rôznym súborom (logy, proprietárne informácie). Vhodné je používanie digitálnych podpisov a digitálnych certifikátov, tak aby boli všetky súbory pri prenosoch pôvodné, bez možnosti úpravy pôvodných súborov.

3. **Dostupnosť** - zaistenie dostupnosti KII znamená minimalizovanie času, kedy je daný sieťový prvok nedostupný. Je teda nutné implementovať tzv. havarijné plány, ktoré budú ošetrovať neželané scenáre proti výpadkom a strate dát pri prenosoch. Z tohoto dôvodu sa využíva redundancie liniek a zariadení tak, ako to je možné vidieť na obr. 1. Väčšina liniek má pre účel zaistenia dostupnosti vždy záložnú trasu pre prípad, keby došlo k výpadku primárnej trasy. Linky a sieťové zariadenia by mali byť monitorované monitorovacími systémami tak, aby boli jasne rozpoznané neželané scenáre.

   K zaisteniu dostupnosti patrí aj obrana proti útokom z oblasti hackingu - rôzne útoky typu DoS (Denial of Service), kde by útočník mohol výrazne narušiť chod KII zamedzením dostupnosti pre ovládanie KII. Z tohoto dôvodu by mala mať KII na zamedzenie týchto útokov implementované dodatočné bezpečnostné prvky v podobe napr. firewall, IDS, IPS, proxy server a i.

   Systém, ktorý ma optimálne zaistenú dostupnosť, ktorý dokáže efektívne a účinne vykonávať požadované úlohy [24]. Takýto systém musí byť zároveň odolný voči možným vzniknutým chybám, ktoré by mohol potenciálny útočník spôsobiť a odoprieť tak pracovníkovi KI úlohy, ktoré musí vykonať.

2 Súčasná situácia a zmeny vo využívaní sietí

Pre úspešné porovnanie technológie MPLS a SD-WAN v nasledujúcich kapitolách ako hlavnej technológie pre prenosy v privátnej WAN je vhodné analyzovanie súčasných trendov v oblasti sietí, z čoho lepšie vyplynie vhodná technológia pre použitie v KI.

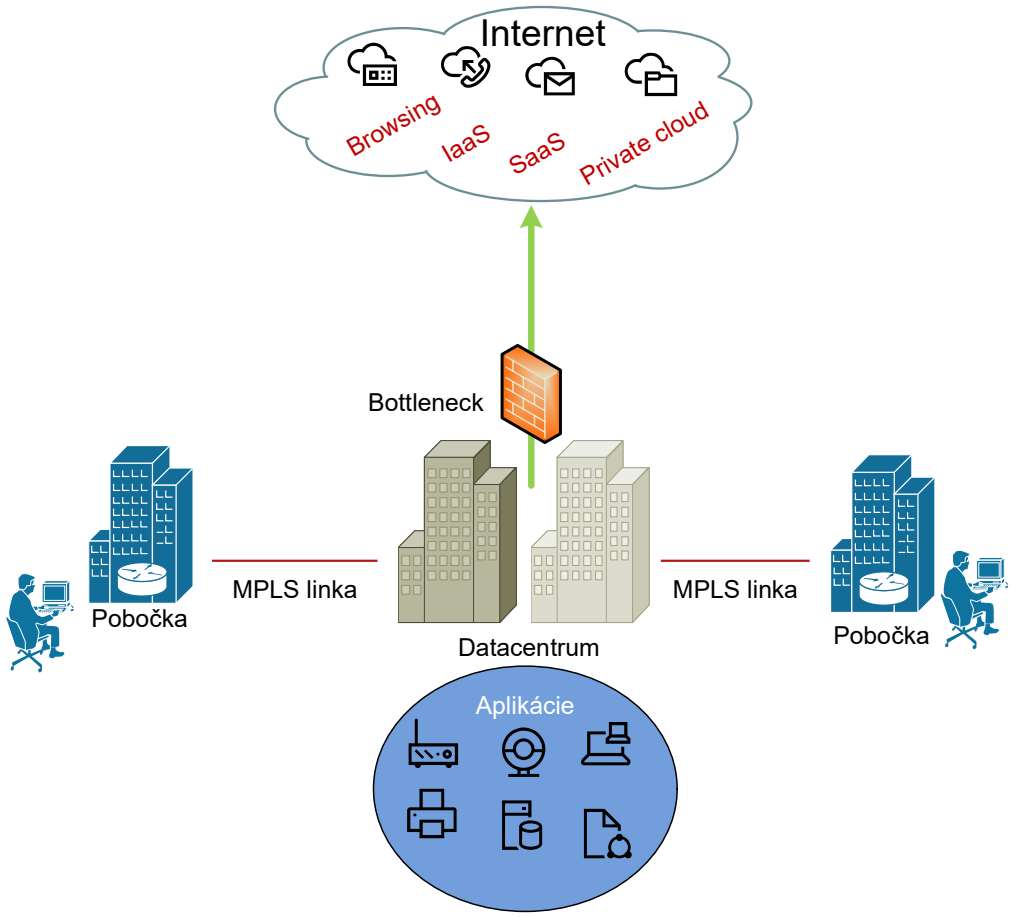
Za posledných pár rokov sa využívanie telekomunikačných sietí zažíva rapídnu zmenu. Aktuálna situácia s COVID-19 výrazne znásobila používanie sietí. Vďaka najnovším trendom sú zamestnanci rôznych firiem schopní efektívne pracovať zo svojich domácností z ľubovolného miesta. Tento spôsob práce objavil nové možnosti práce z domova a zistilo sa, že nie vždy je nutná fyzická prítomnosť na pracovisku. Ako ideálna sa javí hybridná práca, kedy sa z domu dá odviesť rovnaká práca s ušetrením cestovania na pracovisko pre relevantné oblasti zamestnania. Tento spôsob práce je možné očakávať v období nasledujúcich niekoľko rokov.

V tradičnom riešení WAN sietí bolo riešenie prístupu do podnikových sietí založené na princípe VPN, cez ktorú sa používatelia dostali do podnikovej siete. Podniková sieť bola napojená na centrálny bod, kde bola uložená väčšina aplikácií a následne bola pripojená do internetu. Rovnako používatelia sa prostredníctvom VPN pripájali do centrály a odtiaľ ďalej do internetu. Nevýhodou zostáva decentralizovaná distribuovaná architektúra. Pri prístupe vzdialených pobočiek do svetovej siete internet bolo potrebné smerovanie prevádzky cez tradičné MPLS linky do centralizovanej internetovej prípojky umiestnenej v datacentre. V dnešnej dobe tvorí internetová prevádzka 80 % celkovej prevádzky a práve toto predstavuje bottleneck a hlavnú nevýhodu pri používaní tradičných WAN riešení.

2.1 Architektúra tradičnej pobočkovej WAN siete

Tradičná WAN zabezpečovala pripojenie užívateľov na vzdialených pobočkách s ich aplikáciami a dátami, ktoré boli uložené v súkromných datacentrách v jednej centralizovanej lokalite. Takéto datacentrum má centralizovanú prípojku do svetovej siete internet so všetkými bezpečnostnými službami pre bezpečné spojenie. Táto prípojka zároveň zaisťuje centralizovanú konektivitu do siete internet pre prípadné aplikácie obsiahnuté v datacentre. Charakteristickým prvkom tradičných WAN sietí je pomer internej a externej prevádzky. Internou prevádzkou v tomto prípade sa rozumie prevádzka zo vzdialenej pobočky do súkromného datacentra. Patrí sem prevádzka aplikácií uložených v súkromnom datacentre smerom k vzdialenej pobočke a naopak. Externou prevádzkou sa rozumie prevádzka zo vzdialenej pobočky do svetovej siete internet. Patrí sem prevádzka ku cloudovým aplikáciám alebo prehľadávanie internetu. V minulosti bol tento pomer 80 % internej a 20 % externej prevádzky, kedy

bol tento princíp prístupu k aplikáciám uloženým v datacentre postačujúci. Táto architektúra je zobrazená na obr. 2.1, kde sú zobrazené 2 pobočky a datacentrum, ktoré obsahuje využívané aplikácie. Toto datacentrum obsahuje požadované aplikácie, ktoré môžu využívať pracovníci na pobočkách. Problém však nastáva, ak chcú pracovníci na pobočkách využívať svetovú sieť internet, nakoľko všetka prevádzka musí prechádzať cez jednu centralizovanú prípojku.



Obr. 2.1: Bottleneck siete

2.1.1 Zabezpečenie tradičnej WAN

Väčšina riešení bezpečnosti pobočiek spočíva v zabezpečení centralizovanej prípojky do svetovej siete internet a väčšina bezpečnostných riešení je centralizovaných práve v tomto mieste. Takéto riešenie bezpečnosti je v porovnaní s SD-WAN nákladné a neefektívne, pretože je potrebné spravovanie prídavných zariadení.

Pobočkovú bezpečnosť internetovej prípojky na vzdialenej pobočke je možné realizovať 3 možnosťami:

1. **Cloudová bezpečnosť** - ide o prevádzku z pobočky do svetovej siete internet. Táto prevádzka je filtrovaná službami od poskytovateľa cloudovej bezpečnosti. Tento typ zabezpečenia má výhodu vo vysokej škálovateľnosti a nevýhoda spočíva vo viditeľnosti a kontrolovaní prevádzky z pobočky do datacentra.
2. **Dodatočné bezpečnostné zariadenie** - na pobočke je aplikované bezpečnostné zariadenie, ktoré kontroluje prevádzku medzi pobočkou a datacentrom. Nevýhoda spočíva v pridaní zariadenia, teda potreby fyzického miesta na pobočke, správy a manažmentu zariadenia.
3. **Kombinácia obidvoch riešení** - kombinovaná bezpečnosť prídavného zariadenia, čím sa oproti cloudovej bezpečnosti umožní viditeľnosť a kontrola prevádzky medzi pobočkou a datacentrom. Nevýhodou tohoto riešenia je štandardne použitie bezpečnosti od viacerých výrobcov, čo komplikuje celkovú správu (vysoké náklady).

2.1.2 Požiadavky na pripojenie pobočky do WAN

V tejto podkapitole sú popísané aspekty, ktoré rozhodujú pri voľbe architektúry výslednej podoby siete. Pre úspešnú voľbu technológie použitej v sieti je potrebné čo najpresnejšie poznanie účelu takejto siete v normálnych podmienkach a pri poruche. V nasledujúcich bodoch sú popísané všeobecné požiadavky, ktoré sú vyžadované pri prepájaní vzdialených pobočiek vo WAN sieti.

- Všeobecným primárnym požiadavkom na pripojenie vzdialenej pobočky je komunikácia s aplikáciami uloženými v súkromnom datacente. Pre potreby KI podľa informácií obsiahnutých v prvej kapitole tejto práce, pôjde o komunikáciu jednotlivých rozvodní s dispečingovými centrami.
- Ďalším z dôležitých požiadavkov je smerovanie prevádzky kritických aplikácií cez transportnú infraštruktúru, ktorá zaisťuje potrebné SLA parametre. To znamená, že je potrebné aby prevádzka vo WAN sieti nebola smerovaná tradičným spôsobom napr. na základe najkratšej cesty, ale prostredníctvom SLA parametrov, kedy koncový užívateľ dostáva potrebnú šírku pásma pre potreby jeho kritických aplikácií. Technológie MPLS (MPLS-TE) a Cisco SD-WAN (Application aware routing) majú pre tieto potreby vlastné technológie, ktoré budu popísane v ďalších kapitolách.
- Konektivita užívateľa na pobočke s požadovanými aplikáciami uloženými na cloude, kedy je požadovaná konektivitu do svetovej siete internet, ktorá zaistí potrebnú kvalitu služby pre prístup a komunikáciu s cloudovými aplikáciami. Priama konektivita internetu na vzdialenej pobočke nemusí byť využívaná pre komunikáciu s cloudovými aplikáciami, ale môže byť využitá aj pre tradičné surfovanie po internete či už priamo pracovníka alebo návštevníkov na pobočke. Na ta-

kejto pobočke je potrebné sprostredkovať priamu internetovú konektivitu, čo zahŕňa zabezpečenie vlastnej infraštruktúry na pobočke pred potenciálnymi útokmi zo svetovej siete internet.

Zo záveru práce vyplynie, že internetová konektivita pre KII v energetike nie je taká dôležitá, ako pri tradičných kancelárskych pobočkových ústredniach, ktoré nepatria do KI.

2.1.3 Zhrnutie analýzy tradičných WAN riešení

V tradičných WAN sieťach je komunikácia vzdialenej pobočky a aplikácie uloženej na cloude smerovaná do centrálnej internetovej prípojky typicky uloženej v datacentre. Pre tento typ pripojenia bol ustanovený anglický výraz backhauling. WAN linka prepojujúca pobočku s centralizovanou internetovou prípojkou umiestnenou v datacentre obsahuje zvyčajne objemné dátové prenosy, nakoľko obsahuje prevádzku do svetovej siete internet a zároveň aj prevádzku aplikácií uložených v datacentre. Pri uvažovaní užívateľskej skúsenosti užívateľov na vzdialených pobočkách nie je komunikácia s cloudovou aplikáciou konštantná, kedy v prípade veľkej réžie na WAN linkách klesá kvalita spojenia.

Z analýzy tradičných WAN riešení vyplýva, že v súčasnej dobe sa väčšina aplikácií sťahuje z datacentier do cloudového prostredia. Na túto zmenu pružne reaguje nová technológia SD-WAN sietí. Očakávanými zmenami pri SD-WAN sú tak prispôsobenie dátových prenosov do svetovej siete internet so zachovaním škálovateľnosti, bezpečnosti a dôvernosti súkromných pobočkových sietí. Pre potreby KEI a KII je však prístup do svetovej siete minimalizovaný z dôvodov zachovania bezpečnosti KI a nezávislosti na internete. Bližšie porovnanie technológií v súkromnej WAN pre prenosy v KI bude popísaný v závere tejto práce.

Jedným z cieľov práce je porovnanie MPLS technológie ako základnej WAN s inou modernou WAN technológiou. Kvôli praktickým možnostiam dostupným v emulátore GNS3 bola vybraná práve technológia Cisco SD-WAN, ktorá je bližšie popísaná v tretej kapitole. Kvôli HW náročnosti technológie Cisco SD-WAN v emulátore GNS3 sa nepodarilo plne sprevádzkovať rovnakú topológiu, ako tomu bude pri MPLS technológii. Súčasťou záveru práce iba teoretické porovnanie týchto technológií, pričom bola prakticky overená funkčnosť MPLS technológie pre KII, popísaná v štvrtej kapitole.

3 Cisco SD-WAN

Pri SD-WAN technológii sú pobočky pripojené do podnikovej siete priamo cez internet, kedy väčšina dát a aplikácií je uložených v cloudovom prostredí. Nie je potrebná VPN, pretože dáta a aplikácie sú priamo dostupné. V tomto spočíva najnovší trend pri zmenách v infraštruktúre sietí. V rámci Slovenskej a Českej republiky sa dá nájsť aktuálne použitie, či migrácia do SD-WAN technológie najmä u veľkých korporátnych spoločností, ktoré majú menšie v pobočky v ČR a SR, pričom ich hlavné pobočky už technológiu SD-WAN využívajú v iných krajinách.

V prípade SD-WAN neplatia tradičné spôsoby WAN sietí. Výrazná výhoda spočíva v pripojovaní do siete IoT zariadení, mobilných užívateľov (smartphone, tablet) a iných zariadení, ktoré nie je možné plne monitorovať v rámci siete. SD-WAN umožňuje v takomto prostredí bezpečnú segmentáciu siete, teda oddelenie prevádzky jednotlivých zariadení, ktoré nie sú pod správou, tak aby bola zachovaná bezpečnosť podnikovej siete. V dnešnej dobe sa aplikácie, s ktorými užívateľ pracuje nenachádzajú výhradne v súkromných datacentrách, ale sú uložené u poskytovateľa cloudových služieb (Amazon Web Services, Microsoft Azure, Google Cloud). Infraštruktúra SD-WAN siete môže byť zároveň zálohovaná u jedného z poskytovateľov cloudových služieb. Zvyšuje sa tak počet aplikácii fungujúcich na princípe SaaS (Software as a service), napr. služby ako Office 365, Dropbox, Google Drive a i. So zmenou aplikačného prostredia sa výrazne mení pomer internej a externej prevádzky. Externá prevádzka do svetovej siete internet výrazne prevyšuje internú prevádzku medzi pobočkou a súkromným datacentrom.

Cieľom Cisco SD-WAN je automatizovanie stávajúcej infraštruktúry pomocou programovateľných rozhraní. Z infraštruktúry sa pomocou telemetrických dát vytvára približný kontext, ktorý sa následnou analýzou (umelá inteligencia) spracováva a vytvára sa aktuálny obraz siete. Tento aktuálny obraz siete sa dá zobraziť pomocou GUI v tzv. komponente vManage.

3.1 Transformácia z tradičnej WAN na SD-WAN

Pri transformácii z tradičnej WAN na SD-WAN je nutné zvážiť niekoľko aspektov pri návrhu finálnej podoby SD-WAN siete. V nasledujúcich bodoch je popísaný zoznam najdôležitejších uvážení pri navrhovaní SD-WAN siete:

- Dizajn kontrolérov, ktoré riadia sieť. Tieto kontroléry môžu byť uložené v cloudovom alebo vo vlastnom prostredí (datacentrum), podľa potrieb daného zákazníka. Zákazníci si tak podľa svojich finančných možností volia uloženie kontrolérov vo vlastnom/cloudovom prostredí.

- Určenie početnosti vo využívaní cloudových služieb. Pri veľkej internetovej prevádzke sa volí viacero druhov transportov do svetovej siete internet (4G/LTE, MPLS, Internet).
- Bezpečnostné funkcie.
- Segmentácia, kedy SD-WAN dosahuje podobnú segmentáciu ako MPLS. SD-WAN navyše umožňuje segmentáciu nezávislú na transporte.
- Redundancia vrátane redundancie kontrolérov, pre optimálnu funkčnosť siete pri normálnom stave siete a pri poruche.
- Škálovateľnosť, kde SD-WAN predstavuje ideálne riešenie pre prepojenie jednotlivých pobočiek prostredníctvom VPN modelov. SD-WAN dokáže prehľadne spravovať tisícky pobočiek, pričom vďaka využívaniu automatizácie a umelej inteligencii sú tieto pobočky automaticky spravované a monitorované.
- Prepojenie okrajového smerovača so sieťou, kedy pri sa použití Cisco SD-WAN používa komponenta vEdge, ktorá poskytuje tzv. ZTP (Zero-Touch Provisining). Pracovník tak zapojí smerovač do napájania a siete a o ďalšia konfigurácia sa rieši automaticky z centrálneho miesta.
- Druh prevádzky v sieti s využitím príslušných SD-WAN, ktoré budú popísané v kap. 3.4.

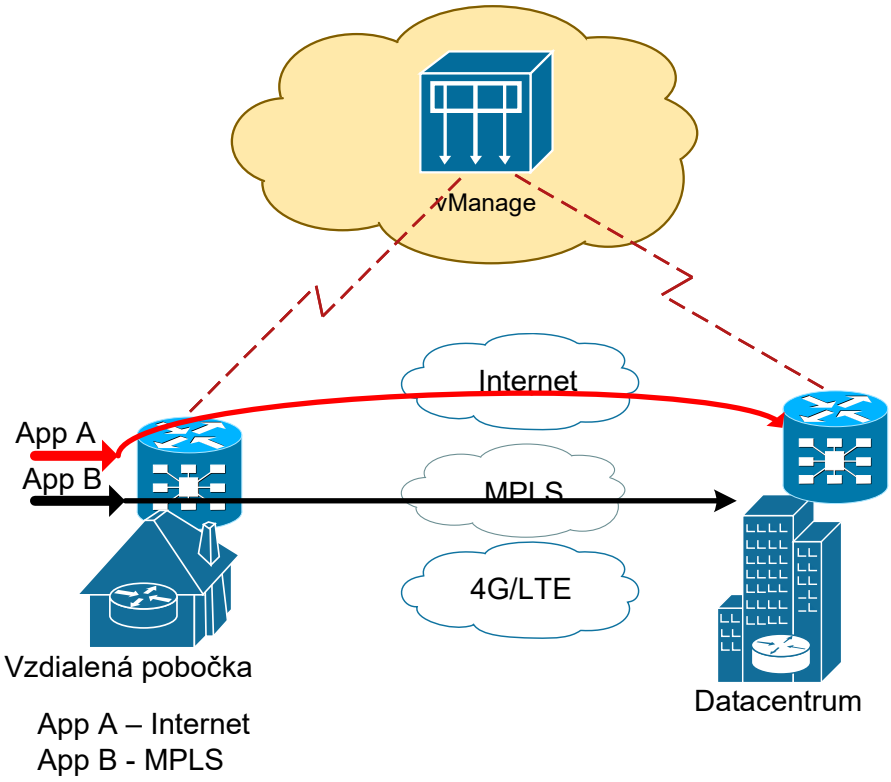
3.2 Dôvody nasadzovania SD-WAN sietí

SD-WAN princíp nie je technológia, ktorá by vyhovovala v každej situácii a tak je nutné analyzovanie danej problematiky siete, podľa čoho sa rozhodne o vhodnej technológii pre spravovanie siete. V prípade SD-WAN sietí sú hlavné výhody:

1. **Lepší manažment** - klient, ktorý má napr. 10 až 100 lokalít môže spravovať celú sieť s menším počtom kontrolérov v porovnaní s tradičnou WAN. Patrí sem napr. jednoduchá konfigurácia okrajových smerovačov, aktualizácie softvéru a i. Tieto operácie sú výrazne jednoduchšie a efektívnejšie pri nasadení SD-WAN technológie.
2. **Cloudové služby** - v súčasnej dobe dochádza k výraznému nárastu používania cloudových aplikácií. V tradičnej WAN sa k aplikáciám pristupovalo cez centrálne miesto (datacentrum), kde bola aplikácia uložená. V súčasnej dobe je väčšina aplikácií uložená na cloude vo svetovej sieti internet a prevádzka vnútri internej sieti tvorí iba 20 % oproti 80 % internetovej prevádzky. SD-WAN reaguje na túto zmenu, nakoľko centralizovaná prípojka v súkromnom datacentre, cez ktorú vzdialené pobočky pristupujú ku cloudovým aplikáciám môže predstavovať bottleneck.
3. **Bezpečnosť** - pri nasadení nového okrajového smerovača je väčšina bezpečnostných funkcií automaticky integrovaná v smerovači. Odpadáva tak nutnosť

použitia prídavných prvkov, akými boli prídavný WAN smerovač alebo firewall.

4. **Traffic-Engineering** - lepší manažment dátových tokov vo WAN sieti pomocou centralizovaných politík (Aplication-aware routing). Zvyšuje sa tak flexibilita siete, nevzniká závislosť na SP (Service Provider) a je možné ľubovolne upravovať politiky pomocou centralizovaného kontroléru.
5. **Lacnejšia konektivita** - nahradenie stávajúcich drahších riešení privátnej konektivity (MPLS) lacnejšou (Internet), ktorá má v určitých prípadoch rovnaké alebo lepšie parametre za nižšiu cenu.
   Pre túto možnosť sa predpokladá viacero možností konektivity do vzdialenej pobočky. Tradične tvorí hlavnú linku MPLS linka a za prídavné označujeme napr. internetovú linku. Pre komunikáciu vzdialenej pobočky a kritickej aplikácie sa môže využívať vo vhodných prípadoch okrem MPLS linky aj sekundárna konektivita (internet). Dochádza tak k rozšíreniu šírky pásma, ktoré majú k dispozícii kritické aplikácie. Princíp zobrazuje obr. 3.1, kde aplikácia označená ako App A využíva internetovú linku, zatiaľ čo aplikácia B označená ako App B používa drahšiu MPLS linku pre kritickejšie prenosy.

