

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

PŘENOS MULTIMÉDIÍ V MPLS SÍTI

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

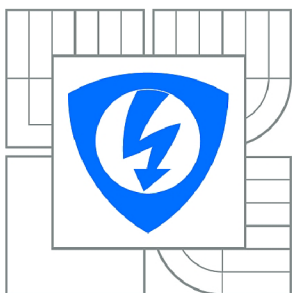
LUKÁŠ VLČEK

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



**FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNOLOGIÍ**

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

PŘENOS MULTIMÉDIÍ V MPLS SÍTI

MULTIMEDIA TRANSMISSION IN MPLS NETWORK

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

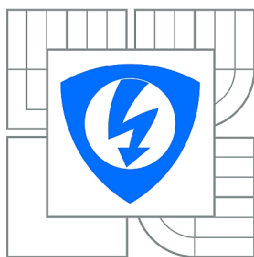
LUKÁŠ VLČEK

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. MICHAL POLÍVKA

BRNO 2011



VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Lukáš Vlček

ID: 120576

Ročník: 3

Akademický rok: 2010/2011

NÁZEV TÉMATU:

Přenos multimédií v MPLS síti

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou směrování provozu v IP/MPLS síti. Pojednejte o problematice směrování a řízení provozu na transportních sítích. Nakonfigurujte experimentální síť tvořenou cca 9 směrovači Cisco, doplněnou o zdroje audio, video, http a ftp provozu. Vytvořenou síť nakonfigurujte tak, aby různé typy provozu procházely různými trasami. Různé trasy budou představovat různou kvalitu transportní sítě.

DOPORUČENÁ LITERATURA:

- [1] Odom, WENDELL, Healy, RUS a Mehta, NAREN. Směrování a přepínání sítí - Autorizovaný výukový průvodce. Brno : Computer Press, a.s.; Cisco System, Inc., 2009. ISBN: 978-80-251-2520-5.
- [2] DOSTÁLEK, Libor, KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. 3. vyd. Praha: Computer Press, 2002. 542 s. ISBN 80-7226-675-6.
- [3] HICKS, Michael. Cisco - Optimalizace aplikací. Praha : Grada Publishing a.s., 2008. ISBN 978-80-247-1610-7.

Termín zadání: 7.2.2011

Termín odevzdání: 2.6.2011

Vedoucí práce: Ing. Michal Polívka

prof. Ing. Kamil Vrba, CSc.

Předseda oborové rady

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Práca uvádza prednostné črty MPLS technológie voči ostatným prenosovým WAN mechanizmom, poukazuje na jej výhody. V ďalšej časti práce je opísaný princíp smerovania a prepínania v MPLS s dôrazom na porovnávanie s IP sieťou. Nasledujúca sekcia práce sa zameriava na problematiku riadenie a smerovania premávky, jej metódy a praktiky. Naväzujúca časť opisuje možnosti riadenia premávky v MPLS. Posledná časť práce opisuje návrh, implementáciu a riadenie experimentálnej MPLS siete. Záver zhrňa dosiahnuté výsledky a vytyčuje finálne ciele k úplnému naplneniu zadania práce.

KLÚČOVÉ SLOVÁ

MPLS, Multiprotocol Label Switching, TE, riadenie premávky, MPLS-TE, PBR, smerovanie na základe pravidiel, RSVP-TE, OSPF-TE, CSPF, WAN networking, viac cestné

ABSTRACT

Thesis introduces positive traits of MPLS technology comparing to other transportation mechanisms in WAN environment, refers to its pros. The next section of thesis describes fundamentals of routing and switching in MPLS trying to make accent of different approaches between routing & switching in IP network and MPLS network. Following part focuses on topic about Traffic Engineering, its methods and practices. Another part of thesis is about Traffic Engineering in MPLS and its possibilities of controlling data flow. Last section describes planning, implementation and operation of experimental MPLS network. Conclusion summarizes achieved results and sets further goals to complete whole fulfillment of thesis assignment.

KEY WORDS

MPLS, Multiprotocol Label Switching, TE, Traffic Engineering, MPLS-TE, PBR, Policy Based Routing, RSVP-TE, OSPF-TE, CSPF, configuration, WAN networking, multiple path

VLČEK, L. *Přenos multimédií v MPLS síti*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011. XY s. Vedoucí bakalářské práce Ing. Michal Polívka.

Prehlásenie

Čestne prehlasujem, že svoju bakalársku prácu na tému „Přenos multimédií v MPLS síti“ som vypracoval samostatne pod vedením vedúceho semestrálnej práce a s použitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej semestrálnej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a som si plne vedomý následkov porušenia ustanovenia § 11 a následujúcich autorského zákona č. 121/2000 Sb., vrátane možných trestnoprávných dôsledkov vyplývajúcich z ustanovenia § 152 trestného zákona č. 140/1961 Sb.

V Brne dňa _____

 podpis autora

Pod'akovanie

Ďakujem vedúcemu práce Ing. Michalovi Polívkovi za užitočne metodické pokyny. Taktiež chcem pod'akovať Ing. Petrovi Palúchovi, PhD za veľmi cenné rady pri úvodnej analýze zadania.

V Brne dňa _____

podpis autora

OBSAH

Obsah	7
Zoznam obrázkov	9
Úvod	10
1. MPLS – Multiprotocol Label Switching.....	12
1.1. MPLS ako nasledovník vo WAN prostredí	12
1.1.1. Prednostné vlastnosti MPLS.....	13
1.2. Doména a jej prvky.....	16
1.2.1. Záhlavie MPLS.....	16
1.2.2. Typy LSR smerovačov	18
1.3. Smerovanie v MPLS sieti	19
1.3.1. Prechod paketu sieťou	19
1.3.2. Informačné bázy smerovača v IP sieti	21
1.3.3. Informačné bázy mechanizmu MPLS	23
1.3.4. Použitie informačných báz pri prepínaní paketu	24
1.3.5. Tvorba Label Switched Path	25
2. MPLS QoS	26
2.1. QoS všeobecne	26
2.2. Klasifikácia premávky	26
2.3. Triedy premávky a ich požiadavky	26
2.4. Zaistenie kvality služieb v MPLS	27
3. Smerovanie a riadenie premávky v transportných sieťach Traffic Engineering.....	28
3.1. Všeobecne	28
3.2. Traffic Engineering v transportných sieťach.....	29
3.3. Možnosti smerovania a prenosu.....	30
4. Traffic Engineering v MPLS.....	32
4.1. RSVP-TE	32
4.1.1. RSVP	32
4.1.2. Uplatnenie RSVP v MPLS-TE	33
4.2. OSPF-TE	34
5. Realizácia	36
5.1. Prípravná fáza.....	36
5.1.1. Výber varianty riešenia.....	36

5.1.2.	Návrh riešenia	36
5.1.3.	Postup realizácie	39
5.2.	Implementačné etapy	39
5.2.1.	Návrh a konfigurácia logickej štruktúry siete	39
5.2.2.	Návrh a konfigurácia IP adresovania siete	40
5.2.3.	Návrh a konfigurácia smerovacích domén	41
5.2.4.	Implementácia prepínacieho mechanizmu MPLS	43
5.2.5.	Implementácia VPN do MPLS	43
5.2.6.	Konfigurácia explicitných ciest (TE tunelov)	44
5.2.7.	Konfigurácia klasifikácie a značkovania premávky	45
5.2.8.	Konfigurácia smerovacej politiky	46
5.3.	Rozbor problému	46
5.4.	Výsledná podoba realizácie	47
5.5.	Zhrnutie	48
Záver	Záver	49
Literatúra	Literatúra	50
Zoznam použitých skratiek	Zoznam použitých skratiek	53
Prílohy:	Prílohy:	55

ZOZNAM OBRÁZKOV

Obr. 1: Full-Mesh topológia.....	14
Obr. 2: Hub-and-Spoke topológia	14
Obr. 3: Referenčný model ISO OSI a zaradenie MPLS vrstvy	16
Obr. 4: Umiestnenie MPLS hlavičky v rámci.....	17
Obr. 5: Záhlavie MPLS	17
Obr. 6: Použité smerovače.....	37
Obr. 7: Logické rozdelenie virtuálnych LAN.....	40
Obr. 8: Plán IP adresovania	41
Obr. 9: Smerovacie domény	42
Obr. 10: Tunely Traffic Engineeringu v MPLS doméne.....	45
Obr. 11: Load-balancing medzi LER	48

ÚVOD

Táto bakalárska práca na tému „Přenos multimédií v MPLS síti“ obsahom svojho zadania inklinuje k technológii MPLS a jej nadstavbu - Traffic Engineering v MPLS (taktiež označované ako MPLS-TE).

V úvodných stranách predstavuje technológiu MPLS, zaraďuje ju medzi ostatné prepínacie mechanizmy WAN sietí, porovnáva ju s nimi a poukazuje na jej prednostné a výhodné vlastnosti.

Ďašia časť práce skúma, ako vyplýva aj z jej zadania, samotnú technológiu MPLS, prvky jej domény, prepínacie mechanizmy a ich činnosť. Naväzuje na to kapitolou ohľadom smerovania paketov v MPLS, kde je dôraz kladený na porovnanie so smerovaním v tradičnej IP sieti. Sekciu uzatvára rozoberaním informačných báz, na ich základe je samotné smerovanie a prepínanie v MPLS vykonávané.

Druhá časť práce je venovaná QoS, kde pohľadom na zadané štyri typy premávky ich hodnotí z hľadiska požiadaviek na službu.

Treťou kapitolou teoretickej časti práca pojednáva všeobecne o téme smerovania a riadenia premávky v transportných sieťach, menuje a hodnotí metódy Traffic Engineeringu.

Nakoľko zadanie sa opiera primárne o MPLS, štvrtá teoretická sekcia je venovaná spôsobom, akými je možné riadiť a smerovať premávku v MPLS doméne.

Praktická časť bakalárskej práce si kladie za cieľ vytvoriť dostatočne veľkú MPLS doménu, na ktorej bude možné praktizovať Traffic Engineering, a tak dátové toky štyroch rôznych typov posielat' rôznymi trasami.

Práca a jej vypracovanie je orientované na Traffic Engineering, policy-based routing nad mechanizmom MPLS. Pokiaľ používa nástroje QoS, ako sú matchng, marking a rezervácia pásma, tak maximálne len v ich v základnom rozsahu, a to konkrétne pre nutné potreby Traffic Engineeringu. Rovnako zadané štyri druhy premávky sú chápané viac-menej ako štyri rovnaké dátové toky a práca si nekladie za cieľ v praktickej časti im vyslovene poskytnúť najlepšie zaobchádzanie s ohľadom na potrebnú kvalitu služieb, nakoľko práca a jej povaha je orientovaná primárne smerom k routingu a nie QoS.

Gró praktického riešenia zadania bude konfigurácia na experimentálnej sieti, kde sa implementuje smerovací protokol, samotný mechanizmus MPLS a jeho obdoba pre Traffic Engineering ako následná nadstavba pre pokročilé riadenie dátovej prevádzky v sieti.

Samotná téma praktického zadania je pomerne rozsiahla, obsahuje zúžitkovanie vedomostí na úrovni pokročilého smerovania (link-state smerovací

protokol, redistribúcia smerovacích tabuliek, smerovanie na základe pravidiel), základné QoS (značovanie, manažment šírky pásma). Ďalej zadanie témy vyžaduje kapitolu o MPLS, a najmä nadstavba Traffic Engineering ako jej kompletná podkapitola.

1. MPLS – MULTIPROTOCOL LABEL SWITCHING

1.1. MPLS ako nasledovník vo WAN prostredí

WAN siete majú v rámci svojho vývinu za sebou už niekoľko generácií technológií. Ako posledný míľnik bol komplex mechanizmov Asynchronou Transfer Mode (ATM). Veľké očakávania od (na danú dobu) pokrokovej technológie ATM pre nasadzovanie do moderných prenosových sietí sa žiaľ nenaplnili [1], i preto priemyselny trh začal hľadať alternatívne riešenia, poučený z ťažkopádneho úspechu ATM.

MPLS vzniklo postupným vývojom pokúsiť sa preklenúť obmedzenia doterajších prepínacích WAN mechanizmov, a to sú problematická škálovateľnosť a komplikovaná spravovateľnosť vo väčších sieťach, prípadne i Multicastové vysielanie. Táto technológia prepínania vo WAN prostredí sa stala štandardom IETF. Jej predchodcom bol proprietárny mechanizmus *tag switching* [2] firmy Cisco Systems, Inc. z ktorej MPLS priamo vychádza. Oba sa dajú označiť ako prepínanie mechanizmy v dátovej sieti pracujúce medzi druhou a treťou vrstvou referenčného modelu ISO OSI podľa pozície, kam sa MPLS hlavička umiestni.

MPLS stalo štandardom IETF začiatkom roku 2001 [3]. Od tohto dátumu prešla technológia markantným vývojom a bola rozšírená o mnohé nadstavby, ako Virtual Private Network (VPN), Quality of Service (QoS), Traffic Engineering (TE), označované ako MPLS VPN, MPLS QoS, resp. MPLS-TE.

1.1.1. PREDNOSTNÉ VLASTNOSTI MPLS

Technológia Multiprotocol Label Switching má v porovnaní s tradičnými technológiami WAN sietí množstvo výhod. Pod pojmom „tradičné technológie WAN sietí“ sa myslia tieto paketové siete prechádzajúce MPLS, a síce:

- X.25
- Frame Relay
- ATM

Tak isto bude porovnávaná s IP sieťou.

Dostupnosť

MPLS ponúka virtuálnu plnú priamu dostupnosť¹ medzi všetkými koncovými sieťami zákazníka. Obmedzením pri tradičných technológiách bola nutnosť si prenajímať privátne virtuálne okruhy (PVC), ich množstvo je dané Reedovým zákonom [4]:

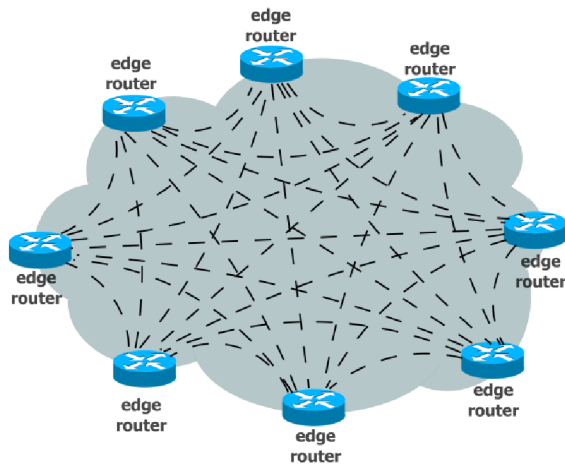
$$\text{okruhov} = \frac{N(N-1)}{2} \quad (1)$$

kde N je počet koncových sietí. Pre zabezpečovanie plnej priamej dostupnosti použitím tradičných technológií WAN sietí je nutné vytvárať Full-Mesh topológie z PVC. To však naráža na nasledujúci krok.

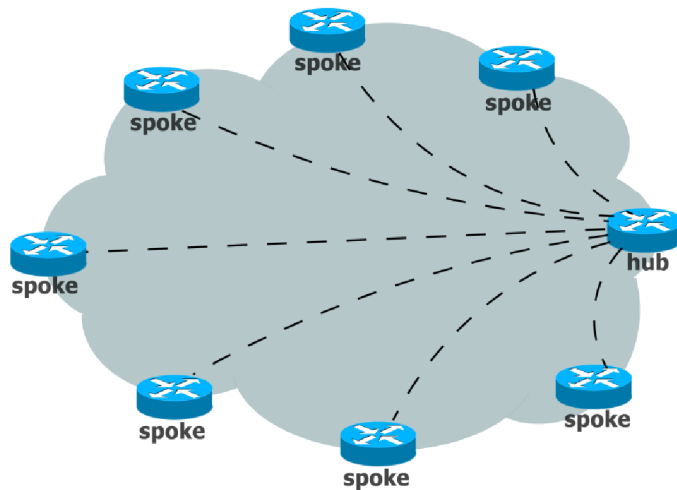
Škálovateľnosť

Jedným z hlavných obmedzení je škálovateľnosť – koncový zákazník bol nútený prenajímať si množstvo PVC za účelom dosiahnutia Full-Mesh topológie, a teda aj plnej priamej dostupnosti znázornené na Obr. 1: Full-Mesh topológia. S počtom potrebných PVC rástla úmerne aj cena, čo pri vyššom počte koncových sietí sa Full-Mesh prevedenie javilo ako nevhodné. Pre tieto prípady sa zavádzali iné topológie použitia, ako sú Partial-Mesh, či najekonomickejšia varianta Hub-and-Spoke (Obr. 2: Hub-and-Spoke topológia). Ich nasadenie má však isté úskalia z toho vyplývajúce, a síce nadbytočné preskoky pre premávku a od toho sa aj odvíjajúce rastúce oneskorenie dátového prenosu s nutným počtom preskokov.

¹ plná priama dostupnosť – dostupnosť, pri ktorej môžu komunikovať akékoľvek dve stanoviská skrz dátovú WAN sieť priamo, bez nutnosti použitia ďalších stanovísk ako medzi-preskokov na ceste dát; prepojenie „každý s každým“



Obr. 1: Full-Mesh topológia



Obr. 2: Hub-and-Spoke topológia

Taktiež škálovateľnosť pri dodržaní „každý-s-každým“ sťažuje počet vzťahov (adjacency) v smerovaní ako vnútri transportnej siete, tak i mimo nej².

Sieť MPLS sa škáluje jednoducho ako akákoľvek bežná IP sieť. Z toho vyplýva jednoduchosť rastu a rozvoja, ktorá mnohokrát bola obmedzujúca pri starších WAN technológiách. S tým priamo súvisí aj nasledujúca vlastnosť.

Jednoduchá spravovateľnosť

Jedná sa predovšetkým o náročnosť udržiavateľnosti a správy domény dátovej siete. Rozširovanie siete zákazníka o jednu ďalšiu koncovú sieť z hľadiska smerovania

² mimo nej - myslí sa tým smerovanie v rámci koncových sietí zákazníka

znamenal v praxi pridávať $N-1^3$ nových záznamov pre VC do infraštruktúry transportnej siete (kde N je počet pobočiek).

Multiprotokolovosť

MPLS bolo navrhnuté ako unifikujúca vrstva prenosu pre multi-protokolové nasadenie, preto nie je obmedzené len na prenos IP vrstvy, čo vyplýva aj z označenia „Multiprotocol“ v názve, no i schopné prenášať iné smerové protokoly sieťovej vrstvy, ako sú IPX, AppleTalk. Do úvahy pripadajú aj riešenia transportu protokolov nižšej - dátovej vrstvy „nad MPLS“, ako napríklad Ethernet, Frame Relay.

