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

TECHNOLOGIE MULTIPROTOCOL LABEL SWITCHING V SÍTÍCH ETHERNET

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

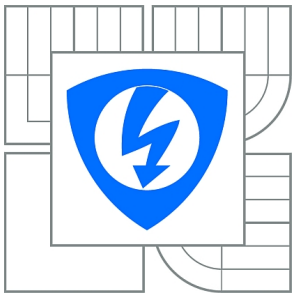
AUTOR PRÁCE
AUTHOR

Bc. MARTIN KIŠKA

BRNO 2014

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

TECHNOLOGIE MULTIPROTOCOL LABEL SWITCHING V SÍTÍCH ETHERNET

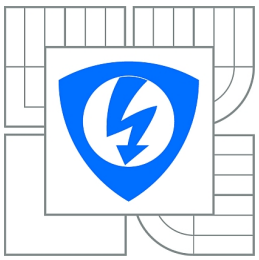
MULTIPROTOCOL LABEL SWITCHING TECHNOLOGY IN ETHERNET NETWORKS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. MARTIN KIŠKA
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. VÍT NOVOTNÝ, Ph.D.
SUPERVISOR

BRNO 2014



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Martin Kiška	***ID:***	128127
Ročník:	2	***Akademický rok:***	2013/2014

NÁZEV TÉMATU:

Technologie MultiProtocol Label Switching v sítích Ethernet

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s technologií MPLS transportu, prostudujte možnosti stavby vícevrstvých Ethernet sítí (Access, Agregation, Core) s využitím MPLS z pohledu zajištění redundancí a QoS pro přenosy IP CCTV a VoIP. Proveďte rozbor možností redundantního připojení agregační vrstvy k páteřní s využitím a bez využití technologie MPLS a posuďte použitelnost variant z pohledu tunelování L2/L3 provozu externích uživatelů. Na základě nabytých zkušeností navrhněte laboratorní úlohu pro předmět Architektura sítí. Zároveň aplikujte jednotlivé modely L2/L3 tunelování na zkušební síti a porovnejte jejich vlastnosti.

DOPORUČENÁ LITERATURA:

[1] DE GHEIN, Luc. MPLS Fundamentals. Indianapolis: Cisco Press, 2007, 672 s. ISBN 1-58705-197-4
[2] GUICHARD, Jim, Ivan PEPELNJAK a Jeff APCAR. MPLS and VPN architectures. Indianapolis: Cisco Press, c2003, 470 s. ISBN 1-5870-5112-5.

Termín zadání:	10.2.2014	***Termín odevzdání:***	28.5.2014

Vedoucí práce: doc. Ing. Vít Novotný, Ph.D.
Konzultanti diplomové práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

V úvodu práce jsou rozebrány důvody pro přechod ze starších technologií na sítě s podporou MultiProtocol Label Switching, které umožňují jednoduchou rozšiřitelnost sítě. V teoretické části jsou zkoumány základní principy této technologie a jejich praktické využití pro poskytování privátních síti zákazníkům přes síť poskytovatele. V praktické části jsou jednotlivé principy rozebrány s analýzou paketů. Společně s tím jsou veškeré technologie otestované na skutečné síti. Nabyté zkušenosti během diplomové práce byly zhodnoceny při vytváření laboratorní úlohy zaměřené na posluchače předmětu Architektura sítí na bakalářském studiu.

KLÍČOVÁ SLOVA

MPLS, LDP, LSR, LSP, VPLS, VPN, VRF, QoS

ABSTRACT

In the introduction of this thesis the reasons for transition from older to a new technology called MultiProtocol Label Switching are mentioned – the modern technology enables simple network extension. The theoretical part contains basic principles of this technology and their practical application for supplying private networks to the customers using provider's network. In practical part packets are analyzed considering the theory. In addition. All the technologies tested on a real network. Experience gained while working on this thesis are assessed during creating laboratory task for class Architecture of Networks intended for students of Bachelor's study programme.

KEYWORDS

MPLS, LDP, LSR, LSP, VPLS, VPN, VRF, QoS

KIŠKA, Martin *Technologie MultiProtocol Label Switching v sítích Ethernet*: semestrální projekt. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2013. 71 s. Vedoucí práce byl doc. Ing. Vít Novotný, PhD.

PROHLÁŠENÍ

Prohlašuji, že svůj semestrální projekt na téma „Technologie MultiProtocol Label Switching v sítích Ethernet“ jsem vypracoval samostatně pod vedením vedoucího semestrálního projektu a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedeného semestrálního projektu dále prohlašuji, že v souvislosti s vytvořením tohoto semestrálního projektu jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu doc. Ing. Vítu Novotnému Ph.D. za odborné vedení a doc. Ing. Františku Urbanovi CSc. za konzultace, podnětné návrhy k práci a zapůjčení přístroje Brocade CER 2024. Dále bych rád poděkoval panu Ing. Radku Krkošovi za spolupráci během vytváření laboratorní úlohy a poskytnutí virtuálního operačního systému. Poděkování také patří Mgr. Lukáši Krasňanovi za zapůjčení zařízení Juniper SRX100 a Cisco Catalyst 6500.

Brno ....

(podpis autora)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Technicka 12, CZ-61600 Brno
Czech Republic
http://www.six.feec.vutbr.cz

PODĚKOVÁNÍ

Výzkum popsaný v tomto semestrálním projektu byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .
(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Cílem této práce je seznámit čtenáře s technologií MPLS, která se využívá u transportních sítí poskytovatelů. K této technologii se přechází již od zastaralých Asynchronous Transport Machine (ATM) a Frame-relay (FR), které svou koncepcí nevyhovují nynějším požadavkům a trendům. V úvodních kapitolách je rozebrán základní princip výměny návěští (labelů) v návaznosti na životnost paketů a podporu kvality služeb. Zrovna poslední zmíněné – podpora kvality služeb má různé způsoby aplikace, přičemž chování vůči síti je odlišné a je důležité tyto rozdíly znát.

Taktéž se práce zabývá fragmetováním a limitem MTU při použití MPLS. Po teoretickém rozboru návěští MPLS se dostaneme k protokolu, který se zabývá distribucí těchto štítků mezi jednotlivými směrovači. Následně budou probrány možnosti tunelování L2 a L3 provozu přes MPLS síť.

Výsledkem diplomové práce je laboratorní úloha, v niž si studenti osvojí základní principy MPLS sítě, kterými je výměna (swap), přidání (push) nebo odebrání (pop) návěští. Studenty se snažím zaujmout možností sledování paketů s MPLS návěštím a jejich víceré zapouzdření pro poskytování privátních sítí zákazníkům a to tak, aby jejich data byla striktně oddělena a nemohlo tak dojít k odposlouchávání.

V praktické části je věnována pozornost vyzkoušení jednotlivých teoretických vlastností a jejich otestování jak ve virtualizovaném prostředí, tak na skutečných zařízeních od různých výrobců (Brocade, Juniper, MikroTik a Cisco).

1 ŘEŠENÍ STUDENTSKÉ PRÁCE

1.1 Úvod

Mnoho let byly pro transportní účely na WAN sítích používané dnes již zastaralé protokoly jako Asynchronous Transport Machine (ATM) a Frame-relay (FR). S příchodem MPLS došlo ke zjednodušení vybudování komplexní sítě nad jednou infrastrukturou. Jednoduchost při zavádění se setkala s velkým úspěchem u poskytovatelů. Ti tak mohli nabídnout svým zákazníkům výhody MultiProtocol Label Switching (MPLS) sítě a získat tak výhodu nad konkurencí.

Počáteční výhody MPLS tkvěly v myšlence jednoduché záměny návěští na vstupním a výstupním rozhraní. Tento princip měl ulehčit prohledávání Internet Protocol (IP) směrovacích tabulek a urychlit celý proces směrování. Postupem času došlo ke zlepšení výkonu páteřních směrovacích směrovačů a smazala se tak tato výhoda. Nicméně vývoj MPLS pokračoval a byly vyvinuty další možnosti aplikace. Některé z nich jsou rozebrány ve zbytku práce. MPLS bylo stvořeno pro transport vyšších protokolů přes páteřní síť poskytovatele. Můžeme pomoci něj přenést například tyto protokoly – IPv4, IPv6, Ethernet, High-Level Data Link Control (HDLC), Point-to-Point Protocol (PPP) a další. Této schopnosti se říká Any Transport over MPLS (AToM). Směrovače nepotřebují znát obsah vlastního paketu, stačí jen vědět, které návěští mají vyměnit za které.

Možnou aplikací těchto principů je např. Traffic Engineering (TE), Ethernet over MPLS (EoMPLS), MPLS Virtual private Network (MPLS VPN), Virtual Private LAN Services (VPLS), Virtual Leased Line (VLL) a další. Neméně důležitou výhodou je možnost mít páteřní síť bez spěrovacího protokolu BGP.

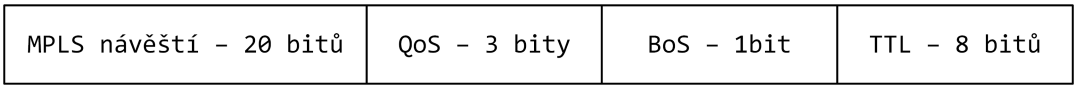
Výhodou MPLS je, že počet návěští v zásobníku (stacku) není omezen. Tímto způsobem mohou být poskytovány privátní sítě.

Pro správnou funkčnost postačí technologii MPLS tři základní operace, mezi které patří swap, push a pop. Jedná se o záměnu, přidání nebo odebrání návěští. Vždy poslední návěští z nich má nastaven bit Bottom of Stack (BoS) na 1, tím naznačuje, že je poslední a že se pod ním již skrývá transportovaný protokol.

1.2 Rozbor MPLS návěští

MPLS záhlaví se skládá z 32 bitů. 20 jich je předurčeno pro číslování návěští. Další bity jsou určeny pro Quality of Services (QoS, 3 bity), Time to Live (TTL, 8 bitů) a 1 bit Bottom of Stack (BoS), který zaručí, že návěští je posledním v zásobníku (bit je nastavený na hodnotu 1). Ačkoliv v původním RFC 3032 se tři bity pro

QoS jmenovaly jako experimentální (EXP), postupem času je všichni výrobci začali využívat pro zavedení QoS. Tudíž v novějším RFC 5462 je definováno využití těchto tří bitů právě pro QoS (skladbu MPLS návěští můžete vidět na obrázku 1.1).



Obr. 1.1: Tvar návěští MPLS.

Základní princip MPLS tehchnologie je ve výměně návěští. Může dojít ke třem různým operacím:

- Swap (záměna) – dojde k záměně jednoho návěští za druhé.
- Pop (odebrání) – z původního paketu je odebráno jedno návěští a zbude jen transportovaný protokol, nebo po odebrání zůstane ještě jedno návěští (či více).
- Push (přidání) – k původnímu paketu se přidá nové návěští nebo už ke stávajícím návěští je přidáno další.

Ukázku můžete sledovat na obr. 1.2.

U MPLS je důležité rozlišovat význam zkratek, které ve zbytku textu budu uvádět. Nyní zde uvedu základní zkratky, které s MPLS souvisí. Popis, která zkratka souvisí s jakým významem je nejlépe patrný na obrázku 1.3.

- Label Distribution Protocol (LDP) – slouží pro distribuci návěští mezi ostatní směrovače, které podporují MPLS.
- Label Switching Router (LSR) – každý směrovač, na kterém je spuštěné LDP.
- Label Switched Path (LSP) – cesta k cíli, při které dochází k záměně návěští.

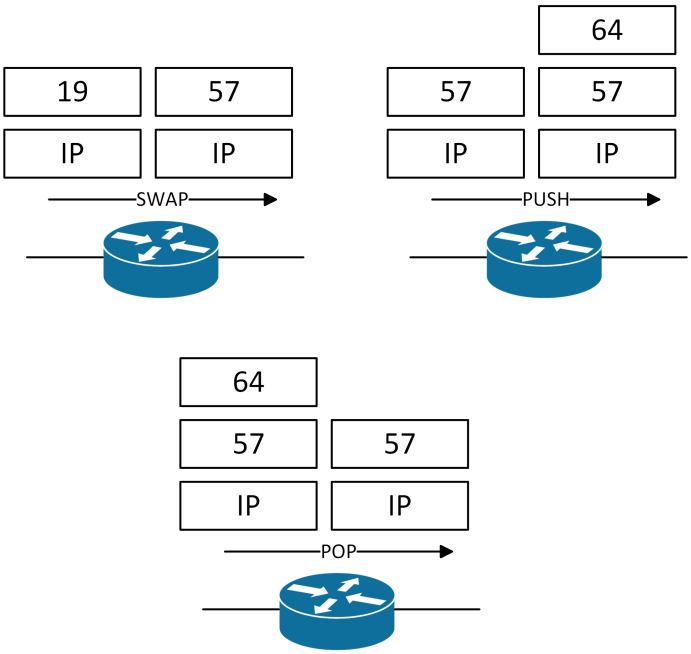
Je důležité si uvědomit, kde se návěští MPLS v celém paketu nachází, to lze vidět na obrázku 1.4. Již v ethernet rámci je stanoveno v poli Ethertyp hex hodnota 8847, která naznačuje přítomnost MPLS návěští.

1.2.1 MPLS návěští

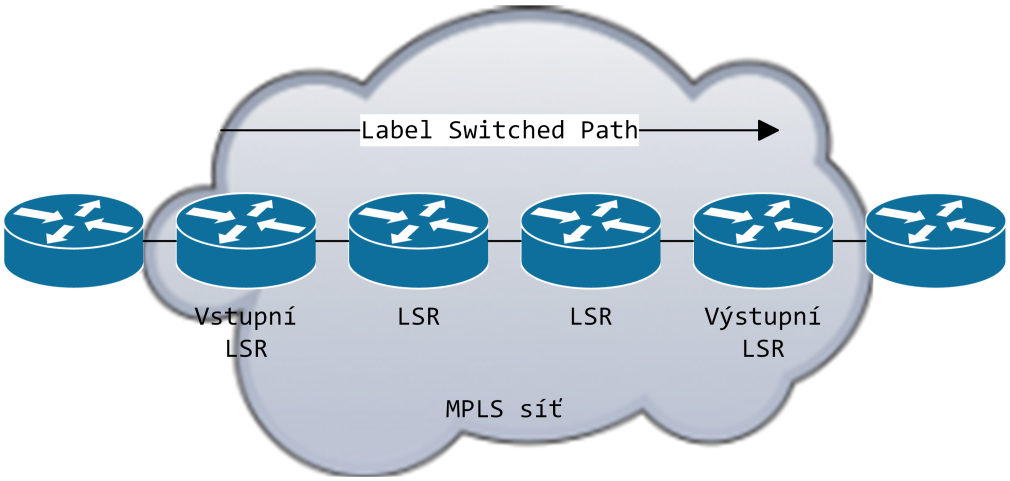
Pro samotné návěští je vyhrazeno 20 bitů, tudíž může nabývat různých hodnot při maximálním počtu kombinací $2^{20} - 1 = 1048575$. Prvních 0 - 15 hodnot je vyhrazeno pro zvláštní účely. Tudíž LSR tyto hodnoty nemůže použít pro posílání normálních paketů. Ostatní hodnoty jsou použity pro přidělování pod stejnou Forwarding Equivalence Classes (FEC), které spojují shodné vlastnosti – například nexthop adresa. Význam některých návěští z řad hodnot 0-15 je zmíněn v následujících odstavcích.

Implicit-NULL

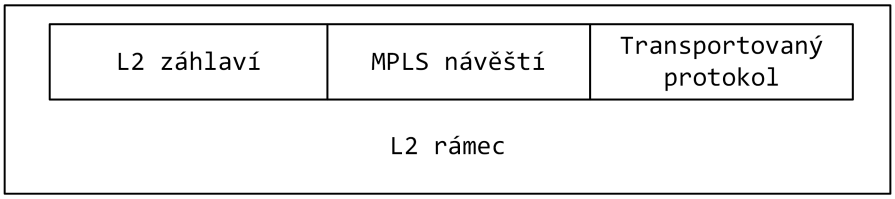
Tato funkce se nazývá Penultimate Hop Popping (PHP). Výstupní nebo vstupní LSR při něm pošle k centrálnímu LSR návěští Implicit-NULL (hodnota 3) a centrální LSR



Obr. 1.2: Základní operace v MPLS technologii.



Obr. 1.3: MPLS síť.



Obr. 1.4: Umístění záhlaví MPLS.

tudíž ví, že má paket posílat již bez MPLS návěští. Toto posílání má však taktéž své nevýhody. Dojde při něm ke ztrátě informace QoS.

Hlavním účelem je, že výstupní LSR nemusí provádět dvě vyhledávání (IP lookup a MPLS lookup). Zmenší se tím nároky na výstupní LSR.

Explicit-NULL

Jakmile výstupní LSR zašle centrálnímu LSR MPLS návěští s hodnotou 0, znamená to, že mu má posílat návěští s hodnotou 0. Výstupní LSR tudíž ví, že nemá hledat další návěští, ale že má provést přímo IP lookup. Výhodou tohoto je, že se k výstupním LSR dostane vždy informace o třech QoS bitech.

1.2.2 Zpracování hodnot TTL

Chování TTL v MPLS je odvozené z chování políčka TTL v paketu v IP sítích. Skládá se z 8 bitů a může nabývat hodnot 0 - 255. Při každém hopu dojde k dekrementaci o hodnotu 1. V případě, že se TTL rovná nule, je celý paket zahozen.

Při přechodu z IP do MPLS a opačně

Při přechodu ze sítě IP do MPLS sítě může dojít k následujícím dvěma variantám. Buďto se MPLS síť chová jako jeden hop pro IP síť (nepropaguje svůj počet hopů) nebo se počet hopů přes MPLS síť propaguje do IP paketu.

V prvním případě je při vstupu do MPLS sítě vygenerována nová hodnota TTL do MPLS návěští, která je postupně při každém hopu dekrementována. Na konci sítě je poté IP paket vyslán bez změny.

Ve druhém případě dojde na vstupním LSR ke zkopírování hodnoty TTL z IP paketu do MPLS návěští. V MPLS návěští je po celé trase hodnota postupně dekrementována a na výstupním LSR poté zkopírována do IP paketu.

Z tohoto lze odvodit, že při jakémkoliv procesu v MPLS síti (swap, push a pop) dojde vždy ke snížení hodnoty TTL o jedna v MPLS návěští.

TTL expirace

Chování LSR při obdržení návěští s TTL 1 je totožné jako v sítích IP. Dojde k vygenerování Internet Control Message Protocol (ICMP) typu 11 (Time Exceeded). Problém nastává, jakmile k vypršení dojde na vnitřním LSR směrovači, který v případě použití MPLS VPN nemá informaci o IP adresách, které se v takovém paketu posílají. Zpráva ICMP message exceeded není zaslaná hned zpět. Prvně je vygenerována zpráva ICMP time exceeded směrem k výstupnímu LSR v naději, že zpráva bude doručena. Výstupní LSR již může správně směrovat a pošle paket nazpět ke zdroji.

K výše popsanému chování dojde pouze tehdy, je-li náplní paketu IPv4 nebo IPv6 protokol. V případě použití jiných (AToM), dojde vždy k zahození paketu a zdroj se tak nikdy nedozví, kde došlo k zahození.

1.2.3 MPLS Maximum Transfer Unit

Při využití ethernet technologie se počítá s velikosti MTU 1518 v případě základního rámce, nebo 1522 v případě použití standardu 802.1Q (zapouzdření VLAN). Maximální náplň ethernet rámce je stanovena na 1500 bytů.

MPLS návěští se nazývá taktéž jako 2,5 vrstva v TCP/IP. Nachází se mezi ethernet záhlaví a IP paketem. Přidáním jednoho MPLS návěští dojde ke zvětšení MTU na třetí vrstvě na 1504 bytů, v případě dvojtého zapouzdření (MPLS VPN) i na 1508 bytů. Některé směrovače tyto „lehce“ větší rámce zvládají, avšak dle ethernet standardu by mělo být vše větší než 1522 bytů zahozeno. Tyto rámce se nazývají „Baby Giant Frames“. Je možné je nastavit na rozhraní příkazem „mpls mtu 1508“.