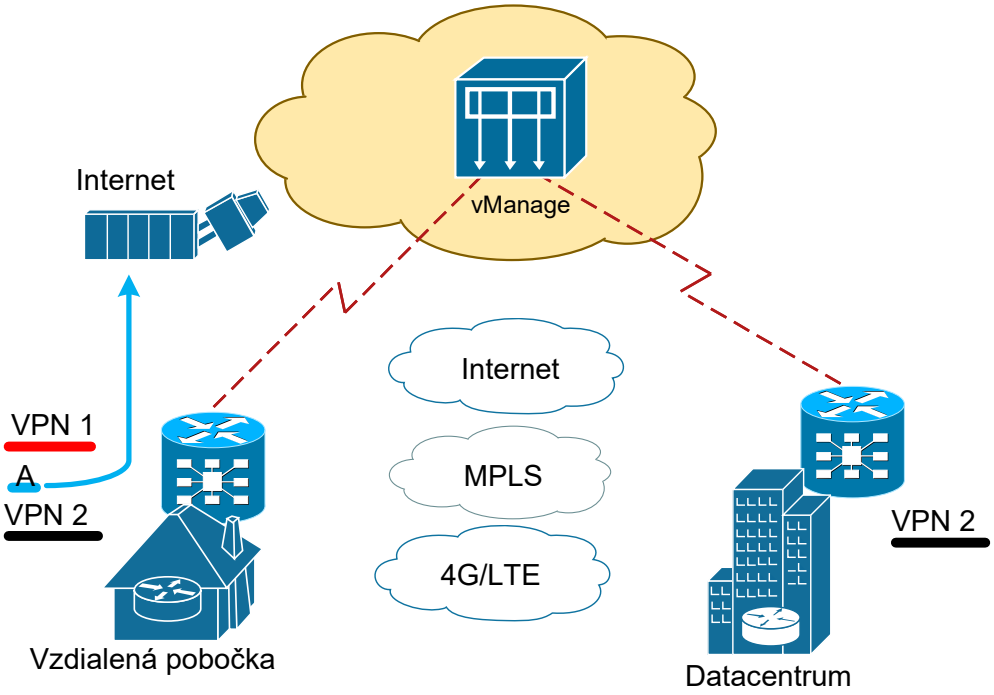


Obr. 3.1: Lacnejšia konektivita

6. **Konsolidácia zariadení** - v tradičnej WAN je potrebné mať väčší počet

prvkov (WAN smerovač, firewall), kým pri SD-WAN sú tieto prvky implementované v rámci jedného zariadenia. Dochádza tak k menšiemu počtu zariadení, menšej cene a jednoduchšej správe týchto zariadení.

7. **Guest WiFi** - povolenie prístupu do svetovej siete internet na vzdialenej pobočke návštevníkom pobočky, pričom konektivita do internetu nebude využívať MPLS infraštruktúru pre transport internetovej komunikácie hostí do centralizovanej internetovej prípojky, ale bude presmerovaná do pomalšej, lokálnej internetovej prípojky na vzdialenej pobočke. Týmto spôsobom je poskytnuté pripojenie do svetovej siete internet bez zaťaženia MPLS liniek smerom do infraštruktúry datacentra. Princíp Guest Wifi je zobrazený na obr. 3.2, kde je prevádzka od návštevníkov vzdialenej pobočky, ozn. ako A smerovaná do lokálnej internetovej prípojky ozn. ako Internet.

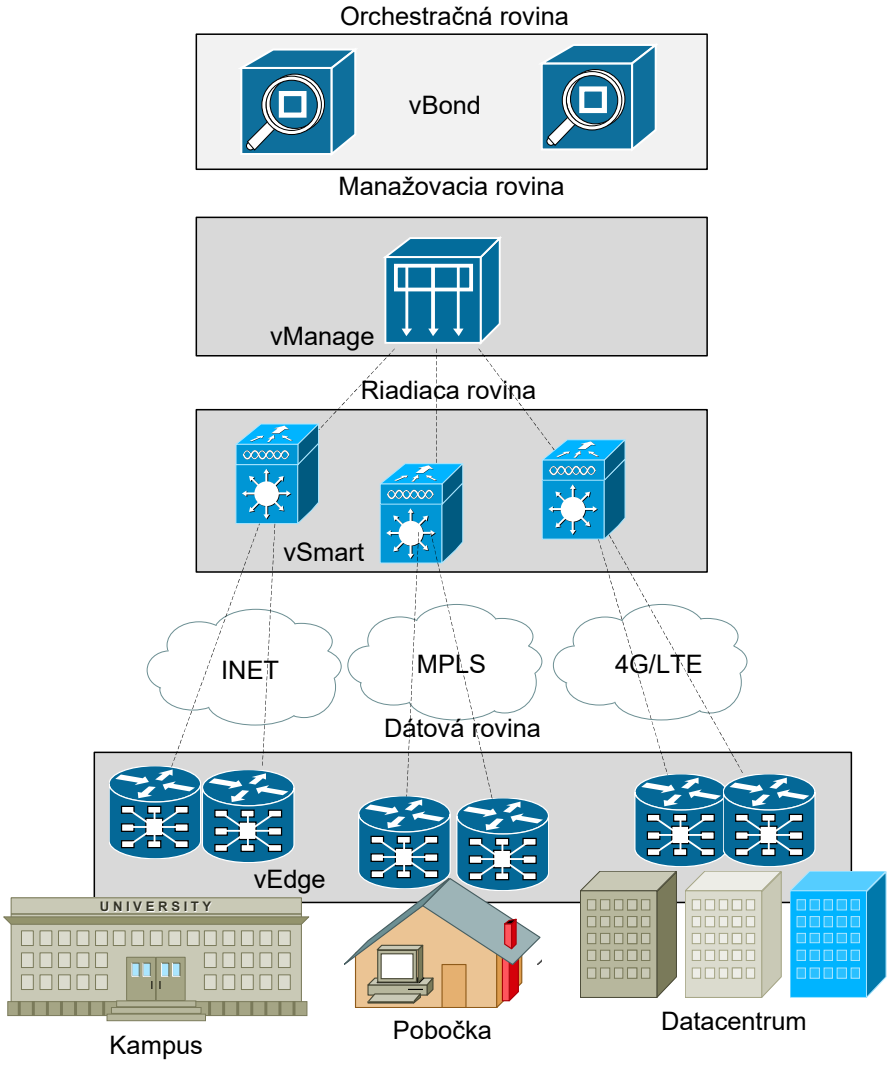


Obr. 3.2: Guest WiFi

3.3 Roviny SD-WAN siete

SD-WAN sieť aplikuje princíp SDN sietí, kde je od seba striktne oddelená dátová a riadiaca rovina. Dátová rovina sa v tomto prípade stará o zaistenie konektivity medzi jednotlivými lokalitami (datacentrum, kampus, cloudová infraštruktúra). Riadiaca rovina umožňuje implementovanie inteligencie SD-WAN siete (distribúcia smerovacích informácií, aplikovanie vlastnej sieťovej príp. bezpečnostnej politiky). Nad

riadiacou rovinou sa nachádza manažovacia rovina, ktorá zaisťuje správu a dohľad celej SD-WAN infraštruktúry. Nad manažovacou rovinou sa nachádza orchestračná rovina. Táto rovina má na starosti inicializáciu SD-WAN infraštruktúry. Prehľadnosť jednotlivých rovín Cisco SD-WAN zobrazuje obr. 3.3 kde sú zobrazené jednotlivé kompomenty a ich príslušná rovina. Koncové pobočkové smerovače označené ako vEdge sú koncovými smerovačmi jednotlivých lokalít (kampus, datacentrum).



Obr. 3.3: Roviny Cisco SD-WAN

3.3.1 Kompomenty Cisco SD-WAN

Komponenty vBond, vManage a vSmart sú implementované formou virtuálnych serverov, ktoré môžu byť nainštalované napr. v prostredí VMware, vSphere, v prostredí KVM virtualizácie alebo v prostredí cloudových operátorov (Microsoft Azure, Amazon Web Services). Cisco SD-WAN tak potrebuje pre svoju funkčnosť 3 samostatné

virtuálne servery a jeden fyzický HW prvok (vEdge).

Pre priblíženie funkcie je vložený stručný popis jednotlivých komponent Cisco SD-WAN.

1. **vBond** - táto kompomenta tvorí orchestračnú vrstvu. Poskytuje konektivitu medzi dátovou a riadiacou rovinou a managementom siete. vBond využíva tzv. ZTP (Zero Touch Provisioning) server pre Cisco SD-WAN komponenty a PnP (Plug and Play) server pre Cisco zariadenia. Uplatnenie týchto serverov sa dá nájsť pri expandovaní siete, kde postačuje zapojenie daného sieťového prvku technikom bez IT vzdelania a o ďalšiu konfiguráciu sa stará sieťový administrátor z centrálneho miesta. ZTP server využíva Zero Trust - architektúru, kedy pri pripojení prvku do SD-WAN infraštruktúry sa môžu pripojiť len tie zariadenia, ktoré sú k tomu oprávnené. vBond automatizuje procesy na sieťových prvkoch a je zároveň prvým bodom autentifikácie, kedy pri zapojení prvku do SD-WAN siete prejde informácia ako prvá práve do komponenty vBond.
2. **vManage** - tento komponent tvorí manažovaciu rovinu a umožňuje riadenie celej SD-WAN siete. Pod týmto pojmom si môžeme predstaviť centrálny bod, odkiaľ sa riadi celá sieť. Označuje sa anglickým výrazom NMS (Network Management System solution). vManage konzola môže byť implementovaná buď priamo v datacentre alebo v cloudovom prostredí.

   Cez vManage sa realizuje napr. troubleshooting siete, konfigurovanie prvkov, ping, traceroute, meranie prevádzky (stratovosť paketov, jitter) akéhokoľvek prvku v SD-WAN sieti. Poskytuje jednoduchý GUI, cez ktorý sa spravuje sieť. Výrazné vylepšenie predstavuje troubleshooting siete, kedy bolo potrebné využívať tradičné postupy, akými boli prihlasovanie sa do smerovača, ping a traceroute. Tieto nástroje sú súčasťou GUI vManage servera. V rámci troubleshootingu je možné jednoduchým spôsobom simulovať aplikačný tok aplikácie, kde dôjde napr. k overeniu funkcie Application-aware routing podľa definovaných SLA parametrov, čo bude predmetom ďalšej podkapitoly.
3. **vSmart** - táto komponenta sa označuje ako riadiaca rovina, určená primárne na distribúciu smerovacích informácií medzi jednotlivými zariadeniami na vzdialených pobočkách, datacentrách alebo v prostredí cloudových infraštruktúr. Ďalej slúži na implementovanie vlastných sieťových politík, ktoré ovplyvňujú smerovanie medzi jednotlivými pobočkami. vSmart je umiestnený na jednom mieste centrálne, a nie je teda distribuovaný v každom zariadení. Nadväzuje susedstvo so všetkými koncovými prvkami, ktorých informuje o konektivite.
4. **vEdge** - táto komponenta sa označuje ako dátová rovina. Je to jediný hardwarový prvok v Cisco SD-WAN architektúre, vykonávajúci jednotlivé operácie podľa pokynov od vSmart. Sú to smerovače na jednotlivých pobočkách, ktoré slúžia k transportu užívateľskej a aplikačnej prevádzky. Tieto koncové

smerovače sú medzi jednotlivými prevádzkami navzájom prepojené pomocou šifrovaného spojenia. Dátová a riadiaca rovina sú teda od seba striktne oddelené, čím sa dosiahlo úplné odstránenie problému tzv. single-point-of-failure. Pri zlyhaní spojenia medzi komponentami vEdge a vSmart si vEdge udržuje smerovaciu tabuľku, čím sa zachová spojenie s pripojenou lokalitou.
vEdge ako koncové smerovače na jednotlivých pobočkách využívajú na komunikáciu medzi sebou IPSec tunely šifrované pomocou algoritmu AES256. Tieto tunely sa môžu ľubovolne modifikovať podla potrieb užívateľa (ACL, QoS) a zároveň sú automaticky nadviazané medzi kocovými smerovačmi (vEdge).

3.4 Funkcie zabezpečujúce užívateľskú skúsenosť

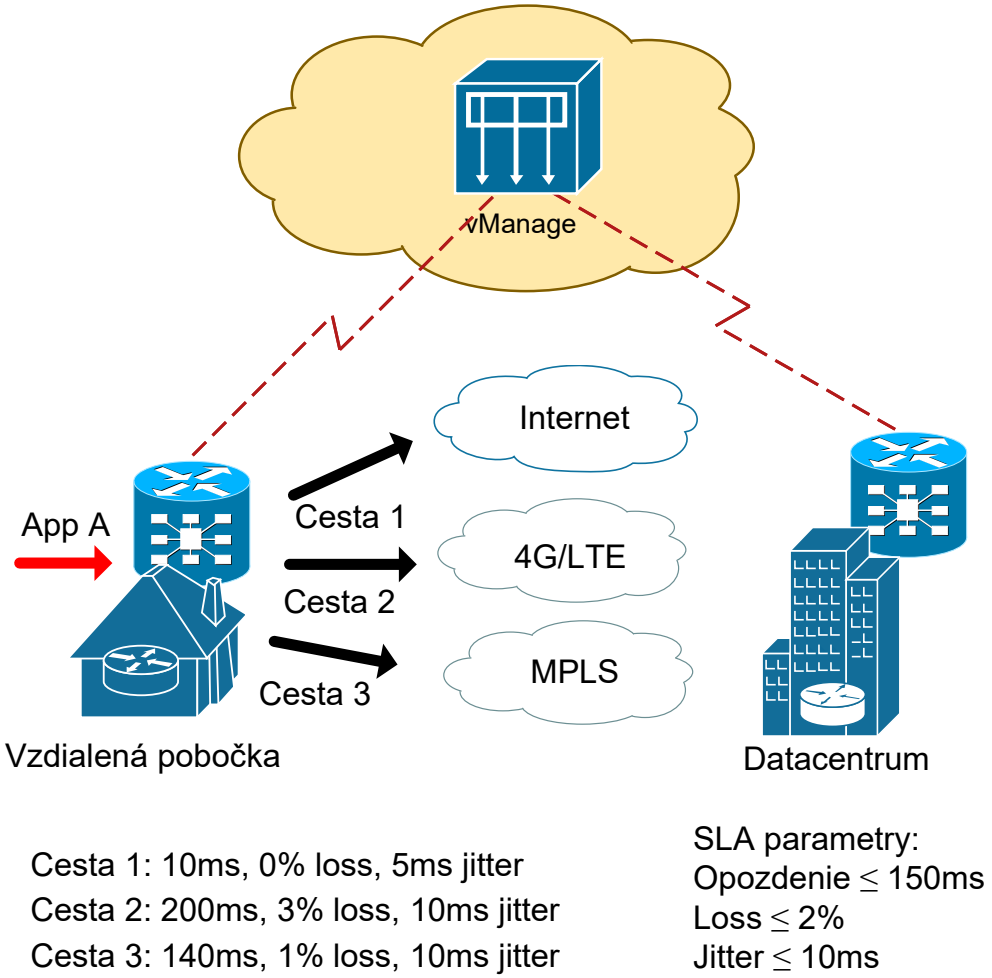
Cisco SD-WAN obsahuje niekoľko funkcií v rámci WAN infraštruktúry, podobne ako iné technológie (MPLS), ktoré majú svoje výhody a nevýhody. Funkcie popísané nižšie zabezpečujú užívateľskú skúsenosť, to znamená potrebnú kvalitu služby pre koncových používateľov na jednotlivých pobočkách bez ohľadu na lokalitu dát a aplikácií. Vďaka týmto funkciám sa SD-WAN princíp odlišuje od tradičných IP princípov a prináša nové moderné možnosti v oblasti sieťovania.

3.4.1 Application-aware routing

Táto funkcia smeruje prevádzku kritickej aplikácie cez transportnú infraštruktúru s definovanými SLA parametrami. Aplikačné SLA parametre monitorujú aktuálny stav transportov a podľa potreby inteligentne smerujú prevádzku v sieti. SLA sú v SD-WAN sieti technicky limitované, čo môže pri návrhu siete predstavovať ťažkosti najmä pri poskytovaní konektivity globálnym klientom, ktorý ma veľký počet pobočiek v rôznych krajinách a práve zaistenie SLA medzi viacerými krajinami nemusí byť jednoduché.

Vďaka tejto funkcii je možné pre daný typ aplikácie posielať prevádzku iným transportom, než sú väčšine prípadov MPLS linky. MPLS linky sú tradične veľmi vyťažené a ak to daná aplikácia dovoľuje tak jej prevádzka sa dá posielať komoditnejším typom transportu (broadband), čím sa zníži vyťaženosť MPLS liniek a využije sa tak iný typ transportu (4G/LTE, Internet).

Obr. 3.4 zobrazuje princíp takéhoto smerovania s preddefinovanými parametrami. Aplikácia označená ako App A má k dispozícii 3 možnosti transportu, z čoho parametre spĺňajú 2 cesty. V tomto prípade dôjde k využitiu cesty ozn. ako Cesta 1, čo predstavuje transport cez Internet pre aktuálne najvýhodnejšie parametre.



Obr. 3.4: Application-aware routing

3.4.2 Samo-opravné kódovanie FEC

Táto funkcia patrí k funkciám zaisťujúcim vysokú kvalitu prenosovej služby pri použití napr. internetovej konektivity ako transportného prostredia. Bloky dát sú doplnené paritnými paketmi, ktoré pri prípadnej strate paketov umožňujú opravu poškodeného bloku.

3.4.3 Software as a service (SaaS)

V dnešnej dobe narastá využívanie aplikácií uložených na cloude a ako bolo spomenuté v predchádzajúcich podkapitolách, práve SD-WAN technológia sa snaží na túto zmenu pružne reagovať. SaaS princíp znamená, že želaná aplikácia, ktorá je požadovaná nie je uložená v tradičnom datacentre, ale v cloudovom prostredí. K prístupu postačuje prístup na internet a webový prehliadač. Zvyčajne je potrebná na strane

poskytovateľa aplikácie uloženej v cloudovom prostredí dodatočná registrácia a niekoľko nastavení pred samotným používaním aplikácie.

Využívaním SaaS služieb dochádza ku zníženiu nákladov. Nie je potrebný fyzický hardware pre aplikácie, ale len prístup k ním pomocou internetu, nakoľko sú uložené v cloudovom prostredí u poskytovateľa.

3.4.4 Infrastructure as a service (IaaS)

V tradičných WAN sieťach sa prepájanie pobočiek s datacentrom, kde je umiestnená centralizovaná internetová prípojka realizovalo pomocou IPSec point-to-point tunelov s využitím technológií ako napr. Azure Express Route, AWS Direct Connect. Toto spojenie prináša niekoľko obmedzení. Z hľadiska segmentácie nie je možné segmentovať prevádzku zo vzdialenej pobočky do datacentra v rámci cloudového prostredia a zároveň pri použití tradičných point-to-point IPSec tunelov je obtiažne implementovať potrebnú kvalitu služby pre rôzne aplikácie.

V prípade použitia SD-WAN infraštruktúry pre implementáciu IaaS dochádza k výraznej optimalizácii použitia cloudovej infraštruktúry, podobne ako pri použití SaaS. Je možné nasadiť koncový SD-WAN smerovač priamo do cloudového prostredia (Amazon Web Services, Microsoft Azure), čím je umožnená segmentácia od vzdialenej pobočky až po cloudové datacentrum.

3.4.5 Duplikácia paketov

Pri použití vysoko-stratovej linky v rámci transportnej SD-WAN infraštruktúry je možné stratovosť paketov výrazne zmenšiť duplikáciou paketov cez jednotlivé transportné linky.

3.5 Segmentácia SD-WAN

V tradičnej WAN nie je možné segmentovať zariadenia, aké predstavujú napr. IoT zariadenia a podobné komunikačné IT zariadenia. Tieto typy zariadení nemusí mať IT oddelenie plne pod kontrolou a pre zaistenie bezpečnosti je potrebné ich oddelenie od tradičných zariadení, akými sú laptop alebo pevná pracovná stanica. Pre segmentáciu end-to-end prevádzky medzi vzdialenou pobočkou a lokalitou dátového centra sa v tradičných WAN využívajú služby MPLS, kde sa pomocou oddelených VPN sietí dosahovalo potrebnej segmentácie. Toto riešenie je označené ako nákladné, pretože každá MPLS VPN služba od poskytovateľa pripojenia je typicky spoplatnená.

V prípade SD-WAN siete je možná segmentácia end-to-end medzi jednotlivými pobočkami alebo pobočkami a datacentrami navzájom. To znamená, že rozhranie

na strane koncového pobočkového smerovača môžeme priradiť do rozličných VPN sietí. Komunikácia medzi VPN sieťami je oddelená a v prípade potreby je možné zlúčiť VPN siete napr. pomocou centrálneho firewallu, čím ostáva zachovaná bezpečnosť. SD-WAN využíva pre segmentáciu tradičné princípy WAN sietí:

- oddelená VRF smerovacia tabuľka pre jednotlivé VPN siete,
- pre rôzne VPN siete je možné vytvárať rôzne topológie (Per-VPN). To znamená, že napr. pre VPN sieť zaisťujúcu napr. IP telefóniu je možné vytvoriť full-mesh topológiu, pre VPN sieť s kritickou aplikáciou je možné vytvoriť Hub-and-Spoke topológiu, prípadne iný typ topológie podľa potreby.

3.6 Zapezpečenie Cisco SD-WAN

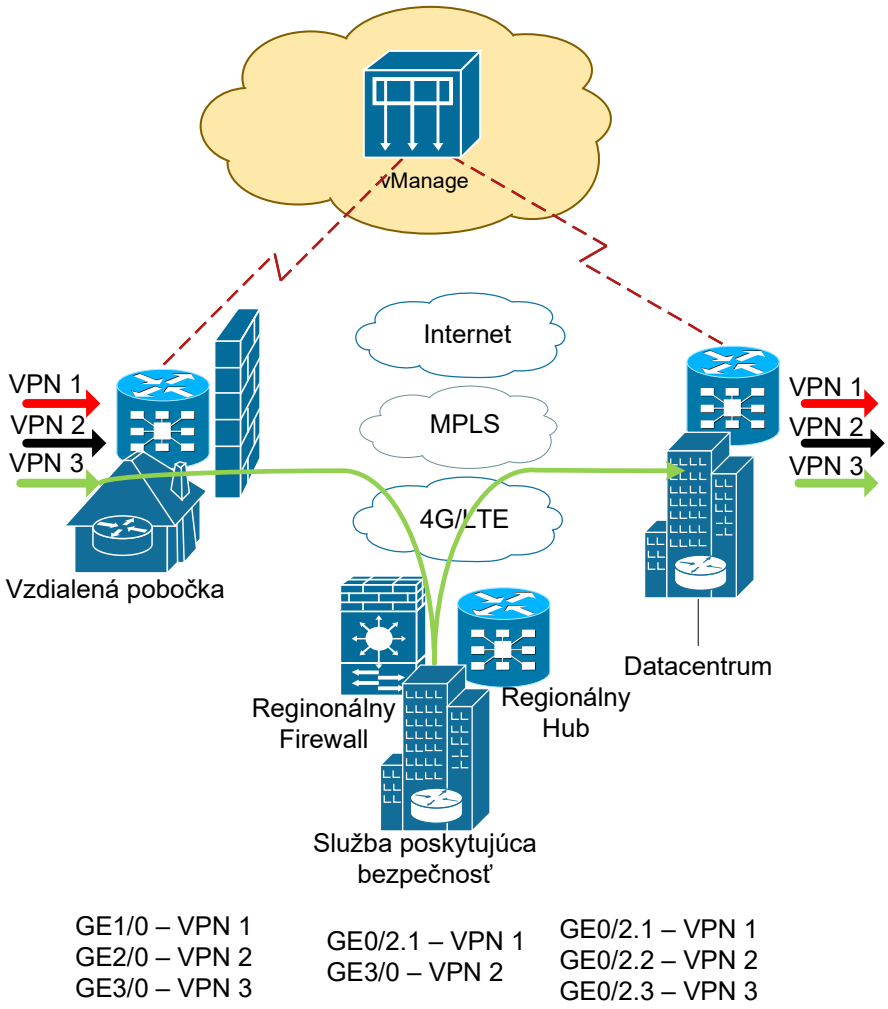
Prepojenie pobočiek pri Cisco SD-WAN infraštruktúre je štandardne zabezpečené pomocou rady pokročilých bezpečnostných funkcií, ktoré sú implementované priamo v smerovači, vrátane cloudovej bezpečnosti. U Cisco SD-WAN sa tieto pokročilé bezpečnostné funkcie označujú ako Security Stack. Security Stack tvoria funkcie ako:

- Enterprise Application-aware firewall,
- Intrusion Prevention System (IPS),
- Advanced Malware Protection (AMP),
- DNS webová bezpečnosť,
- URL filtrovanie,
- SSL Proxy.

Správu bezpečnostných funkcií, ktoré sú implementované na jednotlivých pobočkových SD-WAN smerovačoch je možné konfigurovať prostredníctvom vManage konzoly spomenutej v predchádzajúcej podkapitole (3.3.1), kde je preddefinovaný workflow na aplikovanie a konfiguráciu týchto bezpečnostných funkcií. Obr. 3.5 zobrazuje riešenie bezpečnosti pri použití technológie SD-WAN. Obrázok firewallu zobrazeného na obr. 3.5 na vzdialenej pobočke predstavuje bezpečnostné funkcie implementované priamo v SD-WAN smerovači. VPN 1 a VPN 2 pri komunikácii s datacentom prechádzajú bezpečnostnými funkciami implementovanými v SD-WAN smerovači. Prevádzka z VPN 3 je dodatočne kontrolovaná okrem funkcií SD-WAN smerovača cloudovou bezpečnostnou službou (Cisco Umbrella).