Rovnako MPLS technológia dokáže byť nasadená na rôzne už používané prenosové technológie nižších vrstiev, napríklad ATM obzvlášť [5], či Frame-Relay, čo uľahčuje nasaditeľnosť už do zabehnutého prostredia a umožňuje zjednocovanie sietí rôznych technológií, tak isto aj netradičné technológie, ako je rozvíjajúci sa Ethernet pre WAN nasadenia.

Privátnosť

Popri výhode škálovateľnosti IP siete dokáže MPLS sieť navyše zabezpečiť privátnosť pomocou VPN virtuálnych spojení vo vnútri domény, ktoré sú pre koncového zákazníka transparentné, čím sa značne líši od zdieľanej povahy IP siete a jej verejného prostredia.

Zaistenie kvality služieb

Metodódy QoS sú dnes neoddeliteľnou súčasťou moderných konvergovaných sietí. Sieť MPLS je schopná brať ohľad na prioritizovanú premávku rôzneho druhu a narábať s ňou adekvátnym spôsobom [6], čo sa vo verejnej IP sieti ťažko realizuje bez rozumnej klasifikácie jej pôvodu a typu, a to je pri „spoločných“ dátach na sieti problematické.

Riadenie premávky

Smerovanie premávky cez MPLS doménu môže závisieť na viacerých faktoroch, a to nielen na cieľovej IP adrese (ako je tomu v tradičných IP sieťach), ale napríklad aj na základe zdrojovej IP adresy, zohľadnenie premávky s ohľadom na QoS, prípadne iných parametroch. MPLS s rozšírením o ďalšie protokoly umožňuje aj nasadzovanie riadenia premávky - Traffic Engineering. Sú to metódy zabezpečujúce rozloženie záťaže za účelom lepšej dostupnosti služieb, schopné ošetriť havárie liniek použitím záložných ciest, možnosť explicitne nakonfigurovať trasu dátových tokov cez sieť, čo je obzvlášť vhodné pri údržbe a plánovaných odstávkach siete.

³ kde N je počet pobočiek, a teda koncových sietí zákazníka

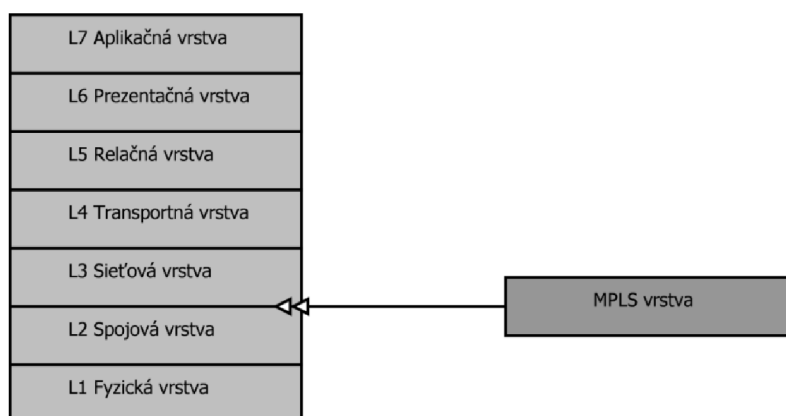
1.2. DOMÉNA A JEJ PRVKY

MPLS sieť (často nazývaná aj MPLS doména) obsahuje skupinu smerovačov pod správou jednej organizácie pracujúcej s technológiou Multiprotocol Label Switching. Ide o prepínací mechanizmus založený na prepínaní na základe značky (label) v záhlaví MPLS.

1.2.1. ZÁHLAVIE MPLS

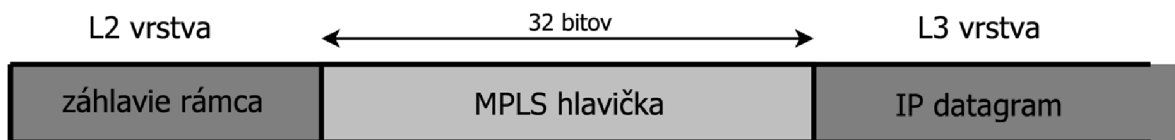
Paket (bežne IP datagram) vstupujúci do MPLS domény je na vstupnom smerovači vyšetrený, a pokiaľ vrstva riadenia rozhodne, že paket bude smerovaný skrz MPLS doménu, priradí sa mu MPLS záhlavie. Týmto záhlavím je paket označený počas celej doby svojho putovania až spravidla k okrajovému smerovaču domény, kde ju paket opúšťa a toto záhlavie je mu odobrané. Obsah MPLS záhlavia sa počas cesty doménou môže meniť.

Záhlavie je hierarchicky umiestnené medzi druhú a tretiu vrstvu referenčného modelu ISO OSI, čo sa niekedy v hovorovom slangu označuje ako dva-a-poltá vrstva. Tento fakt, pri ktorom MPLS zapúzdruje dáta tretej a vyššej vrstvy, určuje samotnú povahu multiprotokolovosti MPLS a umožňuje prenášať prakticky čokoľvek pomocou transportnej siete tohoto typu [5] [7]. Praktické využitie znázorňuje prístup AToM (Any Transport over MPLS).



Obr. 3: Referenčný model ISO OSI a zaradenie MPLS vrstvy

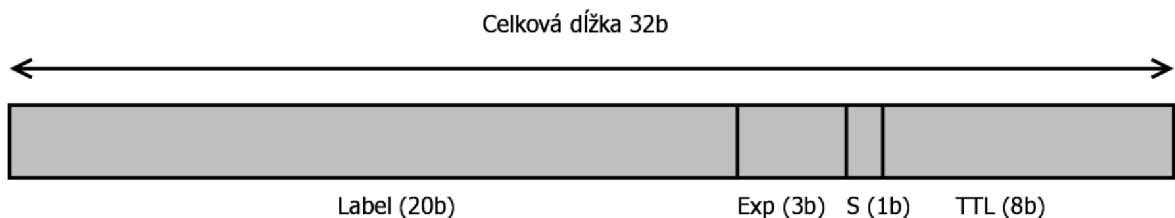
Štruktúra samotného MPLS záhlavia je veľmi jednoduchá, čo predurčuje mechanizmus k rýchlemu spracovávaniu a samotnému prepínaní. Má konštantnú dĺžku 32bitov (4bajty), čo je relatívne málo oproti záhlaviu napr. Ethernetového rámca DOPLNIT, či záhlaviu IPv4, alebo IPv6 datagramu [8]. Pre svoju nevelkosť a vkladanie medzi druhú a tretiu vrstvu sa niekedy slangovo označuje ako tzv. Shim-header.



Obr. 4: Umiestnenie MPLS hlavičky v rámci

Obsahuje štyri polia:

- Značka (label)
- Experimentálne pole (exp)
- Príznak „dna zásobníka“ (Bottom-of-the-stack)
- Time to live



Obr. 5: Záhlavie MPLS

Label (20b)

Prvých 20 bitov MPLS záhlavia plní funkciu smerovej značky, ktorá sa používa pri prepínaní paketu medzi LSR smerovačmi počas cesty MPLS doménou. Spravidla sa mení každým preskokom v závislosti od požadovanej destinácie.

Samotná priradovaná label v hlavičke MPLS môže korešpondovať s cieľovým prefixom adresy, jednoznačne identifikovať VPN koncového zákazníka, označovať QoS triedu s patričným zachádzaním a pod.

Experimental (3b)

Trojbitové pole bolo pôvodne rezervované na experimentálne účely, dnes sa však našlo uplatnenie v praxi pre nasadenie mechanizmu zaistenia kvality služieb QoS v technológií MPLS.

Bottom-of-the-Stack (1b)

MPLS architektúra umožňuje zo svojej špecifikácie transportujúcemu paketu priradiť a nieť viac než jedno záhlavie. Záhlavia MPLS sú pred paket vkladané princípom zásobník, to znamená, že sa pridávajú a odoberajú spôsobom Last-in-First-out (LIFO). Z teoretického hľadiska môže paket nieť v doméne neobmedzené množstvo záhlaví, a teda ľubovoľnú úroveň zanorenia, no z praktického je táto možnosť obmedzená

vlastnosťou Maximal Transfer Unit (MTU), ktorá sa priamo viaže k používaným technológiám nižších vrstiev. Nakoľko sa úroveň zariadenia vôbec nečísluje, je potrebné aspoň minimálne odlišiť prvú úroveň od ostatných. K tomuto účelu je práve vyhradený jednobitový príznak „dna zásobníka“ (Bottom-of-the-Stack) v záhlaví MPLS. Jeho hodnota je nastavená na úroveň logickej 1 vtedy, keď sa jedná o záhlavie prvej úrovne, tzn. bezprostredne za záhlavím sa nachádzajú dáta prenášanej tretej vrstvy referenčného modelu. Logickú hodnotu 0 nadobúdajú záhlavia druhej a vyšších úrovní.

Hierarchická schopnosť značkovania má univerzálne použitie a rozširuje možnosti MPLS. Táto metóda môže byť použitá ako nástroj, ktorý umožňuje vysokú flexibilitu a škálovateľnosť v zjednocovaní menších MPLS domén do väčších celkov. Taktiež sa používa pre potreby VPN v MPLS, či iné.

Time-to-Live (8b)

Podobne ako v záhlaví IP paketu, tak aj v MPLS záhlaví slúži toto osembitové pole ako bezpečnostný mechanizmus proti smerovacím/prepínacím slučkám v rámci MPLS domény. Na začiatku domény sa po dekrementovaní políčka TTL v IP záhlaví (nakoľko sa jedná o bežnú súčasť IP smerovania) nakopíruje jeho hodnota do ôsmich bitov MPLS záhlavia, a ďalej je táto hodnota počas prepínania na každom preskoku dekrementovaná o jedno. Pri výstupe sa podľa ďalšieho nastavenia siete buď nakopíruje finálna hodnota TTL z MPLS do TTL IP hlavičky, alebo sa hodnota IP hlavičky (po dekrementovaní na prvom smerovači) nezmení [7]. Tento princíp použitý pri druhej variante umožňuje transportnej sieti tváriť sa z pohľadu koncového zákazníka ako jeden preskok, a tak poskytujúc ochranu nemožnosťou trasovať MPLS sieť dátového poskytovateľa, a teda zistiť jej topológiu.

1.2.2. TYPY LSR SMEROVAČOV

Smerovač ako entita používajúca MPLS prepínací mechanizmus, z ktorých sa doména skladá, je taktiež označovaný *Label Switch Router* (LSR). Ten sa ďalej rozlišuje podľa toho, v akej pozícii sa v MPLS doméne nachádza.

Hraničný smerovač (edge)

Niekedy nazývaný aj *Label Edge Router* (LER). Smerovač sa stáva hraničným smerovačom, pokiaľ má aspoň jedného suseda nespádajúceho do MPLS domény, a smerujúceho na báze (spravidla) IP protokolu (v prípade IP siete), typicky sa nachádzajúci na okraji domény.

Smerovač jadra (core)

Smerovače jadra sa nachádzajú vnútri domény na ceste medzi hraničnými smerovačmi. Pracujú výhradne s označenými paketmi⁴, ktoré na základe hodnoty label v záhlaví prepínajú skrz MPLS doménu k výstupnému okrajovému smerovaču.

Hraničné smerovače LER v topológií s ohľadom na smer dátového prúdenia sa rozdeľujú na:

- vstupný smerovač (ingress)
- výstupný smerovač (egress)

Vstupný hraničný smerovač

Úlohou vstupného smerovača je zväziť, či prichodzí paket bude prenesený MPLS sieťou a teda vstúpi do domény, alebo nie. Ak áno, tak mu priradí podľa potreby minimálne jedno MPLS záhlavie s patričnou hodnotou značky a odošle sa výstupným rozhraním k nasledujúcemu preskoku v ceste.

Výstupný hraničný smerovač

Hraničný smerovač na výstupe z domény odstráni zostávajúce záhlavia a vyšle výstupným rozhraním už bežný IP datagram smerom k nasledujúcemu preskoku v IP sieti.

1.3. SMEROVANIE V MPLS SIETI

1.3.1. PRECHOD PAKETU SIEŤOU

Prechod paketu MPLS sieťou sa líši od tradičného smerovania v sieti IP. Smerovanie v IP sieti prebieha na každom skoku, teda smerujúcim zariadením (tretej L3) sieťovej vrstvy. Paket je skok čo skok vyšetovaný o cieľovú IP adresu, ktorá sa však bežne zostáva do cieľa nezmenená, a typicky pomocou zhody najdlhšieho prefixu medzi záznamami v smerovacej tabuľke a cieľovej IP adresy z IP záhlavia paketu je určené ďalšie smerovanie. Každý smerovač o smerovaní paketu rozhoduje nezávisle na základe svojej smerovacej tabuľky, čo môže pri nekonzistentnom nastavení smerovania na trase viesť k stavom, keď cieľová sieť bude nedosiadnuteľná, k smerovacím slučkám, či mylným informáciám ohľadom smerovania a adresovania sietí.

⁴ označené pakety – v kontexte MPLS sa tým myslia pakety vyššej vrstvy nesúce aspoň jedno MPLS záhlavie

Pri transporte paketu cez MPLS doménu sa rozhodovanie ohľadom trasy učiní len raz. Keď vstupný LER uváži, že prichodzí paket sa prenesie cez MPLS sieť, ingress LER paket prešetrí, zaradí si ho do vhodnej *Forward Equivalent Class* (FEC), na jeho základe mu prideli (akcia PUSH) MPLS záhlavie (v špeciálnych prípadoch viac než jedno) s hodnotou značky odpovedajúcej pre danú FEC. Takto zaopatrený paket pošle výstupným rozhraním smerom k ďalšiemu LSR smerovaču v ceste (typicky je to typ core). Ten ho spracováva na základe hodnoty značky v MPLS hlavičke prichodzieho paketu, typicky vymení (akcia SWAP) záhlavie s inou značkou a pošle výstupným rozhraním paket ďalšiemu LSR v ceste, kde sa proces z pohľadu ďalšieho smerovača zopakuje.

Počas putovania sieťou môže byť label ponechaná, vymenená, pridaná ďalšia úroveň hlavičky, či aj odobraná (akcia POP). V prípade ďalšej úrovne značky sa ďalšia hlavička MPLS s vlastným políčkom label umiestni „nad“ hlavičku predchádzajúcej úrovne zásobníkovým spôsobom.

Až paket nakoniec dorazí na egress LER, odstránia sa (akcia POP) všetky MPLS záhlavia (ak zostali nejaké), ďalej je paket smerovaný už tradične podľa IP adresy. Sú prípady, kedy sa táto činnosť odstraňovania vykonáva už jeden skok pred výstupným LER. Výhodou je rozloženie záťaže na dva smerovače, kde predposledný odstraňuje záhlavia a posledný uskutočňuje IP smerovanie, ktoré inak obe bežne vykonáva sám egress LER. Táto metóda sa nazýva *Penultimate Hop-Popping* [7].

Počas prechodu doménou žiaden zo smerovačov jadra nesiahajú za MPLS záhlavie do polí vyšších vrstiev za akýmkoľvek účelom, nebolo potrebné opakovane zisťovať cieľovú adresu počas priebehu prepínania. Z tohoto taktiež vypýva, že pokiaľ sa má na paket označený MPLS záhlavím uplatňovať zachádzanie podľa QoS, musí byť tento fakt, a teda príznak dostupný, čiže uvedený už v záhlaví MPLS.

Forward Equivalent Class

V jednej triede FEC sa nachádzajú všetky pakety, ktoré požadujú rovnaký spôsob zaobchádzania počas prepínania v doméne a spájajú ich spoločné vlastnosti i nároky.

V základnom poňatí môžeme pre názornosť nasledujúceho príkladu do rovnakej FEC považovať a radiť pakety s rovnakým cieľovým prefixom IP adresy, trebárs 10.1.2.0/24 . Keď sa paket má dostať do tohoto cieľa, ingress LER použije patričnú hodnotu značky v pridávanom MPLS záhlaví, následne odosielať paket patričným smerom výstupným rozhraním (čím dodržiava danú FEC). Na základe hodnoty značky v záhlaví je paket prepínaný po vopred vytvorenej *Label Switched Path* (LSP). Samotná LSP sa dá považovať ako ekvivalent virtuálneho okruhu VC v ATM sieti.

Keď sa na rovnaký ingress LER dostaví paket smerujúci do iného prefixu, a teda vyžadujúci inú FEC - čiže iné zachádzanie, ingress LER ho zaopatrí inou hodnotou značky v pridanom MPLS záhlaví a odošle iným, eventuelne aj rovnakým smerom, avšak pre danú značku (vzhľadom k odlišnej FEC) bude následne uplatňovaný iný prístup počas prepínania, i keď eventuelne aj rovnaká LSP.

Pakety zdieľajú rovnakú FEC v prípade, keď sú prieposielané:

- do rovnakého cieľa
- tou istou cestou
- s rovnakými požiadavkami a prístupom, s ohľadom na QoS počas prepínania

Hoci je v praxi FEC často typicky spájaná s cieľovou adresou, je všeobecnejšia než len adresa príjemcu spadajúca do rovnakého cieľového prefixu. Môže byť podmienená taktiež zdrojom paketov, alebo hodnotou poľa DSCP, ktoré môžu spôsobiť vytvorenie odlišnej FEC, a teda aj následne zaobchádzania.

Čo sa týka analógie FEC s IP sieťou, tam sa taktiež koná proces ohľadom FEC, a síce prešetruje sa na každom preskoku cieľová IP adresa zo záhlavia IP datagramu. Na základe tejto informácie (prípadne aj ďalších možných faktorov, ako je DSCP pole zo záhlavia, či iné) sa prehľadá smerovacia tabuľka a z nej sa istia informácie o ďalšom prepínaní paketu. V tomto okamihu už pozná smerovač FEC pre daný paket – vie IP adresu ďalšieho preskoku, vie výstupné rozhranie, vie ako s ním zachádzať v zaradovaní do fronty. Pakety, ktoré zdieľajú tieto tri informácie, sa považujú za rovnakú FEC.

Zásadný rozdiel medzi IP sieťou a MPLS sieťou vzhľadom na FEC je, že FEC sa v IP sieti zisťuje na každom preskoku, v MPLS sieti len raz – a to na začiatku LSP.

1.3.2. INFORMAČNÉ BÁZY SMEROVAČA V IP SIETI

Aby paket mohol byť korektne smerovaný a prepínaný IP sieťou, je k tejto činnosti potrebné urobiť rozhodnutie o voľbe toho správneho smeru. Pod pojmom „voľba správneho smeru“ sa v IP sieti rozumie voľba takej trasy z pohľadu rozhodujúceho sa smerovača, ktorá sa relatívne k rozhodujúcemu sa smerovaču javí ako najvhodnejšia, čo v IP sieti znamená cesta najlacnejšia, s najnižšou cenou do cieľa (cost). Aby sa smerovač pracujúci so smerovým protokolom IP vedel rozhodnúť pre správny smer, ktorý sa bude pre jeho subjektívny pohľad javiť ako najvýhodnejší, musí mať znalosti o okolitej topológii a jej adresovaní v jeho tzv. „širšom okolí“.