Ve výchozím nastavení je tato hodnota nastavena na 1500 bytů, velikost IP paketu je z tohoto důvodu jen 1492 a může tak docházet k jeho fragmentaci, která v síti není rozhodně žádoucí.

Z principu MPLS (swap, pop a push) vyplývá i různá hodnotu Maximum Recieve Unit (MRU) na příchozím rozhraní. Počítejme s tím, že je stanovena MTU IP paketu na 1500 a MTU MPLS na 1508 (jsou použita dvě návěští).

Pro MRU mohou nastat tři případy:

- Pop – hodnota příchozího paketu může být až 1512 (tři návěští), protože na odchozím rozhraní bude již MTU pouze 1508.
- Swap – hodnota příchozího paketu musí být maximálně 1508 (dvě návěští), jelikož dochází pouze k záměně návěští.
- Push – hodnota příchozího paketu musí být maximálně 1504 (jedno návěští), protože na odchozím rozhraní bude ještě další návěští přídáné a celková hodnota tak bude znovu maximálních 1508 bytů.

1.2.4 Vysoké nároky na PE směrovače

V této kapitole bych se rád odkázal na informace ohledně Explicit-NULL návěští (kapitola 1.2.1). Na PE směrovače je všeobecně kladen velký nárok – značkování paketů, BGP, spravování VRF instancí, LDP, ...

PE směrovač je možné odprostit od značkování. Celou funkcionalitu lze přesunout na Customer Edge (CE) směrovač. Na CE směrovači tak bude docházet ke značkování, tento směrovač pak hodnotu zašle v návěští 0 (Explicit-NULL návěští).

PE směrovač tak jen převezme tuto hodnotu z tohoto návěští a nemusí již nic dalšího řešit – tj. klasifikovat a značkovat pakety DSCP značkou.

1.3 Zpracování příznaku QoS v sítích MPLS

Přístup k zavedení podpory QoS v obou typech sítě je velice podobný. Ale i tak je nutné zaměřit se na pár rozdílů. V první řadě v sítích MPLS se používají pro vyjádření QoS pouze 3 bity, narozdíl od 6, které se používají v IP paketu v položce Differentiated Service Code Point (DSCP). Z těchto důvodů se pro zachování QoS v MPLS sítí používají první tři bity v DSCP políčku. Tyto tři bity se nazývají precedence a určují jednu z osmi tříd, ve které se paket může nacházet. Další tři bity jsou použity pro upřesnění QoS – vyšší, střední a nižší pravděpodobnost zahození.

Níže jsou uvedena základní výchozí pravidla pro zpracování příznaku QoS, která však lze nastavením změnit:

- 1. pravidlo – do MPLS návěští jsou vždy zkopírovány první tři bity ze záhlaví IP paketu.
- 2. pravidlo – při MPLS operaci swap a jsou zkopírovány QoS bity z jednoho MPLS návěští do přidaného nebo zaměněného.
- 3. pravidlo – při MPLS operaci pop nejsou zkopirovány QoS bity na odchozí rozhraní.
- 4. pravidlo – QoS bity na výstupním LSR nejsou zkopírovány do IP pakety (dojde k tunelování DSCP značky a zachování původní hodnoty pole).
- 5. pravidlo – při jakékoliv operaci MPLS (swap, pop a push) dojde ke změně hodnoty v políčku QoS pouze v prvním návěští, avšak již nikoliv v nižších, či v IP paketu.

Z výše zmíněných pravidel vyplývá, že je možné přes síť Internet Service Provider (ISP) protunelovat vlastní hodnoty DSCP, aniž by do toho ISP jakýmkoliv způsobem zasáhl. Při zavádění QoS je možné si vybrat ze tří uznávaných modelů, každý je něčím specifický. Jedná se o modely – pipe model, short pipe model a uniform model.

1.3.1 Pipe Model

1. Na vstupním rozhraní (PE směrovač) je informace o LSP DiffServ vytvořena z daných pravidel poskytovatelem, může být odvozena taktéž z IP paketu.
2. Na průchozím směrovači (P směrovač) je informace QoS odvozena z LSP DiffServ informace.
3. Na výstupním rozhraní (PE směrovač) je s paketem zacházeno dle informací v MPLS návěští.

1.3.2 Short Pipe Model

Tento model je téměř shodný s modelem Pipe, liší se akorát ve třetím pravidlu. Na výstupním rozhraní (PE směrovač) je s paketem zacházeno dle informací z protunelované DiffServ informace.

1.3.3 Uniform Model

U tohoto modelu se setkáme s trochu odlišným prvním a posledním pravidlem.

1. Na vstupním rozhraní (PE směrovač) je informace o LSP DiffServ převzata vždy ze záhlaví IP paketu.
2. Na průchozím směrovači (P směrovač) je informace QoS odvozena z LSP DiffServ informace – pravidlo zůstává shodné.
3. Na výstupním rozhraní (PE směrovač) je informace z LSP DiffServ vždy propagována do tunelovaného IP paketu.

1.3.4 Zavedení podporu QoS v MPSL síti

Pro zavedení podpory QoS v sítích MPLS se držíme stejných pravidel jako v Ethernet sítích. Prvně navrhujeme, který provoz má mít jakou prioritu. Poté tento provoz vhodně pomocí přístupových listů (Access List, ACL) identifikujeme. Proběhne klasifikace námi definovaného provozu přes síť, kterou následně označkujeme hodnotou DSCP, která se dále šíří sítí. Na základě různých hodnost DSCP/QoS bitů jsou pak pakety zařazeny do různých hardwarových front, které mají různou prioritu a různý druh obsluhy fronty – Round Robin (RR), Weighted Round Robin (WRR), Strict Priority (SP), Strict Priority Weighted Round Robin (SPWRR), ...

Veškerá problematika ohledně QoS je popsáne v mé bakalářské práci – Návrh spolehlivé podnikové sítě s podporou kvalitativních požadavků služeb. V této práci se již nebudu teorií podpory QoS zabývat, budu pouze využívat nabytých poznatků a aplikovat je v síti.

1.4 Label Discovery Protocol

Již víme, že u MPLS jde především o výměnu návěští, které musí být schopen dělat každý LSR směrovač. Z toho vyplývá, že návěští musí být v síti distribuovány. Distribuce návěští mohla být implementována do již známých vnitřních směrovacích protokolů Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP) a Intermediate System to Intermediate System (IS-IS), nebo mohl být vytvořen zcela nový protokol.

Problémem je, že se v tuto chvíli v sítích používají všechny výše zmíněné protokoly a muselo by to tak být implementováno čtyřikrát. Z tohoto důvodu byl vytvořen Label Distribution Protocol (LDP), který se stará o výměnu návěští mezi sousedními LSR se shodnými vlastnostmi. U MPLS záleží totiž na např. stejné next-hop adrese. Cesty, které mají podobné právě tyto a např. ještě QoS vlastnosti jsou shrnuty do jedné Forwarding Equivalence Classes (FEC), pro které je vygenerováno jedno návěští.

V přenosu mezi jednotlivými autonomními systémy (AS) již nedochází k přenosu návěští pomocí LDP. O přenos se již stará MultiProtocol-Border Gateway Protocol (MPBGP), který je uzpůsoben k přenosu různých protokolů.

1.4.1 Navázání sousedství

V případě, že se na rozhraní zapne LDP ihned tento směrovač začne zasílat Hello zprávy na multicast adresu 224.0.0.2 – na té naslouchají všechny směrovače, které podporují multicast. Pro Hello zprávy je využit transportní protokol User Datagram Protocol (UDP) s cílovým portem 646 na kterém každé rozhraní, kde je povoleno LDP naslouchá. V této zprávě je i tzv. Hold time, který specifikuje jak dlouhá má směrovač čekat, dokud sousední LSR nevyškrtne ze své databáze LDP sousedů v případě, že Hello paket nedorazí. Tyto Hello a Hold time intervaly jsou ve výchozím nastavení 5 a 15 sekund.

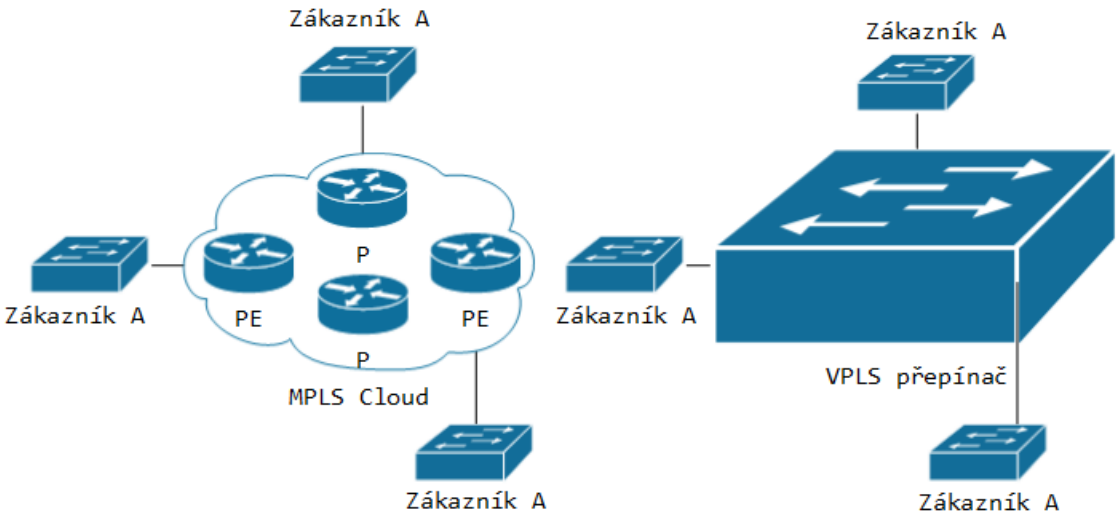
1.4.2 Navázání spojení

V případě, že se dva LSR navzájem objeví pomocí LDP Hello zpráv, pokusí se navázat přes Transmission Control Protocol (TCP) spojení. Pokouší se otevřít TCP port 646 na opačném LSR. V případě, že se podaří otevřít TCP spojení, tak si navzájem oba LSR směrovače přes počáteční zprávy vyjednají parametry tohoto LDP spojení. Navzájem si taktéž vymění jednotlivá návěští pro různé FEC.

V každé zprávě, které jsou posílány mezi dvěma LSR je tzv. LDP identifikátor původce této zprávy. Pokud sousední směrovač nemá cestu k této adrese, spojení se nenaváže. Tímto způsobem lze taktéž vytvářet cílené relace (targeted sessions) při vytváření privátních tunelů.

1.5 Možnost tunelování L2 provozu přes MPLS síť

S MPLS vznikla myšlenka vytvoření virtuálního přepínače, který by existoval nad L3 sítí poskytovatele. Tento přepínač by měl udržet privátní data uživatelů a ne-



Obr. 1.5: Ukázkové schéma s VPLS.

měl je rozšiřovat do síti jiných zákazníků. Dále by se měl přizpůsobit podstatě sítí Ethernet, kterým je způsob komunikace – všesměrová, multicastová a unicastová. Takový přepínač by se měl taktéž starat a přenos L2 servisních protokolů – např. Link Layer Discovery Protocol (LLDP) Spanning Tree Protocol (STP). Taktéž by musel být schopen učení MAC adres a jejich stárnutí. Technologie, která se k tomuto používá, je pojmenována – Virtual Private LAN Services (VPLS). Princip můžete vidět na obrázku. 1.5

Důvod proč VPLS vzniklo je jednoduchý. Při využití AToM sice můžeme přenést jakýkoliv protokol, avšak pouze ve smyslu point-to-point. Co se týče MPLS VPN, tak ty umožňují pouze spojení, která podporují IP protokol.

Zákazník může ještě použít pro připojení svých pracovišť technologii Ethernet over MPLS (EoMPLS), avšak jakékoliv spojení vytvořené pomocí této technologie je taktéž jen point-to-point. Spojení se též nazývá Virtual Leased Line (VLL).

Maximální počet naučených MAC adres

Vzhledem k principu Ethernet technologie dochází na krajních PE směrovačích k učení většího počtu MAC adres. V případě připojení velké sítě zákazníka, může dojít k přeplnění MAC tabulky. To by mohlo mít za následek neblahý vliv na vlastní síť poskytovatele. Proto je možné omezit maximální počet naučených MAC adres například na rozhraní, nebo konkrétní VLAN zákazníka.

1.5.1 Cílené LLDP spojení

Pro vytvoření VPLS je nutné zapouzdřit ethernet rámec dvakrát. První návěští označuje tzv. instanci VPLS. Zajišťuje, že data dojdou ke správným PE směrovačům. Vrchní návěští slouží již jen pro základní operace MPLS pop, push a swap. Pro vytvoření VPLS se používá tzv. cílené LDP spojení. To je navázáno na konkrétní PE směrovač poskytovatele. V případě přidání dalšího PE směrovače musíme navázat LDP spojení na všechny předchozí PE směrovače, které jsou součástí jedné VPLS domény.

1.5.2 Virtuální pronajmuté linky

Jak jsem o sekci výš již zmínil, existuje ještě druhá možnost jak propojit dva CE směrovače přes MPLS síť na L2 vrstvě. Tou je tzv. Virtual Leased Line (VLL). Tato technologie umožňuje spojení point-to-point. Pro některé případy to může být dostačující řešení, pro další nikoliv. Při vytvoření VLL se přesně definuje cílový PE směrovače, na který se vytvoří LDP spojení. Provoz je taktéž zapouzdřen ve více návěštích. Jedno z nich určuje privátní návěští (zkLSP) a druhé slouží pro přenos přes MPLS síť – pop, push a swap návěští. Toto spojení mezi dvěma PE směrovači je nazýváno pseudowire.

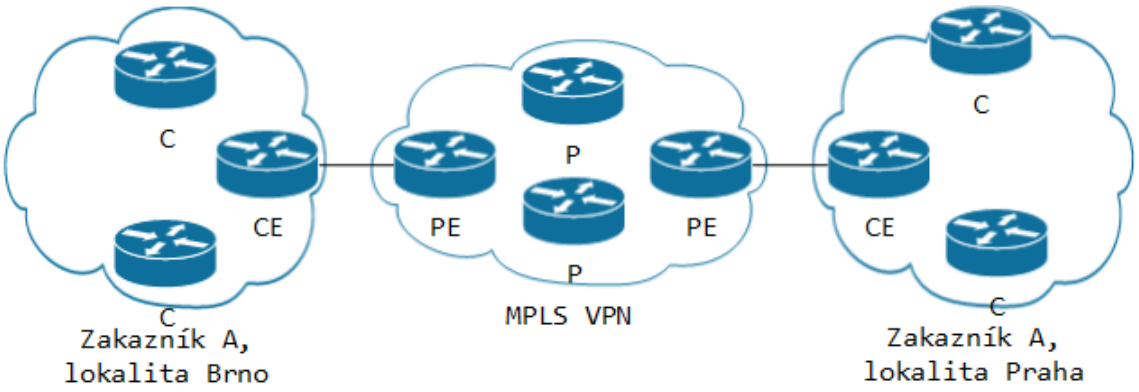
1.6 Možnost tunelování L3 provozu přes MPLS síť

Možnost spojení dvou bodů přes síť poskytovatele už existuje dlouhou dobu. Řešením bylo využití Frame-relay (FR) nebo Asynchronous Transport Machine (ATM). Ve spojení s MPLS se používá technologie MPLS VPN. Při této technologii rozdělujeme funkce směrovačů na následující: Customer (C), Customer Edge (CE), Provider Edge (PE) a Provider (P). Jejich výskyt v síti můžete pozorovat na obrázku 1.6.

Výhodou použití MPLS VPN je následující:

- Zákazník může použít adresy z veřejného rozsahu.
- Zákazník může použít adresy z privátního rozsahu.
- Navzájem se mohou prolínat adresní rozsahy zákazníka A i zákazníka B, které sdíli stejnou síť poskytovatele.

Veškerá správa privátní směrovací tabulku je vedena na PE směrovačích. Na těch běží zvláštní instance směrovací tabulky, tzv. Virtual Routing and Forwarding (VRF).



Obr. 1.6: Označení směrovačů při MPLS VPN

Route Distinguisher

Jednotlivé VPN jsou rozpoznány podle identifikátoru Route Distinguisher (RD). Tento identifikátor je pak přes síť přenesen přes MultiProtocol-BGP. Pro RD je použito 64bitové pole na rozdělení jednotlivých VPN, k ničemu jinému toto políčko neslouží.

Route Target

V případě, že bychom pro rozlišování používali pouze RD, nebylo by možné, aby zákazník A komunikoval se zákazníkem B. Pro tuto možnost je nastavení tzv. Route Target (RT). RT patří mezi parametry rozšiřující komunity BGP, udávající které cesty je možné importovat nebo exportovat z MP-BGP do VRF a opačně.

Borded Gateway Protocol

Pro aplikování samotného MPLS VPN do sítě poskytovatele je zapotřebí již mít znalost protokolu Border Gateway Protocol (BGP). Ten se využívá pro přenos výše zmíněného parametru RD. BGP je navázáno vždy mezi jednotlivými PE směrovači nebo vůči Route Reflektoru, který se používá pro snížení počtu BGP spojení v topologii. Ideálně by měly být veškeré PE směrovače propojeny ve smyslu full-mesh, avšak výhodou je spojit je ve smyslu hub-and-spoke, kdy jsou vždy BGP sousedství navázána na primární a záložní BGP Route Reflektory, které se starají o klonování BGP cest k ostatním BGP směrovačům.

2 LABORATORNÍ ÚLOHA

2.1 Topologie

Praktická část projektu je zaměřena na osvojení teoretických znalostí z teoretické části. Jsou zde zkoumány jednotlivé parametry, na které je vždy odkázano vzhledem k teoretické části.

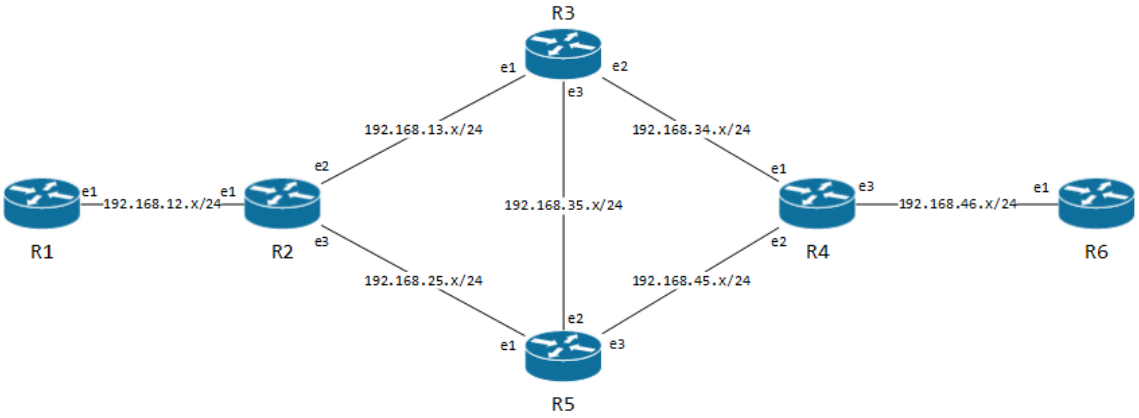
Topologie sítě je zvolena tak, aby na ni bylo možné dokázat dílčí poznatky. Celá topologie byla virtualizování na počítači s operačním systémem Windows 7. Zapojeno v ní bylo 6 zařízení MikroTik s podporou MPLS a verzí operačního systému RouterOS 5.18. Topologie je naznačena na obrázku 2.1.