Okrem bezpečnosti je možné vidieť na obr. 3.5 segmentáciu prevádzky. Prevádzka z vychádzajúceho rozhrania GE1/0 je priradená do VPN 1, pre prevádzku vychádzajúcu z rozhrania GE2/0 je to VPN 2 a prevádzka z rozhrania GE3/0 je v rámci VPN 3 posielaná do cloudovej bezpečnostnej služby. Prevádzka vo VPN 3 je takto je ďalej škálovateľná, kde v prípade podozrivých prenosov je prevádzka duplikovaná

na ďalšiu kontrolu už ďalej ako VPN 1 na danom mieste služby poskytujúcej bezpečnosť. Okrem je duplikovania prevádzky na jej dodatočnú kontrolu je prevádzka posielaná ďalej na určenú destináciu vo VPN 3 na rozhranie datacentra GE0/2.3.



Obr. 3.5: Bezpečnosť SD-WAN siete

3.7 Zhrnutie použitia Cisco SD-WAN

SD-WAN sieť slúži primárne na zaistenie konektivity vzdialených užívateľov s ich aplikáciami, ktoré sú buď uložené v cloudovom prostredí alebo v datacentre. Cisco SD-WAN poskytuje segmentáciu siete z pobočky do požadovanej lokality (datacentrum, cloud), pričom segmentácia využíva pokročilé technológie založené na označovaní prevádzky konkrétneho užívateľa v pobočke. Nepoužívajú sa tradičné princípy segmentácie, ako napr. VLAN siete, ACL, ktoré môže byť ťažké udržovať vzhľadom na škálovateľnosť a expandovanie siete.

SD-WAN infraštruktúra zaisťuje potrebnú kvalitu pre kritické aplikácie naprieč celou sieťou, t.j. prostredie pobočkovej lokality s SD-WAN sieťou a datacentrom. Prevádzka v SD-WAN sieti je monitorovaná a vyhodnocovaná telemetrickými a analytickými údajmi naprieč jednotlivými pobočkami.

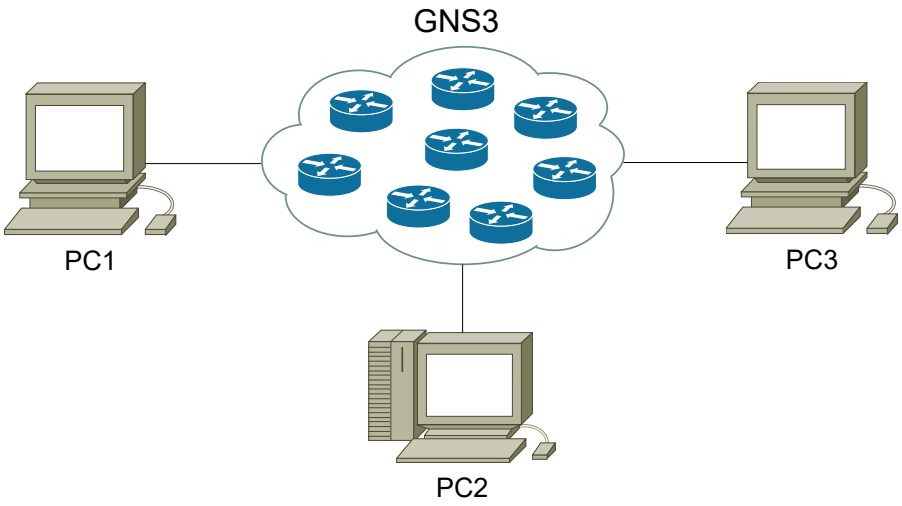
Technológia SD-WAN je vhodná pre tradičné firemné pobočky, kde je približný pomer internej a externej (internet) prevádzky 20 % ku 80 %. Pracovníci na týchto pobočkách využívajú prevažne aplikácie uložené v cloudovom prostredí (Dropbox, Google Drive, Microsoft OneDrive, Amazon Web Services), ku ktorým sa pripájajú cez svetovú sieť internet. Ďalšou veľkou výhodou je voľba alternatívnych typov transportu (4G/LTE, Internet), čím sa dosiahne odľahčenie drahých MPLS liniek, ktorým sa tak uvoľní šírka pásma pre použitie kritických aplikácií. Cisco SD-WAN poskytuje množstvo bezpečnostných funkcií umiestnených vo fyzickom HW sieťových prvkov, ale aj bezpečnostné funkcie v cloudovom prostredí. Hybridnou kombináciou sa dá vytvoriť bezpečný druh komunikácie tam, kde to situácia vyžaduje.

Pre potreby tejto práce a potreby KII zo zhrnutia údajov popísaných v tretej kapitole je možné dôjsť k záveru, že technológia SD-WAN nie je vhodná pre použitie v kritickej infraštruktúre. So zameraním sa na dátové prenosy v KII ide predovšetkým o internú prevádzku, ktorú v predstavuje komunikácia rozvodní s dispečingovými centrami. Táto prevádzka sa označuje ako interná prevádzka a tvorí väčšinu dátových prenosov v KII. V kapitole 1.2.1 sú hierarchicky popísané prenosy v KII. Z analýzy týchto prenosov sa dá usúdiť, že jedno z možných využití internetového pripojenia je v prípade, že sa pracovník dispečingového centra chce pripojiť do siete KII prostredníctvom rôznych VPN spojení mimo internú sieť cez internet tak, aby mohol riadiť KII z iného miesta, než sú rozvodňové pobočky alebo dispečingy. Iným možným prípadom využitia svetovej siete internet môžu byť rôzne aktualizácie operačných systémov. Tieto operácie sú výnimočné a pre potreby KII nepatria medzi dôležité. Internetová konektivita nie je prioritná, čím sa zároveň minimalizuje bezpečnostné riziko.

Ako vyhovujúca technológia pre použitie na kritické dátové prenosy v KII bude použitá MPLS technológia, ktorá ponúka potrebné funkcie na zabezpečenie potrieb takejto siete. Tieto funkcie budú prakticky otestované v piatej kapitole, pričom pre ich testovanie bol zvolený emulačný program GNS3, čo je predmetom nasledujúcej kapitoly. Finálne porovnanie technológií MPLS a SD-WAN bude predmetom záveru práce.

4 Testovacie prostredie a testovacie scenáre

Testy na simulovanej sieti budú realizované v emulátore GNS3 (Graphic Network Simulator-3) pre jeho široké možnosti a graficky prijateľné prostredie. Fyzickú topológiu zapojenia pracoviska zobrazuje obr. 4.1. Takáto topológia obsahuje 3 fyzické počítače, z čoho na počítači ozn. ako PC2 je spustený emulátor GNS3, kde je emulovaná topológia podľa obr. 1. Pri komunikácii PC1 s PC3 tak prebieha komunikácia cez PC2 a to konkrétne cez emulované prvky v GNS3 spustené na PC2.



Obr. 4.1: Fyzické zapojenie topológie

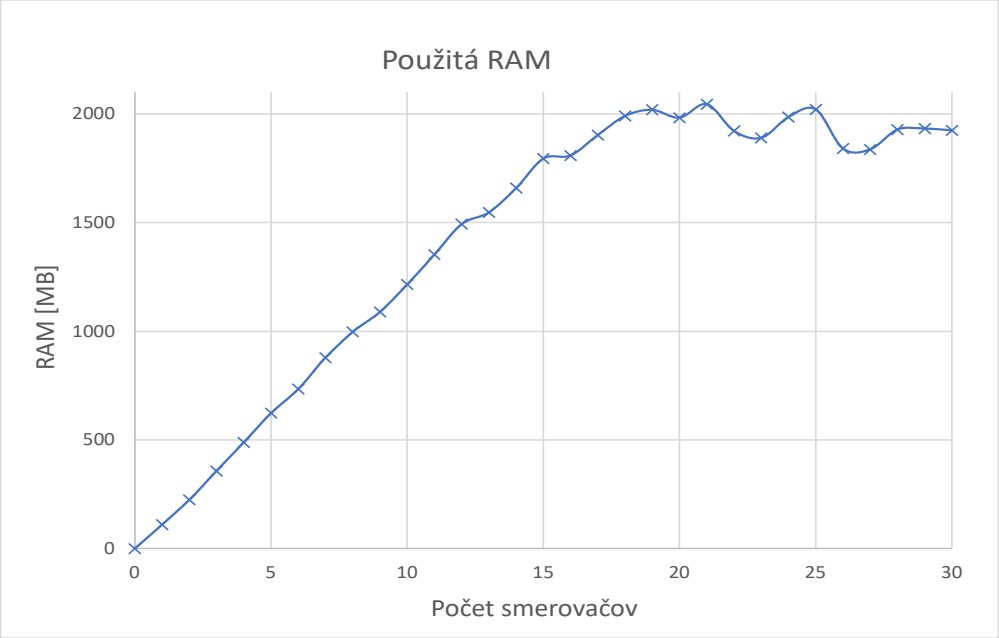
Vzhľadom na veľkosť topológie na obr. 1 sa jedná o jedinú možnosť zapojenia pracoviska, nakoľko pri simulovaní siete zobrazenej na obr. 1 sú vyžadované vysoké nároky na RAM a CPU. Pri spustení virtuálnych PC napr. prostredníctvom virtualizačných nástrojov ako Virtualbox alebo VMware a použití iba zariadenia ozn. ako PC2 sú tak HW nároky privysoké a prevedené testy sa môžu od seba výrazne odlišovať, čím klesá ich dôveryhodnosť. Ďalším faktom sú testy dostupnosti, popísané v podkapitole 4.3. Pri každom generovaní toku paketov stúpa vyťaženosť jednotlivých fyzických zariadení a každý paket musí byť spracovaný na zariadení ozn. ako PC2 v jeho virtuálnej topológii, čím sa opäť zvyšujú HW požiadavky. PC2 by tak musel byť schopný generovať tok paketov, spracovávať ich vo virtuálnej topológii a zároveň ich úspešne odchytávať a analyzovať. Z tohoto dôvodu bolo pre generovanie paketov použité zariadenie ozn. ako PC1 a pakety boli zachytávané na zariadení ozn. ako PC3. Dosiahlo sa tak potrebnej dôveryhodnosti testov a rozloženia záťaže. Ďalšou nutnosťou na použitie viacerých zariadení bol fakt, kedy pri simulovaní VPLS spojenia dochádza k emulovaniu smerovača pomocou QEMU virtualizácie. Súčasné procesory typu Intel vyžadujú na spustenie virtualizovaného PC funkciu procesora

VT-x, čo je funkcia, ktorá umožňuje využiť CPU tak, akoby patrila viacerým nezávislým PC v jednom čase na jednom zariadení. QEMU virtualizácia umožňuje podobnú funkciu ako VT-x, a teda tiež vytvára v hosťujúcom PC ďalšie emulované fyzické zariadenie so svojím virtuálnym CPU. VT-x a QEMU virtualizácia nemôžu byť spustené naraz v jednom čase, a buď bude využívana QEMU virtualizácia alebo VT-x.

4.1 Požiadavky na RAM a CPU

Pred pokusom o samotnú simuláciu siete zobrazenej na obr. 1, je podstatná znalosť toho, aké nároky na CPU a RAM musí PC2 spĺňať pre úspešnú simuláciu takejto veľkej siete.

Priebeh zaberania RAM zobrazuje obr 4.2 a tab. 4.1. Pri testovaní využiteľnosti RAM a zvyšovaní prvkov je podstatná veľkosť súboru pri nahratí daného cisco-image do GNS3. V prípade spomenutého typu c7200 je veľkosť súborového systému tohoto prvku 123 MB. Pri každom pridaní c7200 by sa teda mala zdvihnúť požiadavka na RAM o +123 MB. Podľa grafu na obr. 4.2 a tab. 4.1 je možné pozorovať, že požiadavky na RAM sa nezvýšili presne o +123 MB, a namerané odchýlky je možné adresovať OS, ktorý uvoľňuje RAM podľa potreby a graf nevykazuje dokonalý lineárny priebeh. Pre prehľadnosť boli testované nároky na RAM na zariadení s celkovou kapacitou 5,9 GB RAM, z čoho bolo využitých 3,635 GB pamäte RAM pred samotným meraním.



Obr. 4.2: Graf zaberania RAM

Graf na obr. 4.2 bol vyrobený z nameraných hodnôt v tab 4.1, kde je možné vidieť postupné narastanie RAM. Pri pridaní 20. prvku dochádza k prečerpaniu kapacity pamäte RAM a smerovače prestávajú plniť správnu funkciu, keď reagujú spomalene a obmedzene. Maximálna hodnota RAM pri správnej funkcii bola 5764 MB. Teoreticky bolo možné z celkovej 5,9 GB RAM ešte využiť 0,136 GB, avšak táto kapacita predstavuje rezervu pre OS Windows 10 a nedá sa využiť pre účely GNS3, nakoľko procesy jadra OS majú vždy väčšiu prioritu než užívateľsky zadané. Dané systémové prostriedky dovolili pridať dokopy 39 takýchto zariadení c7200. Pri pridaní 40. prvku došlo k odpojení GNS3 VM, čo je virtuálny linuxový server, na ktorom sú práve emulované smerovače a zlyhaniu celého projektu v GNS3.

Počet smerovačov	Obsadenosť RAM [MB]	Δ [MB]	Použitá RAM GNS3 [MB]
0	3635	0	0
1	3745	110	110
2	3859	114	224
3	3992	133	357
4	4124	132	489
5	4258	134	623
6	4369	111	734
7	4513	144	878
8	4632	119	997
9	4724	92	1089
10	4850	126	1215
11	4988	138	1353
12	5128	140	1493
13	5182	54	1547
14	5294	112	1659
15	5430	136	1795
16	5554	14	1809
17	5648	94	1903
18	5736	88	1991
19	5764	28	2019
20	5728	-36	1983
21	5790	62	2045
22	5667	-123	1922
23	5635	-32	1890
24	5731	96	1986
25	5766	35	2021
26	5586	-180	1841
27	5582	-4	1837
28	5673	91	1928
29	5678	5	1933
30	5669	-9	1924
Pozn. Celková RAM 5,9GB; 3,635 GB RAM využité OS pred meraním			

Tab. 4.1: Tabuľka nameraných hodnôt zaberania RAM

Z uvedeného merania je možné dôjsť k záveru, že nároky na RAM sa zvyšujú priamo-úmerne s určitou odchýlkou podľa ich veľkosti v súborovom systéme GNS3. Pre simulácie veľkej siete, zobrazenej na obr. 1 bude použité zariadenie s kapacitou 32 GB RAM pamäte, a na základe prevedeného merania bude možné simulovať okolo 250 takýchto prvkov.

4.2 Testovacie scenáre pre testovanie

V prípade virtuálnej topológie zobrazenej na obr. 1 bol pre testovanie dostupnosti L3VPN spojenia použitý Cisco IOS i86bi-linux-l3-adventerprisek9-15.2.2.15T.bin. Tento IOS je vďaka svojej jednoduchosti nenáročný na RAM a CPU a splňuje všetky funkcie pre testovanie L3VPN, vrátane neobmedzenej priepustnosti, závislej od HW možností hosťujúceho OS. Vyššie spomenutý IOS neumožňuje vytváranie L2 VPN spojení a BGP signalizáciu L2 VPN spojení. Z tohoto dôvodu museli byť pre testovanie dostupnosti VPLS spojenia koncové prvky nahradené prvkom s operačným systémom IOS XE, konkrétne csr1000v-universalk9.16.12.03-serial.qcow2 s aktivovanou digitálnou licenciou `CSR1000V 2.5 Gbps Full Featured (AX) 60 day evaluation license` pre priepustnosť 2,5 Gb/s. Prvok CSR1000V s operačným systémom IOS XE má obmedzenú priepustnosť na 1000 kb/s, čo predstavuje značný problém pri testovaní MPLS QoS a pri testoch dostupnosti a je teda potrebná aktivácia licencie. Tento prvok zároveň prináša nevýhodu v podobe náročnosti na RAM a CPU, kde je potrebných 3072 MB a pri pridaní jedného takéhoto prvku vzrastie využiteľnosť CPU o +15 až 20 %. Pri použití 3 takýchto prvkov pri testovaní VPLS spojenia pre kombináciu dispečing-rozvodňa-route-reflector sa pohybuje využiteľnosť CPU okolo 50 - 60 % a nie je tak simulovaná celá topológia, ale len jen časť.

4.3 Testy dostupnosti

Jedna z praktických hlavných úloh práce je zameraná na testy dostupnosti pri výpadku spojenia. Testovanie dostupnosti sa dá realizovať tromi princípmi:

- user-space
- kernel-space
- bare-metal based [26].

V tomto prípade sa vďaka prepojeniu troch fyzických PC, z čoho sú dva PC prepojené cez tretí PC s virtuálnou topológiou, jedná o spôsob user-space. Z vyššie troch spomenutých princípov je práve tento princíp najmenej presný, avšak vzhľadom k dostupným možnostiam jediný realizovateľný. Problémom je, že pri user-space

princípe majú všetky procesy operačného systému vyššiu prioritu než tie, ktoré vyvoláva užívateľ. Ľubovoľný proces jadra operačného systému tak môže narušiť užívateľom vytvorený proces (Mausezahn/Wireshark/Tshark), čím narastú nepresnosti a jitter [26].

Pre meranie času dostupnosti bol použitý generátor paketov Mausezahn. Príkazom `mz enp3s0 -t udp -B 192.168.2.2 -d 10 -c 0` bol generovaný nekonečný tok paketov z PC1 na IP adresu PC3 s odstupom 10 µs. Za 1 s sa tak teoreticky odošle 100 000 paketov. Pri menšej časovej hodnote odstupu výrazne vzrástli požiadavky na CPU počítača ozn. ako PC2, ktorý obsahuje virtuálnu topológiu. Preto bola považovaná hodnota 10 µs za optimálnu. Kvôli použitiu graficky prívetivého OS Ubuntu 20.04.2 LTS na všetkých troch PC nie je však táto hodnota presne 100 000 p/s, ale v rozmedzí 13 000 - 14 000 p/s. Pre vyššiu presnosť by bolo potrebné použitie iného real-time OS, avšak pre účely tejto práce je tento nedostatok postačujúci. Pri prechode paketov od PC1 do PC3 a konečné paketov na koncovom zariadení programom Tshark, je táto hodnota zachytených UDP paketov za 1 s priemerne 13 245 a nie 100 000, ako by tomu malo teoreticky byť. Pre ukážku tejto chybovosti boli vložené tabuľky tab. 4.2 a tab. 4.3.

Tab. 4.2 zobrazuje generovanie paketov s 5 s odstupom. Každých 5 s prejde cez virtuálnu topológiu UDP paket a zachytí sa na koncovom zariadení so svojím vloženým časovým razítkom (timestamp). Z pozorovania tab. 4.2 je možné usúdiť, že najvyššia chybovosť pri prijímaní paketov bola 0,0013 % . Táto odchýlka je prijateľná a všetky odoslané pakety boli prijaté a úspešne spracované.

Číslo paketu	Čas [s]	Zdrojová IP	Cieľová IP	Rozdiel od ref. času [s]	Rozdiel od ref. času [%]	Ref. čas [s]
1	0	192.168.3.2	192.168.2.2	0,000000000	0,0000	0
2	5,000037245	192.168.3.2	192.168.2.2	0,000037245	0,0007	5
3	9,999901198	192.168.3.2	192.168.2.2	-0,000098802	-0,0010	10
4	14,99981199	192.168.3.2	192.168.2.2	-0,000188009	-0,0013	15
5	19,99856495	192.168.3.2	192.168.2.2	-0,001435052	-0,0072	20
6	24,99986741	192.168.3.2	192.168.2.2	-0,000132589	-0,0005	25
7	29,99968763	192.168.3.2	192.168.2.2	-0,000312368	-0,0010	30
8	34,99956429	192.168.3.2	192.168.2.2	-0,000435714	-0,0012	35
9	39,99970696	192.168.3.2	192.168.2.2	-0,000293043	-0,0007	40
10	44,99943961	192.168.3.2	192.168.2.2	-0,000560386	-0,0012	45
11	49,9996893	192.168.3.2	192.168.2.2	-0,000310696	-0,0006	50
12	54,99940822	192.168.3.2	192.168.2.2	-0,000591780	-0,0011	55
13	59,99949514	192.168.3.2	192.168.2.2	-0,000504863	-0,0008	60
14	64,99970991	192.168.3.2	192.168.2.2	-0,000290089	-0,0004	65
15	69,99959395	192.168.3.2	192.168.2.2	-0,000406055	-0,0006	70
16	74,99956896	192.168.3.2	192.168.2.2	-0,000431041	-0,0006	75
17	79,99922939	192.168.3.2	192.168.2.2	-0,000770615	-0,0010	80
18	84,99935789	192.168.3.2	192.168.2.2	-0,000642110	-0,0008	85
19	89,99938814	192.168.3.2	192.168.2.2	-0,000611858	-0,0007	90
20	94,99911205	192.168.3.2	192.168.2.2	-0,000887951	-0,0009	95

Tab. 4.2: 5 s odstup

Inak tomu je pri tab. 4.3, kde je najväčšia chyba 23028,28 %. Každých 10 µs je poslaný UDP paket, čo tvorí 100 000 p/s. Kvôli chybám OS sú zhruba tri štvrtiny

paketov nespracované, kedy sa strácajú pakety a vzniká chybovosť. Pre účely merania doby konvergencie je však táto chyba akceptovateľná a pomocou časových razítok a nástrojov na zachytávanie paketov je možné odhaliť výpadky linky v rádu niekoľkých ms.

Číslo paketu	Čas [s]	Zdrojová IP	Cieľová IP	Rozdiel od ref. času [s]	Rozdiel od ref. času [%]	Ref. čas [s]
1	0	192.168.3.2	192.168.2.2	0	0	0
2	0,000000363	192.168.3.2	192.168.2.2	-0,000000637	-63,7	0,000001
3	0,000127198	192.168.3.2	192.168.2.2	0,000125198	6259,9	0,000002
4	0,000471753	192.168.3.2	192.168.2.2	0,000468753	15625,1	0,000003
5	0,000805754	192.168.3.2	192.168.2.2	0,000801754	20043,85	0,000004
6	0,001156414	192.168.3.2	192.168.2.2	0,001151414	23028,28	0,000005
7	0,00115663	192.168.3.2	192.168.2.2	0,00115063	19177,16667	0,000006
8	0,001156707	192.168.3.2	192.168.2.2	0,001149707	16424,38571	0,000007
9	0,00115678	192.168.3.2	192.168.2.2	0,00114878	14359,75	0,000008
10	0,001156868	192.168.3.2	192.168.2.2	0,001147868	12754,08889	0,000009
11	0,001156941	192.168.3.2	192.168.2.2	0,001146941	11469,41	0,00001
12	0,001298629	192.168.3.2	192.168.2.2	0,001287629	11705,71818	0,000011
13	0,001298767	192.168.3.2	192.168.2.2	0,001286767	10723,05833	0,000012
14	0,001717497	192.168.3.2	192.168.2.2	0,001704497	13111,51538	0,000013
15	0,001717713	192.168.3.2	192.168.2.2	0,001703713	12169,37857	0,000014
16	0,002086995	192.168.3.2	192.168.2.2	0,002071995	13813,3	0,000015
17	0,002087226	192.168.3.2	192.168.2.2	0,002071226	12945,1625	0,000016
18	0,002087312	192.168.3.2	192.168.2.2	0,002070312	12178,30588	0,000017
19	0,002087402	192.168.3.2	192.168.2.2	0,002069402	11496,67778	0,000018
20	0,002370552	192.168.3.2	192.168.2.2	0,002351552	12376,58947	0,000019

Tab. 4.3: 10 µs odstup

5 MPLS

MPLS je druhá technológia popri SD-WAN, ktorou sa táto práca zaoberá. V prípade tejto práce je MPLS technológia použitá najmä pre jej funkcie MPLS VPN, MPLS-TE a MPLS-TE FRR. Pre KII bude predovšetkým dôležitá technológia MPLS-TE FRR pri testoch dostupnosti, čím sa rapídne skráti čas nedostupnosti zariadení. MPLS technológia tak prispieva ku presnejšej znalosti aktuálneho stavu energetickej siete, poskytuje lepšie možnosti v oblasti riadenia siete a znižuje čas potrebný pri odstraňovaní porúch, a teda vyššiu efektivitu a zlepšenie kvality dodávky [1]. MPLS v porovnaní s tradičným IP princípom smerovania reaguje na nedostatky IP protokolu. Hlavnými nevýhodami IP princípu sú:

- distribúcia smerovacích informácií na všetkých zariadeniach, čím narastá veľkosť smerovacej tabuľky s časom potrebným k odoslaniu paketov,
- odosielanie paketov založenom výhradne na cieľovej adrese, uprednostňuje sa najkratšia cesta a dochádza tak k neefektívnemu využívaniu šírky pásma bez možnosti load-balancingu,
- nahliadnutie do smerovacej tabuľky na každom skoku (smerovači) pri smerovaní.