Pod pojmom „širšie okolie“ sa rozumejú siete, do ktorých smerovač nie je priamo pripojený svojimi rozhraniami, ale eventuálne sa do nich vie dostať cez ďalší

preskok (typicky cez ďalší smerovač, či reťazec smerovačov). Siete, ktoré sú priamo pripojené, sú považované za „bližšie okolie“ a smerovač vie o nich automaticky, pretože má v nich zapojené svoje rozhrania, pokiaľ majú správne nastavenú fyzickú, linkovú a sieťovú vrstvu.

Informácie o všetkých cieľových sieťach a smeroch smerovač získava jednak z vlastných rozhraní pre priamo pripojené siete v „blízkom okolí“, tak aj pomocou smerovania pre „širšie okolie“, ku ktorému smerovač nemá priamy prístup. Toto smerovanie môže byť statické a teda z jednotlivých smerovacích záznamov zadaných manuálne administrátorom, alebo dynamické - z výmeny informácií smerovacími protokolmi, ako sú napr. RIP, OSPF, IS-IS, BGP. Všetky tieto informácie o nadobudnutých smeroch vrátane preskokov k nim, si smerovač ukladá do svojej *Router Information Base* (RIB).

Routing Information Base (RIB)

RIB je dátová štruktúra, do ktorej smerovač zhromažďuje zo všetkých nadobudnutých smerovacích informácií spôsobom vyššie uvedeným, tie s najlepšou cenou do daných prefixov pre jednotlivé smerovacie protokoly či ostatné spôsoby (statický záznam, resp. priamo pripojená sieť). Obsahuje dôležité údaje ako sú prefix cieľovej siete, cena (cost) cesty, nasledujúci preskok (IP adresa smerovača alebo výstupné rozhranie), a spôsob, odkiaľ bola táto informácia získaná (napr. konkrétny smerovací protokol, či statický záznam). Týmto pričínením obsahuje RIB to najlepšie (teda najvýhodnejšie cesty s najnižšou cost) napr. z RIPu, z OSPF, zo statického smerovania pre dané prefixy cieľových sietí. Z týchto informácií smerovač zostaví smerovaciu tabuľku s ohľadom na čo najnižšiu administratívnu vzdialenosť, ktorá reprezentuje „dôveryhodnosť“ smerovacieho protokolu. Smerovacia tabuľka je menšia a kompaktnjšia, a používa sa na smerovanie IP datagramov s dôrazom na čo s najdlhšiu zhodu v prefixe voči cieľovej IP adrese zo záhlavia paketu.

Smerovanie podľa smerovacej tabuľky máva však aj svoje rýchlostné úskalia. Tými je napríklad dvojitý prechod záznamami v smerovacej tabuľke, kde sa pri prvom prechode hľadá IP adresa nasledujúceho preskoku, a v druhom prechode hľadá sa výstupné rozhranie do priamo pripojenej siete, ktorá tento preskok obsahuje. Taktiež na rýchlosti nepridáva opakované prehľadávanie ARP tabuľky s cieľom zistiť fyzickú adresu ďalšieho preskoku, pokiaľ sa nachádza na zdieľanom médiu, ako je ethernet a je potrebné pripojené zariadenia na druhej vrstve odlišovať a náležite adresovať. Firma Cisco Systems, Inc. s cieľom znížiť dobu potrebnú na smerovanie paketu a zvýšiť smerovací výkon vyvinula technológiu *Cisco Express Forwarding* (CEF) [5]. Táto technológia používa k smerovaniu svoju vlastnú dátovú štruktúru zvanú *Forwarding Information Base* (FIB).

Forwarding Information Base (FIB)

Táto informačná báza obsahuje koncentrované informácie z tabuliek RIB a ARP. Jej výhodou je jej kompaktnosť a úplnosť s ohľadom na smerovacie informácie potrebné k prepínaniu paketu. Obsahuje konkrétny prefix cieľovej adresy, identifikátor výstupného rozhrania a informácie ohľadom ďalšieho preskoku v ceste (ako sú napríklad jeho IP a fyzická adresa). Týmto pričinením je smerovač schopný jediným prehladaním tabuľky FIB získať všetky potrebné informácie, ktoré použije pri konštrukcii spracovávaného paketu a jeho odoslania.

1.3.3. INFORMAČNÉ BÁZY MECHANIZMU MPLS

Pri rozšírení smerovacích schopností smerovača o mechanizmus MPLS, smerovač získava dve nové dátové štruktúry, ktoré sa slúžia na prácu s paketmi nesúcimi MPLS záhlavie.

Label Information Base (LIB)

Tabuľka, ktorá má prehľad o všetkých známych prefixoch⁵ a väzbách k značkám, ktoré ponúkli príhlé LSR, tak ako aj samotný smerovač sa nazýva *Label Information Base* (LIB). Jej úlohou je zhromažďovať a udržiavať informácie párovania prefixu voči značke, ktoré boli oznámené protokolom distribúcie značiek od príhlých smerovačov MPLS, tak vlastnú značku k danému prefixu, ktorú smerovač oznamuje príhlým LSR. Ako bolo uvedené, táto dátová štruktúra obsahuje všetky zozbierané informácie ohľadom párovania prefix – značka, a podieľa sa na tvorbe tabuľky Label Forwarding Information Base (LFIB),

Label Forwarding Information Base (LFIB)

Jedná sa o tabuľku, ktorá v podstate je ekvivalentná voči FIB. Táto tabuľka je optimalizovaná pre prepínanie paketov nesúcich MPLS záhlavie na základe hodnoty značky v záhlaví prichádzieho MPLS paketu. Obsahuje informácie ako je značka z prichádzieho paketu, uskutočňovaná akcia, výstupné rozhranie a informácia o nasledujúcom preskoku LSR. Túto tabuľku využívajú všetky smerovače MPLS domény.

Pre úplnosť je nutné uviesť, že po nasadení MPLS prepínania na smerovač sa rozšíri jeho štruktúra RIB o ďalší atribút, a síce príznak pre MPLS, kde sa uvedie spravidla akcia PUSH a značka, s ktorou bude paket označený pri samotnom odosielaní. V prípade, že sa tento prípad naskytne (je uvedená akcia PUSH s hodnotou

⁵ Slová „prefix“ či „cieľová podsieť“ označujú vo voľnejšom ponímaní „FEC“, a sú tomto rozsahu kontextu voľne navzájom zameniteľné, pokiaľ sa jedná o párovanie značka=FEC

značky) pri zázname daného prefixu, jedná sa tu o MPLS prepínanie, kde sa tento smerovač stáva v tomto okamihu ingress LER a paket vstupuje do domény. Ide o začiatok tzv. *Label Switched Path* (LSP).

1.3.4. POUŽITIE INFORMAČNÝCH BÁZ PRI PREPÍNANÍ PAKETU

V prípade MPLS sa prepína na základe zhody Label značky a nehľadá sa na každom preskoku čo najdlhší prefix ako pri smerovaní v IP sieti. Úvodná značka v hlavičke MPLS sa vyberie už na začiatku v Ingress LER. Značka sa volí s ohľadom na FEC. Štandardne je to na základe cieľovej adresy, ktorá sa získa z IP hlavičky, avšak ako bolo uvedené – nemusí byť FEC obmedzená len na cieľovú adresu.

Pre prípad, že značka sa bude priradovať na základe cieľovej adresy, vstupný hraničný smerovač prehľadá svoju databázu FIB, nájde v nej záznam so zhodou pre čo najdlhší prefix. Na základe informácií uvedených v tomto zázname uskutoční akciu PUSH, čím priradí paketu MPLS hlavičku s danou hodnotou značky. Takto označený paket enkapsuluje s ohľadom na spojovú vrstvu, kam uvedie prípadne fyzickú adresu zo záznamu FIB nasledujúceho preskoku, a následne vyexpeduje rámec výstupným rozhraním taktiež uvedenom v zázname v tabuľke FIB.

Paket prichádza na smerovač jadra. Nakoľko core LSR pracujú výhradne s paketmi obsahujúcimi MPLS záhlavie, na ich prepínanie sa použije databáza LFIB. Prichodzí paket smerovač vyšetrí a zistí hodnotu značky (label) zo záhlavia. Na základe tejto hodnoty vyhľadá záznam so zhodou v tabuľke LFIB pre atribút „lokálna značka“. Je to povaha značky, ktorú vytvoril tento konkrétny smerovač jadra pre daný cieľový prefix a oznámil ostatným príslušným smerovačom. Z tohoto záznamu vyčíta dôležité parametre ako sú vykonaná akcia a výstupná hodnota značky. V roli smerovača jadra je typickou akciou SWAP, ktorá zamieňa záhlavie MPLS s pôvodnou hodnotou značky za záhlavie s hodnotou pre výstup. Následne použije ostatné dáta zo záznamu pre vyexpedovanie paketu tak ako predchádzajúci LSR, čím predáva paket ďalšiemu smerovaču v ceste, kde sa proces spracovania opakuje.

Až takýmto spôsobom dorazí paket na výstupný smerovač domény, uskutoční sa rovnaký začiatok procedúry, až po vyhľadávanie v tabuľke LFIB. Tam nájde egress LER v zázname položku s akciou POP. To znamená, že smerovač odstráni MPLS záhlavie. Pokiaľ je to záhlavie prvej úrovne, čo smerovač zistí pri odstraňovaní podľa príznaku S bitu v záhlavi nastaveného na 1, paket v tomto mieste cestu v doméne končí. Smerovač po odstránení MPLS záhlavia preskúma IP hlavičku a podľa cieľovej IP adresy určí, kadiaľ sa bude paket smerovať. To konkrétne zistí prehľadaním svojej FIB tabuľky a paket vyexpeduje.

Sumárne sa dá zhrnúť, že na prepínanie transportovaných paketov používajú okrajové smerovače FIB databázu, zatiaľ čo LFIB tabuľku všetky. Paket na začiatku

dostane záhlavie, je prepínaný sústavou smerovačov na základe meniacej sa značky, čím kopíruje LSP medzi okrajovými LER spojenú smerovačmi jadra.

1.3.5. TVORBA LABEL SWITCHED PATH

Keď sa hraničný smerovač MPLS domény získa informáciu (spravidla zo smerovacieho protokolu) o novom smerovateľnom prefixe, prideli mu (vytvorí pár) tzv. lokálnu značku (lebo bola vytvorená lokálne) a rozošle protokolom distribúcie značiek tento fakt príľahlým LSR smerovačom oznamujúc prefix a hodnotu značky. Príľahlý smerovač túto správu protokolu distribúcie značiek akceptuje a uloží si do svojej LIB, eventuálne i LFIB informáciu o prefixe, vzdialenej značke a rozhraní, na ktorom túto správu prijal – použije ho ako výstupné rozhranie. Sám smerovač novooznámenému prefixu vytvorí vlastnú značku lokálnej povahy, ktorú použije k nemu ako pár a pomocou protokolu distribúcie značiek túto skutočnosť oznámi svojim susedom. Šírenie týchto značiek je smerom Downstream -> Upstream, kde Downstream je smerovač ten bližšie k cieľovému prefixu, od ktorého sa správa o cieľovom prefixe typicky šíri.

Na distribúciu značiek sa používajú *Label Distribution Protocol* (LDP), alebo *Tag Distribution Protocol* (TDP). Šírenie značiek od výstupného smerovača k vstupnému pomocou LDP, resp. TDP a náväznosť značiek v sieti vytvára spojitú LSP.

2. MPLS QoS

2.1. QoS VŠEOBECNE

Z pohľadu moderných konvergovaných sietí, keď je snahou integrovať všetky služby sietí do jednej zjednotenej siete, je mechanizmus QoS nevyhnutnou súčasťou moderných konvergovaných sietí.

Rastúce požiadavky na moderné konvergované dátové siete, ktoré na rozdiel od legacy dátových sietí prenášajú okrem typických dát aj ostatné typy premávky reprezentované službami, ako je hlas, či videostream v reálnom čase. Tradičná dátová sieť bola určená výhradne pre prenos dát, kde určujúcim parametrom siete bola jej šírka pásma. Tento prístup však pri nasadzovaní nových služieb do siete ako sú hlas, video a iné interaktívne služby citlivé na odozvu a bezchybový prenos nebol dostatočný. Preto bolo potrebné zabezpečiť daným službám adekvátnu kvalitu počas doručovania. Na to, aby s nimi bolo možné odlišne zachádzať, bolo nutné jednotlivé typy premávky dát rozlišovať. V QoS sa na to používajú mechanizmy inšpekcie a klasifikácie paketov.

2.2. KLASIFIKÁCIA PREMÁVKY

Prakticky sa to rieši, že najskôr sa príchodnému paketu preskúmajú vyššie vrstvy hlĺbkovou inšpekciou a na základe ich obsahu sa paketu v IP záhlaví nastaví do príslušného poľa príznak [7]. Takto označený paket sa stáva klasifikovaným. To znamená, že pri prechode sieťou bude naň pri smerovaní braný ohľad podľa prednastavených pravidiel.

2.3. TRIEDY PREMÁVKY A ICH POŽIADAVKY

Hlas

Jeho charakteristikou nepatrný dátový tok v závislosti od použitého audio kodeku. Na druhú stranu jeho najvyššia citlivosť pre oneskorenie (delay) a kolísanie oneskorenia (jitter). Tieto parametre spojenia majú priamy dopad na kvalitu telefonického hovoru pre telefonujúceho. Tento typ dátovej premávky by mal byť na smerovači expedovaný prioritne [8].

Video

Video-streaming je ďalšou real-time službou, ktorá spolieha na nízke oneskorenie. Avšak vzhľadom k bufferovaniu nie je natoľko citlivá na menej významné kolísanie jitter-u. Dátový tok sa líši najmä od použitého video-kodeku a prenášanej kvality videa.

HTTP

Interaktívne web-aplikácie sa zvyčajne vyznačujú premávkou nárazovitého typu rôznych objemov. Z hľadiska interakujúceho koncového užívateľa sa očakáva odozva v rozumnom čase. Taktiež sa modernej internetovej dobe používa na presnos súborov i väčších objemov, dôkazom sú toho mnohé veľké filehostingové služby webových rôznych portálov na internete.

FTP

Tento typ dátového prúdu je nenáročný na latenciu či jitter, avšak generuje najväčšie objemy dát a preto vyžaduje pre prenos najväčšiu šírku pásma. V prípade nenasadených QoS mechanizmov na sieti má tendenciu svojou mohutnosťou zmonopolizovať väčšinu zo šírky dostupného pásma a tak degradovať kvalitu ostatných delay-citlivých služieb na sieti.

2.4. ZAISTENIE KVALITY SLUŽIEB V MPLS

Keďže prepínacie mechanizmy smerovačov v jadre MPLS (core LSR smerovače) siete nepristupujú vôbec do IP záhlavia, bolo potrebné toto označenie preniesť do MPLS hlavičky. K tomuto účelu sa použili 3 bity označované ako EXP [6][7] umožňujúce odlíšiť tak 8 rôznych klasifikovaných tried premávky, a teda osem rôznych prístupov prepínaniu takto označenej premávky. Tie následne môžu byť aplikované na paket po celej dĺžke trasy LSP počas prenášania MPLS doménou a tak prispieť k zaisteniu kvality služieb v transportnej sieti.

3. SMEROVANIE A RIADENIE PREMÁVKY V TRANSPORTNÝCH SIEŤACH TRAFFIC ENGINEERING

3.1. VŠEOBECNE

Výkonosť siete a jej schopnosť efektívne prenášať premávku je záležitosťou dvoch navzájom príbuzných činností, nimi sú plánovanie kapacity siete a riadenie premávky v sieti.

Zatiaľ čo plánovanie kapacity siete je z časového hľadiska dlhodobou záležitosťou, ktorá poukazuje na budúcnosť siete, vývoj jej topológie a optimalizáciu infraštruktúry, počíta s predpokladanými trendmi nárastu dopytu po službách, čo následne vyžaduje navyšovanie kapacity liniek a nasadzovanie nových technológií, riadenie premávky v sieti má inú povahu.

Pre riadenie premávky z časového hľadiska ide o pohľad na výkonnosť siete omnoho krátkodobejší. Je to pohľad na situáciu, ktorá odzrkadľuje aktuálnosť a jej blízku budúcnosť [11]. Je to činnosť, ktorá pružne reaguje na vzniknuté udalosti plánované, tak aj náhle neočakávané so snahou zabezpečiť a dodržať výkonnosť siete a s orientáciu na kvalitu poskytovanej služby.

Traffic Engineering (TE), v preklade riadenie premávky. Je to pojem, ktorý vychádza ešte z čias telekomunikačnej techniky, avšak jeho prístup pre širokopásmové siete je principiálne iný [8]. Myšlienka TE poníma manipuláciu dátových tokov v prenosovej sieti za účelom ich riadenia kvantity a smeru podľa vyžadovanej situácie, majú dopad na premávku v sieti, jej výkon a kvalitu poskytovaných služieb.

V konkrétnom ponímaní je TE súborom nástrojov a metód, ktorými dokáže poskytovateľ dátových služieb spolu v kombinácii s mechanizmami na zaistenie kvality služieb riadiť dátovú premávku, menovite ju:

- diferencovať – rozlišovať aplikácie vyšších vrstiev a zaobchádzanie s nimi,
- prioritizovať – uprednostňovať real-time prevádzku pred best-effort,
- tvarovať – regulovať kvantitu toku, čím predchádzať zahlteniu liniek,
- rozdeľovať – jeden mohutný dátový tok na viaceré menšie,
- smerovať – dátové toky explicitne skrz transportnú sieť,
- agregovať – združovať prístupové siete pred napojením sa na chrbticu,

a nimi riadiť celkový výkon transportnej siete, umožňujúc mu jej lepšiu spravovateľnosť majú dopad na všeobecnú kvalitu poskytovaných služieb.

Metódami vyššie uvedenými a ich kombináciou je schopný dátový poskytovateľ dosiahnuť ciele ako sú rozkladanie záťaže na sieti, odolnosť proti zahlteniu pri nárazových dátových tokoch, zaistenie kvality služby podľa povahy protokolov aplikačnej vrstvy, zaistenie dostupnosti služieb pri plánovaných údržbách siete či rôznych havarijných scenároch, a iné.

3.2. TRAFFIC ENGINEERING V TRANSPORTNÝCH SIEŤACH

Nakoľko sa použité technológie fyzických a linkových vrstiev od seba líšia (a oficiálne zadanie poukazuje na MPLS), a teda aj ich metódy smerovania, rozhodol som sa poňať a riešiť túto VŠKP v duchu riadenia premávky nad druhou vrstvou referenčného modelu ISO OSI. Týmto pričinením nie je poskytovateľ limitovaný z technologického aspektu na homogénnu transportnú sieť a obmedzenia jej technológie, čím nadobúda toto riešenie na univerzálnosti a prenositeľnosti.