O směrování se staral dynamický směrovací protokol Open Shortest Path First OSPF. Pro adresní plán jsem zvolil následující pravidla:

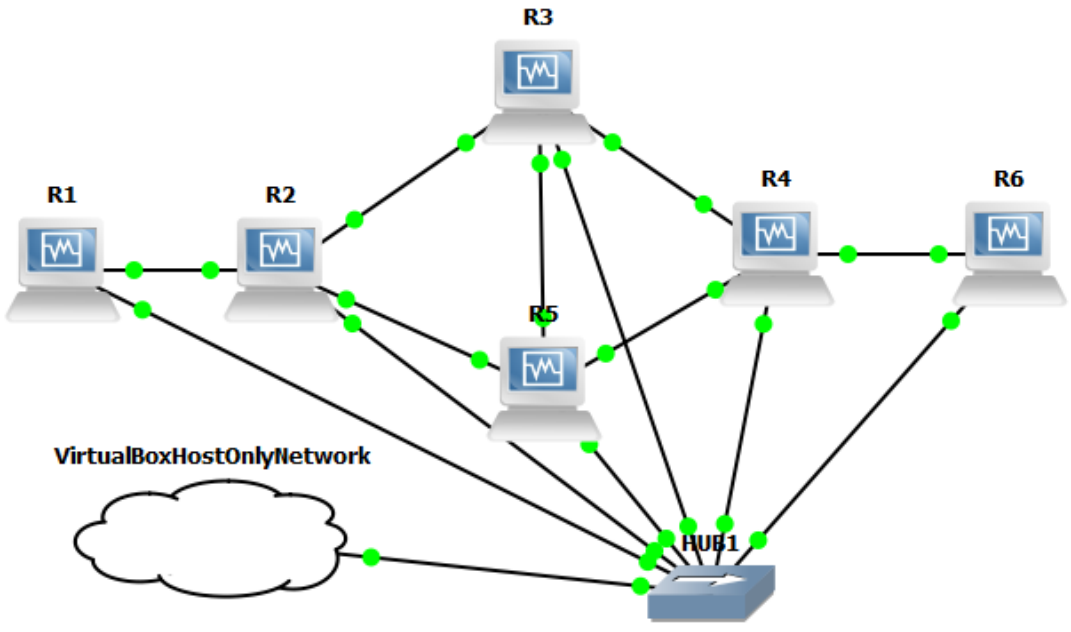
1. Jsou použity sítě třídy B.
2. Mezi dvěma prvky je adresa sítě rovna vždy menšímu a většímu číslu jména směrovače (R1–R2 ... 192.168.12.0/24).
3. Prvek s abecedně menším jménem má nižší adresu (.1) a prvek s abecedně větším jménem má větší adresu (.2).
4. Vždy byly připojeny rozhraní od abecedně menších prvků k abecedně větším prvkům. R3(e1)–(e2)R2, R3(e2)–(e1)R4, R3(e3)–(e2)R6.
5. Rozhraní ether4 je vždy připojeno do zařízení HUB k virtuální síťové kartě (VirtualBox Host-Only Network).
6. Mgmt adresa prvku korespoduje s virtuální sítí VirtualBox Host-Only (192.168.56.0/24).
7. Mgmt adresa jednotlivých prvků souvisí se jménem prvku (IP mgmt adresa R3 – 192.168.56.3/24).

Dále k simulaci byl použit volně dostupný program VirtualBox, na kterém proběhla virtualizace operačního systému RouterOS pro architekturu x86. Topologie byla sestavena v programu GNS3 (Graphical Network Simulator). Do tohoto programu byly naimportovány jednotlivé virtuální stroje společně se zapnutou podporou zachycování paketů programem Wireshark. Ačkoliv RouterOS inkrementuje rozhraní od 1 (ether1), program GNS3 jako počáteční index volí 0 – rozhraní ether1 na prvku R1 je v programu GNS3 identifikováno jako e0. Topologii v programu GNS3 můžete vidět na obrázku 2.2

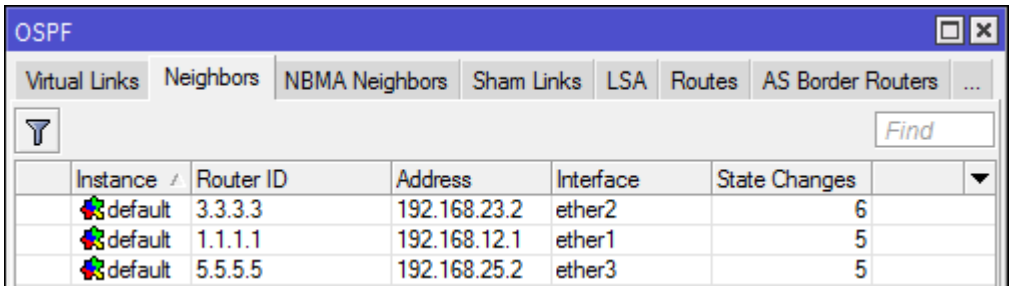
Správa virtualizovaných zařízení MikroTik probíhala jak přes příkazovou řádku, tak i přes jejich program pro správu – WinBox. Konfigurace přes grafické rozhraní WinBox považuji za velmi přehledné. Z tohoto důvodu jsem přiřadil jednotlivým zařízením mgmt IP adresy pro vzdálenou správu bez výpadků.



Obr. 2.1: Topologie MPLS sítě



Obr. 2.2: Topologie MPLS sítě v programu GNS3.



Obr. 2.3: Sousedi u protokolu OSPF na směrovači R2.

2.2 Základní nastavení

Pro zprovoznění jsem nejdříve všem rozhraním přiřadil IP adresy dle adresního plánu (viz výše). Poté jsem jednotlivé rozhraní přidal do směrovacího protokolu OSPF. Všem směrovačům bylo nastaveno RouterID (tuto identifikaci používá směrovací protokol OSPF) na adresu dle jejich jména (R2 – 2.2.2.2). Úspěšné zprovoznění topologie s OSPF můžeme sledovat na obrázku 2.3.

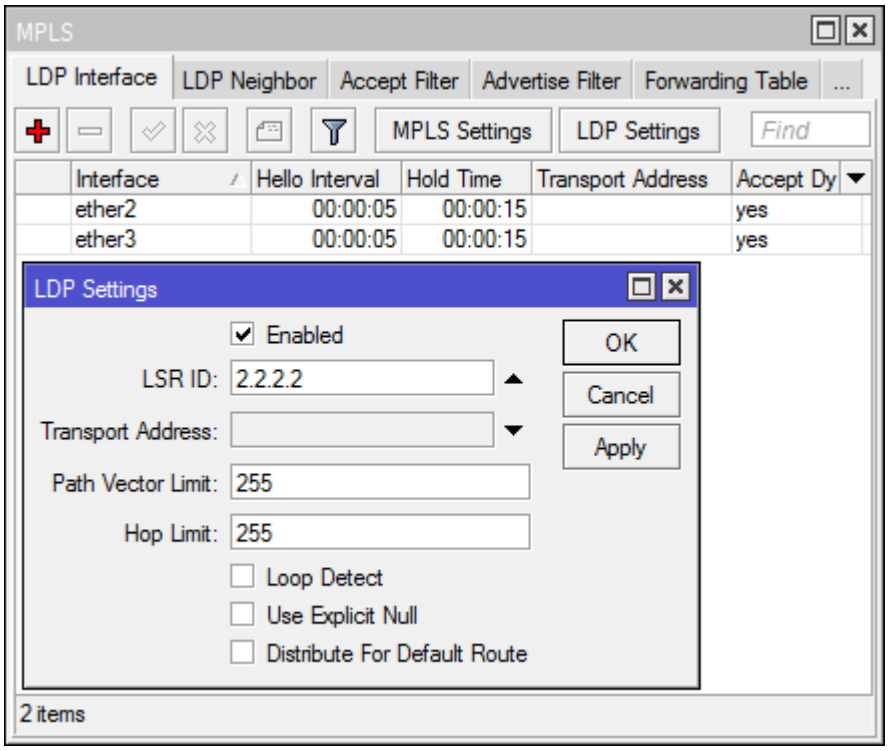
Pro povolení MPLS musíme nejdříve povolit protokol LDP a následně zvolit rozhraní, na kterých chceme, ať tento protokol běží. Nastavení můžeme sledovat na obrázku 2.4. Dále bylo pro proktokol LDP nastavena tzv. LSR ID, vždy na takovou hodnotu, aby korespondovala se jménem směrovače (R2 – 2.2.2.2). Toto nám ulehčí následnou analýzu v programu Wireshark.

Po postupu viz výše lze vidět pakety LDP na rozhraní mezi R2 a R3. Zachycené pakety nalezneme na obrázku 2.5. Na obrázku lze pozorovat taktéž výměnu paketů s namapovanými návěštními, které si mezi sebou směrovače navzájem zasílají. Výpis je dvoubarevný – význam modrého podbarvení je pro paketu UDP a naopak pro pakety TCP je použito lehce fialové podbarvení. Pokud bychom analyzovali paket hlouběji, dozvíme se i porty na kterých se toto sousedství navázalo – Hello zprávy na UDP cílový port 646, navázání TCP relace na cílový port 646.

Sledování paketů ICMP

V této fázi bude proveden PING ze směrovače R1 a zdrojové adresy 192.168.12.1 na adresu 6.6.6.6. Nejdříve zkontrolujeme lokální a vzdálené návěští na směrovačích a poté si ověříme komunikace analyzátorem paketů Wireshark.

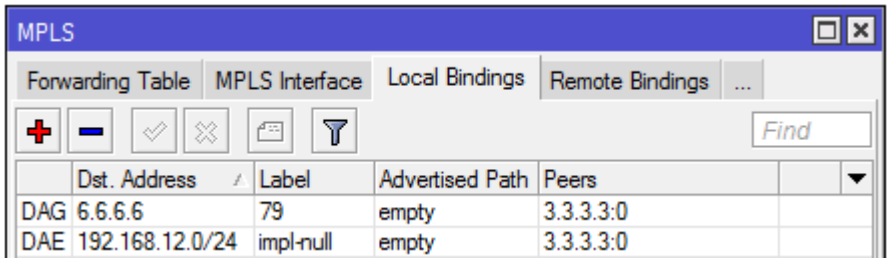
Jelikož jsem během mých pokusů zkoušel více věcí, byly již návěští s hodnotou lehce nad 16 namapovány a v praktické části se tedy vyskytuji výšší hodnoty. Výpisy jsem zkrátil, nechť lze vidět pouze relevantní informace pro danou komunikaci. Ještě zmíním, že výchozí nastavení pro zařízení MikroTik je implicitní signalizace návěští (viz kapitola Implicit-NULL). Dále již v tomto kroku aplikuji i QoS nastavení pro



Obr. 2.4: Nastavení MPLS na směrovači R2.

```
867 955.428088000  192.168.23.2  224.0.0.2  LDP      76 Hello Message
870 959.582163000  192.168.23.1  224.0.0.2  LDP      76 Hello Message
874 959.583052000  3.3.3.3       2.2.2.2    LDP     102 Initialization Message
876 959.583318000  2.2.2.2       3.3.3.3    LDP     110 Initialization Message Keep Alive Message
878 959.583678000  3.3.3.3       2.2.2.2    LDP      84 Keep Alive Message
879 959.584087000  2.2.2.2       3.3.3.3    LDP     110 Address Message
880 959.584362000  3.3.3.3       2.2.2.2    LDP     558 Label Mapping Message
881 959.584545000  2.2.2.2       3.3.3.3    LDP     514 Label Mapping Message
883 961.148416000  192.168.23.2  224.0.0.2  LDP      76 Hello Message
888 965.251838000  192.168.23.1  224.0.0.2  LDP      76 Hello Message
```

Obr. 2.5: Nastavení MPLS na směrovači R2.



Obr. 2.6: MPLS local bindings na R2.

DAG	6.6.6.6	31	empty	4.4.4.4:0, 2.2.2.2:0
DAG	192.168.12.0/24	27	empty	4.4.4.4:0, 2.2.2.2:0

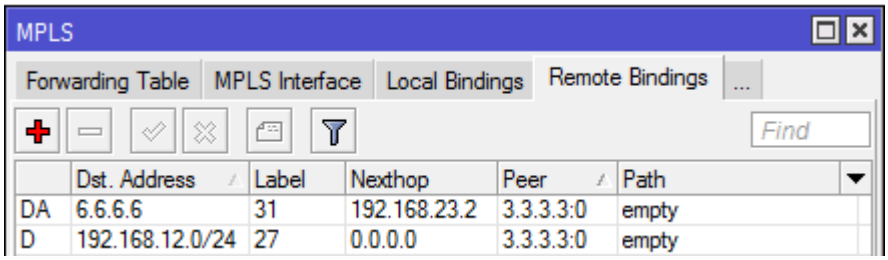
Obr. 2.7: MPLS local bindings na R3.

danou zprávu ICMP, stejně jako TTL chování.

Nyní tedy zkontrolujeme lokální a vzdálené mapování pro rozhraní na směrovačích R2 a R3.

Na obrázku 2.7 můžeme vidět, že směrovač R3 dává na znamení směrovači L2, že pro cílovou adresu 6.6.6.6 má používat návěští 31. To, že informace byla úspěšně přenesena na směrovač R2 si můžeme ověřit na obrázku 2.8, kde vidíme v remote binding tabulce, že pokud je cílová adresa 6.6.6.6 má použít návěští 31. Obrázky jsou vždy pod sebou, nechť jde vidět co který sloupec znamená. Na obrázku 2.6 můžeme také vidět, že pro síť 192.168.12.0/24 zasílá všem návěští imp-null, které značí, že má být paket zasílán zpět bez návěští, nechť směrovači stačí již udělat pouze jedno vyhledávání (pouze v IP route table) a ne dvě (první v MPLS forwarding table a druhé v IP route table).

Pro ověření jsem zachytil a analyzoval komunikace programem Wireshark na rozhraní mezi směrovači R2 a R3. Na prvním obrázku 2.10 lze vidět paket směrem od R2 k R3. Mezi L2 a L3 vrstvou lze ještě sledovat tzv. 2,5 vrstvu – MPLS návěští. Na obrázku můžeme taktéž pozorovat, že je bit BoS v MPLS návěští nastaven na 1 (je to poslední návěští). Bohužel na verzi RouterOS 5.18 není možné převzít prioritu

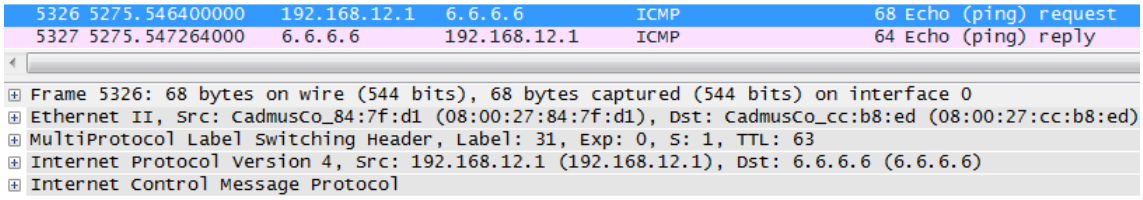


Obr. 2.8: MPLS remote bindings na R2.

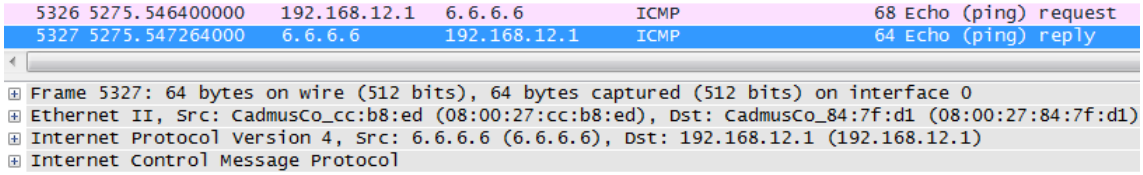
D	6.6.6.6	79	0.0.0.0	2.2.2.2:0	empty
DA	6.6.6.6	54	192.168.34.2	4.4.4.4:0	empty
D	192.168.12.0/24	58	0.0.0.0	4.4.4.4:0	empty
DA	192.168.12.0/24	impl-null	192.168.23.1	2.2.2.2:0	empty

Obr. 2.9: MPLS remote bindings na R3.

do MPLS návěští z DSCP hodnoty, toto lze uskutečnit až na RouterOS 6.x a vyšší příkazem „from-dscp-high-3-bits“. Tudíž nemohu zkoumat namapování hodnot z IP hlavičky políčka DSCP do 3 QoS bitů v MPLS návěští. Na odpovědi na zprávu ICMP v obr. 2.11 můžeme sledovat, že příchozí paket nemá žádné návěští.



Obr. 2.10: Zachycená zpráva ICMP mezi směrovači R2 a R3.



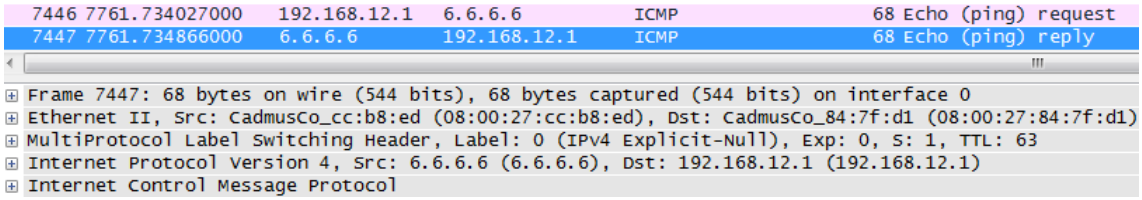
Obr. 2.11: Zachycená odpověď na ICMP zprávu mezi směrovači R2 a R3.

Chování při explicit-null a nepropagování hodnoty TTL

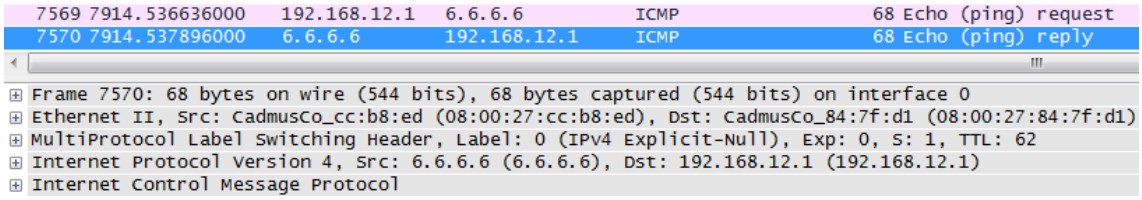
Při tomto testu jsem v nastavení potvrdil používání explicitního návěští. Tudíž směrovač R3 bude vždy zasílat MPLS návěští i v případě, že je R2 okrajový směrovač. Zároveň jsem při tomto testu ještě zakomponoval propagaci hodnoty TTL.

Paket vychází ze směrovače R1 s TTL 64, na směrovači R2 je snížena tato hodnota v IP hlavičce na 63 a tato hodnota je převzata do TTL hodnoty MPLS návěští. Stejným způsobem se snižování TTL chová cestou zpět. Toto lze pozorovat u obrázku 2.12. Hodnota v IP hlavičce je zachována na hodnotě 63, zatímco hodnota v MPLS návěští je snížena na 62 (dva přeskoky) a poté snížena na výstupním rozhraní mezi směrovači R1 a R2 taktéž v IP záhlaví. Toto je chování, při kterém dochází k propagování TTL hodnoty a MPLS síť se nechová jako jeden přeskok.

Na obrázku 2.13 můžeme vidět, že hodnota TTL v záhlaví MPLS návěští je o jedničku větší než v předchozím případě. To je z toho důvodu, že paket byl do sítě MPLS vyslán s hodnotou TTL 64 a došlo tedy zatím jenom k jednomu snížení.

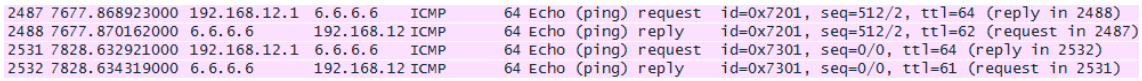


Obr. 2.12: Zachycená zpráva ICMP mezi směrovači R2 a R3 s použitím explicit-NULL a zároveň s propagací TTL hodnoty v MPLS síti.



Obr. 2.13: Zachycená odpověď na ICMP zprávu mezi směrovači R2 a R3 s použitím explicit-NULL a zároveň bez propagace TTL hodnoty v MPLS síti.

Výsledek propagace TTL hodnoty můžeme sledovat na obrázku 2.14. První dvojice požadavku a odpovědi byla zaslána při nastavení nepropagace TTL hodnot. Pro toto nastavení s celá síť chová jako jeden přeskok, zatímco pro druhou dvojici paketů došlo ke změně nastavení sítě (lze sledovat i větší časový odstup z důvodu nastavování) na propagaci TTL hodnot v síti MPLS. V tom případě lze vidět v paketu hodnotu TTL u paketu nastavenou na 61.