Nedostatky IP princípu sa dokázalo čiastočne vyriešiť zavedením MPLS technológie, čo prinieslo významné výhody:

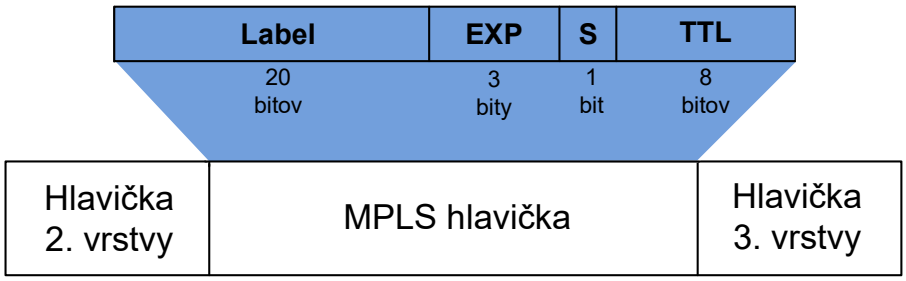
- Pakety sú preposielané podľa hodnoty značky v hlavičke paketu a nedochádza tak ku prehliadaniu smerovacích tabuliek, ale k nahliadnutiu do LFIB.
- Možnosť prenosu ľubovolného sieťového protokolu (IPv4, IPv6) a niektorých protokolov spojovej vrstvy (Ethernet, PPP, HDLC).
- dynamické reagovnanie na zmeny v sieti prostredníctvom technológie MPLS-TE, kedy je možné posielať prevádzku aktuálne najvhodnejšou cestou, vyhýbať sa stratám dát pri havarijných scenároch, čím zároveň dochádza k efektívnemu využitiu šírka pásma na všetkých linkách. Vďaka MPLS-TE FRR (FastRerouting) v prípade výpadku trvá zmena cesty v ráde niekoľkých ms, namiesto tradičnej konvergencie protokolov v ráde niekoľkých sekúnd. Pri spomenutom výpadku linky by zvyčajne došlo ku zahlteniu liniek kvôli nedostatočnej šírke pásma. Vhodnou implementáciou MPLS-TE je možné tomuto zabrániť.
- L3 VPN a VPLS služby.

Motiváciou zavedenia MPLS však nie je vylepšené preposielanie paketov prostredníctvom návestí, ale technológie, ktoré MPLS prináša. Vyššie spomenuté technológie sú boli prakticky otestované vo virtualizovanom prostredí GNS3 a sú bližšie popísané v nasledujúcich podkapitolách.

5.1 Popis MPLS

MPLS protokol je označovaný ako protokol umiestnený medzi druhou a treťou vrstvou ISO/OSI modelu. Veľkosť MPLS záhlavia tvorí celkov 32 bitov. Prevádzka sa smeruje prostredníctvom značiek v MPLS záhlaví paketov. Záhlavie takéhoto paketu je zobrazené na obr. 5.1. Každé MPLS záhlavie obsahuje:

1. **20-bitové návestie** – sú podľa neho preposielané MPLS pakety. Používa sa ako index v MPLS smerovacej tabuľke. Nadobúda hodnoty od 0 – 1,048,575.
2. **Experimental (EXP) bit** - názov tejto položky súvisí s históriou MPLS protokolu, kedy sa v dobe vytvárania technológie nevedela presná funkcia. Veľkosť tejto položky sú 3 bity a používajú sa pre MPLS QoS. Hodnoty bitov 0 - 7 závisia od použitých prvých 3 bitov z IP hlavičky v ToS položke. Jednotlivé mapovanie z IP na MPLS je zobrazené v tab. 5.1 a bude neskorším predmetom pri testovaní MPLS QoS v podkapitole 5.4.
3. **Bottom of stack bit (S-bit)** – tento bit je označovaný aj ako S-bit. Slúži na odlišovanie rôznych MPLS záhlaví. Pôvodne je jeho nastavená hodnota 0, hodnota je 1, ak je dané záhlavie posledné v stohu. V praxi sa jedno MPLS záhlavie využíva zriedkavo.
4. **Time-to-live (TTL)** – používa sa na zamedzenie vzniku smyčiek. Funkcia je rovnaká ako u IP paketov - hodnota TTL sa znižuje s každým hopom a v prípade hodnoty 0 je paket zahodený. Bez TTL by mohol daný paket putovať v sieti donekonečna a zahlcovať sieť.



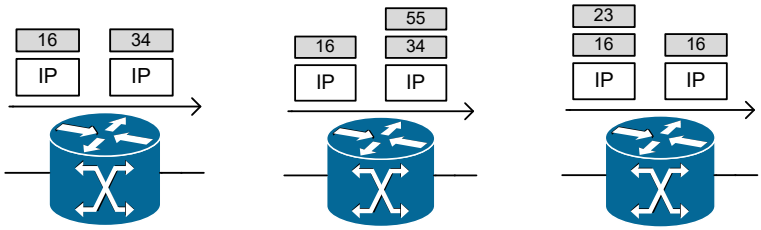
Obr. 5.1: MPLS paket

Operácie s návestím

Podľa hodnoty obsiahnutej v MPLS návestí sa smerovač rozhoduje o akcii, ktorú vykoná. Princíp základných troch typov operácií zobrazuje obr. 5.2. Možné operácie s MPLS paketom sú popísané v nasledujúcich bodoch:

- **Výmena (swap)** – staré návestie sa nahradí novým návestím a paket je preposlaný podľa nového návestia

- **Pridanie (push)** - nové návestie sa uloží nad existujúce návestie, čo funguje ako zaobaľovanie paketu do inej MPLS vrstvy. To umožňuje hierarchické smerovanie MPLS paketov, čo sa využíva pri MPLS VPN.
- **Odobranie (pop)** - z paketu sa odstráni návestie, čím sa môže sprístupniť ďalšie návestie, prípadne paket putuje ďalej ako neoznačený paket.
- **Untagged/No Label** - z paketu sa odoberie MPLS hlavička a paket je preposlaný neoznačený.
- **Aggregate** - z paketu sa odoberie MPLS hlavička, vykoná sa nahliadnutie do IP tabuľky a paket je preposlaný ďalej ako IP paket.



(a) Výmena (b) Pridanie (c) Odobranie

Obr. 5.2: Operácie s návestím

MPLS mechanizmy

MPLS protokol predpokladá pre svoju funkčnosť použitie nasledovných mechanizmov popísaných v nasledovných riadkoch. Tieto mechanizmy tvoria dokopy nutný základ pre funkčnosť MPLS technológie.

1. **Label Edge Router (LER)** – je umiestnený na hranici siete ako vstupný/výstupný smerovač. Vstupný LER pridáva pri vstupe do MPLS siete do paketu MPLS návestie alebo ho pri výstupe zo siete odoberá. Cieľom vstupného LER je zistenie vhodnej LSP na ceste k výstupnému LER.
2. **Label Switching Router (LSR)** – smerujú MPLS pakety naprieč MPLS doménou podľa hodnoty návestia. Pri prijatí paketu sa LSR o ďalšom smerovaní rozhoduje podľa uloženej vyhľadávacej tabuľky (LFIB) sprostredkovanej cez LDP.
3. **Label Distribution Protocol (LDP)** – hlavnou úlohou je distribúcia značiek v sieti. Dáta LDP protokolu obsahujú trojicu informácií označovanú ako TLVs (type–length–value triplets). Type a length sú známe na začiatku prenosu. Typ určuje, ktoré informácie sa budú vymieňať a definuje zvyšok kódu. Value sú prenášané informácie a length je dĺžka položky value.
4. **Forwarding Equivalence Class (FEC)** – tok paketov posielaný cez LSP, ktorý patrí do určitej FEC. Pre príklad pakety, ktoré sú poslané cez: rovnaký

smerovač (next hop), výstupné rozhranie alebo rovnakú riadiacu politiku (queueing policy) patria do rovnakej FEC. LSR nasledovne zachádzajú so všetkými paketmi v jednej FEC rovnako.

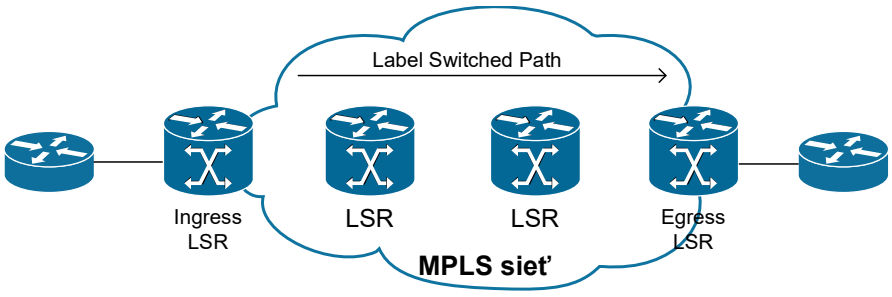
5. **Label Forwarding Information Base (LFIB)** – definuje návestia. Keď LSR rozbalí MPLS hlavičku a prečíta si návestie, pozrie sa do LFIB a vykoná operáciu z 3 hlavných podľa príslušnej hodnoty v LFIB. Pre demonštráciu LFIB a jednotlivých akcií bol vložený výpis 5.1 pre sprehľadnenie problematiky LFIB a ukážky operácií s návestiami.

Výpis 5.1: LFIB

```
P1#show mpls forwarding-table
Local  Outgoing    Prefix          Bytes tag  Outgoing
tag    tag or VC   or Tunnel Id    switched   interface
16     Untagged    10.1.1.0/24        0        Et0/0/0
17     16          10.200.202.0/24    0        Et0/0/0
18     Pop tag     10.200.203.0/24    0        Et0/0/0
19     Pop tag     10.200.201.0/24    0        Et0/0/0
20     18          10.200.254.4/32    0        Et0/0/0
21     Pop tag     10.200.254.2/32    0        Et0/0/0
22     17          10.200.254.3/32    0        Et0/0/0
24     Untagged    12ckt(100)         4771050  Fa9/0/0
```

Podľa výpisu 5.1 by smerovač prijal návestie s hodnotou 22, prebehla by výmena návestia s hodnotou 22 za 17 (label-to-label) a paket sa prepošle ďalej po rozhraní Ethernet0/0/0. Pri prijatí paketu s hodnotou v návestí 16 by smerovač vymazal všetky návestia a preposlal by paket ako IP paket, pretože hodnota 16 predstavuje Untagged, čo je paket bez MPLS hlavičky. Pri prijatí paketu s vrchným hodnotou návestia 18, smerovač odstráni dané vrchné návestie a ďalej prepošle paket buď už ako IP paket alebo ako paket s iným návestím.

6. **Label Switched Paths (LSP)** – cesta v MPLS sieti medzi LER smerovačmi, kedy paket vstupujúci do siete cez vstupný LER je transportovaný k príslušnému výstupnému LER. Príklad takejto LSP zobrazuje obr. 5.3.



Obr. 5.3: Príklad LSP

5.2 L3 MPLS VPN

BGP/MPLS IP virtuálne privátne siete (VPNs), často nazývané ako L3 VPNs, sú najpopulárnejšou MPLS službou [28]. Technológia L3 MPLS VPN vyžaduje samostatný smerovací protokol medzi CE smerovačmi. V praxi sa o toto smerovanie stará poskytovateľ služby (SP). V prípade simulovanej siete na obr. 1 je k smerovačom PE1-070 a PE2-018 pripojený zákazníkov smerovač (CE1-X), na ktorom je zapnutý OSPF protokol. Výpis 5.2 zobrazuje naviazanie OSPF susedstva na CE smerovačoch prostredníctvom ich Loopback 0 rozhraní. Pri L3 VPN PE smerovač vykonáva nahliadnutie do VRF tabuľky, ktorá je pre každého zákazníka samostatná. CE smerovače tak propagujú svoje cesty PE smerovačom. Cesty od odlišných CE smerovačov sú od seba odlíšené, aj keď dochádza ku zhode IP adresného priestoru vďaka samostatným VFI tabuľkám pre pobočky. Prenášanie ciest nakonfigurovanej VRF instancie customer_A cez BGP protokol dokumentuje výpis 5.3.

Výpis 5.2: Nadviazanie susedstva na CE smerovačoch

```
CE1-A#
*Apr 17 18:06:01.973: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.100.1 on Ethernet0/0 from LOADING to
     FULL, Loading Done
CE1-A#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.100.1      1   FULL/BDR        00:00:34    172.16.1.1      Ethernet0/0

CE1-B#
*Apr 17 18:05:52.553: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.100.2 on Ethernet0/0 from LOADING to
     FULL, Loading Done
CE1-B#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.100.2      1   FULL/BDR        00:00:37    172.16.2.1      Ethernet0/0
```

Výpis 5.3: Prenášanie ciest VRF instancie customer_A

```
PE1-070#show ip route vrf customer_A

Routing Table: customer_A
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, - next hop override, p - overrides from PfR

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C        172.16.1.0/30 is directly connected, GigabitEthernet1
L        172.16.1.1/32 is directly connected, GigabitEthernet1
```

```
O        172.16.1.101/32 [110/2] via 172.16.1.2, 00:28:11, GigabitEthernet1
B        172.16.1.102/32 [200/2] via 10.10.9.18, 00:28:13
B        172.16.2.0/30 [200/0] via 10.10.9.18, 00:41:53
C        172.16.100.1/32 is directly connected, Loopback1
O     192.168.2.0/24 [110/11] via 172.16.1.2, 00:28:11, GigabitEthernet1
B     192.168.3.0/24 [200/2] via 10.10.9.18, 00:28:13
```

5.2.1 Popis L3 MPLS VPN

L3 VPN podobne ako VPLS technológia, slúži na prepojenie vzdialených zákazníkových stránok cez sieť poskytovateľa pripojenia. V tejto práci budú predstavovať zákazníkove stránky jednotlivé rozvodne, prepojené s dispečingovými centrami. Oproti technológii VPLS si pri zákazník môže ponechať svoje rozloženie IP adries a SP sa stará o ostatnú funkcionalitu - smerovanie, oddelenie prevádzky jednotlivých zákazníkov, poskytnutie konektivity a i. P smerovače slúžia iba na preposielanie paketov medzi PE smerovačmi a nevedia o CE smerovačoch. Z výpisu 5.4 smerovacej tabulky CE smerovača CE1-A je vidieť, že pozná sieť 172.16.1.0/30, čo je linka medzi PE a CE a prostredníctvom OSPF protokolu pozná cesty do siete 192.168.3.0/24, čo je sieť za smerovačom CE1-B.

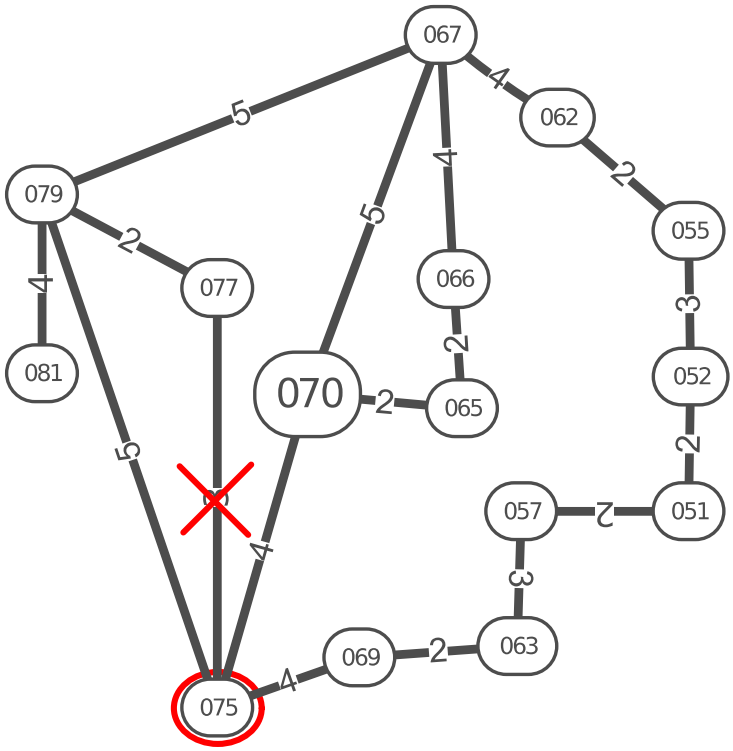
Výpis 5.4: Cesty smerovača CE1-A

```
CE1-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C        172.16.1.0/30 is directly connected, Ethernet0/0
L        172.16.1.2/32 is directly connected, Ethernet0/0
C        172.16.1.101/32 is directly connected, Loopback0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Ethernet1/0
L        192.168.2.1/32 is directly connected, Ethernet1/0
O IA  192.168.3.0/24 [110/20] via 172.16.1.1, 00:05:48, Ethernet0/0
CE1-A#
```

SP takto dokáže v porovnaní s tradičným IP princípom lepšie využiť infraštruktúru. Pri s tradičnými VPN technológiami ako sú Secure VPNs založené na IPsec alebo SSL/TLS, ktoré fungujú na tradičnom IP pricípe, má L3 MPLS VPN technológia výrazné výhody vo flexibilite, škálovateľnosti, riadení a jednoduchosti siete [28].

5.2.2 Testy dostupnosti pre L3VPN spojenie

Pre testovanie dostupnosti bola sústredená pozornosť na rozvodňu s číslom 077, ktorá je zobrazená na orezanom obrázku z celkovej topológie na obr. 5.4. Táto rozvodňa využíva pre spojenie s dispečinkovým centrom trasu 077-075-070. K rozvodni 077 je pripojený fyzický PC, ozn. ako PC1 a na simulovanom dispečingovom centre ozn. ako 070 je pripojený ďalší fyzický PC, ozn. ako PC3. Fyzické zobrazenie jednotlivých fyzických zariadení je zobrazené na obr. 4.1.



Obr. 5.4: Výpadok na trase

Pre testovanie dostupnosti spojenia medzi rozvodňou 077 a dispečingovým centrom 070 budú simulované dva typy výpadkov, a to výpadok linky medzi rozvodňami 077-075 a výpadok celej rozvodne 075. Červený kríž na obr. 5.4 tak znázorňuje výpadok linky na trase 077-075 a červený kruh okolo rozvodne s číslom 075 znázorňuje druhý prípad výpadku, a to výpadok celej rozvodne. Pre spoľahlivé ošetrenie výpadku na trase medzi požadovanou rozvodňou a dispečingom s využitím MPLS-TE FRR je potrebná konfigurácia dvoch náhradných tunelov, z čoho jeden ošetrí výpadok linky a druhý výpadok sieťového prvku. V kapitole 5.6 je bližšie popísaná funkcia a konfigurácia technológie MPLS-TE FRR, ktorá bude použitá pre testy dostupnosti.

Celkovo bolo prevedených 6 testov dostupnosti, ktoré pozostávajú z:

1. testu dostupnosti pri výpadku linky, konvergencia pomocou protokolu OSPF,
2. testu dostupnosti pri výpadku linky, konvergencia pomocou technológie MPLS-TE FRR,
3. testu dostupnosti pri výpadku smerovača, konvergencia pomocou protokolu OSPF,
4. testu dostupnosti pri výpadku smerovača, konvergencia pomocou technológie MPLS-TE FRR,
5. testu dostupnosti pri výpadku RR príkazom `reload`,
6. testu dostupnosti pri výpadku RR prikazom `clear bgp * all 1` a `clear ip ospf process`.

Test dostupnosti pri výpadku linky, konvergencia pomocou protokolu OSPF

Prvý test bol realizovaný bez implementovania MPLS-TE FRR. Pomocou programu Mausezahn bol generovaný tok paketov 100 000 p/s a na koncovej stanici boli pakety zachytávané nástrojom Tshark. Príkazmi na smerovači 075, ktoré sú zobrazené na výpise 5.5 bol simulovaný výpadok linky na trase medzi 077-075.

Výpis 5.5: Výpadok linky

```
075# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
075(config)# interface ethernet 0/0
075(config-if)# shutdown
*May 25 13:41:06.082: %OSPF-5-ADJCHG: Process 100, Nbr 10.10.9.77 on Ethernet0/0 from FULL to
     DOWN, Neighbor Down: Interface down or detached
*May 25 13:41:06.082: %LDP-5-NBRCHG: LDP Neighbor 10.10.9.77:0 (1) is DOWN (Interface not
     operational)
075#
```

Pomocou zachytávania paketov programom Tshark na koncovom zariadení v simulovanej rozvodni 070 je na výpise 5.6 možné pozorovať výpadok linky v čase 8,08739657 s a znovu-obnovenie UDP toku v čase 13,59031226 s. Z rozdielu týchto dvoch časových razítok môžeme usúdiť, že spojenie bolo pri výpadku prerušené na 5,50291569 s. Tento čas je zároveň čas konvergencie OSPF protokolu pri výpadku linky.

Výpis 5.6: Zachytávanie pomocou Tshark

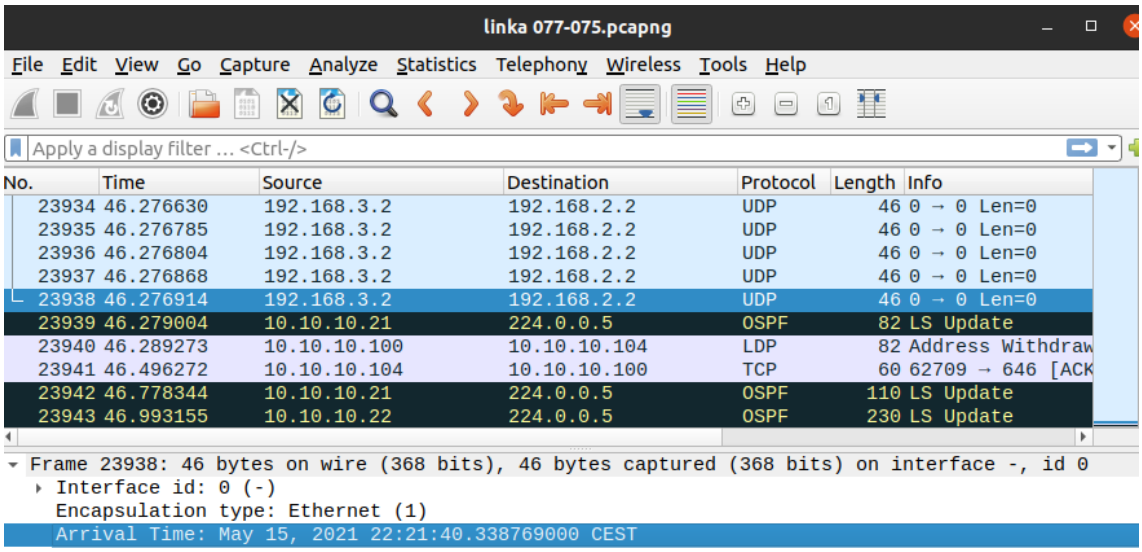
```
67154   8.087135282  192.168.2.2  192.168.3.2  UDP 60 0  0 Len=0
67155   8.087202525  192.168.2.2  192.168.3.2  UDP 60 0  0 Len=0
67156   8.087396573  192.168.2.2  192.168.3.2  UDP 60 0  0 Len=0
67157   9.627178759  192.168.3.1  224.0.0.5    OSPF 90 Hello Packet
67158   13.590312263  192.168.2.2  192.168.3.2  UDP 60 0  0 Len=0
67159   13.590312940  192.168.2.2  192.168.3.2  UDP 60 0  0 Len=0
67162   13.590390244  192.168.2.2  192.168.3.2  UDP 60 0  0 Len=0
```

Pre potreby kritických operácií v KII môže byť tento čas obnovenia spojenia pridlhý a nepostačujúci. Pre ošetrenie tohto stavu je vhodné využiť technológiu

MPLS-TE a to konkrétne MPLS-TE FRR, čo je predmetom ďalšieho testu.