Transportné siete zo svojej povahy majú vo fyzickej topológii zahrnutých mnoho sekundárnych liniek z dôvodu zálohy liniek primárnych pre prípad poruchy, nadobúdajúc nimi topológiu partial-mesh, snažiac sa priblížiť full-mesh každého s každým. Z pohľadu bežného smerovania v IP sieti je premávka prepravovaná cez primárne linky, čo aj viac-menej je štandardne zabezpečené pomocou *Interior Gateway protocol* (IGP) smerovacieho protokolu nasadeného v transportnej sieti, ako napríklad *Open Shortest Path First* (OSPF). Je to protokol zohľadňujúci šírku pásma do výpočtu metriky, v prípade OSPF je to práve:

$$\text{metrika linky} = \frac{100000}{vp} \quad (2)$$

kde vp je prenosová rýchlosť linky v kb/s, a 100000 je referenčná hodnota, ktorej sa počítaná metrika vzťahuje [13].

V prípade OSPF smerovací protokol svojou funkciou rozširuje informácie o topológií v rámci svojho pôsobenia v doméne pomocou svojich *Link State Advertisement* (LSA) o jednotlivých podsietiach a stavoch liniek v doméne a externých sieťach redistribuovaných do smerovacieho protokolu. Následne pomocou Dijkstrovho algoritmu si smerovač z vlastnej perspektívy vypočíta najkratšiu cestu do každej podsiete z dát svojej topologickej tabuľky. Po výpočetnom procese si zákonite tie najlacnejšie cesty s najnižšou metrikou do všetkých cieľových podsietí umiestni do svojej smerovacej tabuľky. Sieť sa stáva skonvergovanou, smerovanie funguje správne. Nakoľko všetky smerovače v rámci domény z povahy smerovacieho

protokolu OSPF majú rovnaké informácie a teda rovnaký pohľad na topológiu, všetky vypočítali metriku do cieľových sietí s použitím tých najrýchlejších liniek, ~liniek s najnižšími cenami, a teda budú jednotne používať tie metricky najvýhodnejšie trajektórie sieťou.

Sieťová premávka prúdi po najvýhodnejších (z pohľadu OSPF najrýchlejších) linkách, či ich kombináciách, transportnou sieťou. V prípade poruchy linky, je smerovací protokol OSPF plne schopný prepočítať nový stav topológie a pri dostatočnej dostupnosti v závislosti na fyzickej topológii nájsť náhradnú trasu sieťou. Toto správanie je normálne a za bežných okolností vítané. V transportnej sieti sa avšak stáva obmedzujúcim činiteľom.

V transportných sieťach nie zas tak ojedinele sa môže naskytnúť scenár, pri ktorej následkom nejakej služby (napríklad pravidelnej synchronizácie distribuovaných databáz) sa nárazovo objaví enormné množstvo dát prevyšujúce dostupnú kapacitu linky. Pokiaľ nie sú aplikované ani základne metódy diferencovania služieb, radenia do front a tvarovania, zákonite linka s najnižšou kapacitou ako súčasť prenosovej cesty sa stane zahltenou, degradujúc kvalitu všetkých prenášaných služieb, obzvlášť tých spoliehajúcich na real-time prenos a nízke hodnoty jitteru. V prípade že aplikované sú, kvalita real-time služieb zostáva relatívne zachovaná, no linka pretrváva v stave zahltenia. Tento fakt nie je žiadúci, nakoľko záložné cesty transportnou sieťou medzi okrajmi vstupu a výstupu dát do transportnej siete zostávajú s nevyužitou kapacitou. Cieľom teda je realizovať prenos viacerými cestami v IP prostredí, aby došlo k lepšej optimalizácii výkonu, rozloženiu záťaže a rovnomernejšiemu vyžívaníu dostupných sieťových prostriedkov.

3.3. MOŽNOSTI SMEROVANIA A PRENOSU

Dosiahnutie rozloženia záťaže počas smerovania v IP sieti medzi okrajovými bodmi A a B na viac ciest dá realizovať ovplyvnením smerovacieho procesu.

Smerovací proces je založený na rozhodovaní výberu smeru na základe údajov zo smerovacej tabuľky. Do smerovacej tabuľky je umiestnený záznam o cieľovej podsieti ten, ktorý:

- má najnižšiu administratívnu vzdialenosť,
- v prípade zhodnej administratívnej vzdialenosti má nižšiu metriku
- v prípade zhodnej najnižšej metriky sa ich do smerovacej tabuľky umiestni viac (maximálne však 6)

Pokiaľ sa v smerovacej tabuľke nachádza viac záznamov do rovnakého cieľového prefixu s rovnakou metrikou, smerovač ich bude striedať a vykonávať tak vyrovnávanie záťaže cez viac liniek s rovnakou cenou [14].

Táto metóda za účelom load-balancing-u sa používa, hoci z praktického hľadiska je v komplexnej fyzickej topológii transportnej siete celkom nepravdepodobná situácia, že sa naskytne dve či viac ciest s rovnakou metrikou, ktoré by mohli byť za týmto účelom použité, čo v prípade rôznorodosti prenosových kapacít záložných liniek i prípadných technológií by bolo možné. Z týchto dôvodov sa diera cena jednotlivých liniek siete, z ktorej sa počíta celková metrika, ovplyvňovala - administratívne upravovala. Výsledkom bolo, že sa v smerovacích tabuľkách objavila iná metrika pre novo vypočítanú SPF nahradzujúca záznam a cestu pôvodnú, a tým sa docielila regulácia smerovania podľa potreby a požiadaviek poskytovateľa. Podľa Cisco by pridelovanie ceny linkám malo byť inverzné im kapacitám. Štúdiá Fortza však ukázali, že optimálnymi nastaveniami cien liniek v OSPF prostredí sa dá vyťažiť z potenciálu tejto metódy omnoho viac [15] [16].

Ďalšou metódou je použitie *IP Source Routing* - smerovanie podľa pravidiel strany odosielateľa, v nej si odosielaťca strana nadefinuje do záhlavia IP paketu cestu, po ktorej bude paket následne smerovaný. Táto metóda sa však na účely Traffic Engineeringu v transportnej sieti nehodí, pretože má početné obmedzenia a odosielaťca strana v prístupovej sieti nemôže poznať topológiu v transportnej sieti [16] a sledovať jej zmeny.

Možnou metódou je taktiež aj použitie *Constraint-Based Routing* (CBR), konkrétne prístup administratívne-orientovaný, alebo službovo-orientovaný.

Policy Based Routing (PBR), vo voľnom preklade explicitné smerovanie na základe pravidiel je administratívne orientovaný prístup k CBR. V Cisco prostredí je toho princípom tzv. objekt *Route Map*, ktorý obsahuje sadu nadefinovaných pravidiel, podľa nich je následne vykonávané rozhodovanie o smerovaní nehľadiac na smerovaciu tabuľku a smerovacie protokoly. Jedná sa o metódu celkom použiteľnú, avšak vhodnú len na malé siete z dôvodu nutnosti konfigurácie na každom smerovači individuálne pre každý tok.

Alternatívne k PBR, ktoré je orientované povahou smerovania podľa administratívnych pravidiel a príkazov, existuje aj varianta orientovaná smerom k službe. Jej príkladom je napr. *IntServ*. Táto služba však spolieha na kooperáciu s aplikáciami v koncových uzloch siete, majúci dost' obmedzujúci charakter.

Poslednou mnou zvažovanou možnosťou bolo použitie protokolu *Multiprotocol Label Switching* (MPLS) a jej nadstavby Traffic Engineering. Je pravdepodobné, že okrem vymenovaných možností riadenia smerovania existujú ďalšie metódy, ktoré som počas bádania nezvážil.

4. TRAFFIC ENGINEERING V MPLS

Hoci bolo MPLS primárne vyvíjané ako mechanizmus rýchleho prepínania, jedným z rozširujúcich nástrojov, ktoré poskytujú pridanú hodnotu poskytovateľovi siete je implementácia TE nad MPLS.

MPLS spolu s rozšírením TE slúži ako nástroj umožňujúci poskytovateľovi služieb nastaviť jasne stanovenú trasu (taktiež označovanú ako TE tunel) transportnou sieťou spĺňajúcou isté, vopred požadované kritéria. Jeho priebeh sa môže zabezpečiť buď smerovacím protokolom vyššie uvedeného typu, alebo manuálnou konfiguráciou po celej dĺžke trasy od vstupného LSR (označovaný taktiež ako Head-end) až po výstupný LSR (Tail-end)

Nakoľko v štandardnej IP sieti medzi dvomi miestami je dátová premávka smerovaná optimálnou (najlacnejšou) cestou trasou najnižšej metriky, stáva sa bežnou situáciou pri redundantných prepojeniach v sieťovej topológii, že ostatné sub-optimálne cesty vedúce do rovnakej podsiete zostanú nevyužité. Tento prípad pri nadmernej premávke spravidla vedie na zahľtenie optimálnej cesty vyúsťujúc do vysokej odozvy, značného jitteru, stratovosti paketov až k úplnej strate dostupnosti služieb.

Pokiaľ sa používa LDP protokol na rozhlasovanie návěstí, zo svojej povahy kopíruje svoju LSP podľa cesty IGP (napríklad OSPF), čím je obmedzený z hľadiska možnosti realizovať Traffic Engineering, a teda explicitne definovať LSP vedúce sub-optimálnymi trasami.

Rozšírenou verziou protokolu LDP je *Constraint-based Routing Label Distribution Protocol* (CR-LDP). Obsahuje rozšírenia, pomocnou nich je tento protokol schopný vytvoriť cestu mimo bežný IP routing ako to robieva LDP. Je možné zadať podmienky, ktoré musí vytváraná LSP spĺňať, ako je napr. minimálna šírka pásma. Začiatkom roka 2003 sa IETF rozhodla upustiť od protokolu CR-LDP zameriavajúc sa výhradne na rozvoj RSVP-TE [18].

4.1. RSVP-TE

4.1.1. RSVP

RSVP-TE vychádza z koncepcie pôvodného protokolu *Resource Reservation Protocol* (RSVP) a rozširuje ho o možnosti Traffic Engineeringu.

Protokol RSVP pracuje na transportnej vrstve, hoci zo svojej špecifikácie neprenáša (netransportuje) dáta aplikačnej vrstvy. Jeho úlohou je zabezpečiť rezerváciu prostriedkov siete potrebných na prenos dát v IP sieťach typu IntServ. Ku

svojmu šíreniu používa informácie zo smerovacích protkolov. Činnosť protokolu RSVP pozostáva z dvoch krokov:

- vyslanie správy PATH z zdroja informácií skrz smerovanú IP sieť k príjemcovi
- vyslanie správy RESV od príjemcu proti prúdu opisujúc trasu PATH

Proces rezervácie je započatý, keď zdroj dátového toku potrebuje vyslať dátový tok príjemcovi cez sieť typu IntServ. Zdroj vyšle správu PATH adresovanú príjemcovi obsahujú požadované parametre toku. Správa je smerovaná podľa smerovacieho protokolu, kopírujúc najlacnejšie smerovanú cestu. Do správy sa postupne zapisujú smerovače, ktoré si postupne predávajú správu PATH a aj vlastnosti trasy smerom k príjemcovi. Pokiaľ sa na ceste na niektorom smerovači vyskytne chyba, spracovávajúci smerovač preruší reťazec predávania a odošle tvorcovi správy PATH správu, nesúcu oznámenie o chybe spolu s číslom chyby. V tom prípade sa musí správa PATH opakovať.

Ak správa dôjde úspešne k príjemcovi, príjemca správy PATH v ten okamih presne pozná cestu, po ktorej budú k nemu smerované dáta zo zdroja. Na základe informácii o parametroch toku a celkovom stave trasy vie príjemca špecifikovať svoje kvantitatívne požiadavky na QoS, tak i popísať dátový tok, na ktorý sa QoS požiadavky vzťahujú. Uložiac tieto informácie do rezervačnej správy RESV následne príjemca dátového toku odosiela požiadavky rezervácie sieťových prostriedkov smerovačom proti prúdu, na základe reverzného poradia zo zoznamu z prijatej správy PATH. Pokiaľ rezervácia prostriedkov zlyhá, je oboznámený chybovou správou s čísleným identifikátorom chyby príjemca dátového toku realizujúci rezerváciu a celý proces počínajúc správou PATH sa musí opakovať. Odosielanie správ PATH a RESV sa periodicky pravidelne opakuje, nakoľko je rezervácia časovo obmedzená a rezervované prostriedky je potrebné udržiavať počas celého prenosu žiadaného dátového toku sieťou.

4.1.2. UPLATNENIE RSVP V MPLS-TE

Schopnosť rezervovať sieťové kapacity pozdĺž vytýčenej trasy sa ďalej využíva pre Traffic Engineering v MPLS. Protokol RSVP dostal rozšírenia pre možnosť vytvárať trasy LSP v MPLS sieti, berúc do zváženia obmedzenia ako sú počet preskokov, či minimálna šírka pásma. Tieto vytvorené LSP pomocou protokolu RSVP-TE sa nazývajú *TE tunnels*.

Analógia RSVP-TE je RSVP v IntServ sieťach rovnako podobná. Na začiatku vyšle ingress LER správu PATH obsahujúcu navrhovanú trasu cesty. Smerovače v ceste si obdobne správu PATH predávajú a kontrolujú vo svojich prostriedkoch, či

sú schopné vytýčiť trasu v správe PATH. Pokiaľ LSR smerovač nie je toho z nejakého dôvodu schopný, preruší predávanie správy a pošle spätnou cestou k ingress LER správu oznamujúcu chybu vo vytyčovanej ceste, na čo môže LER patrične reagovať.

Po úspešnom prechode správy PATH doménou až k egress LER, výstupný smerovač zahájí rezerváciu prostriedkov odosielaním správ RESV v reverznom poradí. Súčasťou zasielania správ RESV je aj nastavenie značiek na smerovačoch, kopírujúc LSP od výstupného LSR smerom k vstupnému. Pokiaľ LSR nie je schopný rezervovať požadovanú časť zo svojej kapacity, oznámi tento fakt egress LER. Tým sa tvorba LSP musí začať znova. Po úspešnom dokončení RESV správ v spätnom kanáli je TE tunel kopírujúc požadovanú trasu nastavený s požadovanými rezervovanými sieťovými prostriedkami [19]. Z povahy pôvodného protokolu RSVP, tak aj v prípade RSVP-TE sa musia správy PATH a RESV pre udržiavanie LSP pravidelne opakovať.

Vytváranie konkrétnej trasy TE tunelu spočíva vo výbere súvislej postupnosti navzájom susediacich LSR smerovačov jadra domény MPLS, ktoré spájajú ingress a egress LER. Výber tejto postupnosti môže byť uskutočnený administrátorom, a síce postupnosť LSR v ceste bude definovaná administrátorom explicitne skok po skoku LSR za LSR, alebo sa tento výber prenechá na smerovací protokol pracujúci so stavom linky. Takým protokolom je napríklad OSPF [19].

4.2. OSPF-TE

Smerovací protokol OSPF je typu *link-state*, čím získava mnohé výhody nad smerovacími protokolmi typu *distance-vector*. Medzi výhody link-state protokolov patrí napríklad rýchlosť konvergenzie na základe schopnosti de facto okamžite reagovať na zmenu topológie v sieti. Smerovače si udržujú databázu informácií o celej fyzickej topológii siete vrátane jednotlivých stavov liniek. Na základe týchto informácií sa spúšťa *Dijkstrov algoritmus Shortest Path First* (SPF), ktorý počíta najlacnejšiu cestu do každej podsiete z relatívneho postavenia smerovača v sieti, teda cestu s najväčšou prenosovou kapacitou.

Smerovací protokol OSPF počas počítania najlacnejšej cesty do cieľa nezohľadňuje vyťaženosť liniek a zostávajúce voľné kapacity. To máva za následok optimálne smerovanie, avšak častokrát po vyťažovaných cestách s najväčšou prenosovou kapacitou. Alternatívou k tomuto priamočiaremu prístupu je *Constrained Shortest Path First* (CSPF). Tento prístup využíva rozšírenie smerovacieho protokolu v podobe OSPF TE.

OSPF bolo rozšírené o ďalšie parametre o stave linky, ktoré zbiera počas vytvárania topológie, akými sú napríklad maximálne rezervovateľné pásmo pre vytváraný tunel, voľné nerezervované pásmo, či administratívna skupina. Na základe topologickej tabuľky smerovacieho protokolu s podrobnejšími informáciami

o stavoch liniek a ich využitých kapacitách, a administrátorsky zadaných požiadaviek (constraints – obmedzení) sa spúšťa SPF zohľadňujúc tieto faktory, hľadajúc cestu z relatívnej pozície smerovača do požadovaného cieľa. Pokiaľ je možné takú cestu zostaviť, CSPF ju vracia ako odpoveď s postupnosťou všetkých LSR kopírujúc trasu od zdroja k cieľu.

Praktické využitie sa naskytuje pri kombinácií RSVP-TE a OSPF-TE pre účely riadenia premávky smerovaním cez sieť. RSVP-TE vykonáva rezerváciu prostriedkov a nastavuje značky pre LSP od egress LER k ingress. Riadi sa odovzdaným zoznamom obsahujúcim postupnosť LSR v sieti. Tento zoznam môže byť generovaný dynamicky, a teda pomocou smerovacieho protokolu, akým je napr. OSPF-TE hľadajúci najlepšiu cestu a berúc do úvahy stav vyťaženia siete a požadované obmedzenia. [21] Vtedy je výsledkom presná (tzv. *strict* – striktná) postupnosť za sebou nasledujúcich LSR, nakoľko počítajúci LER smerovač vie z topologickej tabuľky presnú cestu, ktorú bude LSP kopírovať.

Taktiež zoznam môže byť nakonfigurovaný manuálne administrátorom, a síce skok po skoku používajúc slová *strict* a *loose*. Ten sa odovzdá spolu s požiadavkami na pásmo protokolu RSVP-TE, ktorý sa pokúsi túto cestu zostaviť. Ak uspeje, vracia sa vytvorená LSP, TE tunel, v opačnom prípade chybová hláška. Veľká výhoda Traffic Engineeringu v MPLS je, že explicitná cesta LSP sa nastavuje (manuálne, alebo dynamicky smerovacím protokolom s patričným rozšírením) len na okrajovom LER smerovači a nie pozdĺž celej trasy, ako je tomu napr. v prípade virtuálnych okruhov v technológií ATM

5. REALIZÁCIA

5.1. PRÍPRAVNÁ FÁZA

5.1.1. VÝBER VARIANTY RIEŠENIA

Nakoľko bude nutné, aby každý prúd premávky dát prechádzal cez sieť rôznymi cestami, táto sa nedá vyriešiť použitím čistého IP. Smerovanie v IP sieti je uskutočňované len na základe cieľovej IP adresy, ktorá nie je vôbec určujúca pre obsah, ktorý IP datagram nesie. Okrem toho štandardne sú dáta posielané výhradne cestou najnižšej metriky, čo je spravidla jedna trasa, pokiaľ sa nenasadí vyrovnanie záťaže (Load Balancing).