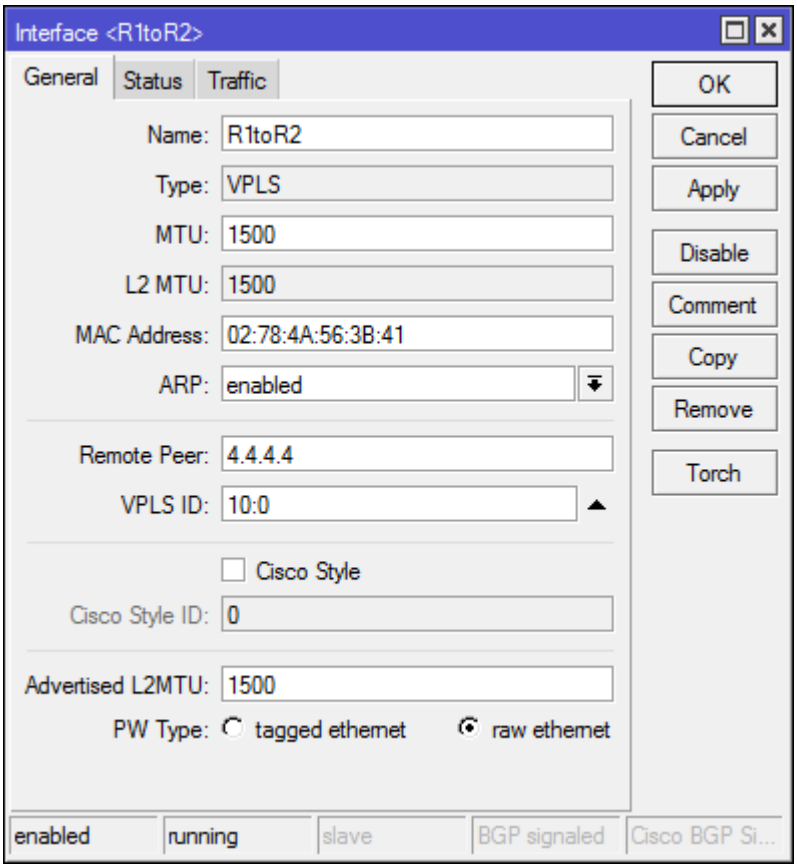


Obr. 2.14: Zachycená zpráva ICMP mezi směrovači R1 a R2 – rozdíl v hodnotě TTL dle nastavení propagace.

Virtual Private Lease Switching

Vzhledem k tomu, že při tomto testování musí být na obou koncích směrovače ve stejné sítí, provedl jsem přeadresování na pravé straně. nastavil jsem tam adresy

z adresního prostoru 192.168.12.0/24 (.3 a .4). Poté jsem vytvořil na krajních směrovačích nové VPLS rozhraní a bridge. Tomuto bridge byly přiřazeny dvě rozhraní – fyzické rozhraní a nově vytvořené VPLS rozhraní. Při vytváření VPLS rozhraní jsem musel identifikovat jednoznačné VPLS ID na obou stranách shodné a taktéž Remote Peer ID, na které se má toto spojení navázat viz obr 2.15. Po tomto kroku došlo k zasílání UDP Hello zpráv ne na multicastovou, ale na unicastovou adresu peeru. V zápětí došlo taktéž k navázání TCP relace a výměně návěští na unicastovou adresu (viz 2.16). Taktéž jsem ukončit propagování této sítě do směrovacího protokolu OSPF na směrovači R2.



Obr. 2.15: Vytvoření VPLS rozhraní na směrovači R2.

Při analýze paketu ICMP zachyceného mezi rozhraními R2 a R3 můžeme sledovat, že jsou v paketu 2 MPLS návěští a že až návěští nejblíže IP paketu má bit BoS nastaven na 1.

MPLS BGP Virtual Private Network

V poslední části jsem prozkoumal možnost připojení jednoho zákazníka přes MPLS síť poskytovatele na třetí vrstvě. K tomu slouží v teorii probraný BGP VPN. Z pů-

```
9334 10114.460715000 2.2.2.2  4.4.4.4  LDP      80 Hello Message
9338 10114.462819000 4.4.4.4  2.2.2.2  LDP     106 Initialization Message
9340 10114.463316000 2.2.2.2  4.4.4.4  LDP     114 Initialization Message Keep Alive Message
9342 10114.464482000 4.4.4.4  2.2.2.2  LDP      88 Keep Alive Message
9343 10114.464995000 2.2.2.2  4.4.4.4  LDP     114 Address Message
9344 10114.465563000 4.4.4.4  2.2.2.2  LDP     656 Label Mapping Message
9345 10114.465676000 2.2.2.2  4.4.4.4  LDP     331 Label Mapping Message
9349 10114.505623000 2.2.2.2  4.4.4.4  LDP     351 Label Mapping Message
9356 10116.865818000 4.4.4.4  2.2.2.2  LDP      80 Hello Message
```

Obr. 2.16: Vytvoření Remote Peer soudsetví.

```
 9369 9295.321439000 192.168.12.4 192.168.12 ICMP      90 Echo (ping) request  id=0x5c01, seq=2048/8
 9370 9295.325862000 192.168.12.1 192.168.12 ICMP      86 Echo (ping) reply    id=0x5c01, seq=2048/8

⊞ Frame 9369: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
⊞ Ethernet II, Src: CadmusCo_ea:b7:a8 (08:00:27:ea:b7:a8), Dst: CadmusCo_88:1d:c9 (08:00:27:88:1d:c9)
⊞ MultiProtocol Label Switching Header, Label: 28, Exp: 0, S: 0, TTL: 64
⊞ MultiProtocol Label Switching Header, Label: 100, Exp: 0, S: 1, TTL: 64
⊞ PW Ethernet Control Word
⊞ Ethernet II, Src: CadmusCo_45:be:ba (08:00:27:45:be:ba), Dst: CadmusCo_4e:c8:47 (08:00:27:4e:c8:47)
⊞ Internet Protocol Version 4, Src: 192.168.12.4 (192.168.12.4), Dst: 192.168.12.1 (192.168.12.1)
⊞ Internet Control Message Protocol
```

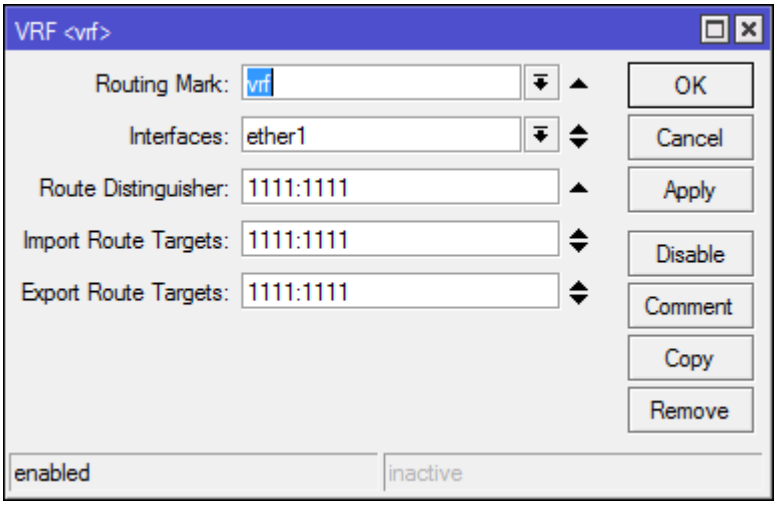
Obr. 2.17: Zachycený paket se dvěmi návěštími.

vodní topologie musela být znovu vytvořena cílená TCP relace na vzdáleného souseda. Musela být vytvořená nová směrovací tabulka, např. v tomto případě se jménem „vrf“, která měla hodnotu Route Distinguisher (RD) nastavenou na 1111:1111, je to rozlišovací symbol v případě výskytu více virtuálních směrovacích tabulek. Taktéž muselo být nastaveno importování a exportování cest do/z směrovací tabulky pokud nesou označení 1111:1111 (viz 2.18). Poté musela být vytvořena nová instance OSPF, která měla svoji vlastní směrovací tabulku pojmenovanou vrf.

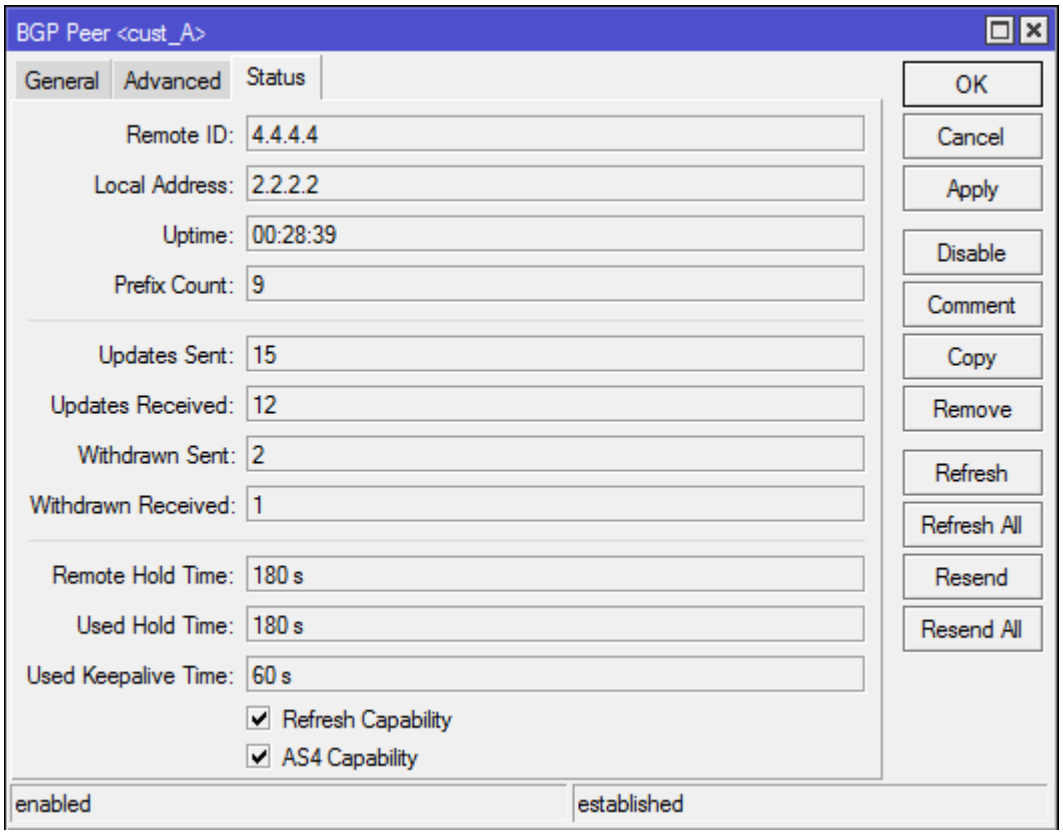
Nyní se vytvoří nová instance BGP navzájem mezi směrovači R2 a R4. U obou se musí zapnout podpora VPNV4 cest a pokud možno i update-source (vlastní loopback). Úspěšné vytvoření této BGP relace můžeme sledovat na obrázku 2.19.

Na posledním obrázku vidíme odlišení cest souvisejících s BGP VPN (viz 2.20). V úvodní kolonce můžeme vidět i jednotlivé příznaky těchto cest. Příznak D znamená, že cesta byla naučena dynamicky, A znamená že je právě aktivní. Poslední příznaky se liší kvůli následujících důvodů:

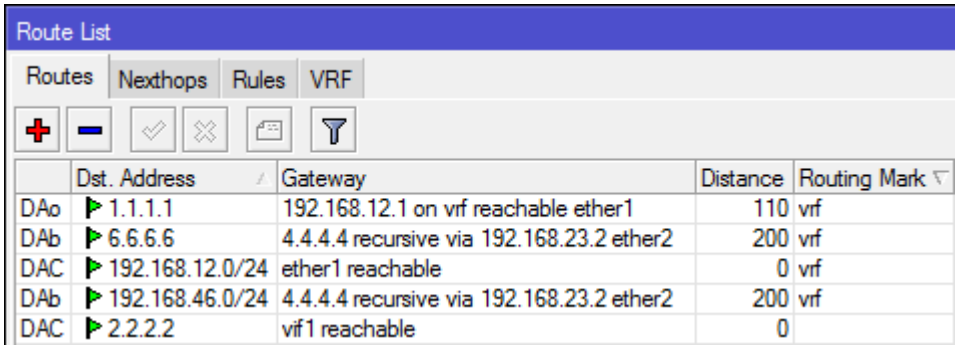
- o – naučeno od sousedního směrovače R1 přes směrovací protokol OSPF.
- b – naučeno od sousedního BGP směrovače R4 přes směrovací protokol OSPF.
- C – označuje přímo připojenou linku.



Obr. 2.18: Vytvoření nezávislé směrovací tabulky.



Obr. 2.19: Vytvoření BGP relace s podporou VPNV4.



Obr. 2.20: Odlišení normálních cest oproti VPNV4 cestám.

3 TESTOVACÍ MPLS SÍŤ

Pro testování skutečné MPLS sítě byla zapůjčeny zařízení od různých výrobců (Brocade, Juniper, MikroTik a Cisco). Testována při tom byla vzájemná možnost spolupráce těchto zařízení se standardizovanými protokoly. Použitá zařízení naleznete v tabulce 3.1. Bohužel až po doručení bylo zjištěno, že zařízení firmy Cisco Catalyst 6500 mělo starou managementovou kartu, tudíž ačkoliv samotné karty MPLS podporovaly, bohužel mgmt karta nebyla schopna MPLS zpracovávat a nešlo tudíž provozovat MPLS na tomto zařízení. Je to nesmírná škoda, jelikož v tomto zařízení byla i karta s analýzou provozu ve skutečném čase. Vzhledem k tomu, že toto zařízení nebylo možné použít, bylo nahrazeno řádově nižším zařízením, které bylo pro toto testování zakoupil – MikroTik.

Tab. 3.1: Použitá zařízení

Výrobce	Model	Operační systém	Verze
Brocade	CER2024	NetIron	5.6.0bT183
Juniper	SRX100b	JunOS	12.1X44-D20.3
MikroTik	RB751U-2HnD	RouterOS	6.13

Pro plné vytížení linek vzhledem k aplikaci QoS byly použity testery firmy Fluke (EtherScope™ Series II Network Assistant). Tato zařízení jsou schopna generovat a analyzovat provoz na metalických nebo optických linkách o rychlosti až 1 Gbps. Vzhledem k nejednotosti použitých zařízení (kvalitativně rozlišné modely) se mohlo testovat pouze na rychlosti 100 Mbps.

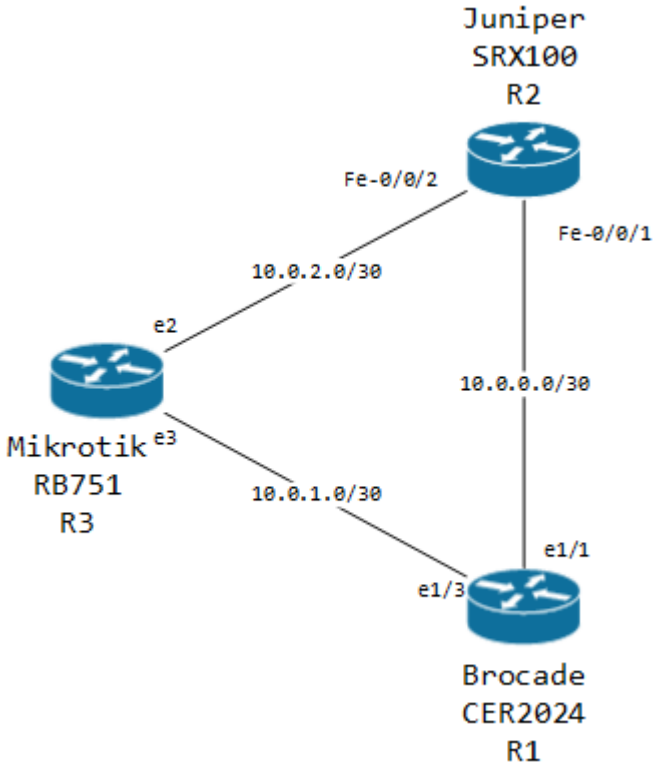
Cílem bylo otestovat provoz multicastu přes jednotlivé tunely přes MPLS síť - Virtual Leased Line (VLL), Virtual Private LAN Services (VPLS) a Virtual Routing and Forwarding ve spojení s BGP (VRF). Dále ověřit, že multicastový provoz s vyšší DSCP značkou bude upřednostňován před podřadným provozem testerů.

3.1 Topologie sítě

Vytvořené jádro sítě se skládá ze tři prvků, které jsou zapojeny do trojúhelníku vždy každý s každým (viz. 3.1). O směrování v síti se stará protokol Open Shortest Path First (OSPF). Na každém prvku existuje loopback rozhraní, pro navázání spojení protokolů OSPF, BGP a LDP. Soupis rozhraní a adresaci sítí naleznete v tabulce 3.2. Foto zařízení lze sledovat na obrázku 3.2.

Tab. 3.2: Adresace na rozhraních

Zařízení	Rozhraní	Adresa
Brocade	e1/1	10.0.0.1/30
	e1/3	10.0.1.1/30
	lo1	1.1.1.1/32
Juniper	fe-0/0/1	10.0.0.2/30
	fe-0/0/2	10.0.2.1/30
	lo0	2.2.2.2/32
MikroTik	e2	10.0.2.2/30
	e3	10.0.1.2/30
	lo1	3.3.3.3/32



Obr. 3.1: Zapojení topologie.

Topologie je plně redundantní. Vzhledem k navázání spojení na loopbackové rozhraní nedojde nikdy k rozpadu spojení, jelikož k tomuto rozhraní má každý prvek vždy záložní cestu.

Obr. 3.2: Fotografie zařízení.

3.2 Virtual Lease Line a Virtual Private LAN Services

Vzhledem k nedostatku portů na zařízeních byla funkčnost obou typů tunelů testována současně. Tímto postupem bylo zároveň i ověřeno, že se navzájem uživatelé z jednoho tunelu nemohou dostat do druhého.

Pro vytvoření VLL tunelu na zařízení Juniper se musely zadat následující příkazy:

```
protocols {
    l2circuit {
        neighbor 1.1.1.1 {
            interface fe-0/0/4.600 {
                virtual-circuit-id 600;
                encapsulation-type ethernet-vlan;
            }
        }
    }
}
interfaces {
    fe-0/0/4 {
        vlan-tagging;
        encapsulation vlan-ccc;
        unit 600 {
            encapsulation vlan-ccc;
            vlan-id 600;
            family ccc;
        }
    }
}
```

Jedná se o tagovaný provoz ve VLAN 600.

Na zařízení výrobce Brocade je kód v running-config následující:

```
router mpls
 mpls-interface e1/1
  ldp-enable
 mpls-interface e1/3
  ldp-enable
 vll vlan600 600
  vll-peer 2.2.2.2
  vlan 600
   tagged e 1/7
```

Úspěšné navázání lze sledovat pomocí show příkazů. Lehce matoucí je, že stejnou funkci nazývá Juniper l2circuit, zatím co Brocade ji nazývá VLL. Na obrázku 3.3 lze pozorovat úspěšné sestavení VLL tunelu. Tunel je ve stavu UP a navzájem si předala návěští, která používají pro tuto komunikaci.

```
Neighbor: 1.1.1.1
    Interface                 Type  St     Time last up          # Up trans
    fe-0/0/4.600(vc 600)      rmt   Up     May 17 14:44:12 2014           1
      Remote PE: 1.1.1.1, Negotiated control-word: No
      Incoming label: 299776, Outgoing label: 851968
      Negotiated PW status TLV: No
      Local interface: fe-0/0/4.600, Status: Up, Encapsulation: VLAN
```

Obr. 3.3: Úspěšné sestavení tunelu.