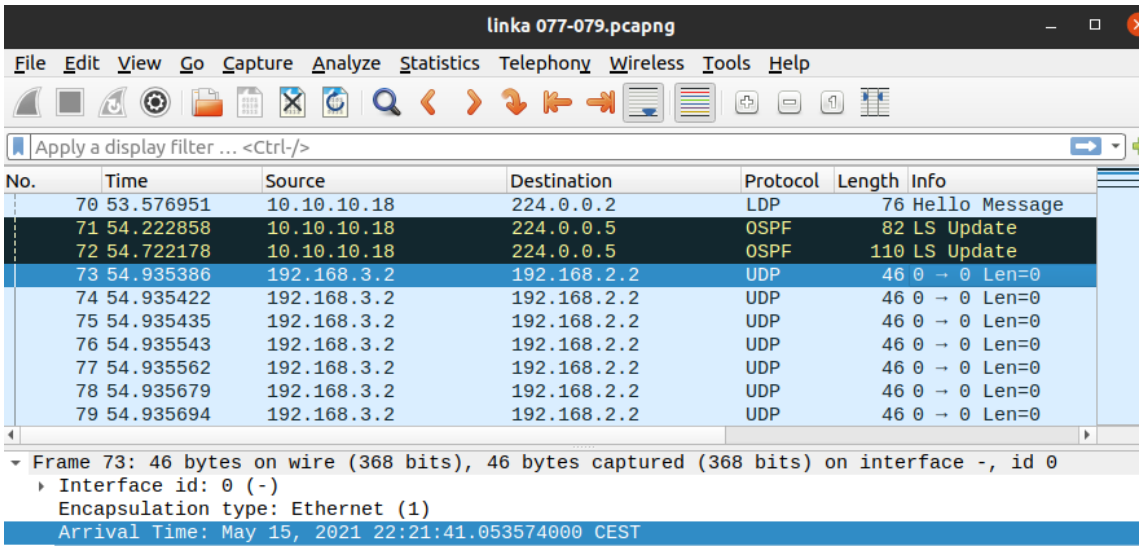
Test dostupnosti pri výpadku linky, konvergencia pomocou technológie MPLS-TE FRR

U technológie MPLS-TE FRR boli podľa očakávaní časy výpadkov odlišné. Výpadok linky netrval viac ako sekundu a odhaliť tento výpadok iba prostredníctvom časových razítok niekoľko-tisíc paketov pomocou nástroja Tshark je náročné. Z tohoto dôvodu bol použitý program Wireshark, ktorý je implementovaný priamo v GNS3. Tento zachytávač paketov je o niečo systémovo náročnejší, avšak poskytuje možnosť synchronizácie času s časom OS. Ku každému paketu so svojím časovým razítkom je pridelený aj systémový čas podľa OS v momente, keď daný paket dorazil na koncové zariadenie. GNS3 zároveň umožňuje spustenie programu Wireshark na jednotlivých linkách v simulovanej topológie. Tento fakt dokumentuje obr. 5.5, kde je zobrazená pôvodná linka 077-075, cez ktorú posledný UDP paket odišiel v čase 22:21:40.338769. Pri vypadnutí linky, rovnakým spôsobom aký je popísaný v predchádzajúcom teste vo výpise 5.6 došlo k okamžitému prepnutiu UDP toku z linky 077-075 na 077-079.



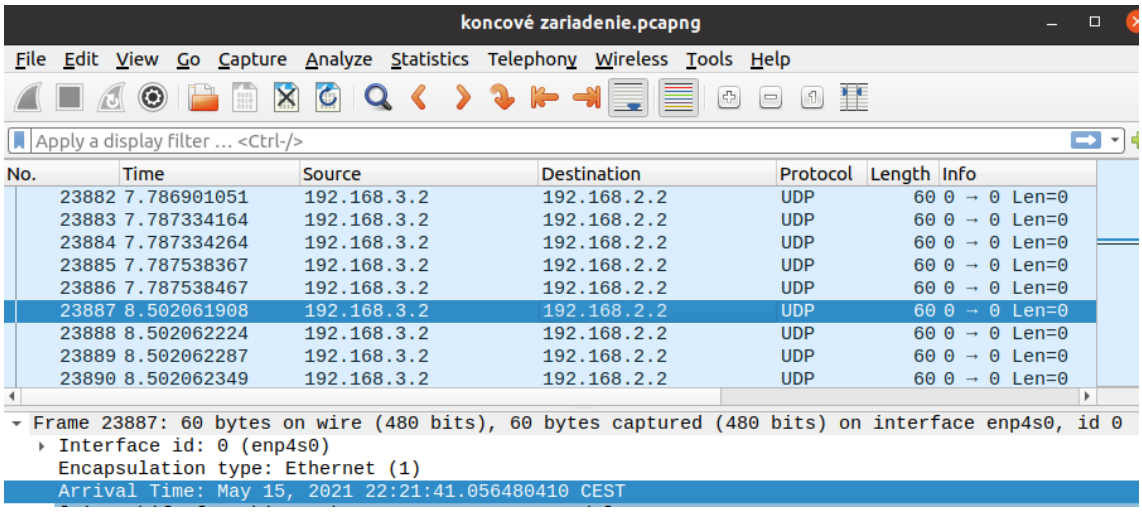
Obr. 5.5: Wireshark na linke 077-075

Obr. 5.6 zobrazuje spustený program Wireshark na náhradnej linku 077-079, ktorá bola vybraná pomocou technológie MPLS-TE FRR. Prvý prichádzajúci UDP paket na túto záložnú linku prišiel v čase 22:21:41.053574. Rozdiel posledného zachyteného UDP paketu na linke 077-075 a prvého UDP paketu na linke 077-079 predstavuje výpadok spojenia, teda 0,714805 s. Pomocou priradeného systémového času OS pri zachytených paketoch je tak možné tento výpadok odhaliť aj na koncovom zariadení v rovnakom čase, čo dokumentuje obr. 5.7.



Obr. 5.6: Wireshark na linke 077-079

Ako bolo spomenuté, tak zachytávanie pomocou programu Wireshark bolo spustené aj na koncovom zariadení. Podľa očakávaní ukazuje Wireshark spustený na linkách v GNS3 na PC2 obdobné hodnoty, ako hodnoty namerané na koncovom zariadení, čo je v tomto prípade fyzický PC pripojený k rozvodni 070, ozn. ako PC3 na obr. 4.1 v kapitole 4. Táto skutočnosť je zobrazená na obr. 5.7, kde je možné sledovať výpadok UDP toku na koncovom zariadení. Podľa časového razítka zvýrazneného paketu môžeme vidieť, že rozdiel medzi zobrazeným a predchádzajúcim paketom je podľa ich časových razítok 0,714523441 s, čo zodpovedá monitorovaniu paketov na linkách v GNS3 s rozdielom 0,00028 s zobrazených na obr. 5.5 a obr. 5.6.



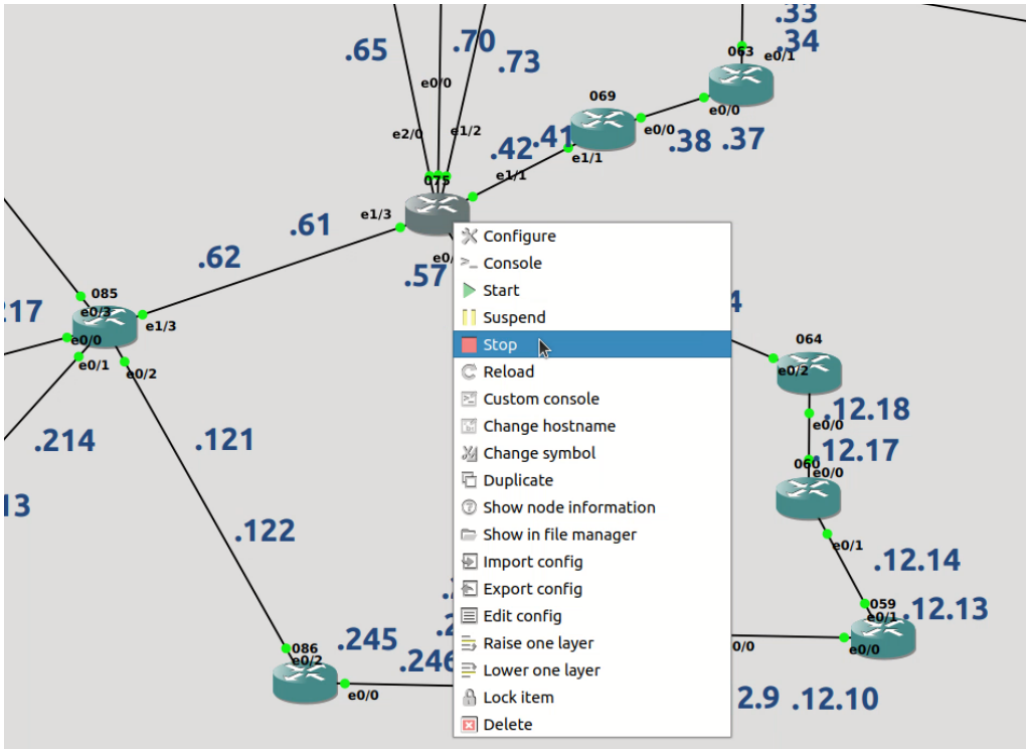
Obr. 5.7: Wireshark na koncovom zariadení

Doba, počas ktorej bolo spojenie neaktívne je teda 0,714805, čo je v porovnaní

s dobou konvergencie OSPF protokolu u výpadku linky rozdiel o 4,78811 s. Takáto doba lepšie vyhovuje požiadavkám KII a je teda vhodné využitie takejto technológie.

Test dostupnosti pri výpadku smerovača, konvergencia pomocou protokolu OSPF

Ďalší, v poradí tretí test dostupnosti bol test dostupnosti pri výpadku celej rozvodne 075. Znovu-nadviazanie spojenia je realizované prostredníctvom OSPF protokolu. Na koncovom zariadení je spustený analyzátor paketov Tshark. Výpadok smerovača bol simulovaný vypnutím smerovača v emulátori GNS3, čo je zobrazené na obr. 5.8. Pravým kliknutím na daný smerovač sa zobrazí ponuka a výberom Stop dôjde k vypnutiu daného prvku. Tento výpadok môže simulovať napr. vypnutie napájanie pre daný smerovač bez možnosti náhradného napájania.



Obr. 5.8: Vypnutie smerovača

Na výpise 5.7 je možné sledovať prerušenie UDP toku s odstupom 10 µs, ktorý bol generovaný rovnakým spôsobom, ako tomu bolo v predchádzajúcich testoch. Z rozdielu časových razítok paketov č. 16368 a 16364 je možné skonštatovať, že výpadok L3VPN spojenia trval 38,3463 s. Tento čas je dlhší oproti už nevyhovujúcemu času konvergencie OSPF protokolu pri výpadku linky (5,5 s) o 32,843 s. Takýto výpadok v KII je nevyhovujúci a musí byť patrične ošetrený, čo je predmetom nasledovného testu.

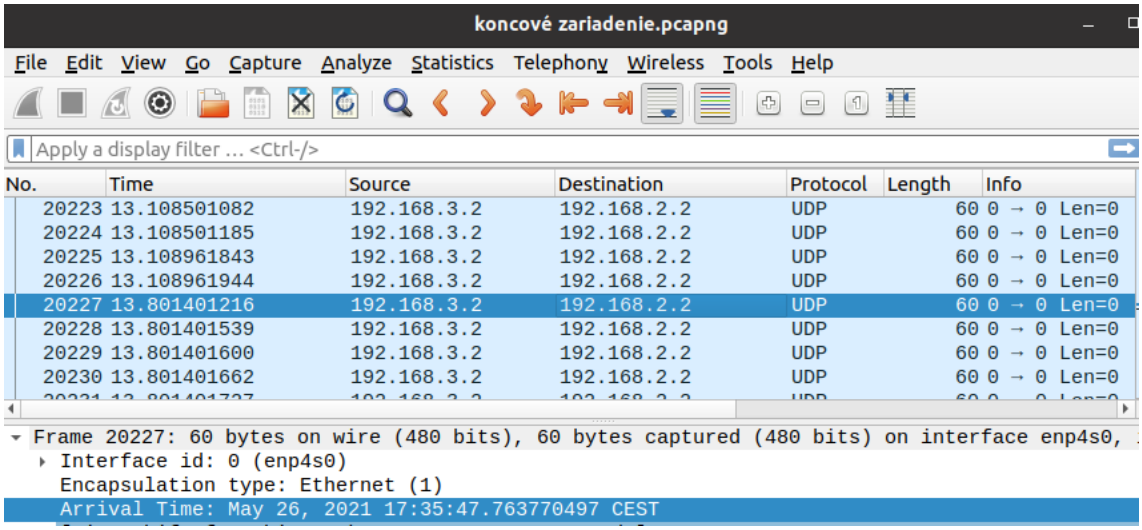
Z prevedeného testu je možné dôjsť k záveru, že výpadok linky a výpadok celého smerovača sa od seba podľa času znovu-nadviazania spojenia odlišuje. Výpadok celého smerovača je podstatne kritickejší prípad v prípade, že sa spojenie obnovuje prostredníctvom OSPF protokolu.

Výpis 5.7: Tshark na koncovom zariadení

```
16362 1.255916223  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
16363 1.255916327  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
16364 1.255916401  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
16365 1.428734951  192.168.2.1  224.0.0.5    OSPF 90 Hello Packet
16366 2.405723404  192.168.3.1  224.0.0.5    OSPF 90 Hello Packet
16367 31.513508188  192.168.3.1  224.0.0.5    OSPF 90 Hello Packet
16368 39.602192285  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
16369 39.602192676  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
16370 39.602900893  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
```

Test dostupnosti pri výpadku smerovača, konvergencia pomocou technológie MPLS-TE FRR

Ďalší test dostupnosti, bol test dostupnosti pri výpadku celej rozvodne 075 s použitím MPLS-TE FRR. Pri takomto výpadku sa volí náhradná trasa 077-079-067-070. Bližšia konfigurácia technológie MPLS-TE FRR je popísaná v kapitole 5.6. Očakávaný výpadok spojenia je vďaka použitiu technológie MPLS-TE FRR v ráde ms a tak bol pre identifikovanie tohoto výpadku použitý program Wireshark. Pre prvotné identifikovanie výpadku bol použitý Wireshark na linkách v GNS3, kde sa podľa systémového času prepnutia liniek z 077-075 na 077-079 mohol identifikovať čas výpadku. Vďaka znalosti tohto času bolo jednoduchšie identifikovať výpadok aj na koncovom zariadení, čo zobrazuje obr. 5.9. Podľa rozdielu časových značiek paketu č. 20227 a 20226 je možné určiť čas nedostupnosti, čo predstavuje 0,6924 s.



Obr. 5.9: Koncové zariadenie

Použitím technológie MPLS-TE FRR pri výpadku celého zariadenia sa tak znížil čas nedostupnosti z pôvodného času 38,3463 s na 0,6924 s. Uvedený kratší čas lepšie vyhovuje požiadavkám KII. Pre náročnosť zobrazení odchytených paketov na linkách GNS3 so systémovým časom ich doručenia je zobrazený len výpadok na koncovom zariadení.

Test dostupnosti pri výpadku RR prikazom `clear bgp * all 1` a `clear ip ospf process`

Ako piaty test dostupnosti bol prevedený test dostupnosti pri výpadku BGP a OSPF spojenia medzi jednotlivými smerovačmi. Výpadok bol simulovaný príkazmi `clear bgp * all 1` a `clear ip ospf process`. Pri výpadku týchto smerovacích protokolov dochádza zároveň k zmazaniu aktuálneho VPN-spojenia a toto spojenie sa tak musí znovu-nadviazať. Tento výpadok trval v ráde pár sekúnd, a tak bol použitý nástroj Tshark na koncovom zariadení, čo dokumentuje výpis 5.8.

Výpis 5.8: Výpadok reštartovaním smerovacích protokolov

```
13478 1.180984894  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
13479 1.180984998  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
13480 1.180985074  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
13481 1.362401453  192.168.2.1  224.0.0.5    OSPF 90 Hello Packet
13484 6.228518815  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
13485 6.228519323  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
13486 6.228519413  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
```

Podľa časových razítok UDP paketov je možné vidieť, že výpadok posledného route-reflectoru trval 5,047534 s. V tomto prípade ide o pomerne vysoký čas nedostupnosti VPN spojenia. Zároveň ide o výpadok posledného route-reflectoru v topológii. Pre potreby KII by malo byť smerovačov určených ako route-reflector viacej tak, aby sa dosahovalo potrebnej redundancie, nakoľko jediný RR smerovač predstavuje tzv. single-point-of-failure, kde pri zlyhaní tohoto prvku nastáva zlyhanie všetkých VPN-spojení pre daný RR.

Tento test bol pridaný z dôvodu použitia rozličných smerovačov v reálnom prostredí, kedy doba plne načítaného smerovača sa môže výrazne líšiť od výrobcu a modelu zariadenia. Preto je potrebné počítať s časom načítania zariadenia a následne s časom po načítaní, kedy zariadenie nadväzuje susedstvá. Tento test teda dokumentuje čas, kedy je zariadenie plne načítané a začne nadväzovať susedstvá. Problematikou načítavania zariadenia a jednotlivých susedstiev sa zaoberá nasledovný test.

Test dostupnosti pri výpadku RR príkazom reload

Šiesty a posledný test dostupnosti L3VPN spojenia, pri výpadku posledného RR bol prevedený príkazom `reload`, ktorý simuluje výpadok zariadenia. Pri takomto

výpadku ide o čas načítania zariadenia (IOS) a čas, za ktorý sa vytvorí obraz siete spolu s nadväzovaním susedstiev. V tomto prípade to je najskôr naviazanie MPLS susedstiev pomocou interného OSPF protokolu, následne sa vytvoria BGP susedstvá so vzdialenými pobočkami a následne sa začnú prenášať VPN cesty jednotlivých pobočiek. Výpadok dokumentuje výpis 5.9. Podľa rozdielu časových hodnôt UDP paketov je celkový čas, počas ktorého bolo spojenie neaktívne 33,29795069 s.

Výpis 5.9: Výpadok príkazom reload

```
15065 15.938269653  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
15066 15.938269731  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
15067 15.938269808  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
15074 29.345080619  192.168.3.1  224.0.0.5    OSPF 90 Hello Packet
15075 31.004084672 aa:bb:cc:00:05:01  CDP/VTP/DTP/PAgP/UDLD CDP 315 Device ID: d_budejovice  Port
    ID: Ethernet1/0
15101 48.876231874  192.168.3.1  224.0.0.5    OSPF 90 Hello Packet
15102 49.236220498  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
15103 49.236220766  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
15104 49.236220846  192.168.3.2  192.168.2.2  UDP 60 0  0 Len=0
```

Podľa debugovacích správ route-reflectoru vo výpise 5.10 sa dajú určiť jednotlivé fázy pri načítavaní zariadenia. V čase 22:55:41.962 bol zadaný príkaz na resetovanie smerovača a začal sa tak resetovací proces. V čase 22:55:49.498 bolo zariadenie resetované a následne za začal nahrávať IOS daného prvku. Samotný reset tak trval 7,536 s. V čase 22:55:50.173 bol tak daný prvok pripravený na svoju funkciu a začal naväzovať susedstvá, kedy došlo rozhranie Ethernet0/0 do stavu up. Prvé BGP-susedstvo bolo naviazané v čase 22:56:13.957. Z rozdielu času resetovania prvku, t.j. 22:55:41.962 a času naviazania prvého BGP susedstva v čase 22:56:13,957 vo výpise 5.10, môžeme určiť čas výpadku, čo prestavuje 31,995 s. Tento čas približne zodpovedá výpadku zobrazenému vo výpise 5.9, s rozdielom 1,30295 s. Túto odchýlku je možné zdôvodniť prenášaním VPN-ciest z rôznych pobočiek, ktoré nie je možné zobraziť v debugovacích správach. Výpis 5.10 je zobrazený len čiastočne pre demonštráciu, nakoľko všetky debugovacie výpisy pri načítavaní smerovača by boli pridlhé.

Výpis 5.10: Debugovacie správy pri načítavaní smerovača

```
RR1#reload
Proceed with reload? [confirm]
*May 26 22:55:41.962: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
*May 26 22:55:49.498: %SYS-5-RESTART: System restarted --
Cisco IOS Software, Linux Software (I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.2(2.15)T,
    ENGINEERING WEEKLY BUILD, synced to V151_4_M3_5
Copyright (c) 1986-2012 by Cisco Systems, Inc.
*May 26 22:55:50.173: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*May 26 22:55:51.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/2, changed state
    to down
*May 26 22:55:55.906: %OSPF-5-ADJCHG: Process 100, Nbr 10.10.9.91 on Ethernet0/0 from LOADING to
    FULL, Loading Done
*May 26 22:55:55.907: %OSPF-5-ADJCHG: Process 100, Nbr 10.10.9.96 on Ethernet0/1 from LOADING to
    FULL, Loading Done
*May 26 22:56:07.063: %LDP-5-NBRCHG: LDP Neighbor 10.10.9.87:0 (1) is UP
```

```
*May 26 22:56:13.957: %BGP-5-ADJCHANGE: neighbor 10.10.9.79 Up
*May 26 22:56:13.965: %BGP-5-ADJCHANGE: neighbor 10.10.9.81 Up
```

5.3 VPLS

Druhou MPLS technológiu, ktorá bude použitá na prepájanie pobočiek je technológia s názvom VPLS (Virtual Private LAN Service). Z porovnania L3 VPN a VPLS vyplývajú 2 zásadné rozdiely:

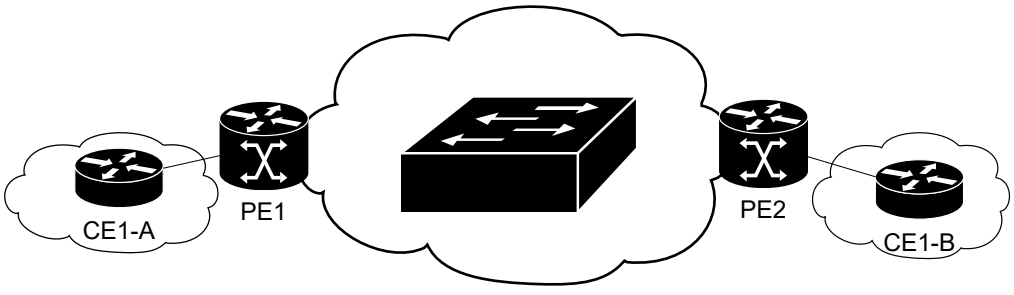
- L3 VPN poskytuje virtualizované smerovanie (routing), kým VPLS poskytuje virtualizované prepínanie (switching),
- PE smerovače distribuujú L3 (napr. IP VPN) cesty, ale nedistribuujú VPLS MAC cesty ostatným PE smerovačom. Pri VPLS tak dochádza k učeniu MAC adries.

VPLS tak poskytuje iba L2 konektivitu typu multipoint-to-multipoint (MP2MP) medzi pobočkami [28].

5.3.1 Popis VPLS

VPLS teda vzniklo ako rozšírenie VPWS (Virtual Private Wire Service). U VPLS je využívaný typ rozhrania PW (Pseudowire), kým VPWS používa AC (Attachment Circuit). Zásadný rozdiel medzi VPWS a VPLS je ten, že VPLS podporuje iba L2 technológiu Ethernet, kým VPWS ich podporuje podstatne viac.

Vďaka VPLS službe vyzerá sieť ako jeden veľký prepínač s vloženou funkciou učenia MAC adries, implementovanou na každom PE. Pobočky sú tak emulované cez MPLS sieť akoby boli umiestnené v jednej LAN, viď obr. 5.10.



Obr. 5.10: MPLS sieť z pohľadu pobočky

Výpis 5.11 smerovača PE-070 zobrazuje funkčný stav rozhrania pseudowire pre VC s ID 100 a názvom customer_A. Vzdialený LDP sused má ID 10.10.9.18, čo je IP adresa rozhrania Loopback0 smerovača PE2-018. Značka pre odchádzajúce rozhranie GigabitEthernet4 smerovača PE1-070 na rozhranie GigabitEthernet1 PE2-018,

ktoré je spojené s pobočkovým smerovačom CE1-B je 17 (remote). V opačnom prípade pre komunikáciu PE-018 s rozhraním GigabitEthernet1 na smerovači PE1-070 je táto značka 16 (local).

Výpis 5.11: Popis nakonfigurovaného VPLS spojenia na PE1-070

```
PE-070#show mpls l2transport vc 100 detail
Local interface: VFI customer_A vfi up
  Interworking type is Ethernet
  Destination address: 10.10.9.18, VC ID: 100, VC status: up
  Next hop PE address: 10.10.9.18
    Output interface: Gi4, imposed label stack {246 17}
    Preferred path: not configured
    Default path: active
    Next hop: 10.10.11.93
  Create time: 00:21:26, last status change time: 00:21:26
    Last label FSM state change time: 00:21:26
  Signaling protocol: BGP
    MPLS VC labels: local 16, remote 17
    Group ID: local n/a, remote n/a
    MTU: local 1500, remote 1500
  Control Word: Off
  SSO Descriptor: 10.10.9.18/100, local label: 16
  Dataplane:
    SSM segment/switch IDs: 8195/4097 (used), PWID: 1
  VC statistics:
    transit packet totals: receive 137, send 2
    transit byte totals:   receive 14770, send 198
    transit packet drops:  receive 0, seq error 0, send 0
```

Príkaz `show vfi` na výpise 5.12 vypíše informácie o všetkých nakonfigurovaných VFI instanciách. V tomto prípade ide o VFI instanciu customer_A, ktorá prepojuje dispečingové cetrá PE-070 s PE-018. Na výpise 5.12 je vidieť, že VFI instancia customer_A má VPN ID 100, VE-ID smerovača PE1-070 je 2, VE-SIZE určuje počet možných spojení pobočkového smerovača s inými smerovačmi (10), ďalej sú zobrazené RD, RT, číslo Bridge-Domain a daný pseudowire ozn. ako pseudowire100002.