Load Balancing v základe vie vyrovnať záťaž tým, že bude dátovú premávku rozosielať dvomi či viacerými smermi najlacnejšími smermi so zhodnou metrikou do rovnakého cieľa. Avšak toto je zaručené málokedy. Používajú sa metódy na administratívne ladenie metriky, jedná sa však skôr o núdzové riešenie multi-homed sietí. Smerovací protokol EIGRP od firmy Cisco je schopný Unequal Load-Balancing [9], avšak jeho nevýhodou jeho proprietárnosť a rieši situáciu len z pohľadu smerovača na vzdialenosť najbližšieho preskoku, na ktorom je technológia implementovaná. Uvedené metódy nezohľadňujú typ/triedu/prúd premávky.

Použitie IP Source Routing sa spolieha na vodpred definovanú cestu pomocou skokov na ceste, či už striktne (strict source and record route – SSRR), alebo „voľne“ (loose source and record route - LSRR) definovanú cestu. Nakoľko tieto skoky si musí zaistiť zdroj IP paketu, metóda nepripadá v úvahu.

Pre implementáciu Policy-Based Routing (PBR) by bolo nutné nakonfigurovať na každom smerovači LSR Route-Map, čo pri veľkých sieťach a mnohých dátových prúdoch sa stáva neúnosným.

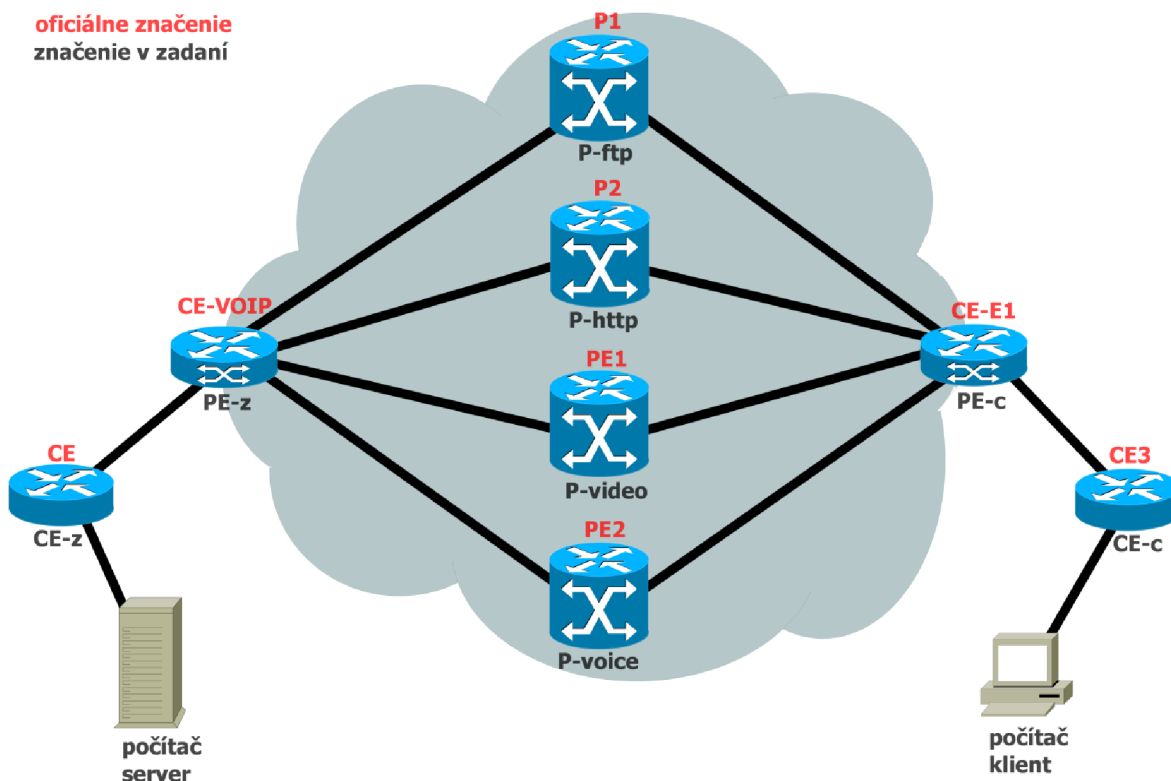
Mnou vybraná realizácia bude spoliehať na prepínací mechanizmus MPLS s použitím jeho nástrojov nadstavby pre Traffic Engineering.

5.1.2. NÁVRH RIEŠENIA

Realizácia praktickej časti bude prebiehať na vybavení vysokorýchlostného komunikačného systému z racku v učebni číslo 429 na Ústave telekomunikácií fakulty FEKT. Použijú sa z neho prepínač spolu so smerovačmi, menovite: P1, P2, PE1, PE2, CE-VOIP, CE-E1, CE, CE3. Všetky smerovače (okrem posledného menovaného) sú zo série 2800, typu 2821. Jednotlivé smerovače sa líšia svojou výbavou hardware, avšak pre potrebu nášho zadania majú dostatok spoločných znakov. Nainštalovaný operačný systém IOS je verzie 12.4(24)T11, číslo vydania fc3. Konkrétne meno

binárky súboru operačného systému je „c2800nm-advipservicesk9-mz.124-24.T1.bin“. Z názvu je patrné (advanced IP services), že obsahuje pokročilé služby potrebné na realizáciu.

Smerovač s oficiálnym označením CE3 je zo série 1800, typu 1812, má nainštalovaný IOS verzie Version 12.4(6)T3. IOS je načítavaný zo súboru „c181x-advipservicesk9-mz.124-6.T3.bin“.



Obr. 6: Použité smerovače

Kabelážna infraštruktúra je zapojená do gigabitového ethernetového prepínača Cataly 2960 typového označenia WS-C2960G-48TC-L. Nainštalovaný operačný systém je 12.2(35)SE5, zavádzaný zo súboru „c2960-lanbase-mz.122-35.SE5.bin“.

Prístup ku smerovačom a prepínaču konzolovým pripojením je realizovaný pomocou konzolového serveru na smerovači 1841.

Okrem uvedenej sieťovej infraštruktúry budú použité dva osobné počítače konfigurácie Intel C2Duo6300, 2GB operačnej pamäte RAM, s nainštalovaným operačným systémom. Ich funkcia bude v úlohe koncových staníc generujúcich a zachytávajúcích všetku potrebnú rôznorodú premávku, a síce ftp, http, streamované video a hlas VoIP telefónie. Toto riešenie bolo zvolené s ohľadom na dostačujúcu funkčnosť sústrediac sa primárne na problematiku transportnej siete. Použité programové vybavenie pre rôznorodú premávku je nasledovné.

Strana serveru (generátor premávky):

- FileZilla ftp server, verzia 0.9.37 beta, ako ftp server
- Apache webový server, verzia 2.2.19, ako webserver
- VLC multimediálny prehrávač, verzia 1.1.9, ako streamovací server
- linphone softvérový VoIP telefón, verzia 3.4.3, ako účastník VoIP hovoru

Strana klienta (konzument premávky):

- FileZilla univerzálny ftp-like klient, verzia 3.5.0, ako ftp klient
- Opera webový prehliadač, verzia 11.11, ako webklient
- VLC multimediálny prehrávač, verzia 1.1.9, ako klient prehrávajúci stream
- Sjphone softvérový VoIP telefón, verzia 1.65.377a, ako účastník VoIP hovoru

Prenos rôznorodej premávky prebiehal majoritne zo strany počítača server na počítač klient. Pre prenos pomocou ftp protokolu bol použitý ako objekt prenosu multimediálny súbor videa s veľkosťou 814MB. Ten istý súbor bol použitý pre prenos pomocou http protokolu. Video stream menovaného videa vo Full-HD bol prenášaný použitím RTP / MPEG transport stream spolu na unicastovú IP adresu klienta formou UDP prenosu. Rovnako ten istý video súbor bol použitý ako zdroj zvuku do VoIP komunikácie, ktorá prebiehala jednosmerne medzi počítačmi server→klient. Zostavovanie hovoru bolo avšak iniciované zo strany softvérového VoIP telefónu na klientskom počítači. Použitý kodek na prenos hlasu bol referenčný priemyselný štandard ITU-T G.711 konštantného dátového toku 64kbit/s. Vzorok (patterny) zachytené sieťovým analyzátorom Wireshark týchto jednotlivých typov premávok sú uvedené v prílohe.

Situácia počas prenosu na strane serveru i klienta je zachytená na snímkoch ich pracovných plôch v prílohe. Takiež je patrné, že ich hardvéru boli značne počas prenosov vyťažené. Išlo hlavne o početné diskové operácie pre prenos ftp a http, a záťažové operácie procesoru a grafickej karty ako sú prehrávanie videa vo Full-HD rozlíšení, rovnako ako aj jeho prekódovanie a streamovanie po sieti.

V pôvodnej fyzickej infraštruktúre zapojenia tieto dva počítače nahradia IP telefóny a tak získajú pripojenie do prepínača a teda experimentálnej siete.

5.1.3. POSTUP REALIZÁCIE

Realizácia riešenia vyžaduje sadu postupných krokov a je rozdelená na niekoľko implementačných etáp:

1. Návrh a konfigurácia logickej štruktúry siete
2. Návrh a konfigurácia IP adresovania siete
3. Návrh a konfigurácia smerovacích domén
4. Implementácia prepínacieho mechanizmu MPLS
5. Implementácia VPN do MPLS
6. Konfigurácia explicitných ciest (TE tunelov)
7. Konfigurácia klasifikácie premávky
8. Konfigurácia smerovacej politiky

Každá etapa pozostáva z dielčích, tematicky súvisejúcich krokov, uzatvára kapitolu a posúva funkcionality siete a riešenie ďalej.

5.2. IMPLEMENTAČNÉ ETAPY

5.2.1. NÁVRH A KONFIGURÁCIA LOGICKEJ ŠTRUKTÚRY SIETE

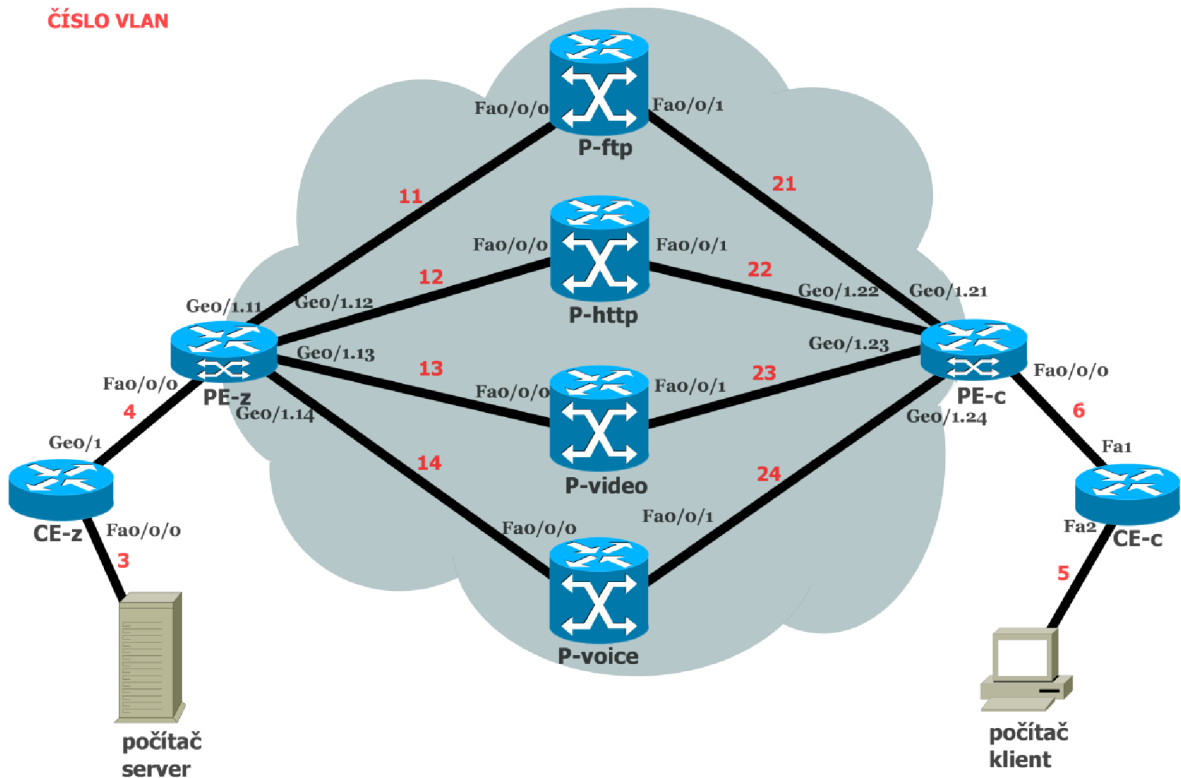
Logická topológia mnou vybranej siete spolieha na tradičnú zostavu dielčích sietí zákazníka zapojených do transportnej siete uprostred. V logickom zapojení siete je kladený dôraz na viac paralelných spojení medzi hraničnými smerovačmi transportnej siete. Fyzická štruktúra je pevne daná, modifikácia jej logickej štruktúry je možná pomocou segmentovania kolíznych a broadcastových domén použitím technológie virtuálnych sietí, *Virtual LAN* (VLAN). „Priame“⁶ spojenia medzi smerovačmi segmentácie dosiahnutej až do tretej úrovne sa realizujú priradením portov smerovačov do jednej zoskupujúcej VLANy.

Pre nízky počet počet fyzických rozhraní na hraničných smerovačoch transportnej siete jadra sa použije technológia trункov. Tá umožňuje v spolupráci s protokolom .1Q zoskupenie viacerých VLAN nad jednou fyzickou linkou formou tagovania, ktorá v konjunkcii s trункovým nastavením portu prepínača umožňuje vytvoriť viac podsietí na jednom rozhraní.

Konečná forma logickej topológie bola navrhnutá ako je znázornené na Obr. 7: Logické rozdelenie virtuálnych LAN. Port smerovača zdieľajúci viac sietí VLAN bol rozdelený na virtuálne podrozhrania (sub-inteface), kde každý sub-interface prináleží

⁶ „Priame“ je relatívny pojem v patričnom kontexte, nakoľko všetky prepojenia medzi smerovačmi idú cez jediný zdieľaný prepínač

do patričnej VLAN. K nim bolo následne priradené zapúzdrowanie (encapsulation) pre tú danú konkrétnu VLAN, čiže logickú linku.



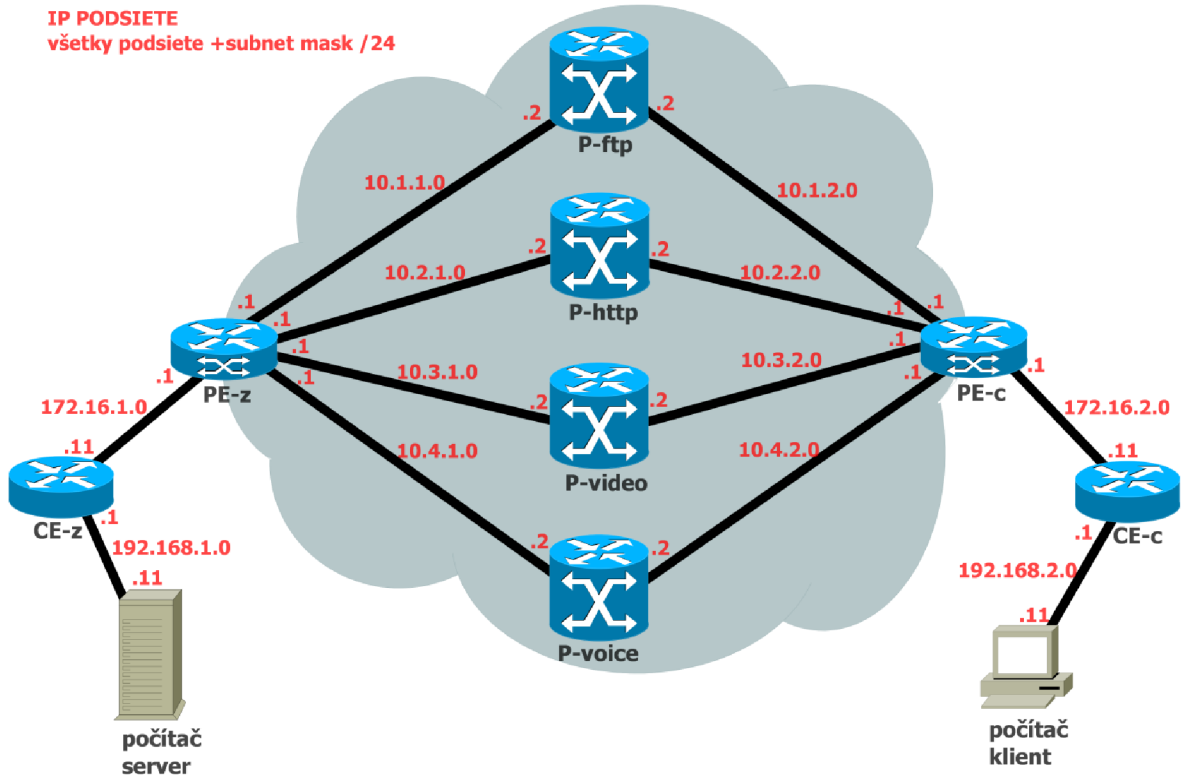
Obr. 7: Logické rozdelenie virtuálnych LAN

5.2.2. NÁVRH A KONFIGURÁCIA IP ADRESOVANIA SIETE

Rozdelenie podsietí bolo vykonané nasledovne, s ohľadom na systematickosť. Transportná sieť zdieľa podsiete z 10.0.0.0/8. Jednotlivé trasy pre ftp, http, video a hlas (voice) sú koncipované ako 10.1.X.X, 10.2.X.X, 10.3.X.X, a 10.4.X.X. Vertikálne polovice zdieľajú masku adresovania 10.X.1.X, resp. 10.X.2.X ako je názorné z obrázku. Prístupové siete sú 172.16.1.0/24 a 172.16.2.0/24, a siete koncových staníc 192.168.1.0/24 a 192.168.2.0. Ucelený pohľad na adresovanie znázorňuje Obr. 8: Plán IP adresovania.