V následujícím kroku byl zprovozněn virtuální přepínač VPLS. Ten byl zprovozněn mezi zařízeními Brocade a Mikrotik. Pro zařízení MikroTik stačí při zprovozněné MPLS síti zadat pouze

```
/interface vpls add name=VPLS10 remote-peer=1.1.1.1 vpls-id=10
```

U zařízení Brocade je konfigurace následující:

```
router mpls
 vpls vpls1 10
  vpls-peer 2.2.2.2 3.3.3.3
  vlan 10
   untagged ethe 1/4
```

V obou konfigrací se shoduje tzv. VPLS-ID, to slouží pro oddělení jednotlivých virtuálních přepínačů VPLS. To, že spojení bylo úspěšně sestaveno můžeme sledovat například na zařízení Brocade, viz obrázek 3.4

V tuto chvíli byla ověřena spojení všech zařízení v daných virtuálních rozhraních pomocí programu ping. V jednotlivých rozhraních VLL a VPLS byla koncová zařízení navzájem dostupná.

Testování QoS

Po zprovoznění topologie bylo možné udělat základní test propustnosti. Výsledky tohoto testování můžete sledovat na obrázku 3.5. Jedno zařízení Fluke (Local) bylo zapojeno do Juniperu do portu fe-0/0/4.600, druhé zařízení (Remote) bylo zapojeno do Brocade do portu e1/7. VLL tunel byl nastaven pro přenos tagovaných rámců ve VLAN 600.

Topologie byla zároveň nachystaná na netagovaný provoz ve virtuálním přepínači VPLS mezi prvky Brocade (e1/4) a MikroTik (e4). Na jednom počítači je multicastový vysílač s datovým tokem +- 12 Mbps. Multicast je ohlašován pomoci Session Announcement Protocol (SAP). Byl k tomu využit program Minisapserver v prostředí OS Debian. Vysíláno je směrem ze zařízení Brocade na zařízení MikroTik.

```
VPLS vpls1, Id 10, Max mac entries: 2048
 Total vlans: 1, Tagged ports: 0 (0 Up), Untagged ports 1 (1 Up)
  Vlan 700
   L2 Protocol: NONE
   Untagged: ethe 1/4
 VC-Mode: raw-pass-through
 Total VPLS peers: 2 (2 Operational)
 Peer address: 3.3.3.3, State: Operational, Uptime: 46 sec
  Flood Domain ID: 4357
  Tnnl in use: tnl0(0)[LDP]    Peer Index:0
  Local VC lbl: 983042, Remote VC lbl: 40
  Local VC MTU: 1500, Remote VC MTU: 1500
  Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
 Peer address: 2.2.2.2, State: Operational, Uptime: 17 sec
  Flood Domain ID: 4357
  Tnnl in use: tnl1(3)[LDP]    Peer Index:1
  Local VC lbl: 983041, Remote VC lbl: 262146
  Local VC MTU: 1500, Remote VC MTU: 1500
  Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
 Local Switching: Enabled
 Counter Mode: Disabled
 Multicast Snooping: Enabled - Active
```

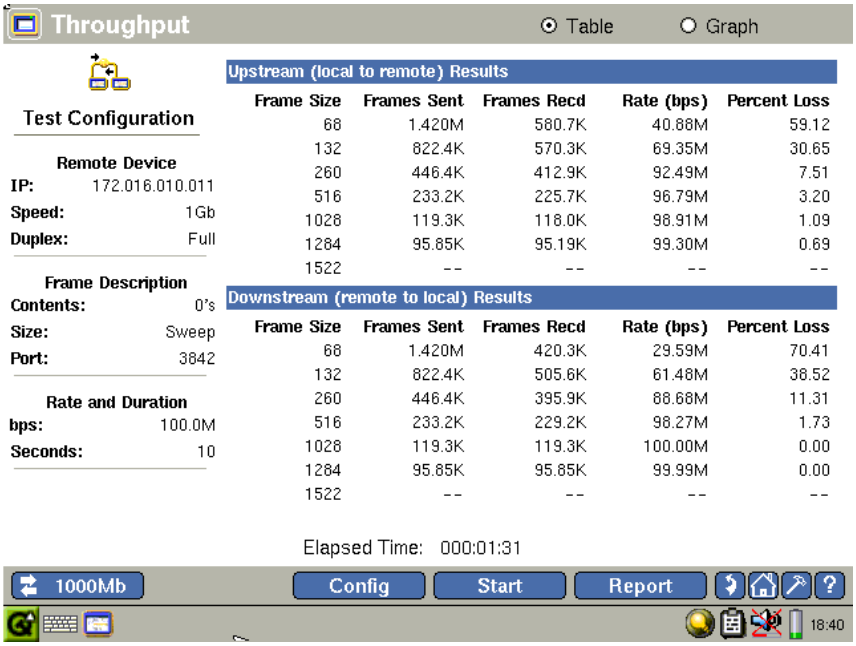
Obr. 3.4: Sestavení VPLS.

Jelikož by v tuto chvíli docházelo k rozdělování zátěže mezi obě zařízení (oba toky dat by směřovaly k různým zařízením - Juniper a Mikrotik), nedocházelo by k přetížení linek. Z tohoto důvodu byla vypnuta linka mezi zařízením Juniper a Brocade. Tudíž zařízení Brocade muselo řešit podporu QoS, jelikož součet provozu z dvou linek byl +- 112 Mbps na pouze 100 Mbps linku.

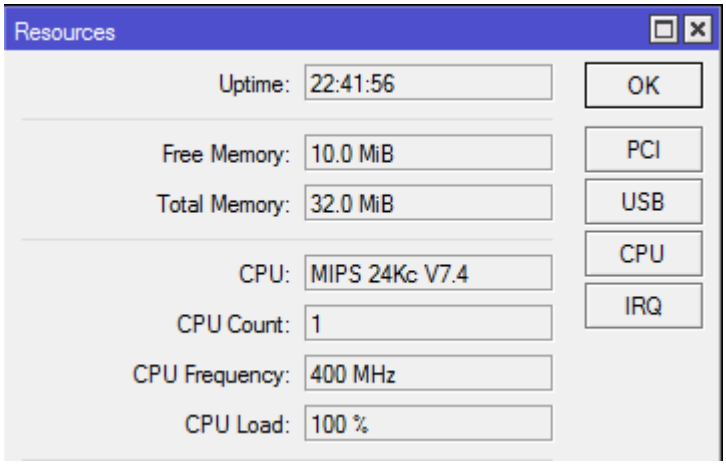
V prvním testu ještě nebyl vysílán multicast, tudíž procházelo linkou čistě 100 Mbps s tím, že docházelo ke změně velikosti rámců během testu. Z výsledku je patrné, že zařízení měla problém s průchodem velmi malých rámců, kde docházelo až k 70% ztrátovosti. Od rámců o velikost 1028 B docházelo k přenosu bez ztrát. Naopak největší rámce o velikosti 1522B neprošly vůbec, jelikož Juniper a MikroTik nezvládal přenést rámce s takto velkým MTU vzhledem k použití 802.1q tagu a dvou MPLS návěští.

Byla odhalena taktéž nedokonalost zařízení MikroTik, který veškerý provoz zpracovává softwarově (viz obrázek 3.6). Ostatní zařízení vše zpracovávala hardwarově.

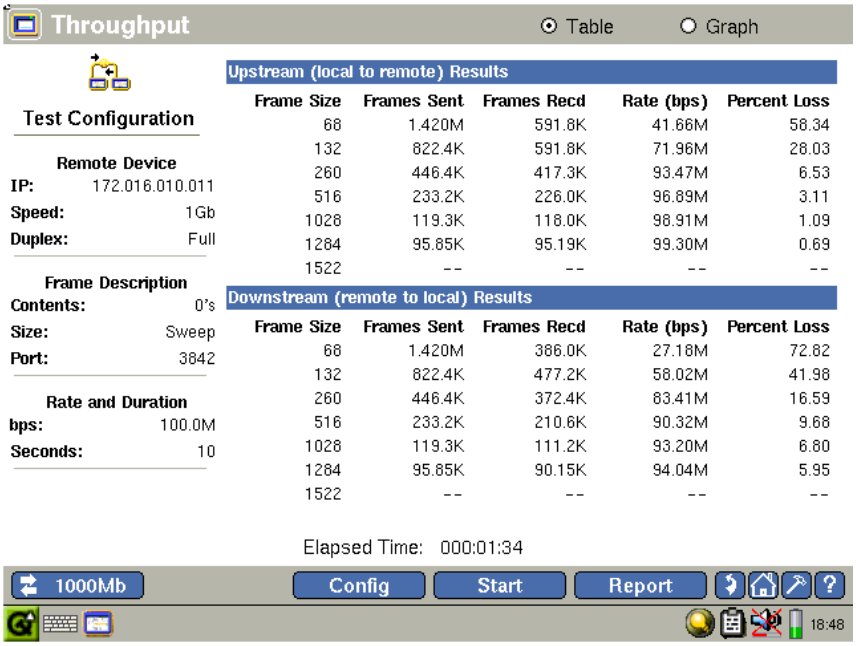
V dalším testu byl do sítě puštěn multicast, avšak stále nebyla aplikována žádná podpora QoS. Na obrázku 3.7 můžete sledovat, že ztrátovost větších rámců dosahovala +- 5-6 %, taktéž docházelo k rozpadům obrazu. Mějmě na paměti, že datový tok multicastu byl ze zdroje +- 12 Mbps. Docházelo tedy k zpracovávání vždy jedno paketu z jednoho rozhraní a druhého paketu z druhého rozhraní. Taktéž lze sledovat že v opačném směru bylo stále přenášo 100 Mbps s nepatrnou ztrátovostí (linka není



Obr. 3.5: Test propustnosti.



Obr. 3.6: Vytížení CPU u zařízení MikroTik.

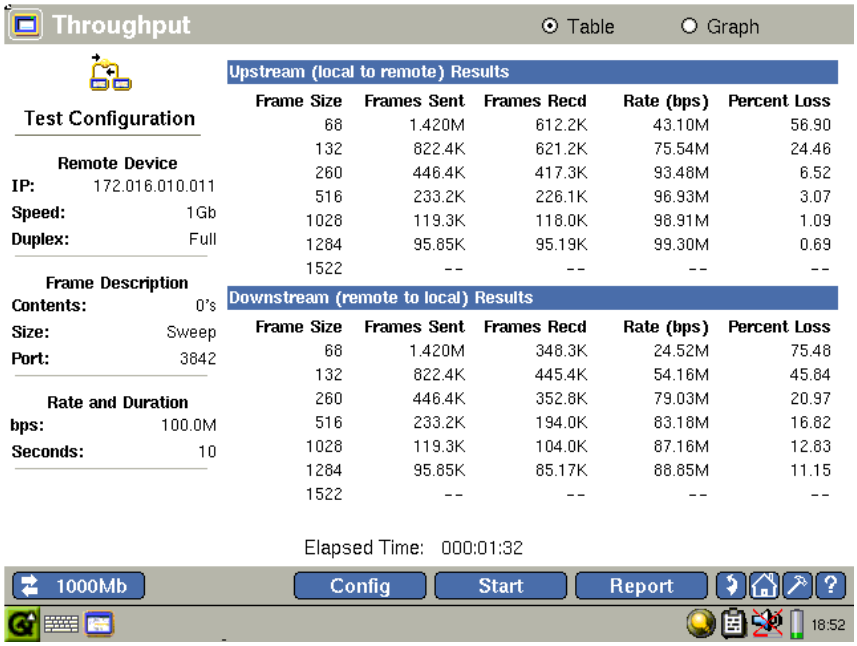


Obr. 3.7: Test propustnosti s multicastem.

v tomto směru co se týče multicastu využita).

Po aplikování pravidel QoS, kde multicastový provoz byl zařazen do nejvyšší fronty, byl rázem multicast přenášen bez ztrát a na klientském zařízení byl zobrazen bez rozpadu obrazu. Situace lze vidět i na testeru, kde ve směru remote-to-local docházelo ke ztrátovosti +- 12 Mbps, což je přesně velikost multicastového streamu. Zatímco bez aplikování QoS docházelo ke ztrátovosti +- 6 %, což odpovídá principu, že z každého zařízení bylo vždy bráno po 1 paketu na výstupní rozhraní.

Situaci s rozpadem lze taktéž sledovat na zachycených snímcích z klientského zařízení, ty naleznete na obrázku 3.9.



Obr. 3.8: Test propustnosti s multicastem a aplikovaným QoS.

Obr. 3.9: Porovnání multicastu, nahoře bez a dole s podporou QoS.

Přenos multicastu byl testován jak přes rozhraní VLL tak přes rozhraní VPLS. V obou případech byl přenost multicastového provozu úspěšný.

L3 VPN přes MPLS síť

Na samotný závěr této práce byla sestavena L3 VPN síť. Do každého prvku byl zapojen zákazník s jinou podsítí. Veškeré tyto podsítě byly poté směrovány na virtuálním směrovači, tzv. Virtual Routing and Forwarding (VRF). Ten byl aplikován na všech zařízeních. Přiřazena adresace zákazníka byla dle tabulky 3.3

Tab. 3.3: Adresace zákazníka s VPN.

Zařízení	Síť	Rozhraní pro připojení
R1	172.16.10.0/24	e1/2
R2	172.16.20.0/24	fe-0/0/6.0
R3	172.16.30.0/24	e5

Tomuto zákazníkovi byl přidělen Route Distinguisher (RD) 20:0. Zároveň na všech směrovačích byl spuštěn BGP proces, který tyto informace přenášel v Network Layer Reachability Information (NLRI). Byl taktéž povolen import a export do zmíněné VRF pouze sítím, které mají RT 20:0.

Na následujícím výpisu ze zařízení Brocade lze sledovat úspěšné oddělení zákaznických sítí od ostatních připojených rozhraních. Nikdo se tak do jeho sítě nedostane.

```
telnet@CER#sh ip route vrf CustB
Total number of IP routes: 3
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
STATIC Codes - d:DHCPv6
        Destination        Gateway    Port        Cost        Type Uptime src-vrf
1       172.16.10.0/24     DIRECT     eth 1/2     0/0         D    12m41s -
2       172.16.20.0/24     DIRECT     LDP (0)     200/0       Bi   12m0s  -
3       172.16.30.0/24     DIRECT     LDP (1)     200/0       Bi   12m0s  -
```

4 ZÁVĚR

V rámci řešení diplomové projektu jsem se seznámil s principy technologie MPLS a řešení různých forem transportu dat přes síť MPLS. Po nabytí teoretického základu jsem navrhnul síť, na které jsem se snažil jednotlivé principy ověřit. Nejdříve virtualizovaně a poté na skutečném hardware.

Analýzou paketů v programu WireShark jsem si osvojil, jakým způsobem probíhá zapouzdření a jaké výhody to přináší do současných sítí.

Prakticky jsem nabral zkušenosti s klasickou čistou MPLS sítí a poté navazujícími aplikacemi privátních sítí na druhé (Virtual Private LAN Services, Virtual Leased Line) a třetí vrstvě (MPLS VPN). Všechny variace privátních sítí pro svoji funkčnost potřebují jádro sítě, které podporuje MPLS směrování.

Každá variace má své výhody a nevýhody - jednoznačnou výhodou obou variací je, že na směrovači zákazníka se nemusí na konfiguraci nic měnit při změně, veškeré nastavení se odehrává na okrajových směrovačích poskytovatele.

Poté již záleží jen na požadavcích zákazníka, zda-li chce svůj provoz tunelovat na L2 nebo L3 vrstvě. S tímto vznikají i problémy s redundancí, kdy na L2 bude kvůli spanning-tree protokolu jedna linka ze dvou vždy nevyužita. Zatímco při tunelování na třetí vrstvě může na spojích probíhat rozkládání zátěže mezi více linkami.

Na základě nabytých zkušeností během virtualizace a reálné simulace sítě v laboratorních podmínkách jsem vytvořil laboratorní úlohu pro studenty druhého ročníku bakalářského studijního programu do předmětu Architektura sítí. V této úloze jsou studenti seznámeni se základními principy MPLS technologie. Budou provádět analýzu paketu, při které si uvědomí, kde se MPLS návěští nachází. V závěru jim je demonstrováno praktické využití MPLS technologie v podobě Virtual Private LAN Services (VPLS). Z úlohy by měli získat základní poznatky o konfiguraci MPLS sítě. Úloha je přiložena jako příloha k této diplomové práci společně s operačním systém (na DVD).

Dále jsem testoval nutnost aplikování podpory kvality služeb v síti poskytovatele, aby nedocházelo k vzájemnému ovlivňování zákazníků. Velkým problémem bylo zařízení MikroTik, které veškerý provoz zpracovávalo pomocí software (docházelo k 100% vytížení CPU), zatímco zařízení Juniper a Brocade pracovaly na úrovni hardware. Taktéž jsem se potýkal s problémem maximální velikosti rámce.

Osobně mi zpracování této úlohu dopomohlo k proniknutí do systému konfigurace zařízení různých výrobců, kdy každý k nastavování přistupuje odlišně. V některých chvílích se situace jevila jako neřešitelná, avšak po trpělivém zkoumání a zkoušení se veškeré požadované náležitosti této diplomové práce podařilo spustit.

LITERATURA

[1] DE GHEIN, Luc. *MPLS Fundamentals.* Indianapolis: Cisco Press, 2007, 672 s. ISBN 1-58705-197-4

[2] GUICHARD, Jim, Ivan PEPELNJAK. *MPLS and VPN architectures.* Indianapolis: Cisco Press, 2001, 420 s. ISBN 1-58705-002-1.

[3] GUICHARD, Jim, Ivan PEPELNJAK a Jeff APCAR. *MPLS and VPN architectures, Volume II.* Indianapolis: Cisco Press, c2003, 470 s. ISBN 1-5870-5112-5.

[4] EVANS, John a Clarence FILSFILS. *Deploying IP and MPLS QOS for multiservice networks: theory and practice.* Amsterdam: Elsevier ; Morgan Kaufmann, 2007, xxiii, 431 s. ISBN 0-12-370549-5.

[5] LUO, Wei, Carlos PIGNATARO, Anthony CHAN a Dmitry BOKOTEY. *Layer 2 VPN Architectures.* Indianopolis: Cisco Press, 2004, 648. ISBN ISBN-13: 978-0-13-279851-8.

[6] KIŠKA, Martin. *Návrh spolehlivé podnikové sítě s podporou kvalitativních požadavků služeb*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2012. 54 s. Vedoucí práce byl doc. Ing. Vít Novotný, PhD.