Výpis 5.12: Prehľad VFI instacií

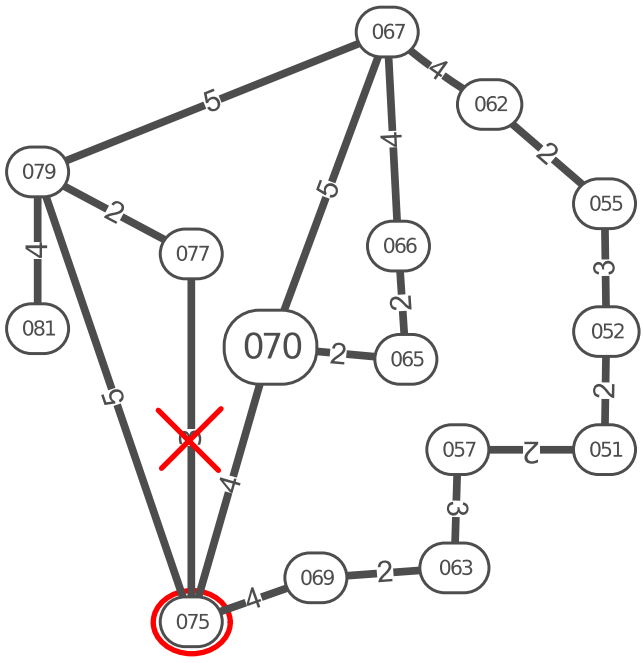
```
PE-070#show vfi
Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No

VFI name: customer_A, state: up, type: multipoint, signaling: BGP
  VPN ID: 100, VE-ID: 2, VE-SIZE: 10
  RD: 1:1234, RT: 1:100, 1:1234,
  Bridge-Domain 100 attachment circuits:
  Neighbors connected via pseudowires:
  Interface          Peer Address    VE-ID  Local Label  Remote Label    S
  pseudowire100002   10.10.9.18      1      16           17              Y
```

5.3.2 Testy dostupnosti VPLS spojenia

Jedna z praktických hlavných úloh práce je zameraná na testy dostupnosti pri výpadku spojenia. Konkrétne sa jedná o výpadok rozhrania `pseudowire`, zobrazeného vo výpise 5.12. Testy dostupnosti boli vykonané rovnakým spôsobom, aký bol popísaný v kapitole 5.2.2. V tomto prípade ide o výpadok spojenia medzi smerovačom 077 a dispečingovým centrom 070. Tieto dve pobočky sú prepojené pomocou VPLS spojenia. Aktuálna topológia a problematika je prehľadnosť znovu zobrazená na obr. 5.12. Červený kríž medzi linkami 077 a 075 znázorňuje prvý prípad výpadku, a teda výpadok linky. Druhý prípad výpadku znázorňuje červený kruh okolo rozvodne ozn. ako 075, čo predstavuje výpadok celej rozvodne.

Celkovo bolo prevedených 6 testov dostupnosti, ktoré pozostávajú z:

1. testu dostupnosti pri výpadku linky, konvergencia pomocou protokolu OSPF,
2. testu dostupnosti pri výpadku linky, konvergencia pomocou technológie MPLS-TE FRR,
3. testu dostupnosti pri výpadku smerovača, konvergencia pomocou protokolu OSPF,
4. testu dostupnosti pri výpadku smerovača, konvergencia pomocou technológie MPLS-TE FRR,
5. testu dostupnosti pri výpadku RR príkazom `reload`,
6. testu dostupnosti pri výpadku RR prikazom `clear bgp * all 1` a `clear ip ospf process`.



Obr. 5.11: Aktuálna topológia

Test dostupnosti pri výpadku linky, konvergencia pomocou protokolu OSPF

Všetky testy dostupnosti bol prevedené rovnakým spôsobom, akými boli testy pre L3VPN spojenie popísané v podkapitole 5.2.2. Jediným rozdielom je zmena technológie pri prepájaní rozvodní z L3VPN na VPLS a zmena použitých zariadení v emulátore GNS3, nakoľko pôvodné smerovače pre L3VPN spojenie nepodporovali L2VPN a BGP-L2 VPN signalizáciu.

Prvý test bol test dostupnosti pri výpadku VPLS spojenia, kedy sa spojenie nadviaže prostredníctvom OSPF protokolu. Ide o výpadok spojenia rozvodne číslo 077 s dispečingovým centrom ozn. ako 070. Aktuálna využívaná trasa je 077-075-070 a na trase 077-075 nastal výpadok linky. Prostredníctvom OSPF protokolu dôjde k znovu-obnoveniu spojenia, čo popisuje výpis 5.13.

Výpis 5.13: Výpadok linky 077-075

```
11974 0.915457228  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
11975 0.915457325  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
11976 0.915705067  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
11977 5.235213397 ASUSTekC_45:32:03  aa:bb:cc:00:06:10 ARP 42 Who has 192.168.5.1? Tell
    192.168.5.2
11978 5.235557557 aa:bb:cc:00:06:10  ASUSTekC_45:32:03 ARP 60 192.168.5.1 is at aa:bb:cc:00:06:10
11979 7.235776325  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
11980 7.235776746  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
11983 7.235890971  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
```

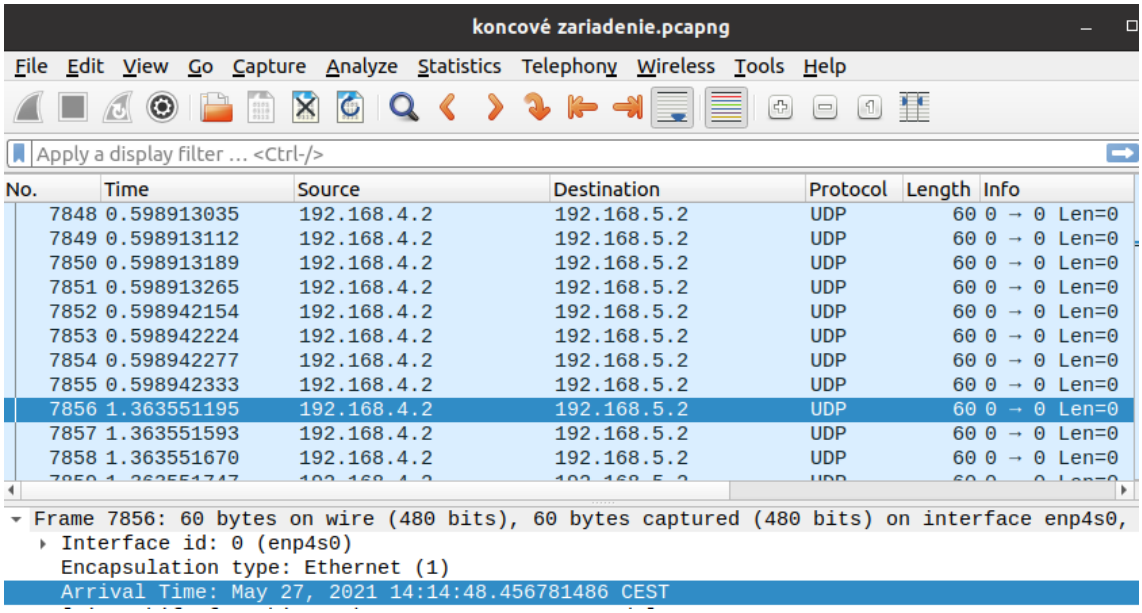
Výpadok linky sa znovu určí podľa prerušeného toku UDP paketov s odstupom 10 µs. Z výpisu 5.13 vyplýva, že spojenie generované programom Mausezahn bolo prerušené na 6,32007 s, čo je zároveň možné považovať za čas nedostupnosti. Takáto doba nedostupnosti nespĺňa požiadavky KII a tento stav by mal byť ošetrený, čo je predmetom nasledujúceho testu.

Test dostupnosti pri výpadku linky, konvergencia pomocou technológie MPLS-TE FRR

Ďalším testom dostupnosti bol test dostupnosti VPLS spojenia s využitím technológie MPLS-TE FRR. K rozvodni 077 bol pripojený fyzický PC generujúci tok 100 000 p/s na dispečingové centrum ozn. ako 070, ku ktorej bol pripojený ďalší fyzický PC zachytávajúci generovaný tok UDP paketov. Výpadok linky na trase 077-075 bol ošetrený konfiguráciou, ktorá je bližšie popísaná v kapitole 5.6.

Pomocou odchytávania paketov na linkách v GNS3 sa určil čas, kedy došlo k prepnutiu posielaniu UDP paketov na linkách 077-075 a 077-079, čo umožnilo ľahšiu identifikáciu výpadku na koncovom zariadení pripojenom k dispečingovému centru ozn. ako 070. Obr. 5.12 zobrazuje časovú medzeru medzi paketom č. 7855 a 7856. Rozdiel časových značiek týchto dvoch paketov je 0,76461 s, čo je takmer identický

výpadok, ako v prípade výpadku L3VPN spojenia pri použití technológie MPLS-TE FRR pri výpadku linky. Takýto čas nedostupnosti pri výpadku linky na 0,765 s je považovaný ako vyhovujúci pre KII.



Obr. 5.12: Výpadok VPLS spojenia - MPLS-TE FRR

Test dostupnosti pri výpadku smerovača, konvergencia pomocou protokolu OSPF

Tretí test dostupnosti je test dostupnosti pri výpadku rozvodne č. 075. Namiesto trasy 077-075-070 sa tak volí náhradná trasa 077-079-067-070. Výpadok zariadenia bol spôsobený rovnakým spôsobom, aký je popísaný v kapitole 5.2.2 pri výpadku smerovača a zobrazený na obr. 5.8.

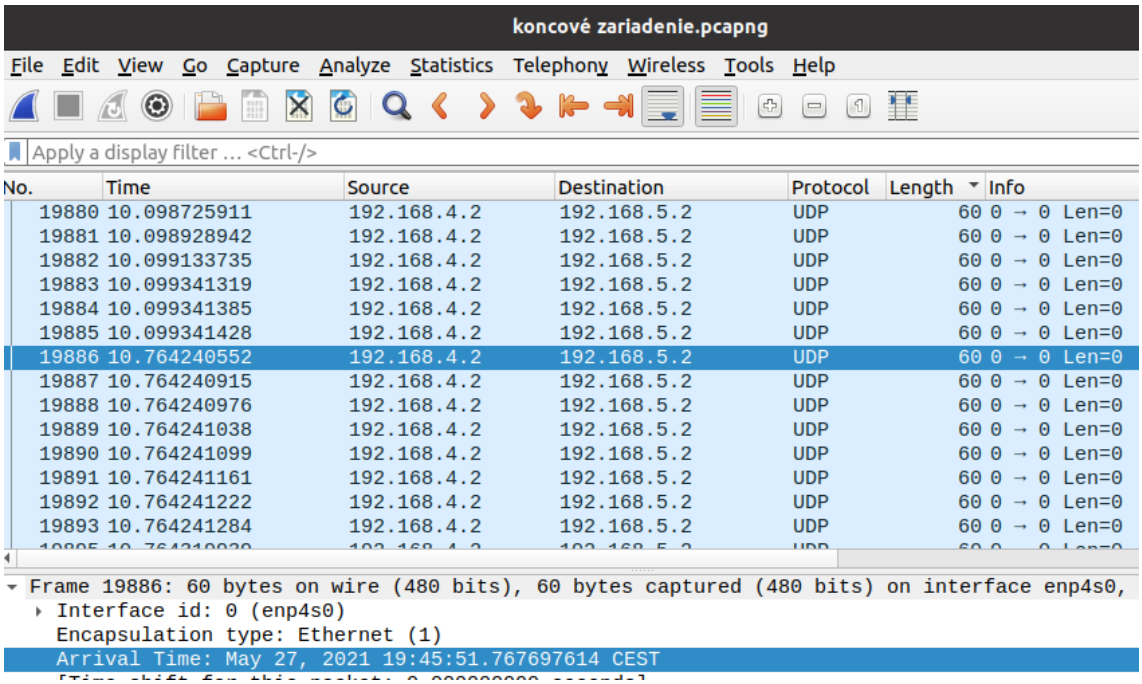
Výpis 5.15 programu Tshark na koncovom zariadení dokumentuje tento výpadok. Výpadok dostupnosti bol prítomný na 23,880 s, čo je síce kratší čas nedostupnosti oproti výpadku zariadenia pri L3VPN spojení (32,843 s) o 8,963 s, avšak tento výpadok je možné považovať za veľmi nevyhovujúci, rovnako ako pri výpadku zariadenia pri L3VPN spojení. Nasledujúci test ošetruje tento stav výpadku zariadenia prostredníctvom MPLS-TE FRR technológie.

Výpis 5.14: Výpadok VPLS spojenia pri výpadku smerovača

```
15195 1.159717984  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
15196 1.159718057  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
15197 1.159921799  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
15198 5.048659341 ASUSTekC_45:32:03  aa:bb:cc:00:06:10 ARP 42 Who has 192.168.5.1? Tell
    192.168.5.2
15199 25.040148686  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
15200 25.040149050  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
15201 25.040149130  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
```

Test dostupnosti pri výpadku smerovača, konvergencia pomocou technológie MPLS-TE FRR

Obr. 5.13 zobrazuje odchytávanie paketov na koncovom zariadení. K nájdeniu tohoto výpadku bol rovnako ako v predchádzajúcich prípadoch prvotne použitý nástroj Wireshark na linkách v GNS3 a následne po nájdení času prepnutia liniek bolo jednoduchšie identifikovanie výpadku spojenia na koncovom zariadení. Časový rozdiel paketov s číslom 19885 a 19886 predstavuje výpadok spojenia, čo predstavuje 0,665 s. Takto ošetrený výpadok v porovnaní s predchádzajúcim testom splňuje podmienky KII.



Obr. 5.13: Výpadok VPLS - MPLS-TE FRR

Test dostupnosti pri výpadku RR príkazom `clear bgp * all 1` a `clear ip ospf process`

Ďalším testom bol test dostupnosti pri simulovanom výpadku spojení rozvodní s route-reflectorom. V tomto prípade ide o výpadok posledného RR, kedy sa tento RR stáva bodom, ktorý ak zlyhá, tak vypadnú všetky VPN spojenia. Príkazmi `clear ip bgp * all 1` a `clear ip ospf process` dôjde k resetovaniu všetkých BGP a OSPF spojení na RR. Spojenia RR s ostatnými rozvodňami sa tak musia znovu-nadviazať a vymeniť si potrebné cesty. Výpadok spojenia je zaznamenaný na výpise 5.16. Pri toku UDP paketov s odstupom 10 µs bol posledný prichádzajúci paket na koncové zariadenie pred výpadkom spojenia zachytený s časovým razítkom 1.57676314 s a po obnovení potrebných spojení s RR a rozvodňou 070 prišiel

ďalší UDP paket s časovým razítkom 18.97224869. Rozdiel týchto dvoch paketov predstavuje čas výpadku 17,39548559 s.

Výpis 5.15: Výpadok RR pre VPLS spojenie

```
20499 1.576763001  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
20500 1.576763071  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
20501 1.576763143  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
20502 5.019567846 ASUSTekC_45:32:03  aa:bb:cc:00:06:10 ARP 42 Who has 192.168.5.1? Tell
    192.168.5.2
20503 5.019896383 aa:bb:cc:00:06:10  ASUSTekC_45:32:03 ARP 60 192.168.5.1 is at aa:bb:cc:00:06:10
20504 11.711811441 aa:bb:cc:00:06:10  CDP/VTP/DTP/PAgP/UDLD CDP 324 Device ID: d_budejovice  Port
    ID: Ethernet0/1
20505 18.972248697  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
20506 18.972249071  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
20507 18.972249148  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
```

Dôvod pridania tohoto testu bol spomenutý pri L3VPN testoch dostupnosti, kedy sa dá výpadok zariadenia rozdeliť na dve časti. Prvú časť tvorí nahratie OS zariadenia a zapnutie zariadenie. Druhú časť tvorí nadväzovanie susedstiev s ostatnými zariadeniami v sieti. Tento test sa tak sústreďuje na druhú časť výpadku zariadenia, nakoľko prvá sa môže v praxi odlišovať od použitia zariadenia od jednotlivého výrobcu a modelu.

Test dostupnosti pri výpadku RR príkazom `reload`

Posledným testom dostupnosti bol výpadok RR pre VPLS spojenie. Tento test môže byť výrazne ovplyvnený použitým typom smerovača. Ako RR bol použitý Cisco IOS XE, ktorého plné načítanie OS trvá približne 125-135 s, v závislosti od aktuálneho HW zaťaženia počítača. V reálnom svete platí rovnaká zásada, kedy každý smerovač v závislosti od výrobcu a modelu načítava svoju funkčnosť časovo-odlišne. Výpadok spojenia zobrazuje výpis 5.16. Príkazom `reload` došlo k simulovanému výpadku RR. Časový rozdiel toku UDP paketov pred a po výpadku spojenia je 171,3278 s.

Výpis 5.16: Výpadok RR príkazom `reload`

```
26729 17.407989426  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
26730 17.407989522  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
26731 17.408192677  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
26770 41.687180236 fe80::724d:7bff:fe46:c027  ff02::16     ICMPv6 110 Multicast Listener Report
    Message v2
26794 185.366058572 aa:bb:cc:00:03:10  CDP/VTP/DTP/PAgP/UDLD CDP 324 Device ID: d_budejovice
    Port ID: Ethernet0/1
26795 188.736010656  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
26796 188.736011074  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
26797 188.736011150  192.168.4.2  192.168.5.2  UDP 60 0  0 Len=0
```

Podobne ako pri debugovaní výpisov smerovača s Cisco IOS image i86bi-linux-l3-adventerprisek9-15.2.2.15T.bin pri L3VPN spojení sa dajú sledovať postupné výpisy pri načítavaní smerovača s operačným systémom IOS XE s image csr1000v-universalk9.16.12.03-serial.qcow2. Tieto debugovacie výpisy je možné pozorovať na vý-

pise 5.17. V čase 13:13:37.150 za začal resetovací proces a v čase 13:16:28.074 sa nadviazalo prvé BGP-spojenie. Rozdiel týchto časov je 170,924 s, čo približne odpovedá výpadku spojenia nameraného v tomto teste s rozdielom 0,4038 s.

Výpis 5.17: Debugovacie výpisy RR CSR1000V

```
Proceed with reload? [confirm]
*May 27 13:13:37.150: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
  Booting 'CSR1000v-packages.conf'
*May 27 13:16:19.047: %SYS-6-BOOTTIME: Time taken to reboot after reload =  162 seconds
*May 27 13:16:23.518: %LINK-3-UPDOWN: Interface GigabitEthernet1, changed state to up
*May 27 13:16:28.074: %BGP-5-ADJCHANGE: neighbor 10.10.9.102 Up
```

5.4 MPLS QoS

V MPLS sieťach sa technológia MPLS QoS používa na prioritizáciu paketov rovnako, ako pri IP paketoch. V prípade IP princípu sa nastavujú v poli CoS hodnoty bitov IP precedence alebo DiffServ Codepoint (DSCP) v IP hlavičke. V prípade MPLS paketov sa nastavuje EXP bit v MPLS hlavičke [29]. EXP bit sa dá nastaviť tromi spôsobmi:

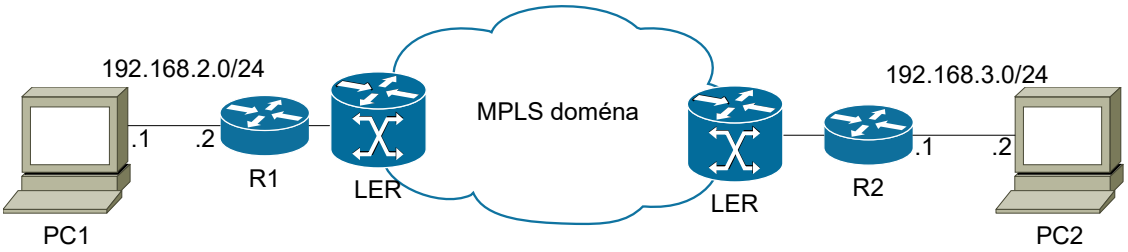
- statickým nastavením EXP bitu v smerovači,
- nastavením IP precedence/DSCP hodnoty a následným prevodom na na EXP bit. Prehľad mapovania z IP na MPLS je zobrazený v tab. 5.1,
- použitím informácií z ethernetového rámca [29].

ToS hodnota	MPLS EXP bit
0 - 7	0
8 - 15	1
16 - 23	2
24 - 31	3
32 - 39	4
40 - 47	5
48 - 55	6
56 - 63	7

Tab. 5.1: Mapovanie IP - MPLS

Pri testovaní MPLS QoS bola simulovaná komunikácia medzi rozvodňou a dispečingovým centrom. Na obr. 5.14 je zobrazená topológia KII z pohľadu pracovníka, ktorý je pripojený do siete. Komunikácia medzi PC1-R1, rovnako ako R2-PC2 podlieha IP politike nastavenej medzi týmito zariadeniami podľa tradičných IP princípov. Pri ďalšej komunikácii vo vnútri MPLS siete sa všetky pakety zaobalujú

do MPLS hlavičky a sú ďalej preposielané podľa politiky nastavenej vnútri MPLS siete.



Obr. 5.14: Topológia pre testovanie MPLS QoS

5.4.1 Implementácia MPLS QoS

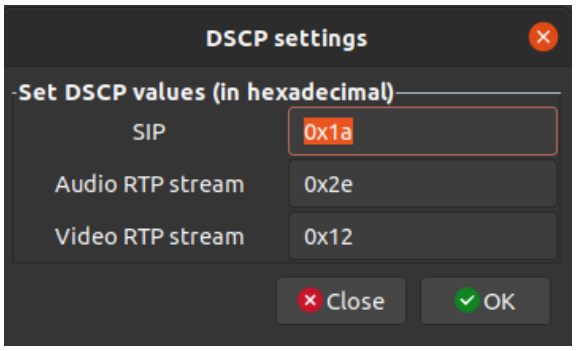
Pri implementácii MPLS QoS je prvým krokom identifikácia prevádzky, na ktorú má byť aplikovaná politika. V prípade testovania MPLS QoS je prevádzka označená DSCP hodnotou priamo konfiguráciou smerovača, viď výpis 5.18 alebo prostredníctvom značkovania v aplikácii, ako to umožňuje aplikácia Linphone, ktorá bude použitá neskôr na simuláciu videohovoru na obr. 5.15.

Na výpise 5.18 je možné sledovať nastavenie DSCP hodnoty af11 pre prevádzku zo zariadenia PC2 zobrazeného na obr. 5.14, pričom je označená prevádzka využívajúca TCP protokol zo siete 192.168.3.0/24 práve DSCP hodnotou af11. Obr. 5.15 zobrazuje nastavenie DSCP hodnoty pre zvuk a video pochádzajúci z webkamery pripojenej k PC1. DSCP hodnota je v hexadecimálnom formáte, kedy pre audio zodpovedá hodnota 46 v decimálnej hodnote (EF) a pre video to je 22 (af21).

Výpis 5.18: Nastavenie DSCP v smerovači

```
class-map match-any ftp_traffic
 match access-group 101
!
policy-map EGRESS
 class ftp_traffic
  set ip dscp af11
!
interface Ethernet 0/0
  service-policy input EGRESS
!
access-list 101 permit tcp 192.168.3.0 255.255.255.0 any
```

Z výpisu 5.18 vyplýva, že najskôr sú odchytávané akékoľvek TCP pakety z adresy 192.168.3.0/24 v číselnom ACL. Následne je tento ACL vložený do class-mapy `ftp_traffic`, class-mapa vložená do policy-mapy `EGRESS` a tá je v poslednom rade aplikovaná na prichádzajúce rozhranie `Ethernet 0/0`.