IP adresy na hraničných smerovačoch poskytovateľa sú pridelované až k podrozhraniám adekvátne k VLANám. Rozhrania (porty) FastEthernet 0/0/0 prepínacích modulov v smere downstreamu na hraničných smerovačoch poskytovateľa PE a zákazníka CE boli použité z dôvodu nedostatočného počtu plnohodnotných L3 portov. Tieto porty boli priradené do VLANy číslo 1 lokálneho pôsobenia daného sieťového zariadenia. Následne na *Switch Virtual Interface (SVI)* tejto VLANy bola nastavená IP adresa umožňujúca smerovanie, a teda úplnú

funkcionalitu sieťovej vrstvy. Z mnohú získaných znalostí z Cisco akadémie pre potreby našej siete by funkčnosť nemala byť nijak limitovaná.



Obr. 8: Plán IP adresovania

Na všetkých použitých rozhraniach prepínacích modulov smerovačov vzniklo varovanie o nezhode v natívnych VLANách voči prepínaču. Táto skutočnosť bola oznámená servisným protokolom firmy Cisco – *Cisco Discovery Protocol* (CDP). Nakoľko na strane smerovača je switchport nastavený do módu prístupového (access) a teda daná linka poníma len jednu VLANu, je hlásenie o nezhode natívnych VLAN bezpredmetné; VLAN pre prepínacie moduly má len lokálne pôsobenie na smerovači z dôvodu funkcionality tretej vrstvy switchportu.

Pre efektívnejšiu debugovateľnosť a ladenie siete z hľadiska jej logickej topológie a adresovania na tretej vrstve sa na prepínači nastavili IP adresy na SVI ku každej VLANe so vzorom X.X.X.5 opisujúc adresu danej podsiete.

Po úspešnom završení tejto fázy pri správnej funkcionality je smerovač schopný pomocou požiadavky Echo Request protokolu ICMP úspešne zistiť dostupnosť IP adresy zo zariadení podieľajúcich sa k nemu pripojených VLANách.

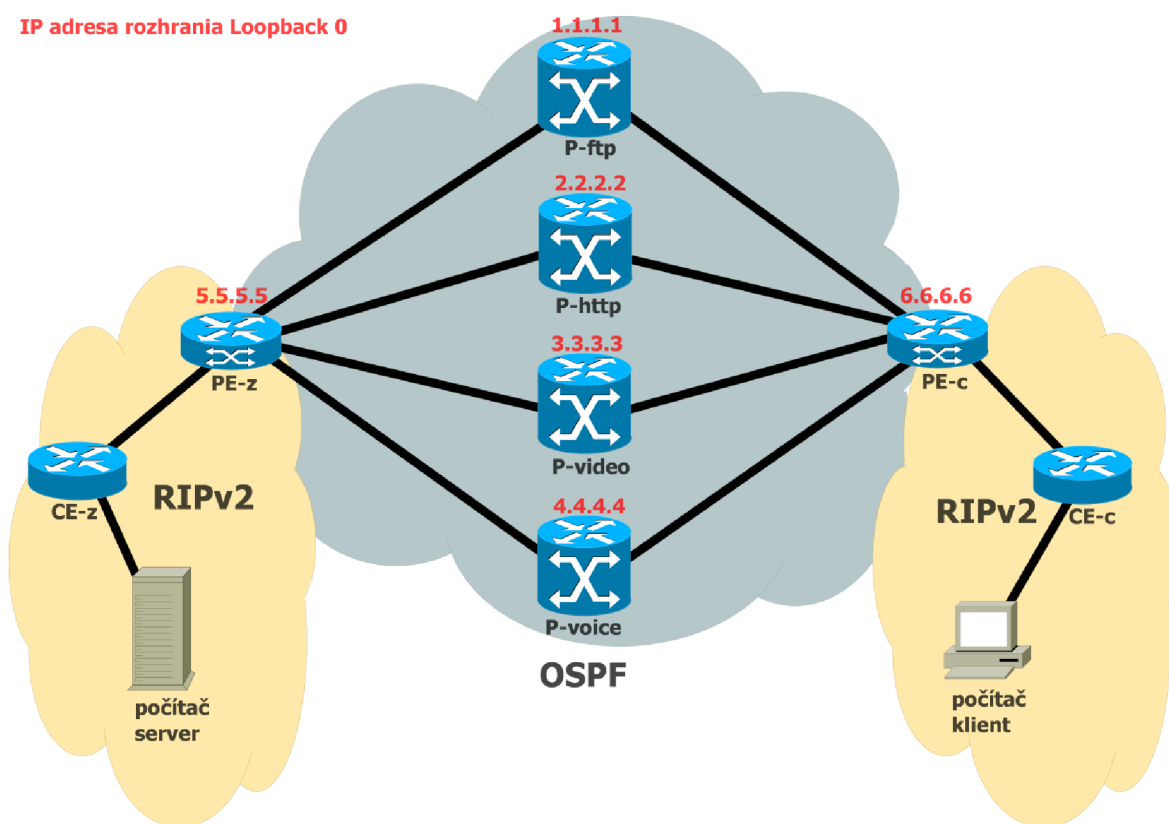
5.2.3. NÁVRH A KONFIGURÁCIA SMEROVACÍCH DOMÉN

Pre transportnú doménu, v ktorej má byť nasadené MPLS s možnosťami Traffic Engineeringu bol zvolený smerovací protokol OSPF z dôvodov skôr opísaných

v teoretickej časti tejto VŠKP. Celá transportná sieť bude z pohľadu OSPF umiestnená v chrbticovej oblasti (Area 0). Pre stabilnejšiu funkčnosť protokolu OSPF boli nakonfigurované aj tzv. virtuálne rozhrania *Loopback* s adresami 1.1.1.1 až 6.6.6.6.

Pre účely nášho OSPF bola taktiež upravená konštanta referenčnej šírky pásma, z nej počíča smerovací protokol cenu jednotlivých liniek. Štandardná hodnota zohľadňuje rýchlosť linky do 100Mbit/s vrátane, pre náš prípad bola upravená zo 100 na 100000 (v Mbit/s).

Na prístupové a koncové siete bola zvolená beztriedna (classless) varianta v podaní smerovacieho protokolu *Routing Information Protocol* (RIP) verzie 2. Jeho funkcionálna potrebná pre oznamovanie týchto sietí typu „stub network“ je úplne dostačujúca. Pohľad na situáciu ilustruje nasledujúci obrázok-



Obr. 9: Smerovacie domény

Uvedené smerovacie protokoly boli aplikované na príslušné sieťové rozhrania smerovačov do patričných smerovacích domén. V prípade CE smerovačov bolo aplikované pravidlo pasívneho rozhrania (passive interface) z pohľadu smerovacieho protokolu RIPv2 na rozhrania koncových sietí, čo obmedzilo zasielanie smerovacích informácií na koncové stanice. Napriek tomuto obmedzeniu RIP tieto siete (192.168.X.X/24) rozhlasuje aj naďalej, čo je v rámci výsledku realizácie žiadané.

Na konci tejto etapy majú smerovače jadra (P) úplnú znalosť o smerovaní v transportnej sieti. Hraničný smerovač PE má znalosť okrem ciest do posietí transportnej siete aj ohľadne prístupovej a koncovej siete na svojej strane domény. Smerovač na hrane zákazníka (CE) pôsobí ako zdroj smerovacích informácií zo strany zákazníkového členenia siete pre nepriamo pripojené siete voči transportnej sieti.

5.2.4. IMPLEMENTÁCIA PREPÍNACIEHO MECHANIZMU MPLS

Implementácia MPLS bola pomerne jednoduchá. Po globálnom „zapnutí“ a označení rozhraní prináležiacich v MPLS doméne sa explicitne nastavil protokol distribúcie značiek. Uprednostnil sa protokol LDP, nakoľko je priemyselným štandardom a spĺňa rovnakú funkcionality ako TDP.

Ako prax ukázala, mechanizmy MPLS dedia identifikátor smerovača z IP adresy rozhrania Loopback a pre správnu funkčnosť je potrebné, aby tieto IP boli oznámené a smerovateľné z pohľadu záznamu smerovacej tabuľky smerovača LSR v doméne. LDP rovnako OSPF využíva tieto adresy na identifikáciu, avšak na rozdiel od OSPF, LDP vyžaduje si k nim smerovateľnú cestu. Bez nej neprebehne automatická výmena párovania značiek medzi LSR smerovačmi. Z tohoto dôvodu boli rozhrania Loopback 0 dodatočne priradené do rozhlasovania smerovacieho protokolu OSPF.

Úspešným zavŕšením tejto sate je funkčnosť prepínania MPLS spolu s naplnenou databázou párovania značiek voči FEC, a to o záznamy svoje i susedných LSR. Funkcia MPLS sa dá otestovať trasovaním.

5.2.5. IMPLEMENTÁCIA VPN DO MPLS

Ďalším veľmi dôležitým krokom v implementačnom postupe je konfigurácia VPN nad MPLS sieťou. V našej experimentálnej sieti sa pokúsime nastaviť typ VPN L3, čo znamená transport smerovacích informácií medzi smerovačmi zákazníka CE. Z pohľadu smerovačov CE budú mať vedomosti o svojich prístupových a koncových sieťach získané pomocou smerovacieho protokolu RIP.

K tomuto účelu musíme vytvoriť virtuálnu smerovaciu tabuľku *Virtual Routing and Forwarding* (VRF), ktorá bude obsahovať informácie z protokolu RIP. Táto tabuľka obsahuje smerovacie informácie, ktoré je potrebné označiť unikátnym identifikátorom *Route Distinguisher* (RD) viažúcim sa k danej VRF (v našom prípade 65001:1), umožňujúc ich odlišiť v prípade použitia viacerých VRF a zákazníckych sietí. Následne sa VRF umiestni na rozhrania VLAN 1 hraničných smerovačov PE. Pre výmenu smerovacích informácií medzi VRF tabuľkami navzájom sa použije smerovací protokol *Border Gateway Protocol* (BGP) pracujúci vnútri jedného autonómneho systému.

Posledným dielčím krokom tejto implementačnej fázy je zapnutie redistribúcií medzi smerovacími protokolmi, a to sú nasledovné dve:

- z RIP do BGP, kde BGP následne prenesie smerovacie informácie z jednej VRF cez MPLS sieť do VRF na druhom PE
- z BPG do RIP, kde sa smerovač CE na druhej strane siete dozvie z protokolu RIP o existencii druhej časti koncovej siete zákazníka a jej prístupovej sekcii

Funkčné naplnenie tejto fázy je stav, v ktorom CE smerovače zákazníka zdieľajú vedia smerovacie informácie pomocou RIPu a koncové stanice sú schopné vzájomnej komunikácie.

5.2.6. KONFIGURÁCIA EXPLICITNÝCH CIEST (TE TUNELOV)

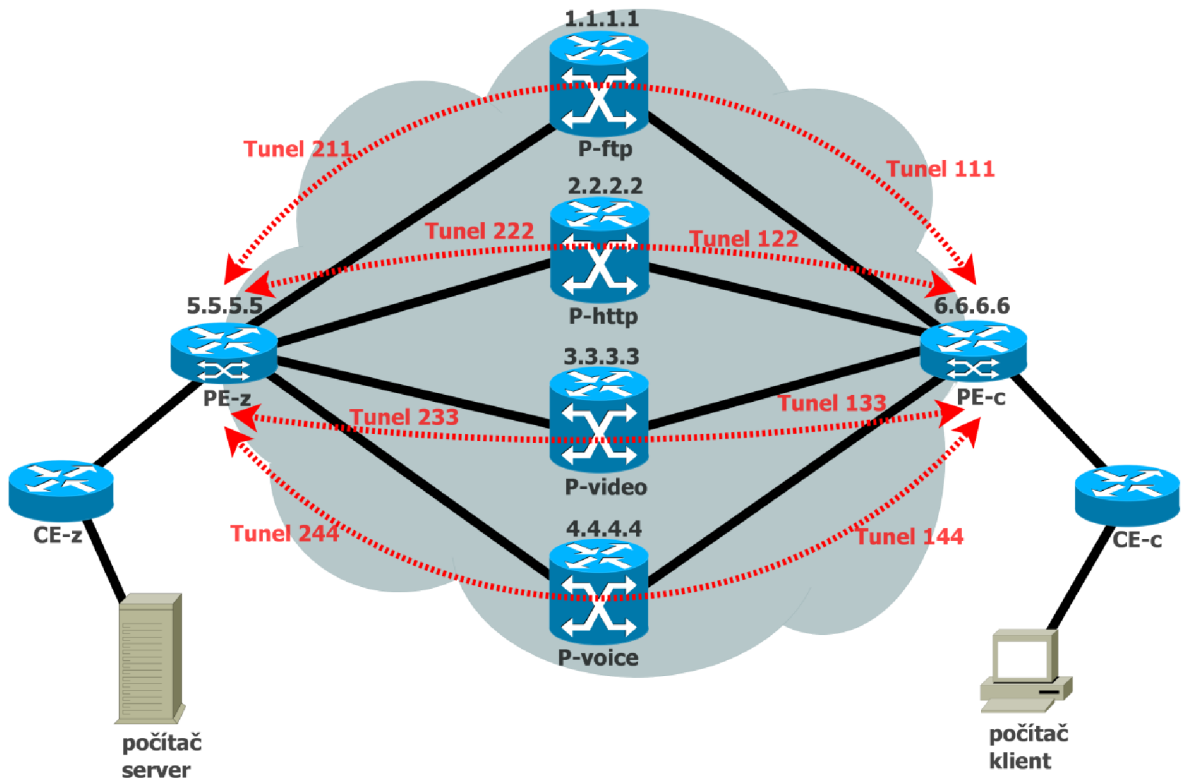
Implementácia TE do MPLS sa skladá z viacerých krokov. Najskôr je potrebné aplikovať na všetky rozhrania a podrozhrania, ktoré budú použité pre technológiu „tunelovania“, maximálne rezervovateľné pásmo, tak aj maximálnu možnú veľkosť rezervovateľného pásma pre jeden tunel (v našom prípade boli použité hodnoty 70Mbit a 65Mbit).

Následne je potrebné zapnúť možnosť vytvárania MPLS TE tunelov v globálnom konfiguračnom režime tam, kde je to potrebné (v našom prípade na všetkých LSR), tak aj na konkrétnych fyzických rozhraniach podieľajúcich sa v MPLS doméne, na nich sa budú TE tunely realizovať (taktiež všetky MPLS rozhrania).

Po tejto konfigurácii je nutné oznámiť smerovaciemu protokolu OSPF fakt, že sa nastavba pre TE bude používať, a teda aktivovať jeho rozširujúce funkcie OSPF-TE identifikujúce mu pole jeho pôsobnosti na oblasť chrbticovej siete (Area 0), taktiež nastavenie identifikátora smerovača použitím virtuálneho rozhrania Loopback 0.

Takto nastavené LSR v MPLS doméne sú pripravené prevádzkovať Traffic Engineering. Konfigurácia samotných tunelov sa vykonáva už len na hraničných smerovačoch LER. Tunel (či LSP) je zo svojej povahy záležitosť jednosmerná, takže bolo potrebné nakonfigurovať dva tunely na jednu trasu (jeden v smere zdroj-cieľ, druhý v smere cieľ-zdroj), dohromady 8 tunelov: dvojice pre FTP, HTTP, VIDEO, VOICE. Každému tunelu bola priradená požiadavka na alokáciu prenosových prostriedkov o veľkosti 60Mbit/s. Situáciu a jednotlivé tunely vykresľuje Obr. 10: Tunely Traffic Engineeringu v MPLS doméne. Znázornené sú obojsmerné tunely, avšak v skutočnosti sa jedná o páry protichodných tunelov medzi smerovačmi PE. Tunelom boli pridelené IP adresy z virtuálneho rozhrania Loopback 0, a zadané cieľové IP adresy taktiež virtuálneho rozhrania druhého smerovača LER. Trasy boli nadefinované explicitne skok po skoku, ako je uvedené v konfiguračných súboroch

v elektronickej prílohe. Taktiež bolo pri všetkých tuneloch zadaná požiadavka na umiestnenie do smerovacích tabuliek smerovačov LER, kde nahradili pôvodné OSPF oznámenia.



Obr. 10: Tunely Traffic Engineeringu v MPLS doméne

Na konci tejto implementačnej etapy máme nadefinovaných osem explicitných trás, po nich sa rozosiela premávka (pretože boli umiestnené do smerovacej tabuľky) formou load-balancingu, nakoľko tunelom bolo priradené rovnaké pásmo. V prípade komplexnejšej logickej topológie by bola názornejšia použiteľnosť ich konfigurácie (napr. pri full-mesh prepojení smerovačov jadra).

5.2.7. KONFIGURÁCIA KLASIFIKÁCIE A ZNAČKOVANIA PREMÁVKY

Pôvodná myšlienka implementácie mala spoľiehať na funkcie značkovania (marking) premávky, podľa nej by sa premávka rozlíšila – klasifikovala (classification) v mape politiky (policy-map) použitím tried map (class-map) pre definovanie pravidiel zhody jednotlivých typov premávky. Takto klasifikovaná premávka mala byť označená poľom IPP (IP precedence) v záhlavi IP paketu, jeho hodnota mala byť rozhodujúca pre zatriedovanie do kontrétneho tunelu pri použití smerovacej mapy (route-map). Avšak ako sa mi v praxi ukázalo, tak konštrukcia route-map pravdepodobne nedokáže zohľadňovať svoje rozhodnutia na základe hodnot z informačných polí

používaných v QoS službách, a teda myšlienka klasifikácie a značkovania neuspela a ich konfigurácia nie je vo finálnych konfiguračných súboroch zahrnutá.

5.2.8. KONFIGURÁCIA SMEROVACEJ POLITIKY

Nakoľko pôvodný plán s klasifikáciou a značkováním premávky sa ukázal ako nerealizovateľný, bolo potrebné použiť iný prístup.

Druhým prístupom bolo použitie štyroch policy-máp pre individuálne typy premávky, kde každá policy map zahŕňala v sebe jednu class-map, jej úlohou bola klasifikácia jednotlivých typov. Následne tieto policy-mapy boli zahrnuté ako podmienky zhody v jednoduchých záznamov route-map ako podmienky zhody. Táto konfigurácia – hoci tentokrát syntakticky možná a správna, v sebe zahrňovala pravdepodobne sémantickú chybu, lebo nefungovala vôbec.

Ako poslednou vyskúšanou možnosťou bolo podľa [22] použitie rozšírených prístupových zoznamov – extended Access-List (ACL) v konštrukcii route-mapy. Toto riešenie taktiež sa pre zadanie práce nejavilo ako funkčné, a teda cieľ zostáva nenaplnený.

Pre všetky tri varianty bolo samozrejmosťou zahrnutie vŕf do pravidiel nastavenia pre použitú route-mapu.

5.3. ROZBOR PROBLÉMU

Správanie použitej tretej varianty (viac-menej oficiálneho zo strany výrobcu) riešenia PBR v našej experimentálnej sieti bolo rozobrané.