[7] MIKROTIK. *MikroTik Wiki* [online]. 2008 [cit. 2013-12-14]. Dostupné z: http://wiki.mikrotik.com

[8] MPLS VPNs and Junos config groups: a match made in router heaven. WEIDENBACHER, Nik. *Packet Pushers* [online]. 2013 [cit. 2014-03-20]. Dostupné z: http://packetpushers.net/mpls-vpns-and-junos-config-groups-a-match-made-in-router-heaven/

[9] Deploying Datacenter MPLS/VPN on Junos. STRETCHB, Jeremy. *PacketLife* [online]. 2014 [cit. 2014-04-20]. Dostupné z: http://packetlife.net/blog/2014/apr/15/deploying-datacenter-mpls-vpn-junos/

SEZNAM ZKRATEK

ACL Access List

AS Autonomous System

ATM Asynchronous Transport Machine

AToM Any Transport over MPLS

BGP Border Gateway Protocol

BoS Bottom of Stack

C Customer

CE Customer Edge

DSCP Differentiated Service Code Point

EIGRP Enhanced Interior Gateway Routing Protocol

EoMPLS Ethernet over MPLS

FEC Forwarding Equivalence Classes

FR Frame-relay

HDLC High-Level Data Link Control

ICMP Internet Control Message Protocol

IP Internet Protocol

IS-IS Intermediate System to Intermediate System

ISP Internet Service Provider

LDP Label Distribution Protocol

LFIB Label Forwarding Information Base

LLDP Link Layer Discovery Protocol

LSP Label Switched Path

LSR Label Switching Router

MPLS MultiProtocol Label Switching

MPLS VPN MPLS Virtual private Network

MRU Maximum Recieve Unit

MTU Maximum Transfer Unit

MPBGP MultiProtocol-Border Gateway Protocol

NLRI Network Layer Reachability Information

OSPF Open Shortest Path First

P Provider

PPP Point-to-Point Protocol

PE Provider Edge

PHP Penultimate Hop Popping

QoS Quality of Services

RD Route Distinguisher

RIP Routing Information Protocol

RR Round Robin

RT Route Target

SAP Session Announcement Protocol

SP Strict Priority

STP Spanning Tree Protocol

SPWRR Strict Priority Weighted Round Robin

TTL Time to Live

TCP Transmission Control Protocol

TE Traffic Engineering

UDP User Datagram Protocol

VLL Virtual Leased Line

VPLS Virtual Private LAN Services

VPN Virtual Private Network

VRF Virtual Routing and Forwarding

WRR Weighted Round Robin

SEZNAM PŘÍLOH

A PŘILOŽENÁ KONFIGURACE JEDNOTLIVÝCH ZAŘÍZENÍ

A.1 Konfigurační soubor zařízení MikroTik

```
# jan/01/2002 01:30:12 by RouterOS 6.13
# software id = BLHX-JVG2
#
/interface bridge
add name=Lo1 protocol-mode=none
add disabled=yes name=bridge_VPLS10 priority=0x9000
add disabled=yes name=bridge_vll
/interface ethernet
set [ find default-name=ether1 ] name=ether1_mgmt
set [ find default-name=ether2 ] name=ether2_toJunOS
set [ find default-name=ether3 ] l2mtu=2028 name=ether3_toCER
set [ find default-name=ether4 ] name=ether4_VPLS
/interface vpls
add cisco-style=yes cisco-style-id=40 disabled=no l2mtu=1500 mac-address=
02:80:32:DE:99:A6 name=vll_JunOS pw-type=tagged-ethernet remote-peer=2.2.2.2
add cisco-style=yes cisco-style-id=10 disabled=no l2mtu=1500 mac-address=
02:94:FD:29:E8:09 name=vpls10_JunOS remote-peer=2.2.2.2
add cisco-style=yes cisco-style-id=10 disabled=no l2mtu=1500 mac-address=
02:FC:28:0F:D2:7B name=vpls_Brocade remote-peer=1.1.1.1
/ip neighbor discovery
set wlan1 discover=no
/interface vlan
add disabled=yes interface=bridge_VPLS10 name=vlan1 use-service-tag=yes vlan-id=700
add disabled=yes interface=ether5 name=vlan600 use-service-tag=yes vlan-id=600
add disabled=yes interface=ether4_VPLS name=vlan700 use-service-tag=yes vlan-id=700
/routing bgp instance
set default router-id=3.3.3.3
/interface bridge port
add bridge=bridge_VPLS10 disabled=yes interface=ether4_VPLS
add bridge=bridge_VPLS10 disabled=yes interface=vpls_Brocade
add bridge=bridge_vll disabled=yes interface=ether5
add bridge=bridge_vll disabled=yes interface=vll_JunOS
add bridge=bridge_VPLS10 disabled=yes interface=vpls10_JunOS
/ip address
add address=10.33.222.232/24 interface=ether1_mgmt network=10.33.222.0
add address=10.0.1.2/30 interface=ether3_toCER network=10.0.1.0
add address=10.0.2.2/30 interface=ether2_toJunOS network=10.0.2.0
add address=3.3.3.3/32 interface=Lo1 network=3.3.3.3
add address=172.16.30.1/24 interface=ether5 network=172.16.30.0
/ip firewall filter
add chain=input
add chain=forward
/ip route
add distance=1 gateway=10.33.222.1
/ip route vrf
add export-route-targets=20:0 import-route-targets=20:0 interfaces=ether5
route-distinguisher=20:0 routing-mark=custB
/mpls interface
```

```
set [ find default=yes ] mpls-mtu=1512
/mpls ldp
set enabled=yes lsr-id=3.3.3.3 transport-address=3.3.3.3 use-explicit-null=yes
/mpls ldp interface
add interface=ether3_toCER transport-address=3.3.3.3
add interface=ether2_toJunOS transport-address=3.3.3.3
/routing bgp instance vrf
add redistribute-connected=yes routing-mark=custB
/routing bgp network
add disabled=yes network=172.16.30.0/24 synchronize=no
/routing bgp peer
add address-families=ip,vpnv4 multihop=yes name=Brocade remote-address=1.1.1.1
remote-as=65530 ttl=default update-source=3.3.3.3
add address-families=ip,vpnv4 multihop=yes name=JunOS remote-address=2.2.2.2
remote-as=65530 ttl=default update-source=3.3.3.3
/routing ospf network
add area=backbone network=10.0.1.0/24
add area=backbone network=10.0.2.0/24
add area=backbone network=3.3.3.3/32
/routing pim interface
add protocols=igmp
/system leds
set 0 interface=wlan1
```

A.2 Konfigurační soubor zařízení Juniper

```
set version 12.1X44.3
set system host-name Juniper
set system root-authentication encrypted-password admin
set system name-server 208.67.222.222
set system name-server 208.67.220.220
set system login class super-user-local idle-timeout 30
set system login user admin uid 2001
set system login user admin class super-user
set system login user admin authentication encrypted-password
"$1$MTF1vyIJ$$IDisVFqDxhbhuE7fHmbs0/"
set system services ssh
set system services telnet
set system services xnm-clear-text
set system services web-management http interface vlan.0
set system services web-management http interface fe-0/0/7.0
set system services web-management https system-generated-certificate
set system services web-management https interface vlan.0
set system services web-management https interface fe-0/0/7.0
set interfaces fe-0/0/0 unit 0 family mpls
set interfaces fe-0/0/1 unit 0 family inet address 10.0.0.2/30
set interfaces fe-0/0/1 unit 0 family mpls
set interfaces fe-0/0/2 unit 0 family inet address 10.0.2.1/30
set interfaces fe-0/0/2 unit 0 family mpls
set interfaces fe-0/0/3 vlan-tagging
set interfaces fe-0/0/3 encapsulation vlan-ccc
set interfaces fe-0/0/3 unit 1 encapsulation vlan-ccc
set interfaces fe-0/0/3 unit 1 vlan-id 600
set interfaces fe-0/0/3 unit 1 family ccc
```

```
set interfaces fe-0/0/4 vlan-tagging
set interfaces fe-0/0/4 encapsulation vlan-ccc
set interfaces fe-0/0/4 unit 600 encapsulation vlan-ccc
set interfaces fe-0/0/4 unit 600 vlan-id 600
set interfaces fe-0/0/4 unit 600 family ccc
set interfaces fe-0/0/5 flexible-vlan-tagging
set interfaces fe-0/0/5 native-vlan-id 700
set interfaces fe-0/0/5 encapsulation vlan-vpls
set interfaces fe-0/0/5 unit 40 encapsulation vlan-vpls
set interfaces fe-0/0/5 unit 40 vlan-id 700
set interfaces fe-0/0/5 unit 40 family vpls
set interfaces fe-0/0/5 unit 701 encapsulation vlan-vpls
set interfaces fe-0/0/5 unit 701 vlan-id 701
set interfaces fe-0/0/5 unit 701 family vpls
set interfaces fe-0/0/6 unit 0 family inet address 172.16.20.1/24
set interfaces fe-0/0/6 unit 0 family mpls
set interfaces fe-0/0/7 unit 0 family inet address 10.33.222.231/24
set interfaces lo0 unit 0 family inet address 2.2.2.2/32
set interfaces vlan unit 0 family inet address 192.168.1.1/24
set routing-options router-id 2.2.2.2
set routing-options autonomous-system 65530
set protocols mpls interface fe-0/0/0.0
set protocols mpls interface fe-0/0/1.0
set protocols mpls interface fe-0/0/2.0
set protocols mpls interface lo0.0
set protocols bgp group vpn type internal
set protocols bgp group vpn local-address 2.2.2.2
set protocols bgp group vpn import vpn-import-vrf
set protocols bgp group vpn family inet unicast
set protocols bgp group vpn family inet-vpn unicast
set protocols bgp group vpn export vpn-export-vrf
set protocols bgp group vpn peer-as 65530
set protocols bgp group vpn neighbor 3.3.3.3
set protocols bgp group vpn neighbor 1.1.1.1
set protocols ospf area 0.0.0.0 interface fe-0/0/1.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface fe-0/0/2.0
set protocols ldp transport-address 2.2.2.2
set protocols ldp interface fe-0/0/1.0
set protocols ldp interface fe-0/0/2.0
set protocols ldp interface all
set protocols l2circuit neighbor 1.1.1.1 interface fe-0/0/4.600
virtual-circuit-id 600
set protocols l2circuit neighbor 1.1.1.1 interface fe-0/0/4.600
encapsulation-type ethernet-vlan
set protocols lldp interface all
set protocols stp
set policy-options policy-statement vpn-export-vrf term 1 from protocol direct
set policy-options policy-statement vpn-export-vrf term 1 from interface fe-0/0/6.0
set policy-options policy-statement vpn-export-vrf term 1 then community add vpn1
set policy-options policy-statement vpn-export-vrf term 1 then accept
set policy-options policy-statement vpn-export-vrf term 2 then reject
set policy-options policy-statement vpn-import-vrf term 1 from protocol bgp
set policy-options policy-statement vpn-import-vrf term 1 from community vpn1
set policy-options policy-statement vpn-import-vrf term 1 then accept
set policy-options policy-statement vpn-import-vrf term 2 then reject
```

```
set policy-options community vpn1 members target:20:0
set security forwarding-options family mpls mode packet-based
set security zones security-zone trust interfaces fe-0/0/7.0
set security zones security-zone trust interfaces fe-0/0/0.0
set routing-instances CustB instance-type vrf
set routing-instances CustB interface fe-0/0/6.0
set routing-instances CustB route-distinguisher 20:0
set routing-instances CustB vrf-import vpn-import-vrf
set routing-instances CustB vrf-export vpn-export-vrf
set routing-instances CustB vrf-target target:20L:0
set routing-instances CustB vrf-table-label
set routing-instances CustB routing-options auto-export
set routing-instances vpls instance-type vpls
set routing-instances vpls vlan-id none
set routing-instances vpls interface fe-0/0/5.40
set routing-instances vpls interface fe-0/0/5.701
set routing-instances vpls protocols vpls no-tunnel-services
set routing-instances vpls protocols vpls vpls-id 10
set routing-instances vpls protocols vpls neighbor 3.3.3.3
set routing-instances vpls protocols vpls neighbor 1.1.1.1
```

A.3 Konfigurační soubor zařízení Brocade

```
Current configuration:
!
ver V5.6.0bT183
!
cpu-port
!
!
no spanning-tree
!
vlan 1 name DEFAULT-VLAN
 no untagged ethe 1/4 ethe 1/7
!
vlan 700
 priority 7
!
vrf CustB
 rd 20:0
 ip router-id 1.1.1.1
 route-target export 20:0
 route-target import 20:0
 address-family ipv4
 exit-address-family
exit-vrf
!
telnet server
!
hostname CER
!
router ospf
 area 0
!
```

```
interface loopback 1
 ip ospf area 0
 ip address 1.1.1.1/32
!
interface management 1
 ip address 10.33.222.230/24
 enable
!
interface ethernet 1/1
 enable
 ip ospf area 0
 ip address 10.0.0.1/30
!
interface ethernet 1/2
 enable
 vrf forwarding CustB
 ip address 172.16.10.1/24
!
interface ethernet 1/3
 enable
 ip ospf area 0
 ip address 10.0.1.1/30
!
interface ethernet 1/4
 enable
 no spanning-tree
!
interface ethernet 1/5
 port-name VPLS_interface
 enable
!
interface ethernet 1/7
 enable!
interface ethernet 1/9
 enable
!
interface ethernet 1/11
 enable
!
router bgp
 local-as 65530
 neighbor 2.2.2.2 remote-as 65530
 neighbor 2.2.2.2 ebgp-multihop 3
 neighbor 2.2.2.2 update-source 1.1.1.1
 neighbor 3.3.3.3 remote-as 65530
 neighbor 3.3.3.3 ebgp-multihop 3
 neighbor 3.3.3.3 update-source 1.1.1.1

 address-family ipv4 unicast
 exit-address-family

 address-family ipv4 multicast
 exit-address-family

 address-family ipv6 unicast
 exit-address-family
```

```
 address-family ipv6 multicast
 exit-address-family

 address-family vpnv4 unicast
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community both
 neighbor 3.3.3.3 activate
 neighbor 3.3.3.3 send-community both
 exit-address-family

 address-family vpnv6 unicast
 exit-address-family

 address-family ipv4 unicast vrf CustB
 local-as 65530
 neighbor 2.2.2.2 remote-as 65530
 neighbor 2.2.2.2 ebgp-multihop 3
 neighbor 2.2.2.2 update-source 1.1.1.1
 neighbor 3.3.3.3 remote-as 65530
 neighbor 3.3.3.3 ebgp-multihop 3
 neighbor 3.3.3.3 update-source 1.1.1.1
 redistribute connected
 exit-address-family
!
router mpls
 mpls-interface e1/1
  ldp-enable
 mpls-interface e1/3
  ldp-enable
 vll vlan600 600
  vll-peer 2.2.2.2
  vlan 600
   tagged e 1/7
 vpls vpls1 10
  vc-mode raw-pass-through
  vpls-peer 3.3.3.3 2.2.2.2
  vlan 700
   untagged ethe 1/4
!
access-list 100 permit ip any any dscp-marking 32
!
!
lldp enable ports ethe 1/1 to 1/24
lldp run
!
end
```

B LABORATORNÍ ÚLOHA

B.1 Přiložené DVD s laboratorní úlohou

V obalu diplomové práce je přiložené DVD s operačním systémem, ve kterém jsou nainstalované veškeré zdrojové soubory nutné pro spuštění úlohu a správné fungování. Jelikož je úloha dvojitě virtualizovaná, je možné spustit úlohu na jakémkoliv počítači s podporou importu formátu *.ova.

Na DVD se nachází:

\xkiska00_diplomova_prace.pdf
\Windows XP.ova (úloha s veškerým obsahem)
\conf\... (úplné konfigurační soubory)

B.2 Znění laboratorní úlohy

Níže je přiloženo znění úlohy pro studenty 2. ročníku předmětu BARS. Vzhledem k tomu, že celá diplomová práce byla psána v jazyku LaTeX a požadavek na úlohu byl, aby byla možná lehká editace, byla úloha uložena z formátu *.doc do *.pdf a vložena. Z tohoto důvodu má jiné formátování než celé znění diplomové práce.

Technologie MultiProtocol Label Switching v sítích Ethernet

Cíl:

Seznámení se s protokolem MultiProtocol Label Switching a jeho výhod pro vytvoření privátních sítí

Požadavky na vybavení pracoviště:

1. Virtuální Operační systém Windows XP
2. 6x virtualizované zařízení MikroTik s operačním systémem RouterOS verze 6.7
3. Nainstalované programu pro virtualizaci, sestavení topologie a analýzu paketů – VirtualBox, Graphical Network Simulator 3 (GNS3) a WireShark

Úkol:

1. Seznámit se s principem směrování pomoci technologie MultiProtocol Label Switching.
2. Zprovoznit síť s podporou MPLS.
3. Analyzovat pakety ping procházející přes tuto síť
4. Zprovoznit síť MPLS s podporu privátních sítích na druhé vrstvě (Virtual Private LAN Services)

Teoretický úvod:

Důvodu ke vzniku MultiProtocol Label Switching

Mnoho let byly pro transportní účely na WAN sítích používané dnes již zastaralé protokoly jako Asynchronous Transport Machine (ATM) a Frame-relay (FR). S příchodem MPLS došlo ke zjednodušení vybudování komplexní sítě nad jednou infrastrukturou. Jednoduchost při zavádění se setkala s velkým úspěchem u poskytovatelů. Ti tak mohli nabídnout svým zákazníkům výhody MultiProtocol Label Switching (MPLS) sítě a získat tak výhodu nad konkurencí.

Počáteční výhody MPLS tkvěly v myšlence jednoduché záměny návěští na vstupním a výstupním rozhraní. Tento princip měl ulehčit prohledávání Internet Protocol (IP) směrovacích tabulek a urychlit celý proces směrování. Postupem času došlo ke zlepšení výkonu páteřních směrovacích směrovačů a smazala se tak tato výhoda. Nicméně vývoj MPLS pokračoval a byly vyvinuty další možnosti aplikace. Některé z nich jsou rozebrány ve zbytku práce. MPLS bylo stvořeno pro transport vyšších protokolů přes páteřní síť poskytovatele. Můžeme pomoci něj přenést například tyto protokoly – IPv4, IPv6, Ethernet, High-Level Data Link Control (HDLC), Point to-Point Protocol (PPP) a další. Této schopnosti se říká Any Transport over MPLS (AToM). Směrovače nepotřebují znát obsah vlastního paketu, stačí jen vědět, které návěští mají vyměnit za které.

Možnou aplikací těchto principů je např. Traffic Engineering (TE), Ethernet over MPLS (EoMPLS), MPLS Virtual private Network (MPLS VPN), Virtual Private LAN Services (VPLS), Virtual Leased Line (VLL) a další. Neméně důležitou výhodou je možnost mít páteřní síť bez spěrovacího protokolu BGP.

Výhodou MPLS je, že počet návěští v zásobníku (stacku) není omezen. Tímto způsobem mohou být poskytovány privátní sítě.

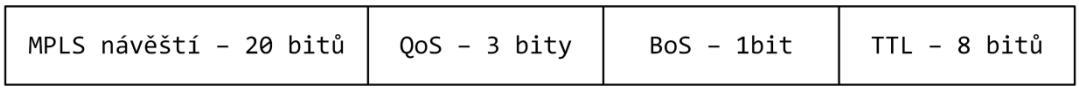
Pro správnou funkčnost postačí technologii MPLS tři základní operace, mezi které patří swap, push a pop. Jedná se o záměnu, přidání nebo odebrání návěští. Vždy poslední návěští z nich má nastaven bit Bottom of Stack (BoS) na 1, tím naznačuje, že je poslední a že se pod ním již skrývá transportovaný protokol.

Rozbor paketu MPLS

MPLS záhlaví se skládá z 32 bitů. 20 jich je předurčeno pro číslování návěští. Další bity jsou určenu pro Quality of Services (QoS, 3 bity), Time to Live (TTL, 8 bitů) a 1 bit Bottom of Stack (BoS), který zaručí, že návěští je posledním v zásobníku (bit je nastavený na hodnotu 1). Ačkoliv v původním RFC 3032 se tři bity pro 10 QoS jmenovaly jako experimentální (EXP), postupem času je všichni výrobci začali využívat pro zavedení QoS. Tudíž v novějším RFC 5462 je definováno využití těchto

tří bitů právě pro QoS (skladbu MPLS návěští můžete vidět na Obrázek 1). Základní princip MPLS tehchnologie je ve výměně návěští. Může dojít ke třem různým operacím:

- Swap (záměna) – dojde k záměně jednoho návěští za druhé.
- Pop (odebrání) – z původního paketu je odebráno jedno návěští a zbude jen transportovaný protokol, nebo po odebrání zůstane ještě jedno návěští (či více).
- Push (přidání) – k původnímu paketu se přidá nové návěští nebo už ke stávajícím návěští je přidáno další.



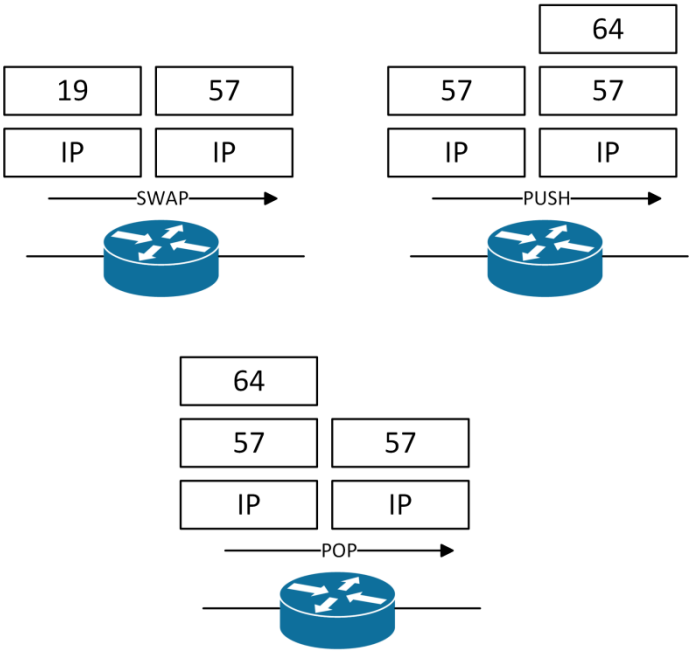
Obrázek 1: Tvar návěští MPLS.