Obr. 5.15: Nastavenie značkovania DSCP v aplikácii

Okrajový LER (PE) smerovač zobrazený na obr. 5.14 zodpovedá za preklad z IP QoS domény (IP2MPLS) do MPLS QoS domény a naopak (MPLS2IP). Takýto princíp MPLS QoS je označovaný ako: Uniform mode. Pre tento princíp je charakteristické riadenie celej infraštruktúry prostredníctvom poskytovateľa služby. Okrem Uniform mode existujú ďalšie 3 princípy - Pipe mode, Short Pipe mode, Long Pipe mode. Ich popis nie je predmetom tejto práce.

Nastavenie MPLS QoS vnútri MPLS domény

Výpis 5.19 dokumentuje nastavenie MPLS QoS vnútri MPLS domény. Celkovo sú prioritizované 3 druhy prevádzky:

- VOIP - vnútri MPLS domény je pre tento typ prevádzky nastavený MPLS EXP bit 5 na základe nastavenej DSCP hodnoty v aplikácii Linphone. Pre VOIP prevádzku je tradične nastavená príkazom v policy-map `priority percent 30` fronta typu LLQ. Táto fronta sa vyznačuje tým, že v prípade zahltenia linky sa alokuje pre danú prevádzku v tomto prípade 30% z celkovej šírky pásma. Takto je garantovaných vždy voľných 30 % z celkovej šírky pásma (3000 kb/s) pre VOIP potreby na všetkých linkách, kedy jednotlivé linky v GNS3 majú nastavenú šírku pásma 10 000 kb/s.
- Video z webkamery - v aplikácii Linphone je pre tento typ nastavená DSCP hodnota af21, pre čo zodpovedá MPLS EXP bit 2. Príkazom v policy-map `bandwidth percent 30` sa nastaví fronta typu CBWFQ (Class-based weighted fair queueing) a pri zahltení linky sa alokuje 30% z dostupnej šírky pásma. Takýto typ fronty garantuje šírku pásma jednotlivým triedam, čo aj vyplýva z názvu fronty. Jednotlivým triedam sa dá následne určovať váha.
- FTP prenos - pre tento typ prevádzky platí rovnaká CBWFQ politika ako v prípade prevádzky videa z webkamery. Pre prioritizáciu je značenie prevádzky nastavené priamo vo smerovači, čo je popísané vo výpise 5.18. Nastavenej DSCP hodnote af11 zodpovedá MPLS EXP bit 1, čo znamená že táto

prevádzka patrí do rovnakej triedy s MPLS EXP bitom 1. Podľa výpisu 5.19 je možné vidieť, že pre tieto prenosy bolo vyčlenených 20 % z celkovej šírky pásma. Tento typ predstavuje prenos súboru z PC1 na PC2 prostredníctvom FTP protokolu.

- Zostávajúca šírka pásma je určená pre neoznačenú prevádzku v prednastavenej triede class-default. Takáto prevádzka má IP precedence/DSCP hodnotu nastavenú na 0 a teda aj MPLS EXP bit je 0. Príkazom `fair-queue` je nastavená fronta typu Fair Queuing a teda rovnaké rozdelenie zostávajúcej šírky pásma pre jednotlivé prevádzky na základe adries alebo protokolov. Takáto fronta neumožňuje garanciu šírky pásma.

Výpis 5.19: Nastavenie QoS vnútri MPLS domény

```
085#show policy-map interface ethernet 0/0 output
 Ethernet0/0

  Service-policy output: INGRESS

    queue stats for all priority classes:
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0

    Class-map: voip_mpls_domain (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: mpls experimental topmost 5
      Priority: 30% (3000 kbps), burst bytes 200000, b/w exceed drops: 0


    Class-map: video_mpls_domain (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: mpls experimental topmost 1
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth 30% (3000 kbps)

    Class-map: ftp_mpls_domain (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: mpls experimental topmost 2
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth 20% (2000 kbps)

    Class-map: class-default (match-any)
      1707 packets, 128057 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

```
Queueing
queue limit 64 packets
(queue depth/total drops/no-buffer drops/flowdrops) 0/0/0/0
(pkts output/bytes output) 1706/143434
Fair-queue: per-flow queue limit 16 packets
```

5.4.2 Meranie MPLS QoS

Pre demonštráciu funkčnosti bol najskôr prevedený test bez implementácie QoS. Zahltenie linky prebieha na okrajových LER smerovačoch, kde bola obmedzená šírka pásma na 10Mb/s príkazom `platform hardware throughput level mb 10`. Pre nastavovanie priepustnosti bolo potrebné aktivovať digitálnu licenciu od spoločnosti Cisco z webstránky [30]. Vzhľadom na nedokonalosti GNS3 nie je možné ovplyvňovať šírku pásma a priepustnosť na ostatných smerovačov okrem okrajových LER smerovačov, ktoré využívajú Cisco IOS XE.

Wireshark · RTP Streams · PC1-cong.pcapng

Source Address	Source Port	Destination Address	Destina	SSRC	Payload	Packets	Lost
192.168.2.2	7078	192.168.3.2	7078	0x...49	opus	3209	0 (0.0%)
192.168.2.2	9078	192.168.3.2	9078	0x...96	VP8	5786	0 (0.0%)
192.168.3.2	7078	192.168.2.2	7078	0x...33	opus	478	452 (48.6%)
192.168.3.2	9078	192.168.2.2	9078	0x...51	VP8	2102	2933 (58.3%)

Obr. 5.16: Stratovosť PC1

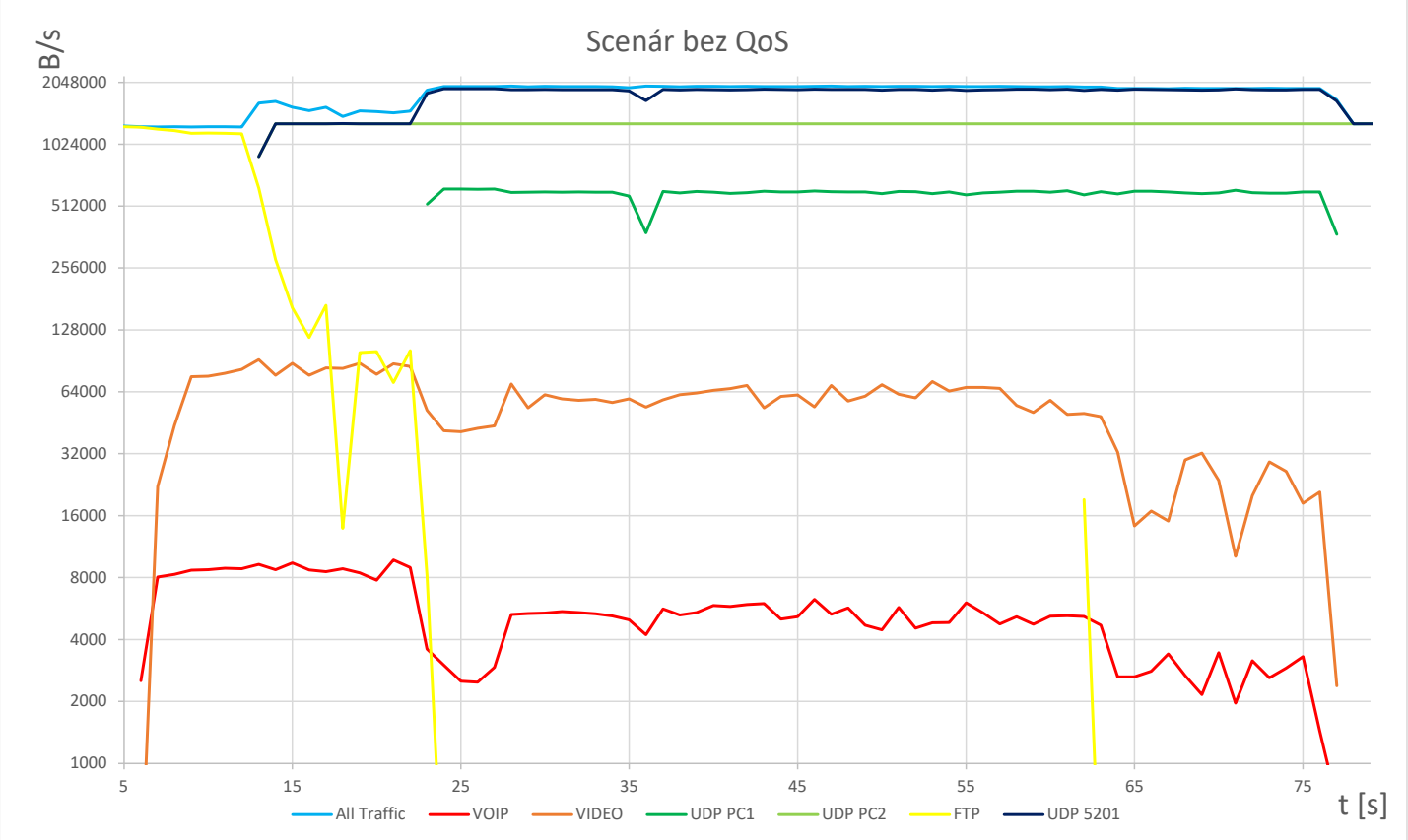
Wireshark · RTP Streams · PC2-cong.pcapng

Source Address	Source Port	Destination Address	Destina	SSRC	Payload	Packets	Lost
192.168.3.2	9078	192.168.2.2	9078	0x...51	VP8	5462	0 (0.0%)
192.168.3.2	7078	192.168.2.2	7078	0x...33	opus	1009	0 (0.0%)
192.168.2.2	7078	192.168.3.2	7078	0x...49	opus	1572	1405 (47.2%)
192.168.2.2	9078	192.168.3.2	9078	0x...96	VP8	2495	2852 (53.3%)

Obr. 5.17: Stratovosť PC2

Obr 5.16 a obr. 5.17 zobrazujú priebeh komunikácie VOIP hovoru medzi dvomi zariadeniami. Z dôvodu použitia softvéru Wireshark nie je možná obojsmerná analýza prevádzky, a preto bolo zachytávanie paketov spustené na oboch zariadeniach. PC1 s IP adresou 192.168.3.2 má tak stratovosť videa vysielaného z PC2 58,3% a stratovosť prenášaného zvuku z webkamery je 48,6%. Obdobné výsledky merania sú na PC2. Takto nakonfigurovaná sieť nespĺňa požiadavky kritickej infraštruktúry definované v kapitole 1.2.1 a je vyžadovaná dodatočná konfigurácia na prevenciu takéhoto scenára.

Priebeh prevádzky jednotlivých prevádzok v čase zobrazuje graf na obr. 5.18. Kvôli veľkému rozdielu v objemnosti jednotlivých prevádzok je použité logaritmické zobrazenie grafu. Popis priebehu jednotlivých prevádzok v čase je popísaný pod grafom.



Obr. 5.18: Graf priebehu bez QoS

Zobrazený graf je výsledkom zachytávania paketov na zaradení ozn. ako PC2. Pre generovanie prevádzky s názvom UDP PC1 a UDP PC2 bol využitý nástroj iperf3, čím bol posielaný jednosmerný tok UDP paketov vo veľkosti 10 Mb/s. Obdobný prípad je prevádzka UDP PC2 s tým rozdielom, že na zobrazenom grafe je táto prevádzka rovná čiara, kedy sa konštantne generuje tok paketov 10 Mb/s. Zo zariadenia ozn. ako PC1 sa odosiela vzájomný tok UDP paketov na zariadenie ozn. ako PC2 na cieľový port 5201 . Kvôli nedostatočnej šírke pásma je prevádzka označená ako UDP PC1 z pôvodnej odoslanej veľkosti 10 Mb orezaná na priemerne 4.8 Mb/s. Najkritickejšia je prevádzka využívajúca TCP protokol V tomto prípade ide o FTP prenos súboru z PC1 do PC2. Pri začiatku meraní bolo sťahovanie súboru spustené a využívalo maximálnu dostupnú šírku pásma, následne sa spustili toky paketov UDP PC1, UDP PC2 a videohovor, čo malo za následok úplný výpadok

TCP spojenia. Pre potreby kritickej infraštruktúry je takáto situácia neprípustná, nakoľko najdôležitejšia prevádzka v kritickej infraštruktúre je práve SCADA komunikácia, ktorá využíva TCP spojenie. Prevádzka ozn. ako UDP 5201 predstavuje súčet odchádzajúcej prevádzky UDP PC2 (10 Mb) a prichádzajúcej UDP PC1 (4.8 Mb). Rozdiel medzi prevádzkou All Traffic a UDP 5201 je dostupná šírka pásma, ktorej je v prípade bez nakonfigurovania QoS kladený veľmi malý dôraz. Zvyšnú šírku pásma tak využíva videohovor, ktorý používa RTP protokol a ktorý má určitú stratovosť preneseného zvuku a videa, čo bolo zobrazené na obr. 5.16 a obr. 5.17.

Obr. 5.18 zobrazuje priebeh komunikácie VOIP hovoru na zaradení ozn. ako PC2 s nakonfigurovanými parametrami QoS. Je možné vidieť, že vhodnou konfiguráciou sa dá znížiť stratovosť VOIP hovoru a prenosu videa na 0%. Obdobná stratovosť ako je na obr. 5.18 je na PC1, a teda 0 %.

Wireshark · RTP Streams · QoS.pcapng

Source Address	Source Port	Destination Address	Destina	SSRC	Payload	Packets	Lost	Max Delta (ms)
192.168.2.2	9078	192.168.3.2	9078	0x...b4	VP8	2572	0 (0.0%)	519.038
192.168.2.2	7078	192.168.3.2	7078	0x...96	opus	3234	0 (0.0%)	43.956
192.168.3.2	9078	192.168.2.2	9078	0x...5e	VP8	4428	0 (0.0%)	124.837
192.168.3.2	7078	192.168.2.2	7078	0x...8e	opus	1027	0 (0.0%)	92.312

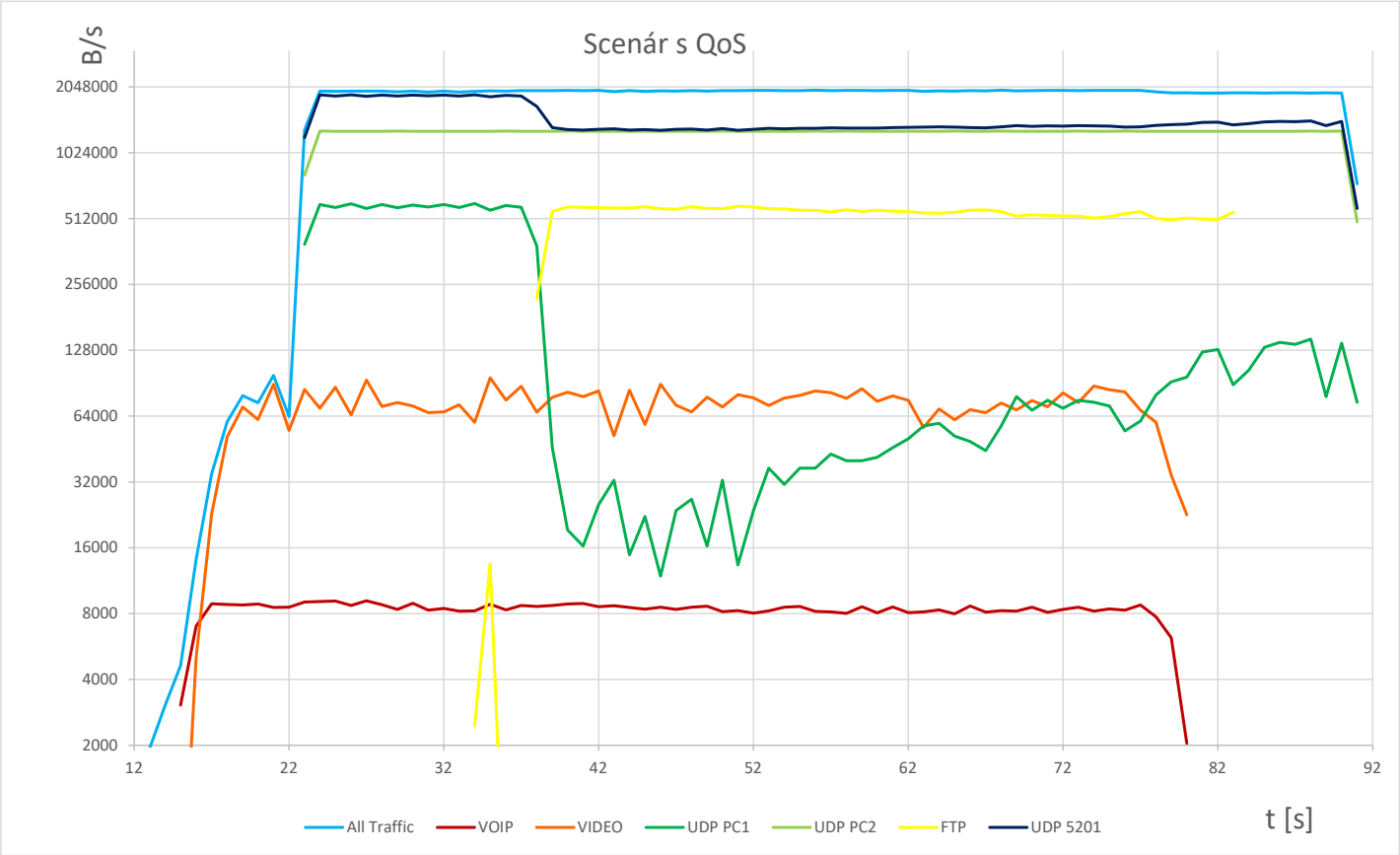
Obr. 5.19: Stratovosť s QoS

Graf z nakonfigurovanými parametrami pre kvalitu služby zobrazuje graf na obr. 5.20. Táto konfigurácia je potrebná pre zabezpečenie spoľahlivosti kritických aplikácií, nakoľko im je vždy garantovaná šírka pásma pri normálnych podmienkach, ale aj pri poruche. Tento scenár lepšie vyhovuje požiadavkám KII, nakoľko poskytuje ochranu pre požadované dátové prenosy.

Z porovnania grafu na obr. 5.18 a grafu obr. 5.20 je možné pozorovať niekoľko zásadných rozdielov:

- prevádzka VOIP a VIDEO má vyrovnanejšiu krivku, čo znamená že nedochádza ku stratovosti, príliš veľkému kolísaniu a opozdeniu,
- prevádzka využívajúca FTP má garantovanú šírku pásma a nedochádza tak k výpadku tohto typu prevádzky, nakoľko bola zahltená prenosmi využívajúcimi UDP protokol,
- prichádzajúca prevádzka označená ako UDP PC1 (4.8 Mb/s) je v zhruba 37. sekunde nahradená FTP prevádzkou a nastane tak pokles rapídny prijímania prevádzky typu UDP PC1,
- rozdiel medzi prevádzkou All Traffic a UDP 5201 je väčší na grafe s nakonfigurovanou kvalitou služby, z dôvodu garantovanej šírky pásma pre ostatné

druhy prevádzok. Prevádzka UDP 5201 tak využíva väčšinu šírky pásma bez konfigurácie QoS, čo je tiež možné pozorovať na obr. 5.18.



Obr. 5.20: Graf priebehu s QoS

5.5 MPLS-TE

Väčšina dôvodov pre používanie technológie MPLS je pre možnosť, ktorú MPLS ponúka a to je práve technológia MPLS-TE. V tejto práci sa bude technológia využívať predovšetkým pre jej funkciu rozloženia záťaže na viaceré linky a ošetrenie kritických stavov pri výpadku pomocou technológie MPLS-TE FRR.

S rozvojom IoT technológií sa značne znásobili dátové prenosy v kritickej energetickej infraštruktúre. Do roku 2025 sa očakáva 75,4-miliónov pripojených IoT zariadení, z čoho 50% bude tvoriť práve priemyslový sektor. V prípade tejto práce ide o komunikáciu zariadení u koncového zákazníka s poskytovateľom služby a naopak. Ďalším faktorom pre prispôsobenie infraštruktúry je fakt, kedy 1. júla 2024 dôjde k platnosti vyhlášky o meraní č. 359/2020 Sb., ktorá hovorí o tom, že v ČR a EU pri

inštalácii nového odberného miesta pre elektrinu, pričom odberné miesto má potenciál nad 6 MWh za 1 rok, tak takéto odberné miesto musí byť vybavené inteligentným elektromerom s daným komunikačným rozhraním (NB-IoT, LoRaWAN, LTE CAT-M, Wireless M-BUS). S rastúcim počtom zariadení bude rásť objemnosť datových prenosov a práve vďaka možnostiam MPLS-TE bude možné efektívne škálovať prevádzku tak, aby boli všetky linky rovnomerne využité a ošetrené proti stratám dát pri poruchách.

Pre testovacie účely technológie MPLS-TE bola upravená šírka pásma všetkých liniek v topológii na 100 Mb. Následne príkazom `ip rsvp bandwidth percent 90` bolo na linkách všetkých smerovačov v topológii alokovaných maximálne 90 Mb pre účely tunelovania prevádzky. Na výpise 5.20 je zobrazená alokácia 40 Mb z maximálne možných 90 Mb na rozhraniach `Ethernet 0/0` a `Ethernet 0/1`. Následne je na výpise 5.20 zobrazený prehľad tunelov príkazom `show mpls traffic-eng tunnels brief`, cez ktoré prechádzajú MPLS-TE tunely. Cez smerovač 085 teda prechádzajú 2 tunely, z čoho tunel s názvom `PE070-T2-ALL-TRAFFIC` má za destináciu smerovač PE-018 s príslušnou IP adresou, obdobne ako tunel s názvom `PE018-T5-ALL-TRAFFIC`.

Výpis 5.20: Alokácia šírky pásma

```
085#show ip rsvp interface
interface    rsvp  allocated  i/f max  flow max sub max  VRF
Et0/0        ena   40M        90M      90M      0
Et0/1        ena   40M        90M      90M      0
085#
085#show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:            running
    Passive LSP Listener:           running
    RSVP Process:                   running
    Forwarding:                     enabled
    Periodic reoptimization:        every 3600 seconds, next in 3262 seconds
    Periodic FRR Promotion:         Not Running
    Periodic auto-bw collection:    every 300 seconds, next in 262 seconds
TUNNEL NAME                     DESTINATION      UP IF      DOWN IF    STATE/PROT
PE070-T2-ALL-TRAFFIC              10.10.9.18     Et0/0      Et0/1      up/up
PE018-T5-ALL-TRAFFIC              10.10.9.70     Et0/1      Et0/0      up/up
Displayed 0 (of 0) heads, 2 (of 2) midpoints, 0 (of 0) tails
085#
```

Dokopy je v topológii vytvorených 8 tunelov, čo dokumentuje výpis 5.21. Tunelmi, ktoré majú v názve VOIP prechádza prevádzka patriaca VOIP rovnako ako v prípade prevádzky ozn. ako VIDEO, kedy týmito tunelmi prevádzka simulovaného videohovoru programom Linphone. Takýmto tunelom je určená priorita a najkratšia cesta pre dosiahnutie najlepších prenosových vlastností (opozdenie, jitter, stratovosť). Tunelmi označenými ako ALL-TRAFFIC prúdi ostatná prevádzka a ich cesta je odlišná oproti prioritizovaným tunelom. Prevádzku ALL-TRAFFIC tvoria rovnako ako v kapitole 5.4 obojsmerné UDP prenosy generované nástrojom iperf3

a prenos súboru s využívajúci FTP protokol.

Výpis 5.21: Prehľad vytvorených tunelov

```
PE-070#show mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:            running
    Passive LSP Listener:           running
    RSVP Process:                   running
    Forwarding:                     enabled
    auto-tunnel:
  p2p    Disabled (0), id-range:62336-64335

    Periodic reoptimization:        every 3600 seconds, next in 2655 seconds
    Periodic FRR Promotion:         Not Running
    Periodic auto-bw collection:    every 300 seconds, next in 255 seconds
    SR tunnel max label push:       13 labels

P2P TUNNELS/LSPs:
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
PE070-tunnel0                      10.10.9.18    -         n/a       up/up
PE070-T1-VOIP                      10.10.9.18     -         Gi3       up/up
PE070-T2-ALL-TRAFFIC               10.10.9.18     -         Gi2       up/up
PE070-T3-VIDEO                     10.10.9.70     -         Gi3       up/up
PE018-T4-VOIP                      10.10.9.70     Gi3       -         up/up
PE018-T5-ALL-TRAFFIC               10.10.9.70     Gi2       -         up/up
PE018-T6-VIDEO                     10.10.9.70     Gi3       -         up/up
Displayed 4 (of 4) heads, 0 (of 0) midpoints, 3 (of 3) tails