Sieť bola sledovaná v stave počas implementácie riešenia. Po aplikovaní route-mapy na rozhranie a odstránení VRF tabuľky sa automaticky systémom odstránila IP adresa, ktorá bola zviazaná s VRF tabuľkou. Týmto okamihom stratila koncová a prístupová sieť konektivitu so svojou druhou polovicou za transportnou sieťou. Použitím trasovania z koncového uzla siete (počítača) sa zistilo, že blízky PE smerovač nemá dostupnú nami vybranú cieľovú sieť (konkrétne počítač na opačnom konci). Následne pozorovaním smerovacej tabuľky príslušného smerovača CE sa zistilo, že záznamy oznamované protokolom RIP starnú, až sa formou časovačov stanú neplatnými a sú zo smerovacej tabuľky odstránené.

Z tohoto správania siete som zhodnotil, že aplikáciou route-mapy na rozhranie prístupovej siete smerovača PE sa prerušuje konektivita s druhou časťou siete zákazníka. Smerovacie informácie nie sú z nejakého dôvodu prenášané pomocou BGP medzi PE smerovačmi, čo vyúsťuje k starnutiu smerovacích informácií v smerovacej tabuľke, a následnej strate aj tej čiastočnej konektivity od koncového uzlu po bližší smerovač PE.

Otázny taktiež zostáva, či má byť odstránená VRF tabuľka z rozhrania VLAN 1, alebo nie. Avšak ako zdroj REFERENCIA uvádza,

%% Policy Based Routing is NOT supported for VRF" interfaces

no dané riešenie podľa zdroja nevedie k úspechu.

Daná situácia je dosť už komplexná, nakoľko v nej hrá veľa faktorov navzájom sa ovplyvňujúcich, menovite:

- používanie VRF na rozhraní
- redistribúcia medzi VRF navzájom pre potreby VPN
- prístupové zoznamy vyhodnocujúce premávku
- route-mapa nejasnej konštrukcie (pokiaľ má byť VRF jej súčasťou alebo nie) spoliehajúca na správne podmienky prístupových zoznamov
- usmiestnenie route-mapy kolidujúce s použitím VRF na rozhraní

Pravdepodobným problémom bude redistribúcia VRF po aplikovaní route-mapy, kde tento fakt musí byť pravdepodobne do route-mapy explicitne zahrnutý.

Na ujasnenie tejto komplexnej situácie by bola potrebná pomoc tretej strany v podobe skúseného odborníka v roli konzultanta, a konzultácií s ním ohľadom riešenia problému, nakoľko dostupná literatúra popisuje jednotlivé problematiky učebnicovo a osobitne, nie ich vzájomnú súvislosť, ovplyvňovanie sa a vylučovanie navzájom. Avšak podstúpením tohoto kroku by sa táto VŠKP a jej vypracovanie dostalo do rozporu s čestným prehlásením, a to spôsobiť nechcem.

5.4. VÝSLEDNÁ PODOBA REALIZÁCIE

Nakoľko triedenie premávky podľa typu do TE tunelov nefungovalo ako bolo v pláne zaumienené, časť zadania uvádzajúca rôznu kvalitu transportnej siete nebola do výslednej realizácie zahrnutá, keďže správanie siete na PBR nástroja nekorenšpondovalo s predpokladaným, a zmenalo by výber cesty podľa najlacnejšej linky. Ten by sa dal ovplyvniť zmenou OSPF ceny pre daný tunel za účelom load-balancingu, avšak pri linkách s rôznou kvalitou by to nebolo férové správanie pri nezohľadňovaní kvality služieb.

Samotné nastavenie liniek pre rôznu kvalitu sa dá jednoducho ovplyvniť upravením množstva dostupného a rezervovateľného pásma v protokole RSVP, tak prípadne aj pri vytváraní na TE tunela.

V terajšom stave bez aplikovaného PBR je na transportnej sieti vykonávaný load-balancing rozkladania záťaže, ako aj znázorňuje snímka trasovania zo smerovača na Obr. 11: Load-balancing medzi LER. Sieť dosahuje aj pod plným

nasadením premávky z koncových počítačov výbornú odozvu, ako je možné vidieť na snímkoch pracovných plôch serveru aj klienta. Snímky sú priložené v prílohe.

```
PE-z#traceroute
Protocol [ip]:
Target IP address: 6.6.6.6
Source address: 5.5.5.5
Numeric display [n]: 8
Timeout in seconds [3]: 1
Probe count [3]: 4
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]: Verbose
Loose, Strict, Record, Timestamp, Verbose[v]:
Type escape sequence to abort.
Tracing the route to 6.6.6.6

 1 10.3.1.2 [MPLS: Label 29 Exp 0] 0 msec
   10.1.1.2 [MPLS: Label 23 Exp 0] 0 msec
   10.4.1.2 [MPLS: Label 24 Exp 0] 0 msec
   10.2.1.2 [MPLS: Label 23 Exp 0] 0 msec
 2 10.3.2.1 0 msec
   10.1.2.1 0 msec
   10.4.2.1 0 msec
   10.2.2.1 0 msec
PE-z#
```

Obr. 11: Load-balancing medzi LER

5.5. ZHRNUTIE

V praktickej realizácii sa nám podarilo nakonfigurovať MPLS sieť vo funkcií transportnej siete spájajúcej dve okrajové smerovacie domény.

Bol implementovaný mechanizmus VPN pre zachovanie privátnosti riešenia (jedna z typických požiadaviek na transportnú sieť) z pohľadu koncových sietí, a možnú škálovateľnosť.

Taktiež do experimentálnej siete bolo aplikované rozšírenie MPLS o možnosti Traffic Engineeringu. Vytvorili sa explicitné trasy, avšak korektné nasmerovanie rôznorodej premávky do nich už bolo problematické, ako je opísané v sekcii vyššie. Samotný problém a jeho možná príčina je v časti „Rozbor problému“. Sieť je i napriek tomu funkčná, nastavená do módu load-balancingu. Konfiguračné súbory smerovačov a prepínača sú umiestnené v elektronickej podobe v prílohe.

Samotné nastavenie liniek s rôznou hodnotou sa nepoužilo z dôvodu, opísaného v predchádzajúcej sekcii. Samotný proces je jednoduchý, avšak činnosť stráca význam bez funkčného PBR. Toto je taktiež opísané v predchádzajúcej sekcii.

K úplnému naplneniu zadania postačuje pravdepodobne len jedna, avšak sofistikovane konštruovaná route-mapa.

ZÁVER

Bakalárska práca popísala problematiku a princíp smerovania paketov v transportnej sieti postavenej na prepínanom mechanizme MPLS s dôrazom na porovnávanie smerovania a prepínania v IP sieti.

Ďalej pojednala o princípe, metódach a možnostiach Traffic Engineeringu v transportných sieťach. Na základe vlastností jednotlivých metód bol uskutočnený výber jednej metódu pre realizáciu praktickej časti experimentálnej siete podľa zadania. K danej metóde bola venovaná ešte samostatná kapitola použiteľných nástrojov.

Praktická časť tejto VŠKP obsahuje úvahy ohľadom možných riešení, opis praktickej realizácie a implementačný postup konfigurácie siete. Konfigurácia bola zvládnutá korektne skoro do posledného kroku, ako bolo uvedené a zhodnotené v texte k praktickej časti.

Z celého zadania zostala posledná vec, ktorú je potrebné implementovať. Je ňou route-map sofistikovanej konštrukcie (pravdepodobne).

LITERATÚRA

- [1] **PETERKA, J.** *Báječný svět počítačových sítí, Část XXVI: ATM, technologie, která neztvrdila.* e-archiv Jiřího Peterky. [Online] Posledná aktualizácia: Marec 2007 <http://earchiv.cz/b07/b0600001.php3>.
- [2] **REKHTER, Y.; DAVIE, B.; KATZ, D.** *RFC 2105 - Cisco Systems' Tag Switching Architecture Overview.* The Internet Engineering Task Force (IETF). [Online] Február 1997. <http://tools.ietf.org/html/rfc2105>.
- [3] **ROSEN, E.; VISWANATHAN, A.; CALLON, R.** *RFC 3031 - Multiprotocol Label Switching Architecture.* The Internet Engineering Task Force (IETF). [Online] Január 2001. <http://tools.ietf.org/html/rfc3031>.
- [4] **REED, D. P.** *That Sneaky Exponential.* The Website of David P. Reed and his family. [Online] <http://www.reed.com/dpr/locus/gfn/reedslaw.html>.
- [5] **DE GHEIN, L.** *MPLS Fundamentals.* s.l. : Cisco Press, 2007. 1-58705-197-4
- [6] **ALVAREZ, S.** *QoS for IP/MPLS networks.* s.l. : Cisco Press, 2006. ISBN 1-58705-233-4.
- [7] **Cisco Systems, Inc.** *Any Transport over MPLS.* [dokument pdf] 2007.
- [8] **BENVENUTI, Ch.** *Understanding Linux Network Internals.* s.l. : O'Reilly Media, 2005. ISBN 0596002556.
- [9] **ODOM, W.; HEALY, R.; MEHTA, N.** *Směrování a přepínání sítí.* s.l. : Computer Press, 2009. 978-80-251-2520-5.
- [10] **ŠMRHA, P.; VERICH, J.** *QoS Design and Implementation in the CESNET2 MPLS-based Backbone.* s.l. : PB tisk, 2009. ISBN 978-80-904173-4-2.
- [11] **CHRIS.** *MPLS-TE and network traffic engineering.* *TechnologyInside.* [Online] [Dátum: 15. April 2011.] <http://technologyinside.com/2007/04/02/traffic-engineering-capacity-planning-and-mpls-te/>.
- [12] **KALUNGA, J.** *What is the role of teletraffic engineering in broadband networks?* Connexions®. [Online] Február 2006. <http://cnx.org/content/m13376/latest/>.

- [13] **Cisco Systems, Inc.** *OSPF Design Guide*. Cisco Systems. [Online] Aug 2005.
[Dátum: 28. April 2011.]
http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.shtml. Document ID: 7039.
- [14] **Cisco Systems, Inc.** *How Does Load Balancing Work?* [Online] August 2005.
[Dátum: 1. May 2011.]
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094820.shtml. Document ID: 5212.
- [15] **FORTZ, B.** *Internet Traffic Engineering by optimizing OSPF weights.*
- [16] **FORTZ, B.** *Traffic Engineering with traditional IP routing protocols.*
- [17] **ARGYRAKI, K.** *Loose source routing as mechanism for traffic policies.*
- [18] **ANDERSSON, L.; SWALLOW, G.** *RFC 3468: The Multiprotocol Label Switching (MPLS) Working Group decision on MPLS signaling protocols.* 2003.
- [19] **DOYLE, J.** *Understanding Signaling in MPLS Networks.* Network World. [Online] 27. March 2008. [Dátum: 5. May 2011.]
<http://www.networkworld.com/community/node/26395>.
- [20] **KATZ, D.; KOMPPELLA, K.; YEUNG, D.** *RFC 3630 - Traffic Engineering (TE) Extensions to OSPF Version 2.* 2003.
- [21] **OSBORNE, E.; SIMHA, A.** *Traffic Engineering with MPLS.* s.l. : Cisco Press, 2002.
ISBN 1-58705-031-5.
- [22] **Cisco Systems, Inc.** *How Does Unequal Cost Path Load Balancing (Variance) Work in IGRP and EIGRP?* [Online]
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a008009437d.shtml.
- [23] **Cisco Systems, Inc.** *MPLS VPN VRF Selection using Policy Based Routing.* Cisco Systems. [Online] 2007.
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_pbrsv.html.

[24] **AWDUCHE, D.; BERGER, L.; GAN, D.** *RFC 3209 - RSVP-TE: Extensions to RSVP for LSP Tunnels*. The Internet Engineering Task Force (IETF). [Online] December 2001. <http://tools.ietf.org/html/rfc3209>.

ZOZNAM POUŽITÝCH SKRATIEK

ATM	-	Asynchronou Transfer Mode
BGP	-	Border Gateway Protocol
CDP	-	Cisco Discovery Protocol
CE	-	Customer Edge
CR LDP	-	Constraint-based Routing Label Distribution Protocol
CSPF	-	Constrained Shortest Path First
DiffServ	-	Differentiated Services
DSCP	-	Differentiated Services Code Point
EIGRP	-	Enhanced Interior Gateway Routing Protocol
EXP	-	Experimental
FIB	-	Forwarding Information Base
ftp	-	file transfer protocol
http	-	hypertext transport protocol
IETF	-	Internet Engineering Task Force
IntServ	-	Integrated services
IOS	-	Internetwork Operating System
IP	-	Internet Protocol
IS-IS	-	Intermediate System – Intermediate System
ISO OSI	-	International Organization for Standardization Open Systems Interconnection
LDP	-	Label Distribution Protocol
LER	-	Label Edge Router
LFIB	-	Label Forwarding Information Base
LIB	-	Label Information Base
LIFO	-	Last in-First out
LSP	-	Label Switched Path
LSR	-	Label Switched Router
LSRR	-	Loose Source and Record Route
MPLS	-	Multiprotocol Label Switching
OSPF	-	Open Shortest Path First
PBR	-	Policy Based Routing

PE	-	Provider Edge
PVC	-	Private Virtual Circuit
QoS	-	Quality of Service
RD	-	Route Distinguisher
RIP	-	Routing Information Protocol
RSVP	-	Resource Reservation Protocol
SPF	-	Shortest Path First
SSRR	-	Strict Source and Record Route
SVI	-	Switch Virtual Interface
TE	-	Traffic Engineering
TTL	-	Time to Live
VC	-	Virtual Circuit
VLAN	-	Virtual LAN
VoIP	-	Voice over IP
VPN	-	Virtual Private Network
VRF	-	Virtual Routing and Forwarding
WAN	-	Wide Area Network

PRÍLOHY:

A1: PATTERN FTP PREMÁVKY

A2: PATTERN HTTP PREMÁVKY

A3: PATTERN VIDEO PREMÁVKY

A4: PATTERN VOICE PREMÁVKY

A5: PROSTREDIE PRACOVNEJ PLOCHY SERVERA

A6: PROSTREDIE PRACOVNEJ PLOCHY KLIENTA

Realtek RTL8139/810x Family Fast Ethernet NIC - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: not icmp && not arp && not stp && not cdp && not loop && not dhcpv6

No.	Time	Source	Destination	Protocol	Info
63623	14.349825	192.168.1.11	192.168.2.11	FTP-DATA	FTP Data: 824 bytes
63624	14.354039	192.168.1.11	192.168.2.11	FTP-DATA	FTP Data: 1452 bytes
63625	14.354113	192.168.2.11	192.168.1.11	TCP	50397 > 50676 [ACK] Seq=1 Ack=60392877 Win=4194304 Len=0
63626	14.354155	192.168.1.11	192.168.2.11	FTP-DATA	FTP Data: 1452 bytes
63627	14.354276	192.168.1.11	192.168.2.11	FTP-DATA	FTP Data: 1452 bytes
63628	14.354313	192.168.2.11	192.168.1.11	TCP	50397 > 50676 [ACK] Seq=1 Ack=60395781 Win=4194304 Len=0
63629	14.354399	192.168.1.11	192.168.2.11	FTP-DATA	FTP Data: 1452 bytes
63630	14.354522	192.168.1.11	192.168.2.11	FTP-DATA	FTP Data: 1452 bytes
63631	14.354565	192.168.2.11	192.168.1.11	TCP	50397 > 50676 [ACK] Seq=1 Ack=60398685 Win=4194304 Len=0
63632	14.354643	192.168.1.11	192.168.2.11	FTP-DATA	FTP Data: 1452 bytes
63633	14.354769	192.168.1.11	192.168.2.11	FTP-DATA	FTP Data: 1452 bytes
63634	14.354808	192.168.2.11	192.168.1.11	TCP	50397 > 50676 [ACK] Seq=1 Ack=60401589 Win=4194304 Len=0
63635	14.354892	192.168.1.11	192.168.2.11	FTP-DATA	FTP Data: 1452 bytes
63636	14.355015	192.168.1.11	192.168.2.11	FTP-DATA	FTP Data: 1452 bytes

Frame 63630: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits)

Ethernet II, Src: Cisco_09:2e:f8 (00:18:ba:09:2e:f8), Dst: Micromet_0e:bd:da (00:11:3b:0e:bd:da)

Internet Protocol, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.2.11 (192.168.2.11)

Transmission Control Protocol, Src Port: 50676 (50676), Dst Port: 50397 (50397), Seq: 60397233, Ack: 1, Len: 1452

Source port: 50676 (50676)

Destination port: 50397 (50397)

[Stream index: 2]

Sequence number: 60397233 (relative sequence number)

[Next sequence number: 60398685 (relative sequence number)]

Acknowledgement number: 1 (relative ack number)

Header length: 20 bytes

Flags: 0x10 (ACK)

Window size: 66560 (scaled)

Checksum: 0xf8c3 [validation disabled]

[SEQ/ACK analysis]

FTP Data

[truncated] FTP Data: \016\221P\225_\270\2a-\213\303\220,\322w\003\80Q\244\367\264\217\274\240G\373\224\321p8+\300\0\360\360d\3059\037\261G\307\200\245\036\017\276\004\225\352\212\217*\0021\

```

0030 01 04 f8 c3 00 00 be 91 50 95 5f b8 07 7e 8b c3 .....P.....
0040 90 3c 58 02 77 03 0a 25 31 34 47 b4 09 8f 0a bc .....v.w.x.0.....
0050 a0 87 fb 94 d1 70 38 2b c0 29 4f f0 f0 64 c5 39 .....0...p8+ )0...d.9
0060 1f b1 47 c7 80 a5 1e 0f be 04 95 ea 8a 8f 2a 02 .....G.....*
0070 49 f1 e3 78 c4 29 69 0d 42 72 68 24 b7 92 d8 dd .....I..x.)i. Brh$. ...
0080 40 f0 a8 d3 76 a8 e4 e7 38 f9 3d b4 dc e0 c0 ab .....[...].8.....
0090 e1 de 4e 69 95 73 9e 6d cd ef ef 6f ba 9f 6f 7d .....Ni.Sm...o.rpt
00a0 dc ac 6e 74 dd bd 6d ed 6f 6b 7f de 5d 4d c0 d3 .....rnt..m. ok..M.
00b0 ae c6 c6 f4 71 b8 f3 9c 3d e8 d0 d8 8e 1d 73 63 .....q...=...sc
00c0 57 bc 9e 9d dc 35 68 26 48 7c 3b dd a7 34 ec 19 .....w...5h& H|;..4..
00d0 24 12 78 04 d8 ce 23 8c 9d 3b 8d 27 b9 ce 72 2c .....S.X...#. .|. .P.
00e0 32 70 64 a8 e8 77 47 b9 ce a1 1d fb 74 0d 31 cb .....2p...wG...2..1.
00f0 3d cc 6e ef 74 eb ee ff a9 64 be 7a ae ff 79 .....n..n. d.zzz..p
0100 0b a7 e7 9b 19 78 f8 06 09 3c 12 07 e0 c0 e0 a5 .....X...<.....p
0110 e5 41 98 42 1f 5d 55 e6 98 05 9a 2d 00 c2 af d0 .....A.B.]U... ..
0120 4e 4f 00 c0 88 24 f8 21 17 7c 7e ac 46 f7 75 b1 .....NO...S.! |.-.F.u.
0130 80 07 00 70 3f 7c 0f be a0 a1 1d fb 74 0d 31 cb .....p?|... ..t.1.
0140 d1 d8 8e 82 18 04 00 3e ac 0f 2d d5 63 80 27 78 .....6.....-c..w
0150 0e 84 98 bc 48 9e 1d ab 56 06 bc da 74 c9 56 a8 .....H...V...t.V.
0160 cc 25 6c 03 68 38 e8 bb 04 32 f6 c1 d2 03 8d ca .....&l.h8...R.....
0170 b4 1c 9f 42 62 ff d5 3d 11 6a 05 07 40 63 23 15 .....Bb..=..j..0c#.
0180 08 6a d7 81 b5 04 c0 4c 1a 08 e4 ca cb bc a6 ac .....j.....l
0190 ab dd 57 40 b4 29 30 24 ff e0 f6 5c c2 b7 ca ae .....MB.J0$ ..\.....
01a0 03 ee 71 57 f9 dc dd 24 78 3a a1 06 81 fd f0 29 .....oW...$ xi.....