Ukázku můžete sledovat na Obrázek 2.

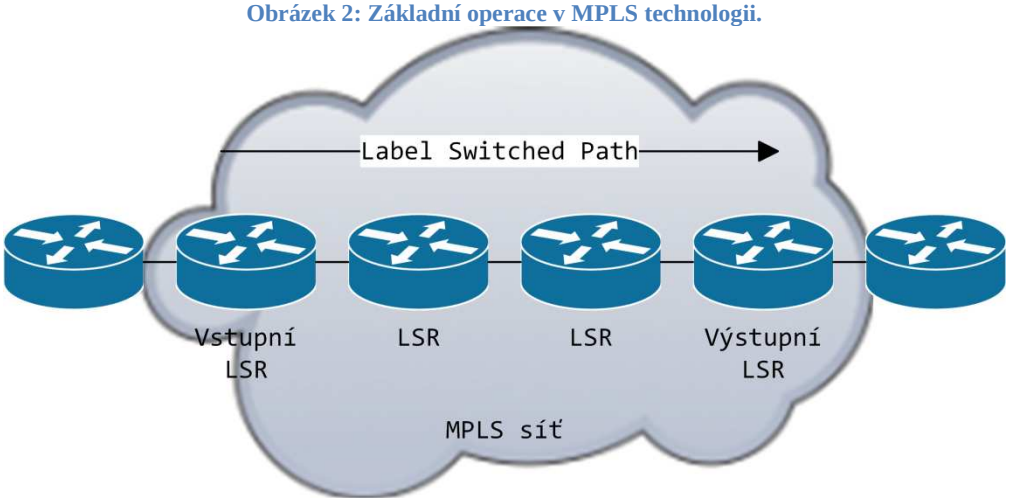
U MPLS je důležité rozlišovat význam zkratek, které ve zbytku textu budu uvádět. Nyní zde uvedu základní zkratky, které s MPLS souvisí. Popis, která zkratka souvisí s jakým významem je nejlépe patrný na Obrázek 3.

- Label Distribution Protocol (LDP) – slouží pro distribuci návěští mezi ostatní směrovače, které podporují MPLS.
- Label Switching Router (LSR) – každý směrovač, na kterém je spuštěné LDP.
- Label Switched Path (LSP) – cesta k cíli, při které dochází k záměně návěští.

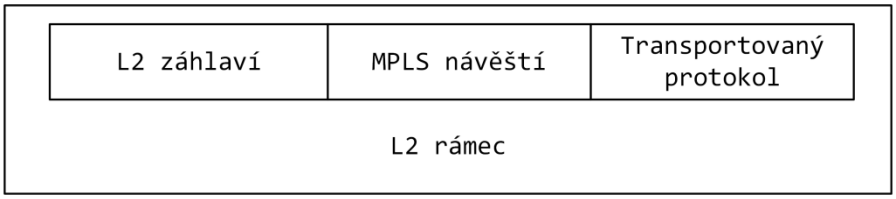
Je důležité si uvědomit, kde se návěští MPLS v celém paketu nachází, to lze vidět na Obrázek 4. Již v ethernet rámci je stanoveno v poli Ethertyp hex hodnota 8847, která naznačuje přítomnost MPLS návěští.



Obrázek 2: Základní operace v MPLS technologii.



Obrázek 3: MPLS síť.



Obrázek 4: Umístění záhlaví MPLS.

MPLS návěští

Pro samotné návěští je vyhrazeno 20 bitů, tudíž může nabývat různých hodnot při maximálním počtu kombinací $2^{20} - 1 = 1048575$. Prvních 0 - 15 hodnot je vyhrazeno pro zvláštní účely. Tudíž LSR tyto hodnoty nemůže použít pro posílání normálních paketů. Ostatní hodnoty jsou použity pro přidělování pod stejnou Forwarding Equivalence Classes (FEC), které spojují shodné vlastnosti – například nexthop adresa. Význam některých návěští z řad hodnot 0-15 je zmíněn v následujících odstavcích.

Implicit-NULL

Tato funkce se nazývá Penultimate Hop Popping (PHP). Výstupní LSR při něm pošle k centrálnímu LSR návěští Implicit-NULL (hodnota 3) a centrální LSR tudíž ví, že má paket posílat již bez MPLS návěští. Toto posílání má však taktéž své nevýhody. Dojde při něm ke ztrátě informace QoS.

Hlavním účelem je, že výstupní LSR nemusí provádět dvě vyhledávání (IP lookup a MPLS lookup). Zmenší se tím nároky na výstupní LSR.

Explicit-NULL

Jakmile výstupní LSR zašle centrálnímu LSR MPLS návěští s hodnotou 0, znamená to, že mu má posílat návěští s hodnotou 0. Výstupní LSR tudíž ví, že nemá hledat další návěští, ale že má provést přímo IP lookup. Výhodou tohoto je, že se k výstupním LSR dostane vždy informace o třech QoS bitech

Label Discovery Protocol

Již víme, že u MPLS jde především o výměnu návěští, které musí být schopen dělat každý LSR směrovač. Z toho vyplývá, že návěští musí být v síti distribuovány. Distribuce návěští mohla být implementována do již známých vnitřních směrovacích protokolů Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP) a Intermediate System to Intermediate System (IS-IS), nebo mohl být vytvořen zcela nový protokol.

Problémem je, že se v tuto chvíli v sítích používají všechny výše zmíněné protokoly a muselo by to tak být implementováno čtyřikrát. Z tohoto důvodu byl vytvořen Label Distribution Protocol (LDP), který se stará o výměnu návěští mezi sousedními LSR se shodnými vlastnostmi. U MPLS záleží totiž na např. stejné next-hop adrese. Cesty, které mají podobné právě tyto a např. ještě QoS vlastnosti jsou shrnuty do jedné Forwarding Equivalence Classes (FEC), pro které je vygenerováno jedno návěští.

V přenosu mezi jednotlivými autonomními systémy (AS) již nedochází k přenosu návěští pomocí LDP. O přenos se již stará MultiProtocol-Border Gateway Protocol (MPBGP), který je uzpůsoben k přenosu různých protokolů.

Navázání sousedství

V případě, že se na rozhraní zapne LDP ihned tento směrovač začne zasílat Hello zprávy na multicast adresu 224.0.0.2 – na té naslouchají všechny směrovače, které podporují multicast. Pro Hello zprávy je využit transportní protokol User Datagram Protocol (UDP) s cílovým portem 646 na kterém každé rozhraní, kde je povoleno LDP naslouchá. V této zprávě je i tzv. Hold time, který specifikuje jak dlouhá má směrovač čekat, dokud sousední LSR nevyškrtne ze své databáze LDP sousedů v případě, že Hello paket nedorazí. Tyto Hello a Hold time intervaly jsou ve výchozím nastavení 5 a 15 sekund.

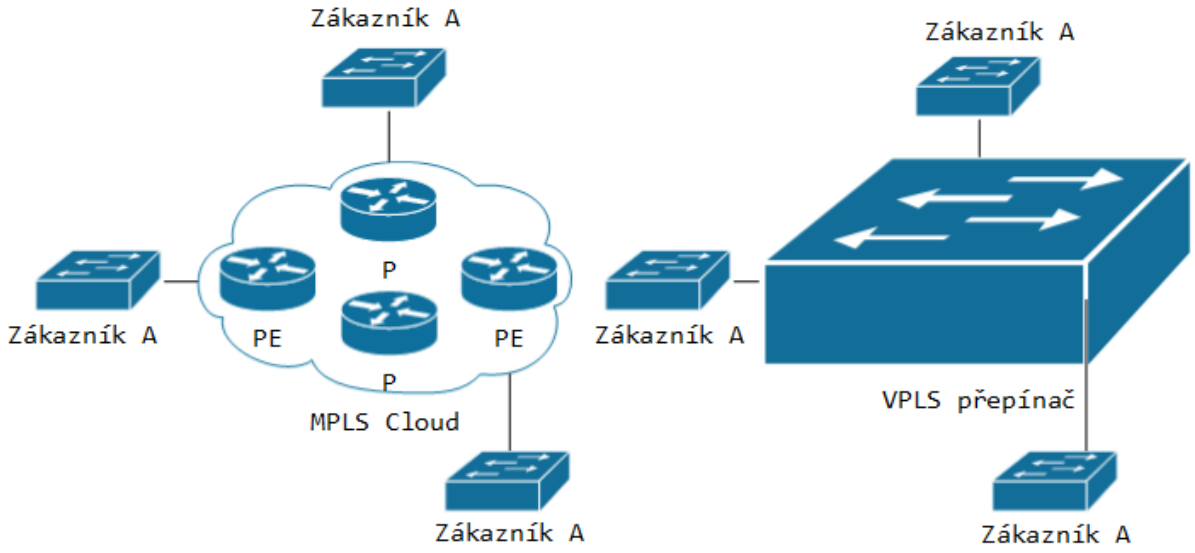
Navázání spojení

V případě, že se dva LSR navzájem objeví pomocí LDP Hello zpráv, pokusí se navázat přes Transmission Control Protocol (TCP) spojení. Pokouší se otevřít TCP port 646 na opačném LSR. V případě, že se podaří otevřít TCP spojení, tak si navzájem oba LSR směrovače přes počáteční zprávy vyjednají parametry tohoto LDP spojení. Navzájem si taktéž vymění jednotlivá návěští pro různé FEC.

V každé zprávě, které jsou posílány mezi dvěma LSR je tzv. LDP identifikátor původce této zprávy. Pokud sousední směrovač nemá cestu k této adrese, spojení se nenaváže. Tímto způsobem lze taktéž vytvářet cílené relace (targeted sessions) při vytváření privátních tunelů.

Možnosti tunelování L2 provozu přes MPLS síť

S MPLS vznikla myšlenka vytvoření virtuálního přepínače, který by existoval nad L3 sítí poskytovatele. Tento přepínač by měl udržet privátní data uživatelů a neměl je rozšiřovat do síti jiných zákazníků. Dále by se měl přizpůsobit podstatě sítí Ethernet, kterým je způsob komunikace – všesměrová, multicastová a unicastová. Takový přepínač by se měl taktéž starat a přenos L2 servisních protokolů – např. Link Layer Discovery Protocol (LLDP) Spanning Tree Protocol (STP). Taktéž by musel být schopen učení MAC adres a jejich stárnutí. Technologie, která se k tomuto používá, je pojmenována – Virtual Private LAN Services (VPLS). Princip můžete vidět na obrázku. 1.5



Obrázek 5: ukázkové schéma s VPLS.

Důvod proč VPLS vzniklo je jednoduchý. Při využití AToM sice můžeme přenést jakýkoliv protokol, avšak pouze ve smyslu point-to-point. Co se týče MPLS VPN, tak ty umožňují pouze spojení, která podporují IP protokol.

Zákazník může ještě použít pro připojení svých pracovišť technologii Ethernet over MPLS (EoMPLS), avšak jakékoliv spojení vytvořené pomocí této technologie je taktéž jen point-to-point. Spojení se též nazývá Virtual Leased Line (VLL).

Maximální počet naučených MAC adres

Vzhledem k principu Ethernet technologie dochází na krajních PE směrovačích k učení většího počtu MAC adres. V případě připojení velké sítě zákazníka, může dojít k přeplnění MAC tabulky. To by mohlo mít za následek neblahý vliv na vlastní síť poskytovatele. Proto je možné omezit maximální počet naučených MAC adres například na rozhraní, nebo konkrétní VLAN zákazníka.

Cílené LLDP spojení

Pro vytvoření VPLS je nutné zapouzdřit ethernet rámec dvakrát. První návěští označuje tzv. instanci VPLS. Zajišťuje, že data dojdou ke správným PE směrovačům. Vrchní návěští slouží již jen pro základní operace MPLS pop, push a swap. Pro vytvoření VPLS se používá tzv. cílené LDP spojení. To je navázáno na konkrétní PE směrovač poskytovatele. V případě přidání dalšího PE směrovače musíme navázat LDP spojení na všechny předchozí PE směrovače, které jsou součástí jedné VPLS domény.

Postup práce:

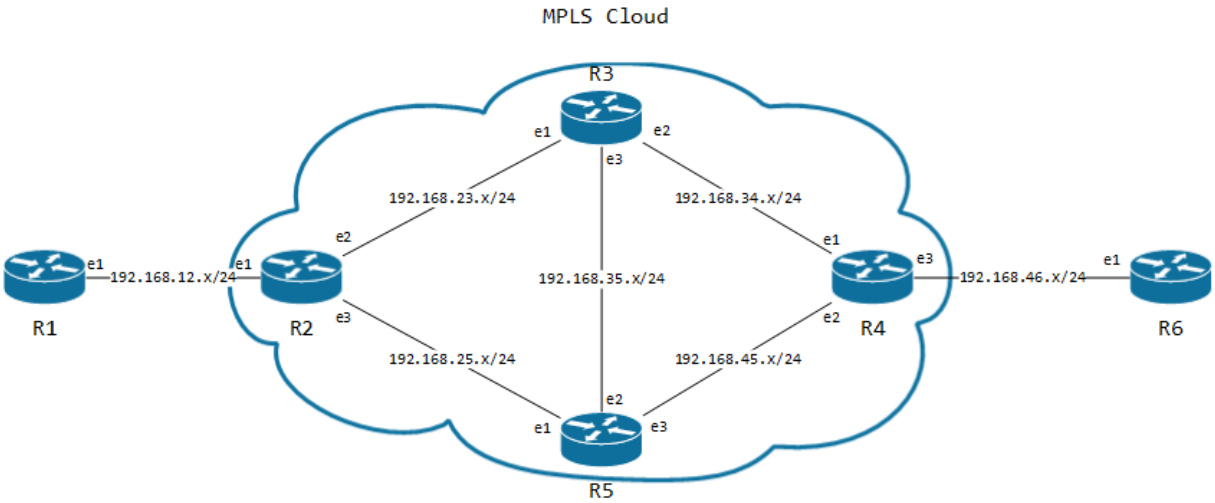
Úkol č. 1: Nastudování teoretického úvodu, který budete potřebovat pro nastavení a pochopení principů směrování v síti.

Úkol č. 2 a 3.:

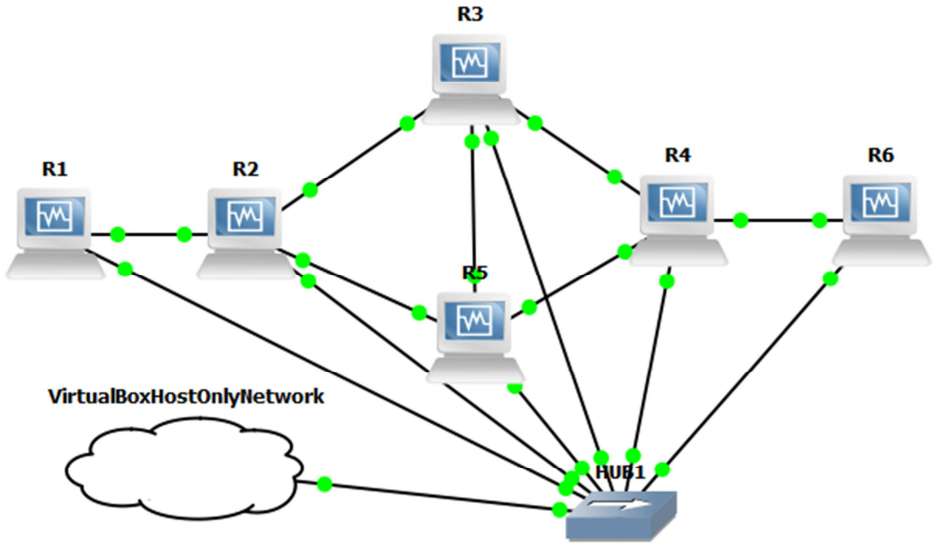
Je pro vás nachystaná síť s šesti virtualizovanými směrovači MikroTik V prostřední VirtualBox a GNS3. Spusťte soubor na ploše lab_uloha_topologie.net, díky kterému se Vám otevře program GNS s celou topologií. Veškeré nastavení sítě je pro Vás předpřipraveno. Na Vás zbývá nastavit směrovač R2 (Provider Edge).
Adresaci sítě naleznete na obrázku. Co se týče adresace prvků, jsou dodržena následující pravidla:

1. Jsou použity sítě třídy B.
2. Mezi dvěma prvky je adresa sítě rovna vždy menšímu a většímu číslu (R1–R2 ... 192.168.12.0/24).
3. Prvek s abecedně menším jménem má nižší adresu (.1) a prvek s abecedně větším jménem má větší adresu (.2).
4. Vždy byly připojeny rozhraní od abecedně menších prvků k abecedně větším prvkům. R3(e1)–(e2)R2, R3(e2)–(e1)R4, R3(e3)–(e2)R6.
5. Rozhraní ether4 je vždy připojeno do zařízení HUB k virtuální síťové kartě (VirtualBox Host-Only Network).
6. Mgmt adresa prvku korespoduje s virtuální sítí VirtualBox Host-Only (192.168.56.0/24). Adresa jednotlivých prvků souvisí se jménem prvku (IP mgmt adresa R3 – 192.168.56.3/24).

Ačkoliv RouterOS inkrementuje rozhraní od 1 (ether1), program GNS3 jako počáteční index volí 0 – rozhraní ether1 na prvku R1 je v programu GNS identifikováno jako e0.
Správu jednotlivých prvků budete dělat přes obslužný program WinBox, který taktéž naleznete na ploše. Login pro přihlášení je admin, heslo není použito.



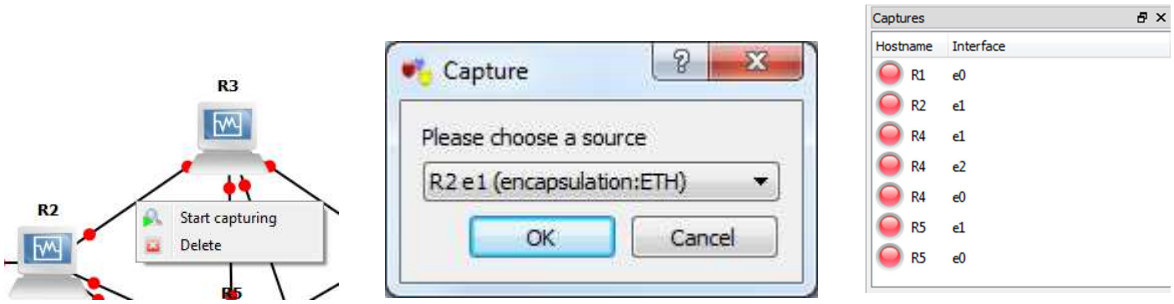
Obrázek 6: topologie MPLS sítě.



Obrázek 7: topologie MPLS sítě v programu GNS3.

Tím, že jsou veškerá nastavení přednastaveno je míněno následující: na všech zařízeních jsou přiřazeny IP adresy dle adresního plánu. Je zapnutý dynamický směrovací protokol OSPF na všech potřebných rozhraních. Na Vás je pouze zprovoznění MPLS na směrovači R2 a sledování provozu na lince R2-R3.