P2MP TUNNELS:
Displayed 0 (of 0) P2MP heads

P2MP SUB-LSPS:
Displayed 0 P2MP sub-LSPs:
          0 (of 0) heads, 0 (of 0) midpoints, 0 (of 0) tails
PE-070#
```

Tunel s názvom PE070-tunnel0 vo slúži ako master-tunnel. Detail tohto tunelu popisuje výpis 5.22. Vďaka tomuto tunelu je možné ľubovolne škáľovať prevádzku a posielať ju určenými LSP. Rovnaký tunel je nakonfigurovaný aj na smerovači PE2-018 a preto nie je vidieť v prehľade tunelov vo výpise 5.21. Tento tunel nie je viazaný k žiadnemu rozhraniu, nakoľko združuje ostatné 3 tunely, pomocou ktorých bolo prevedené škálovanie prevádzky. V tomto prípade sa toto škálovanie dosiahlo pomocou dopredu nastavených MPLS EXP bitov pre jednotlivé typy prevádzok. Tunel ozn. ako Tunnel1 tak prenáša prevádzku s MPLS EXP bitom 5, čo je VOIP prevádzka a obdobná vlastnosť platí pre ostatné tunely.

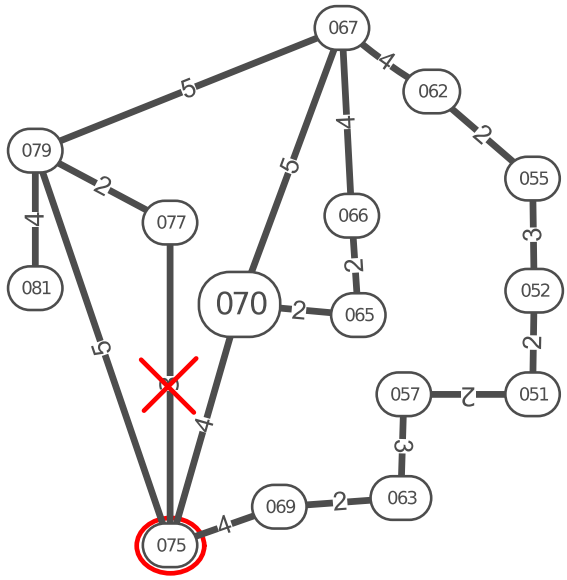
Výpis 5.22: Master tunel

```
PE-070#show mpls traffic-eng tunnels detail

P2P TUNNELS/LSPs:

Name: PE070-tunnel0                          (Tunnel0) Destination: 10.10.9.18
  Status: Master
    Admin: up         Oper: up     Signalling: N/A
```

```
  Member Tunnels:         Member Autoroute: Inactive

  Tunnel1: Config Exp:  5
  Tunnel2: Config Exp:  0 1 3 4 6 7
  Tunnel3: Config Exp:  2

  Path-selection Tiebreaker:
    Global: not set   Tunnel Specific: not set   Effective: min-fill (default)
  Hop Limit: disabled
  Cost Limit: disabled
  Path-invalidation timeout: 10000 msec (default), Action: Tear
Binding SID: 16

History:
  Tunnel:
    Time since created: 25 minutes, 55 seconds
    Number of LSP IDs (Tun_Instances) used: 0
```

5.6 MPLS-TE FRR

Pre demonštráciu funkčnosti MPLS-TE FRR boli vytvorené pre rozvodňu 077 dva záložné tunely, jeden v prípade zlyhania linky a druhý v prípade zlyhania smerovača 075. Pre prehľadnosť zobrazuje túto problematiku obr. 5.21 z celkovej topológie na obr. 1. Pre rozvodňu 077 je vyžadovaná neustála dostupnosť s dispečingovým centrom ozn. ako 070.



Obr. 5.21: Aktuálna topológia

Červený kruh okolo rozvodne 075 na obr. 5.21 značí poruchu celého smerovača. V takomto prípade sa ako náhradná trasa použije trasa 077-079-067-070. Červený

kríž medzi linkami 077-075 značí poruchu tejto linky, kedy je využitá náhradná linka s trasou 077-079-075-070.

Výpis 5.23 zobrazuje dvojicu nakonfigurovaných tunelov pre potreby MPLS-TE FRR. Tunely sú v stave ready a pri poruche linky/next-hop smerovača sa prepnú od stavu active. Head Hop označuje IP adresu rozhrania Loopback 0 smerovača 077, Tail Hop IP adresu rozhrania Loopback 0 smerovača 070, čo je zároveň aj destinácia tohto tunelu.

Výpis 5.23: Zoznam tunelov pre MPLS-TE FRR

```
077#show mpls traffic-eng fast-reroute database detail
FRR Database Summary:
  Number of protected interfaces: 1
  Number of protected tunnels: 2
  Number of backup tunnels: 2
  Number of active interfaces: 0
LSP identifier 10.10.9.77 1000 [32], ready
  Input label 29, Output label Et0/1:29, FRR label Tu2:implicit-null
  Role Mid  Head Hop 10.10.9.77 Tail Hop 10.10.9.70
LSP identifier 10.10.9.77 2000 [33], ready
  Input label 19, Output label Et0/1:28, FRR label Tu1:implicit-null
  Role Mid  Head Hop 10.10.9.77 Tail Hop 10.10.9.70
```

Výhodou Cisco IOS je, že cesty ochranných tunelov nie je potrebné konfigurovať explicitne, čo môže byť pri veľkých topológiach náročné. Postačuje tak určenie IP adresy, cez ktorú nemôže tunel prechádzať. V tomto prípade ide o cesty `avoid_link` a `avoid_node`. V explicitne určenej trase `avoid_link` vo výpise 5.24 ide o IP adresu rozhrania smerovača 075 na linke 077-075. Pri druhej spomenutej explicitnej IP adrese `avoid_node` ide o IP adresu rozhrania Loopback 0 smerovača 075. Ich konfiguráciu dokumentuje výpis 5.24. Pri prechode záložného tunela zo stavu ready do stavu active tak dôjde k nájdeniu novej trasy s podmienkou určenou v explicitnej trase pre daný tunel. Čas nájdenia novej trasy pri poruche je podľa testovania v kapitolách 5.2.2 a kapitole 5.3.2 v rozmedzí od 0,6-0,7 s. Tento čas by sa dal ešte skrátiť konfiguráciou explicitnej trasy, kde by bolo potrebné presne určiť jednotlivé skoky na trase podľa IP adries.

Výpis 5.24: Explicitné cesty

```
ip explicit-path name avoid_link enable
 exclude-address 10.10.11.69
!
ip explicit-path name avoid_node enable
 exclude-address 10.10.9.75
```

5.7 Route-reflector

Vďaka použitiu RR dôjde k výraznému zjednodušeniu BGP-smerovacích záznamov na dispečingových staniciach. Topológiu zobrazenú na obr. 1 tvorí celkovo 107 prv-

kov, z toho 105 rozvodní, ktoré komunikujú prostredníctvom L3VPN alebo VPLS spojenia s dvomi dispečingovými centrami. V prípade jedného dispečingového centra, musí riadenie prevziať druhý dispečing, a preto každá má každá rozvodňa naviazané 2 BGP-susedstvá, a to s dispečingovým centrom v Brne a Českých Budejoviciach. Celkovo takto pripadá na 1 dispečingové centrum 106 BGP susedstiev. Tento počet je vysoký a náročný na udržiavanie. Z tohoto dôvodov je potrebné použitie RR. Dispečingové centrum tak nenadväzuje spojenie s jednotlivými rozvodňami, ale iba s RR, v závislosti od počtu použitých RR. Pri použití 4 RR, dôjde k zníženiu na dispečingovom smerovači zo 106 BGP susedstiev, na 5 BGP susedstiev (dispečing-dispečing, 4 RR). Na jeden RR tak pripadá udržiavanie 27 BGP susedstiev so svojimi rozvodňami.

V topológii na obr. 1 sú jednotlivé RR nakonfigurované zo 6 možných možností, ako P-smerovač, poskytujúci funkciu pre IPv4 a zároveň pre VPNv4 RR. Takýto P-RR smerovač neposkytuje len distribúciu ciest pre IPv4, ale aj VPNv4 cesty a zároveň vykonáva preposielanie IPv4 a VPNv4 prevádzky [31].

Na výpise 5.25 je možné pozorovať BGP VPNv4 smerovaciu tabuľku prvých piatich smerovačov (siete 172.16.0.0/16) a ich príslušných ciest s metrikou 2 (siete 192.168.0.0/16).

Výpis 5.25: Smerovacia BGP L3VPN tabuľka

```
RR1# show ip bgp vpnv4 all
BGP table version is 21, local router ID is 10.10.9.202
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:100 (default for vrf customer_A)
 *>i 172.16.1.0/24    10.10.9.82               0    100      0 i
 *>i 172.16.2.0/24    10.10.9.89               0    100      0 i
 *>i 172.16.3.0/24    10.10.9.88               0    100      0 i
 *>i 172.16.4.0/24    10.10.9.79               0    100      0 i
 *>i 172.16.5.0/24    10.10.9.81               0    100      0 i
 *>i 192.168.1.0      10.10.9.82               2    100      0 i
 *>i 192.168.2.0      10.10.9.89               2    100      0 i
 *>i 192.168.3.0      10.10.9.88               2    100      0 i
 *>i 192.168.4.0      10.10.9.79               2    100      0 i
 *>i 192.168.5.0      10.10.9.81               2    100      0 i
```

Závěr

Prevedené testy dostupnosti pre L3VPN a VPLS spojenie sú zobrazené v tab. 5.2 a tab. 5.3. V týchto testoch je možné pozorovať jednotlivé výpadky spojenia s použitím konvergencie OSPF protokolu a výpadky pri použití technológie MPLS-TE FRR. Je možné dôjsť k záveru, že technológia MPLS-TE FRR umožňuje rapídne znížiť čas, kedy je zariadenie nedostupné.

Ďalším typom testov bolo testovanie výpadkov route-reflectora, čo dokumentuje v tab. 5.2 a tab. 5.3 test ozn. ako „Výpadok RR (clear)“. Prvý simulovaný test výpadku RR bol prevedený resetovaním OSPF a BGP protokolu na RR, čím došlo k vymazaniu všetkých susedstiev a smerovacích tabuliek. RR tak musel znovu nadviazať všetky spojenia s ostatnými zariadeniami v sieti. Tento čas bol pri L3VPN kratší, nakoľko pri L3VPN nedochádza k učeniu MAC adries na L2 vrstve a vytváranie smerovacej tabuľky je tak jednoduchšie a rýchlejšie.

Druhým typom testov RR bol výpadok príkazom `reload`, čím došlo k simulovanému vypnutiu a zapnutiu smerovača. Smerovač tak okrem fáze popísanej v predchádzajúcom teste musel navyše prejsť načítavacím procesom. Tento čas sa ale výrazne odlišuje od použitého výrobcu a modelu zariadenia. Pre L3VPN a VPLS boli použité rozličné modely Cisco smerovačov, čo svedčí o výrazne odlišnom čase obnovenia spojenia s ostatnými zariadeniami.

Typ testu	Výpadok [s]
Výpadok linky (OSPF)	5,5029
Výpadok linky (MPLS-TE FRR)	0,7145
Výpadok zariadenia (OSPF)	38,3463
Výpadok zariadenia (MPLS-TE FRR)	0,6924
Výpadok RR (clear)	5,0475
Výpadok RR (reload)	33,298

Tab. 5.2: Testy dostupnosti L3VPN spojenia

Typ testu	Výpadok [s]
Výpadok linky (OSPF)	6,3201
Výpadok linky (MPLS-TE FRR)	0,7646
Výpadok zariadenia (OSPF)	23,8802
Výpadok zariadenia (MPLS-TE FRR)	0,6649
Výpadok RR (clear)	17,3955
Výpadok RR (reload)	171,3278

Tab. 5.3: Testy dostupnosti VPLS spojenia

Ďalším z cieľov práce bolo porovnanie MPLS technológie s inou modernou technológiou. Pre tento účel bola vybraná technológia SD-WAN. Obidve technológie boli prakticky otestované v emulátore GNS3, avšak pri SD-WAN technológii sa pre vysoké HW požiadavky nepodarilo bližšie otestovať funkčnosť na väčšej topológii, a tak bola len sprevádzkovaná základná SD-WAN technológia, ktorú tvorili 3 virtuálne servery potrebné pre správnu funkčnosť a jedna pobočka. Táto simulácia mala však sama o sebe vysoké HW nároky a pri bližšom testovaní kvôli vysokým hodnotám RAM a CPU dochádzalo k odpájaniu pobočky. Z tohoto dôvodu bolo súčasťou druhej kapitoly tejto práce analyzovanie súčasnej situácie využívania sietí. Z tejto analýzy vyplynul spolu s informáciami obsiahnutými v tretej kapitole fakt, kedy SD-WAN technológia reaguje na najnovšie trendy v oblasti sieťovania. V súčasnosti dochádza k migrácii väčšiny aplikácií do cloudového prostredia, ku ktorým sa pristupuje cez svetovú sieť internet. Pomer internej a externej prevádzky pre pobočky v minulosti bol 80 % internej, čo predstavovalo komunikáciu vnútri infraštruktúry a 20 % externej, čo predstavuje prevádzku do svetovej siete internet. V súčasnej dobe je tento pomer opačný a SD-WAN reaguje na túto zmenu tak, aby pri tradičnom prepájaní pobočiek nenastával tzv. bottleneck siete popísaný v druhej kapitole. Prenosy KII popísané v kapitole 1.2.1 však vyžadujú internetovú konektivitu zriedkavo a preto je vhodnejšia technológia MPLS než SD-WAN.

Pre potreby KII v energetike je technológia MPLS vyhovujúca. V takejto sieti ide predovšetkým o dôležitú internú prevádzku, ktorá tvorí drvivú väčšinu dátových prenosov. K využitiu externej prevádzky dochádza iba v ojedinelých prípadoch, kedy môže ísť napr. o aktualizácie zariadení, príp. pripojenie sa do KII pracovníkom dispečingu cez VPN z iného miesta, než je dispečingové centrum. Táto možnosť by však pre zachovanie bezpečnosti KII mala byť obmedzená, nakoľko celková infraštruktúra v tejto práci je monitorovaná dvomi dispečerskými centrami v Brne a v Českých Budejoviciach, ktoré vyžadujú neustálu dostupnosť ostatných rozvodní. Pre dátové prenosy boli použité a prakticky otestované technológie MPLS-TE, MPLS-TE FRR a MPLS QoS, čím sa dosiahlo požadovanej odolnosti proti havarijným scenárom. Pri prípadnej poruche je tak čas nedostupnosti minimalizovaný prostredníctvom MPLS-TE FRR a zároveň využitím MPLS-TE a MPLS-QoS nedochádza k zahlteniu liniek a stratovosti prevádzky. Prevádzka prostredníctvom MPLS-TE posielaná viacerými smermi tak, aby dochádza k efektívnemu využívaniu šírky pásma na všetkých linkách. Pri veľkých dátových prenosoch sú typy prevádzok označené podľa dôležitosti (tried) a je im priradená odpovedajúca šírka pásma. Následne im je určená cesta podľa toho, či to daná aplikácia vyžaduje čo najmenšiu stratovosť, opozdenie alebo jitter. Jednotlivé pobočky (rozvodne) boli prepojené s dispečingovými centrami L3VPN alebo VPLS spojením, čo predstavuje bezpečný spôsob prepájania pobočiek, nakoľko datové prenosy sú v internej MPLS sieti bezpečne zašifrované.

Literatúra

[1] *Přenosová a distribuční soustava - 3. část: Dispečink, systémy chránění, komunikace a HDO* [online]. E.ON Distribuce [cit. 2020-12-11]. Dostupné z URL: <https://www.eon-distribuce.cz/clanek/prenosova-distribucni-soustava-3-cast>.

[2] Čl. 2 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky.

[3] Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

[4] Zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon), ve znění pozdějších předpisů.

[5] KOPECKÝ, Z. Východiska zvýšení odolnosti subjektů kritické infrastruktury [online]. V: *15. medzinárodná vedecká konferencia*, Fakulta špeciálneho inžinierstva ŽU, Žilina, 2. - 3. jún 2010. [cit. 2020-12-28]. Dostupné z URL: <https://www.fbi.uniza.sk/uploads/Dokumenty/weby/rks-archiv/2010/articles/clanky/Kopecky_.pdf>.

[6] ŘEHÁK, D.; HROMADA, M.; ŠENOVSKÝ, P.;KROČOVÁ, Š.; APELTAUER, L. *Souhrn způsobů hodnocení kvality a odolnosti infrastruktury: Závěrečná zpráva k veřejné zakázce Úřadu vlády ČR* [online]. 120 stran. Praha: Odbor pro udržitelný rozvoj, Úřad vlády České republiky, 2016 [cit. 2020-12-11]. ISBN 978-80-7440-186-2. Dostupné z URL: <https://www.vlada.cz/assets/ppov/udrzitelny-rozvoj/dokumenty/Infrastruktura--web-compressed.pdf>.

[7] *Roční zpráva o provozu 2006.* [online]. Energetický regulační úřad. Dostupné z URL: <http://www.eru.cz/documents/10540/462820/Rocni_zprava_provoz_ES_2006.pdf>.

[8] NOVAK, M.; KOPECKÝ, V.; ROCH, M.; BRACINÍK, P. *ELEKTROENERGETIKA* [online]. Žilina: Elektrotechnická fakulta Žilinskej univerzity vo vydavateľstve MARKAB spol. s r.o. [cit. 2021-01-18]. ISBN 978-80-89072-41-5. Dostupné z URL: <http://www.oze.stuba.sk/wp-content/themes/ObnovitelneZdrojeEnergie/elearning/EENERGETIKA/La-4.htm>

[9] PROCHÁZKA, R. *Venkovní vedení VVN (I)* Úvod do problematiky přenosové soustavy. Tzbinfo [online]. Topinfo s.r.o, 2007, 21. 5. 2007 [cit. 2021-01-18]. Dostupné z URL: <https://elektro.tzb-info.cz/teorie-elektrotechnika/4142-venkovni-vedeni-vvn-i>

[10] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů

[11] § 2 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

[12] § 2 písm. h) zákona č. 127/2005 Sb., ve znění pozdějších předpisů.

[13] Zákon č. 181/2014 Sb.,o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

[14] CASTALDINI, S.: Control system Pcs7 and M.I.S. together for the complete automation of the process in the sugar beet factory of Co.Pro.B. – Minerbio – Italy. In 17 th European Symposium on Computer Aided Process Engineering, 24, 2007, s. 841–846.

[15] BALDA, P. *Informační a řídicí systémy SCADA a HMI systémy* [online]. Plzeň: ZČU v Plzni, FAV, KKY, 2007, 24.4.2007 [cit. 2021-01-19]. Dostupné z URL: <`https://vendulka.zcu.cz/Download/Free/IRS1/IRS1-08_SCADA_HMI.pdf`>

[16] *Čo je HDO?* [online]. SSE a.s, 2020 [cit. 2020-12-11]. Dostupné z URL: <`https://www.sse.sk/co-je-hdo?page_id=9205`>

[17] PREdistribuce: Význam jednotlivých čísel kódu HDO [online]. Pražská energetika, 2008 [cit. 2021-01-19]. Dostupné z URL: <`https://web.archive.org/web/20110818055512/http://www.predistribuce.cz/distribuce/sluzby-a-ceny/sluzby/hdo/vyznam-cisel-kodu.html`>

[18] BURDA, K.; STRAŠIL I. *Zabezpečovací systémy.* 188 s., 2011 Fakulta elektrotechniky a komunikačních technologií VUT v Brně.

[19] BREEN, J. Vše o průmyslu: *Rozdíl mezi průmyslovým a kancelářským Ethernetem* [online]. 4.10.2020: Control Engineering, 2020 [cit. 2021-01-21]. Dostupné z URL: <`https://www.vseoprumyslu.cz/automatizace/site-a-komunikace/rozdil-mezi-prumyslovym-a-kancelarskym-ethernetem.html`>

[20] Bezpečnostná stratégia Slovenskej republiky, 2005.

[21] WALKOWSKI, Debbie. *What Is the CIA Triad?: Understanding the significance of the three foundational information security principles: confidentiality, integrity, and availability.* [online]. 9. júl 2019 [cit. 2021-5-25]. Dostupné z URL: <https://www.f5.com/labs/articles/education/what-is-the-cia-triad>

[22] Zákon č. 45/2011 Z.z. o kritickej infraštruktúre, príloha č. 3.

[23] Spyridon, S. a Coss, D. *The CIA strikes back: Redefining confidentiality, integrity and availability in security.* Journal of Information System Security, 10.3, 2014 [cit. 2021-01-21]. Dostupné z URL: <http://www.proso.com/dl/Samonas.pdf>

[24] WEIR, C. S., DOUGLAS, G., CARRUTHERS, M. a JACK, M. *User perceptions of security, convenience and usability for ebanking authentication tokens.* , Computers & Security, 2009 28, 1-2, pp. 47-62.

[25] FUSZNER, Mike. *Graphical Network Simulator* [online]. Tutorial (Verze 1.0). 48 s., 2011 [cit. 2020-12-11]. Dostupné z URL: <http://www.av.it.pt/salvador/LR/GNS3-0.5-tutorial.pdf>.

[26] DANIELSSON, M. ASHJAEI, M. BEHNAM, T. SORENSEN, M. SJODIN a T. NOLTE, *Performance evaluation of network convergence time measurement techniques.* 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2017, 7 s., doi: 10.1109/ETFA.2017.8247600.

[27] OSBORNE, E., SIMHA, A. *Traffic Engineering with MPLS.* Indianapolis: Cisco Press, 2003. ISBN 1-58705-031-5.

[28] SZARKOWICZ, K. a SÁNCHEZ-MONGE A. *MPLS in the SDN Era: Interoperable scenarios to make networks scale to new services.* Sebastopol: O'Reilly Media, 2016. ISBN 978-1-491-90545-6.

[29] DE GHEIN, L. *MPLS fundamentals: a comprehensive introduction to MPLS : theory and practice.* Indianapolis: Cisco Press, 2007. ISBN 15-870-5197-4.

[30] Cisco Software Central: Access everything you need to activate and manage your Cisco Smart Licenses [online]. Dostupné z URL: <https://software.cisco.com/#SmartLicensing-Alerts>.

[31] LOBO, L. a LAKSHMAN, U. *MPLS Configuration on Cisco IOS Software.* Indianapolis: Cisco Press, 2006 [cit. 2021-5-21]. ISBN 1-58705-199-0.

Zoznam symbolov, veličín a skratiek

AC	Attachment Circuit
ACL	Access Control List
AMI	Advanced Metering Infrastructure
ARP	Address Resolution Protocol
AWS	Amazon Web Services
BGP	Border Gateway Protocol
CBWFQ	Class-based Weighted Fair Queueing
CCTV	Closed-circuit Television
CE	Customer Edge
CIA	Confidentiality Integrity Availability
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DSCP	Differentiated Services Code Point
EXP	Experimental
FEC	Forwarding Equivalence Class
FTP	File Transfer Protocol
GB	Gigabyte
GE	Gigabit Ethernet
GNS3	Graphical Network Simulator 3
GUI	Graphical User Interface
HDLC	High-Level Data Link Control
HDO	Hromadné diaľkové ovládanie

HMI	Human-Machine Interface
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IOS	Internetworking Operating System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPv6	Internet Protocol version 6
IT	Information Technology
KEI	Kritická energetická infraštruktúra
KI	Kritická infraštruktúra
KII	Kritická informačná infraštruktúra
kV	Kilo Volt
KZL	Kombinované zemné lano
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
LDP	Label Distribution Protocol
LER	Label Edge Router
LFIB	Label Forwarding Information Base
LLQ	Low Latency Queuing
LSR	Label Switch Router
MB	Mega Byte

MP2MP	Multipoint-to-multipoint
MPLS	Multi Protocol Label Switching
TE	Traffic-Engineering
FRR	Fast ReRoute
mWh	megaWatt-hour
NB	Narrowband
NMS	Network Management System
NTP	Network Time Protocol
OS	Operating System
OSPF	Open Shortest Path First
P	Provider
PC	Personal Computer
PE	Provider Edge
PLC	Programmable Logic Controller
PnP	Plug and Play
PPP	Point-to-Point Protocol
PW	Pseudowire
QEMU	Quick EMUlator
QoS	Quality of Service
RAM	Random Access Memory
RD	Route Distinquisher
RDP	Remote Desktop Protocol
RR	Route-reflector
RT	Route Target
SaaS	Software as a Service

SCADA	Supervisory Control And Data Acquisition
SD-WAN	Software-defined Wide Area Network
SDN	Software-defined Networking
SLA	Service Level Agreement
SP	Service Provider
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time to live
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VFI	Virtual Forwarding Instance
VLAN	Virtual Local Area Network
VOIP	Voice over Internet Protocol
VPLS	Virtual Private LAN Services
VPNv4	Virtual Private Network version 4
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network
WiFi	Wireless Fidelity
ZTP	Zero Touch Provisioning