```

Text item (text), 1452 bytes

Packets: 118159 Displayed: 118141 Marked: 0 Dropped: 0

Profile: Default

SK 21:45 29.5.2011

~ 56 ~

Realtek RTL8139/810x Family Fast Ethernet NIC - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: not icmp && not arp && not stp && not cdp && not loop && not dhcpv6

No.	Time	Source	Destination	Protocol	Info
2266	6.706643	192.168.1.11	192.168.2.11	TCP	[TCP segment of a reassembled PDU]
2267	6.706690	192.168.2.11	192.168.1.11	TCP	50394 > http [ACK] Seq=468 Ack=2140465 Win=211700 Len=0
2268	6.706767	192.168.1.11	192.168.2.11	TCP	[TCP segment of a reassembled PDU]
2269	6.706906	192.168.1.11	192.168.2.11	TCP	[TCP segment of a reassembled PDU]
2270	6.706954	192.168.2.11	192.168.1.11	TCP	50394 > http [ACK] Seq=468 Ack=2143369 Win=211700 Len=0
2271	6.707031	192.168.1.11	192.168.2.11	TCP	[TCP segment of a reassembled PDU]
2272	6.707154	192.168.1.11	192.168.2.11	TCP	[TCP segment of a reassembled PDU]
2273	6.707207	192.168.2.11	192.168.1.11	TCP	50394 > http [ACK] Seq=468 Ack=2146273 Win=211700 Len=0
2274	6.707278	192.168.1.11	192.168.2.11	TCP	[TCP segment of a reassembled PDU]
2275	6.707400	192.168.1.11	192.168.2.11	TCP	[TCP segment of a reassembled PDU]
2276	6.707450	192.168.2.11	192.168.1.11	TCP	50394 > http [ACK] Seq=468 Ack=2149177 Win=211700 Len=0
2277	6.707523	192.168.1.11	192.168.2.11	TCP	[TCP segment of a reassembled PDU]
2278	6.707646	192.168.1.11	192.168.2.11	TCP	[TCP segment of a reassembled PDU]
2279	6.707895	192.168.2.11	192.168.1.11	TCP	50394 > http [ACK] Seq=468 Ack=2152081 Win=208796 Len=0

Frame 2274: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits)

- Ethernet II, Src: Cisco_09:2e:f8 (00:18:ba:09:2e:f8), Dst: Micronet_0e:bd:da (00:11:3b:0e:bd:da)
- Internet Protocol, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.2.11 (192.168.2.11)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 50394 (50394), Seq: 2146273, Ack: 468, Len: 1452
 - Source port: http (80)
 - Destination port: 50394 (50394)
 - [Stream index: 0]
 - Sequence number: 2146273 (relative sequence number)
 - [Next sequence number: 2147725 (relative sequence number)]
 - Acknowledgement number: 468 (relative ack number)
 - Header length: 20 bytes
 - Flags: 0x10 (ACK)
 - Window size: 65536 (scaled)
 - Checksum: 0x6f8a [validation disabled]
 - [Good Checksum: False]
 - [Bad Checksum: False]
 - [SEQ/ACK analysis]
 - [Number of bytes in flight: 1452]

TCP segment data (1452 bytes)

```

0030 01 00 6f 8a 00 00 b9 3f a8 84 94 52 a8 b9 4c 5d ..O...?...R..L
0040 07 1b 5c 6e 1f 19 7b 9d 05 89 3a 71 89 63 6d 27 [N]...[...q...m]
0050 47 e6 9e 0d 2d bb 8b 13 17 e9 37 37 3a db 71 e6 G]...-...77:..qf
0060 b6 31 b0 67 ba a7 eb 7a 9e f8 1b bd 36 79 3a fd .1.g...z...6y..
0070 6e 9e 1f 2b 03 aa fc a9 89 df 8b be 6c 79 e5 db n.+... ..ly..
0080 04 77 49 c9 df f0 70 8a 47 7d b4 3c e9 58 50 5e .w]...p.g]...zXP
0090 12 2b 0e 52 e3 66 35 a1 45 88 08 27 9d 3d 57 d9 +.R..5.E...+m
00a0 ef 51 1b 78 2e 09 ab 47 8b a3 d1 f8 79 1a 26 08 .Q.X...G...y..&
00b0 8b 3a d8 ad 3d 5f fa 55 50 32 8c 5d 41 27 fd c6 ..=..U P2.]A...
00c0 d3 a6 42 91 26 bc a7 1b 0a d0 b0 be 8a 0c db de ..B.&.....
00d0 e1 86 c3 c7 f7 93 57 cb ab a6 18 fd bd c4 03 71 .....W.....G
00e0 89 f4 06 0e e5 18 9f 7f ad e2 5c 83 70 37 1d .....U... \p]
00f0 89 b1 78 e4 93 29 06 68 74 34 4f 03 ca f5 4a .x.Y]..h...40...J
0100 2c 8b 51 f4 b4 56 20 f1 72 73 e8 bc 3e 47 4e 0a .KQ.V...ps..SGN
0110 2b de a8 2e 67 5c 70 07 c6 e7 8b de 4e ae e7 13 +..g\p...N...
0120 df b6 e9 cc ac 81 9e 0d 9e ec e8 0d 94 e5 c3 e4 .....
0130 e9 00 77 bd ff 7d a0 39 8b f7 58 48 47 e6 89 58 .w...e...XHG..X
0140 86 8b 93 04 98 26 1f 2a db ed d8 22 2b 19 90 d6 ....&...*...YB
0150 32 78 1f 21 d8 ca 7d e8 6c fd 6c 55 36 f7 6a 6c 2x]...]...1..6..j]
0160 b9 23 cc 64 b4 a3 e2 e9 00 e0 b5 53 0a 13 f3 4a .#.d... ..S...J
0170 be b1 21 35 43 b5 20 b2 0f e1 41 0f 45 6f 71 3d .]SC... ..A.E.=
0180 41 db 08 38 c0 38 b4 47 d9 5a 21 23 32 19 aa ce A..8..G..ZI#2...
0190 99 27 ab 47 ab c2 e2 a0 0a 11 d6 b1 0f c1 e7 0a .:G... ..
01a0 7b e9 f0 0a 23 86 ad ef 34 3f 41 cb 1b 47 7f 5f ...%...T.A..G..

```

Text item (text), 1452 bytes

Packets: 6134 Displayed: 6089 Marked: 0 Dropped: 0

Profile: Default

SK 21:43 29.5.2011

~ 57 ~

Realtek RTL8139/810x Family Fast Ethernet NIC (net (ip port: 3289)) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filters: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
6794	5.835460	192.168.1.11	192.168.2.11	UDP	Source port: 50782 Destination port: avt-profile-1
6795	5.835571	192.168.1.11	192.168.2.11	UDP	Source port: 50782 Destination port: avt-profile-1
6796	5.833887	192.168.1.11	192.168.2.11	UDP	Source port: 50782 Destination port: avt-profile-1
6797	5.840005	192.168.1.11	192.168.2.11	UDP	Source port: 50782 Destination port: avt-profile-1
6799	5.840113	192.168.1.11	192.168.2.11	UDP	Source port: 50782 Destination port: avt-profile-1
6800	5.840228	192.168.1.11	192.168.2.11	UDP	Source port: 50782 Destination port: avt-profile-1
6801	5.840337	192.168.1.11	192.168.2.11	UDP	Source port: 50782 Destination port: avt-profile-1
6802	5.840451	192.168.1.11	192.168.2.11	UDP	Source port: 50782 Destination port: avt-profile-1
6803	5.844902	192.168.1.11	192.168.2.11	UDP	Source port: 50782 Destination port: avt-profile-1
6804	5.845013	192.168.1.11	192.168.2.11	UDP	Source port: 50782 Destination port: avt-profile-1
6805	5.845126	192.168.1.11	192.168.2.11	UDP	Source port: 50782 Destination port: avt-profile-1
6806	5.845238	192.168.1.11	192.168.2.11	UDP	Source port: 50782 Destination port: avt-profile-1

Frame 6799: 1370 bytes on wire (10960 bits), 1370 bytes captured (10960 bits) on interface 0

Ethernet II, Src: Cisco09:2e:f8 (00:18:b8:09:2e:f8), Dst: Micronet_0e:b4:da (00:11:3b:0e:b4:da)

Internet Protocol, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.2.11 (192.168.2.11)

Version: 4

Header Length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 1356

Identification: 0x6b28 (27432)

Flags: 0x00

Fragment offset: 0

Time to live: 123

Protocol: UDP (17)

Header checksum: 0x4b12 [correct]

Source: 192.168.1.11 (192.168.1.11)

Destination: 192.168.2.11 (192.168.2.11)

User Datagram Protocol, Src Port: 50782 (50782), Dst Port: 50782 (50782)

Source port: 50782 (50782)

Destination port: avt-profile-1 (5004)

Length: 1336

Checksum: 0x5ede [validation disabled]

Data (1328 bytes)

Data: 80a1dc307af6c415846700004700611e1b1620af41c30831... [Length: 1328]

```

0040 02 06 c6 5e 13 8c 05 38 5e 6e 80 a1 6c 30 7a f8
0044 15 84 67 00 00 47 00 61 1e b3 16 20 af 41 c3
0048 11 30 69 77 ea 78 c4 85 89 9c 80 90 02 db
004c 49 36 75 9a 28 63 dd 0f 52 3a 7d 50 af 6a 82
0050 ca 57 06 7c 23 06 0f 12 b4 8f d8 db 5f 9f 46 a2
0054 48 0d 0c 4d 48 92 25 78 76 ab 55 7f 10 b7 0b 2e
0058 00 de 74 8f c5 26 45 07 41 e2 bf 02 89 56 89 62
005c 00 56 1e 59 70 0f ec 78 25 2d 82 8e 45 63 6f
0060 00 56 1e 59 70 0f ec 78 25 2d 82 8e 45 63 6f
0064 78 9c 72 8c a9 c9 00 23 09 53 3d 45 76 7d 13 c8
0068 25 11 14 43 2a 8d 27 0f 57 01 0b cd 95 65 18 d4
006c fd a1 6c 01 75 27 88 b8 16 80 0b b3 55 9e 8f 82
0070 18 8a 47 00 61 4f 55 42 45 89 85 f2 83 6d 84 02
0074 05 8a 47 00 61 4f 55 42 45 89 85 f2 83 6d 84 02
0078 05 8a 47 00 61 4f 55 42 45 89 85 f2 83 6d 84 02
0084 72 8a 83 f8 f9 81 0a b8 8a 94 f8 e1 c0 1b 34 16
0088 00 04 e9 40 28 85 79 b9 a7 90 f8 9f 8d 6f 10 91
0094 eb 52 50 5d a3 ec 7a 66 c0 91 7a 56 12 09 23
0098 18 06 23 0a 85 87 3a e3 58 64 48 15 6d 5e 29 28
  
```

Data (d30a.d30a)... 1328 bytes | Packets: 9538 Displayed: 9538 (Filtered: 0 Dropped: 0)

Profile: Default

SK

21:30 29.5.2011

Realtek RTL8139/810x Family Fast Ethernet NIC - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: not icmp && not arp && not stp && not cdp && not loop && not dhcpv6

No.	Time	Source	Destination	Protocol	Info
5	4.518466	192.168.2.11	192.168.1.11	SIP/SDP	Request: INVITE sip:192.168.1.11, with session description
6	4.522247	192.168.1.11	192.168.2.11	SIP	Status: 100 Trying
7	4.522248	192.168.1.11	192.168.2.11	SIP	Status: 101 Dialog Establishment
8	4.531245	192.168.1.11	192.168.2.11	SIP	Request: OPTIONS sip:192.168.2.11:5060
11	4.561962	192.168.2.11	192.168.1.11	SIP	Status: 501 Not Implemented
12	4.570949	192.168.1.11	192.168.2.11	SIP	Status: 180 Ringing
19	12.623838	192.168.1.11	192.168.2.11	SIP/SDP	Status: 200 OK, with session description
20	12.625884	192.168.2.11	192.168.1.11	SIP	Request: ACK sip:192.168.1.11
21	12.731213	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=0, Time=400
22	12.731214	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=1, Time=560
23	12.761158	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=2, Time=720
24	12.761177	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=3, Time=880
25	12.817110	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=4, Time=1040
26	12.817111	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=5, Time=1200
27	12.847170	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=6, Time=1360
28	12.847172	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=7, Time=1520
29	12.857098	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=8, Time=1680
30	12.857119	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=9, Time=1840
31	12.927126	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=10, Time=2000
32	12.927128	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=11, Time=2160
33	12.967578	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=12, Time=2320
34	12.967580	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=13, Time=2480
35	13.007161	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=14, Time=2640
36	13.007162	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=15, Time=2800
37	13.047112	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=16, Time=2960
38	13.047113	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=17, Time=3120
39	13.037099	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=18, Time=3280
40	13.037100	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=19, Time=3440
41	13.127189	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=20, Time=3600
42	13.127190	192.168.1.11	192.168.2.11	RTP	PT=ITU-T G.711 PCMA, SSRC=0x22B, Seq=21, Time=3760

Frame 31: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0

- Ethernet II, Src: Cisco_09:2e:f8 (00:18:ba:09:2e:f8), Dst: Micronet_0e:bd:ida (00:11:3b:0e:bd:ida)
- Internet Protocol, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.2.11 (192.168.2.11)
- User Datagram Protocol, Src Port: 7078 (7078), Dst Port: 49158 (49158)
- Real-Time Transport Protocol
 - [Stream setup by SDP (frame 5)]

```

0000 00 11 3b 0e bd da 00 18 ba 09 2e f8 08 00 45 00  ...:.....E.
0010 00 c8 0a 61 00 00 7b 11 b0 5d c0 a8 01 0b c0 a8  ...a.[.].....
0020 02 0b 1b a6 c0 06 00 b4 1c 04 80 08 00 0a 00 00  ...+..hg.v.....
0030 07 00 00 00 02 2b 17 17 68 57 7f 76 d5 d6 c8 e0  ...+..Sxv.....
0040 ef 95 94 97 e8 e6 e5 f2 53 76 6e 17 12 1e 1b    ...od.H.....
0050 18 1e 19 19 1e 10 6f 64 48 c8 e7 e2 ed 94 92 9f  ...od.H.....
0060 9c 92 92 9d 92 9c 9e 92 96 e9 e0 f3 58 70 60    .....>P
0070 16 1e 19 19 1a 1e 1d 13 14 67 51 c7 f8 ed 94 90  ...g.....
0080 91 92 9c 82 97 ec f1 50 73 52 68 69 69 15 11 16  ...P sbmih.....
0090 16 14 69 6d 6e 62 61 65 4b 51 44 c3 e4 e8 94 97  ...tim'bae kq....
00a0 94 96 91 97 97 eb ef e5 5e 7d 67 6d 6e 68 14    .....}gmnh.
00b0 11 16 11 6a 66 72 49 53 d5 c2 e6 e2 ec 94 91 96  ...}frIS .....
00c0 96 90 91 eb fa c3 dc 58 43 41 53 4f 7d 73 71 65  ...X CASO}sqe
00d0 60 62 62 67 7c 7a                                bbg|z

```

File: C:\Users\student\AppData\Local\Temp\wir... Packets: 756 Displayed: 726 Marked: 0 Dropped: 0 Profile: Default

~ 59 ~

~ 60 ~

The screenshot displays a Windows desktop environment with several applications running:

- Linphone:** A SIP client window showing a call in progress to an unknown number (sip:192.168.2.11) with a duration of 00:13:03. It includes buttons for 'Ztlumit' (End Call) and 'Odložit' (Pause).
- Streamování - Multimediální přehrávač VLC:** A VLC media player window showing a playlist with one item titled 'Streamování' with a duration of 10:53. The playback progress is at 06:55/10:53.
- FileZilla Server (127.0.0.1):** A terminal window showing the output of an FTP session. The logs indicate a successful connection and file transfer of ED_HD.avi (627,539,968 bytes) at 7.4 MB/s. A table below summarizes the transfer details.
- Command Prompt:** A terminal window showing the output of a 'tracert' command to 172.16.2.11, displaying a 5-hop route with round-trip times.

ID	Account	IP	Transfer	Progress	Speed
-C>000006	ftp_user	192.168.2.11			
-E>000013	ftp_user	192.168.2.11	/ED_HD.avi	627 539 968 bytes (73.4%)	7.4 MB/s

	1	2	3	4	5
Time	4 ms	6 ms	3 ms	4 ms	5 ms
Source	1 ms	1 ms	2 ms	6 ms	1 ms
Destination	3 ms	2 ms	3 ms	2 ms	5 ms
Address	192.168.1.1	172.16.1.1	10.1.1.2	172.16.2.1	172.16.2.11

A5

The screenshot displays a Windows desktop environment with several active windows:

- Opera Browser:** Shows a download progress for 'ED_HD.avi' (815,0 MB, 29.5% complete, 630,7 KB/s).
- sJphone:** A VoIP application window showing a call to 192.168.1.11.
- Command Prompt:** Displays the output of a traceroute command to 192.168.1.11, showing a path through several hops with low latency.
- LAN Monitor:** A network monitoring tool showing a graph of network activity.
- VLC Media Player:** Playing a video clip from the URL 'rtsp://192.168.2.11:5004 - Multimediální přehrávač VLC'.
- FileZilla:** An FTP client window showing a connection to 192.168.1.11. The local directory 'C:\Users\student\Desktop\ftpget\' contains files 'ED_1024.avi' and 'ED_HD.avi'. The remote directory '/' contains 'ED_1024...' and 'ED_HD.avi'. A progress bar indicates the transfer of 'ED_HD.avi' is 79.0% complete.