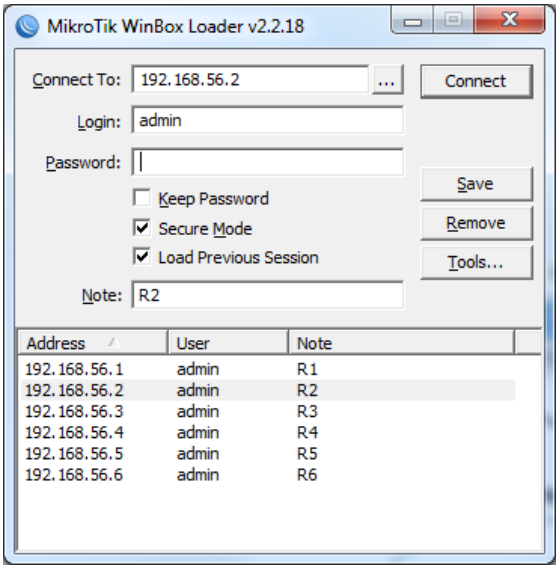
1. Spusťte VirtualBox a naimportujte soubor windowsxp.ova (soubor -> importovat aplianci, potvrďte výchozí nastavení a počkejte, než se soubor naimportuje. Poté tyto WinXP spusťte. **Od této chvíle budete pracovat pouze v nich.**
2. Spusťte soubor lab_uloha_topologie.net, který naleznete na ploše, tím se vám otevře vaše topologie.
3. Než celou topologii spustíte (doporučuji spouštět prvek po prvku) nastavte zachycování paketů programem WireShark na každé lince mezi zařízeními. Stačí kliknout na linky pravým a zmáčknout Start Capturing a potvrdit. Linka se Vám přemístí do lišty Captures. Postup opakujte i pro zbylé spoje. (viz Obrázek 8)



Obrázek 8: Nastavení zachytávání paketů.

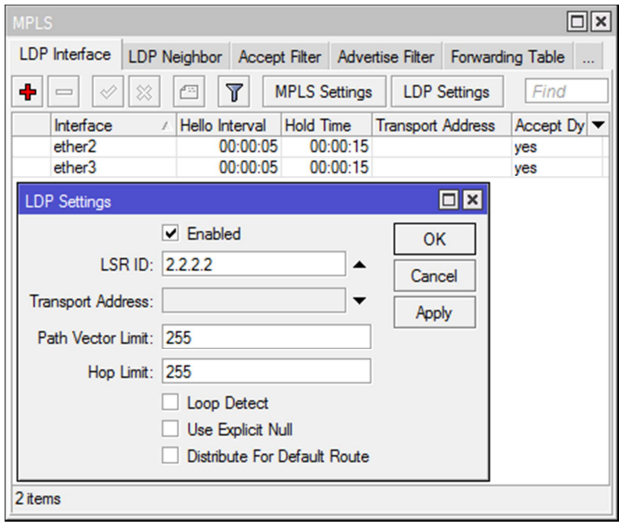
4. Doporučuji ze začátku pro jednudochost nezapínat prvek R5. Tudíž na každý prvek krom R5 klikněte pravým a zmáčkněte Start. Spustí se vám okna VirtualBoxu, ve kterém probíhá virtualizace směrovače MikroTik se systémem RouterOS.

5. Přihlašte se k prvku R2 přes program WinBox. (viz Obrázek 9)



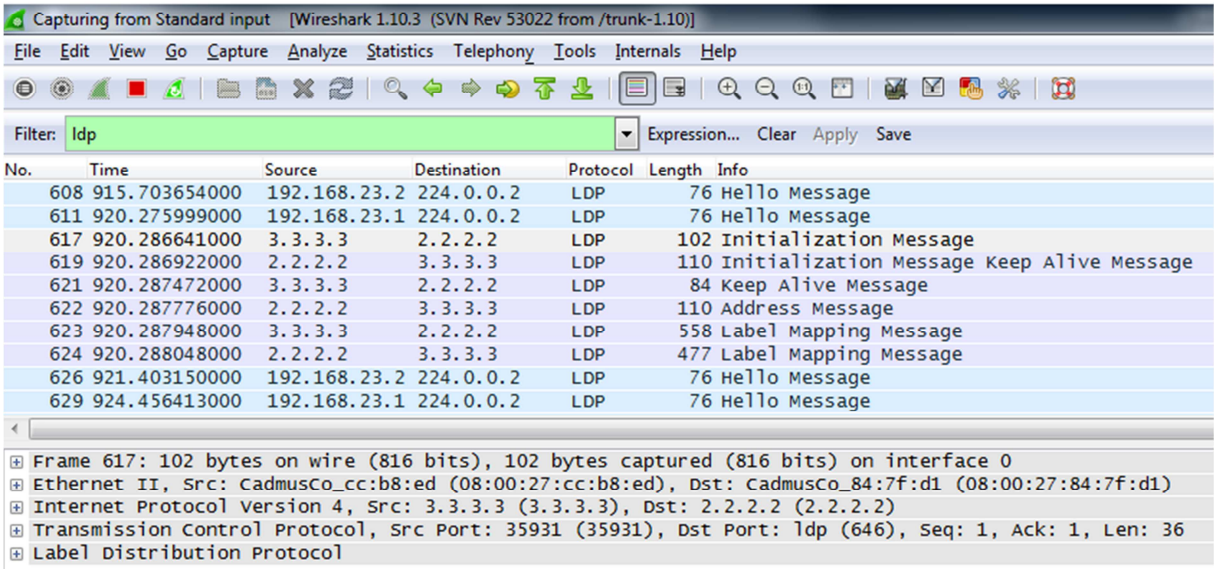
Obrázek 9: Přihlášení k směrovači přes program WinBox.

6. Zapnutí protokolu LDP provedete v záložce MPLS -> MPLS -> LDP Sttings. Poté pomocí tlačítka PLUS přidejte rozhraní, na kterých bude MPLS povoleno (ether2 a ether3). Do políčka LSR ID ještě vyplňte identifikátor směrovače (2.2.2.2). (viz Obrázek 10)



Obrázek 10: Povolení LDP protokolu.

7. Nyní byste měli sledovat v programu WireShark zasílání Hello paketů na multicastovou adresu všech směrovačů (224.0.0.2) a navázání TCP spojení na portu 646 na unicastovou adresu. Pro ulehčení orientace v tomto programu si vyfiltrujte pouze pakety LDP (do políčka „Filter:“ vepište ldp a potvrďte buďto entrem nebo tlačítkem „Apply“). Sledujte tedy pakety zachycené na lince mezi R2 a R3, Sledování spustíte přes program GNS3.

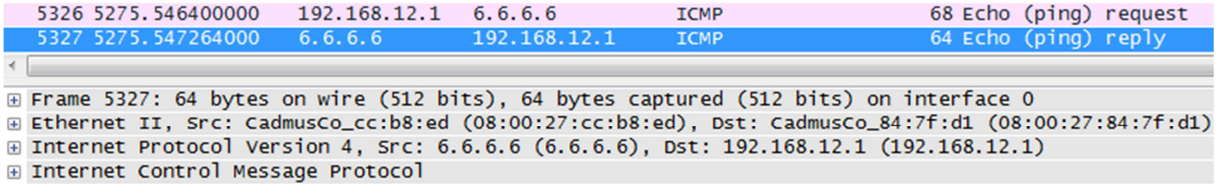


Obrázek 11: Zachycení navázení LDP spojení přes TCP, následné Hello pakety.

To že se Vám sestavení podařilo, zjistíte tak, že naleznete v záložce LDP Neighbor dynamicky přidaného LDP souseda. Všimněte si taktéž posledních dvou fialových paketů, kde dochází k výměně mapování MPLS návěští. Údaje v těchto dvou paketech korespondují s informacemi v záložkách Local Bindings a Remote Bindings v okně MPLS ve WinBoxu (důkladně tyto záložky prozkoumejte, všimněte si shody vygenerovaných MPLS návěští v Local binding na R2 s Remote binding na R3). Viz Obrázek 11.

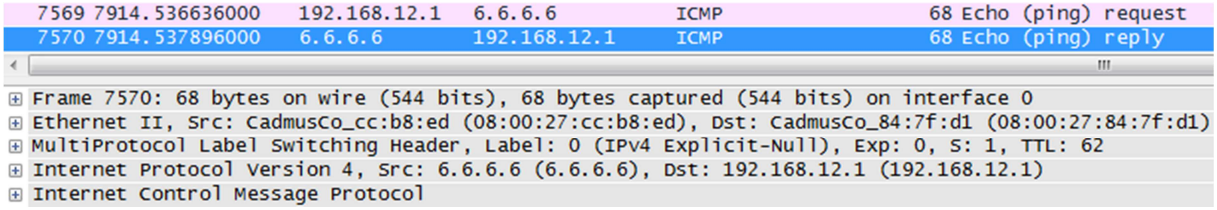
8. Nyní se přes WinBox přihlašte ke směrovači R1 a proveďte ping na adresu 6.6.6.6 se zdrojovou adresou 192.168.12.1. (Tools -> Ping). Podívejte se na pakety mezi směrovači R2 a

R3. V paketu ICMP request sledujte přidané MPLS návěští s určitou hodnotou. V ICMP reply zprávách vidíte, že žádné návěští MPLS není (viz Obrázek 12). To je z důvodu výchozího chování – implicit-NULL, které je popsáno v teoretickém úvodu.



Obrázek 12: Implicit-NULL - bez MPLS návěští.

9. Změňte nastavené na směrovači R2, aby používal Explicit-NULL (MPLS -> MPLS -> LDP Settings -> Use explicit Null). Znovu zachyťte pakety. Všimněte si, že je zasílané návěští s hodnotou 0, avšak je zachována informace QoS v MPLS návěští pro další zpracování (viz Obrázek 13).



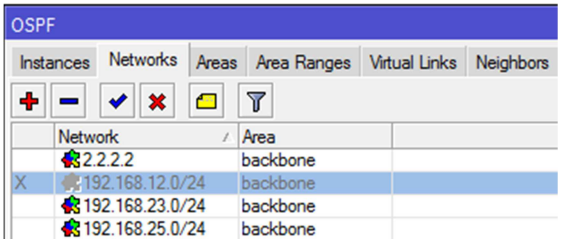
Obrázek 13: Explicit-NULL - s MPLS návěštním.

10. Všimněte si taktéž bitu S (BoS) nastaveného na 1 – tímto je naznačeno, že se jedno o poslední MPLS návěští před IP paketem.

Úkol 4:

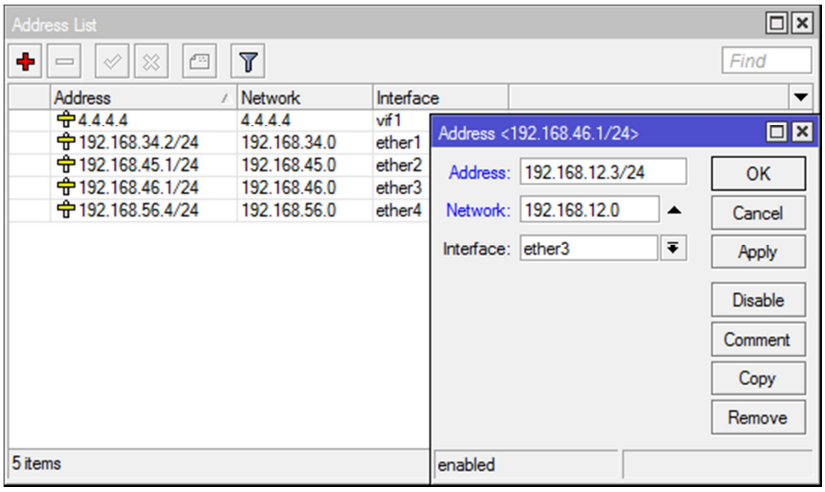
Při tomto úkolu budeme muset trochu pozměnit topologii. Nejdříve zrušíme propagování sítí mezi R1-R2 a R4-R6 v OSPF, poté přeadresujeme síť R4-R6 na adresy z rozsahu R1-R2. Jakmile bude toto hotovo provedeme vytvoření VPLS rozhraní, u kterého navážeme cílenou relaci na protější směrovač. Po veškerých těchto změnách bychom měli být schopni provést ping ze směrovače R1 na směrovač R6 a sledovat dvojité zapouzdření paketu. Vnitřní MPLS návěští označuje virtuální privátní síť.

1. Na směrovačích R2 zakážeme propagování sítě 192.168.12.0/24. Do tohoto podmenu se proklikáme přes: Routing -> OSPF -> Networks. Označíme danou síť a zakážeme propagování pomocí křížku, síť nám zašedne (Obrázek 14).



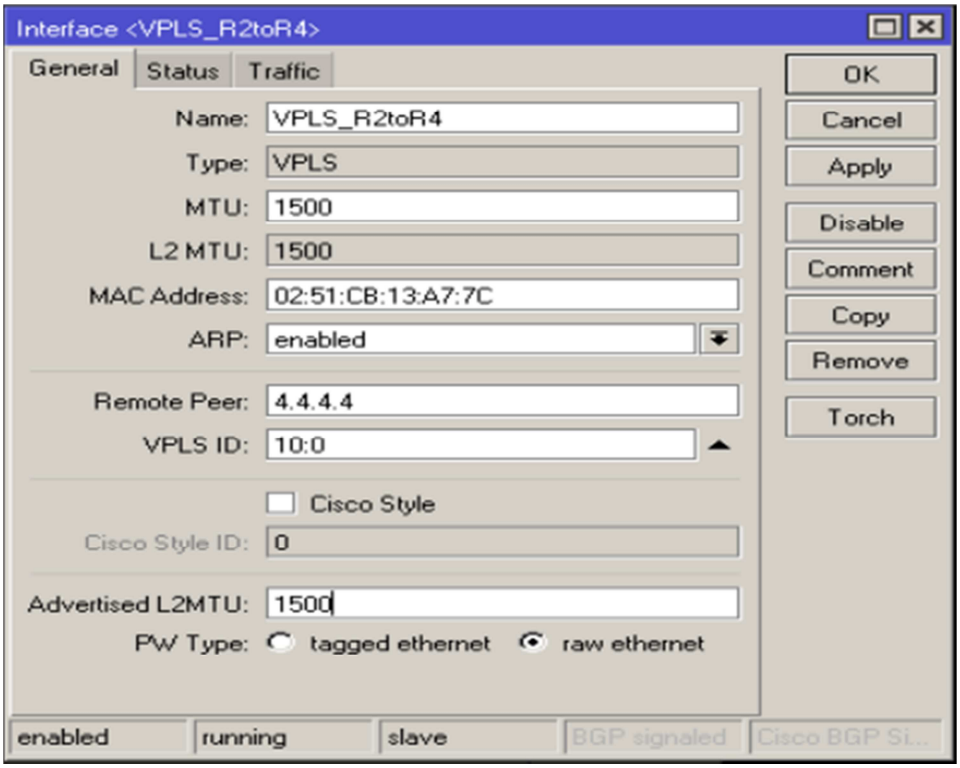
Obrázek 14: Zakázání propagece sítě do OSPF.

2. Přeadresujeme rozhraní na R4 a R6 na adresy z rozsahu 192.168.12.0/24: IP -> Address-> dvakrát poklepnout na adresu 192.168.46.1/24 a změnit (.3), to samé provést na R6 akorát na jinou adresu (.4). Obrázek 15.



Obrázek 15: Změna adresy na rozhraní.

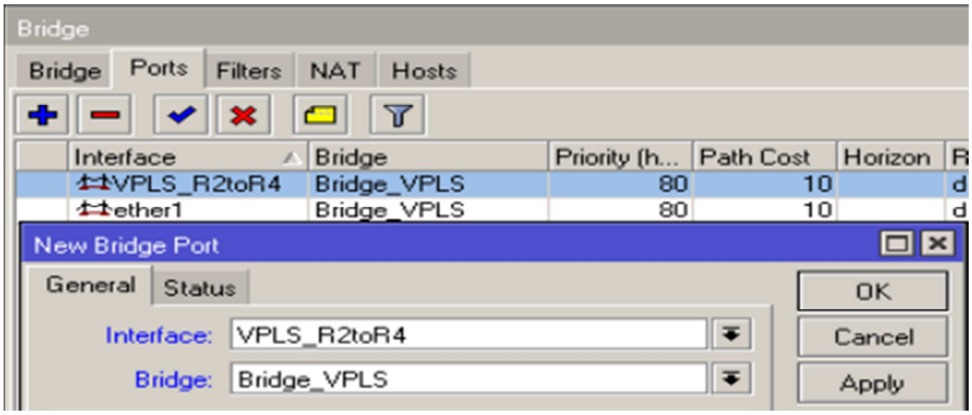
3. V záložce Interfaces přidáme nové rozhraní VPLS s nastavením viz Obrázek 16: Musíme dodržet především nastavení Remote Peer na protější směrovač a shodné VPLS ID (viz Obrázek 16).



Obrázek 16: Nastavení VPLS rozhraní.

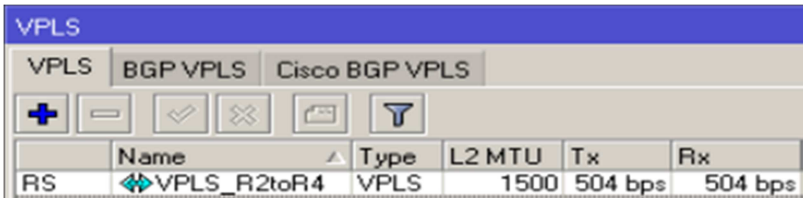
4. Přidáme nové rozhraní Bridge s jakýmkoliv jménem (Bridge -> plus -> ok). Překlikneme se do záložky Ports a přidáme porty k vytvořenému Bridge. U směrovače R2 přidáme rozhraní

ether1 a u R4 rozhraní ether3. Dále přidáme vytvořené rozhraní VPLS dle jména, které jsme mu dali. Totéž provedeme na směrovači R4 (viz Obrázek 17).



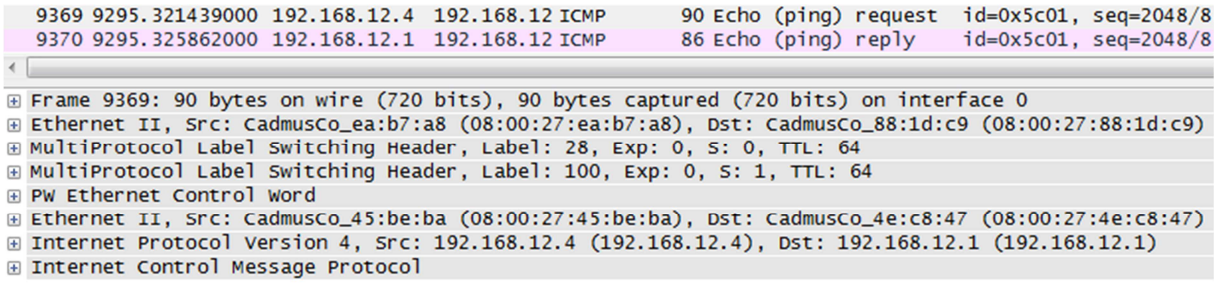
Obrázek 17: Přidání portů do VPLS přepínače.

5. Pokud vše proběhlo v pořádku, v záložce MPLS -> VPLS uvidíte aktivní VPLS rozhraní s příznakem R (running). Obrázek 18.



Obrázek 18: Spuštěné VPLS rozhraní.

6. Nyní provedeme ping ze směrovače R1 (se zdrojovou adresu 192.168.12.1) na adresu směrovače R6 (192.168.12.4). V programu WireShark sledujte dvojité zapouzdření paketu a zároveň bit BoS nastavený u vrchního návěští na 0 (tzn. není poslední v zásobníku). Obrázek 19.



Obrázek 19: Dvojité zapouzdření MPLS při použití VPLS.

Poznámka – ping na adresy 1.1.1.1 nebo 6.6.6.6 nebudou fungovat, museli byste upravit nastavení směrovacího protokolu OSPF. Avšak není problém protunelovat přes tento VPLS přepínač i pakety OSPF a navázat tak sousedství mezi směrovači R1 a R2. Dále si můžete všimnout, že pokud vyfiltrujete veškerý provoz MPLS ve WireSharku, tak uvidíte i zapouzdřené ARP pakety.

Na závěr si představte, jak by tato simulovaná síť mohla vypadat. Páteřní směrovače si můžete představit, že jsou ve větších městech ČR – Praha, Brno, Ostrava a Pardubice. Zákazníkovi A nabídnete propojení lokality, kterou mají v Praze s lokalitou, kterou mají v Ostravě. Tímto způsobem mu můžete zajistit L2 propojení. Zároveň můžete nabídnout zákazníkovi B tu samou službu, aniž by se navzájem zákazníci ovlivňovali.

Otázky:

1. Mezi kterými vrstvami se nachází MPLS návěští?
2. Který protokol slouží pro výměnu MPLS návěští?
3. Je možné tunelovat L2 provoz přes MPLS síť?
4. Co označuje bit Bottom of Stack v návěští MPLS nastavený na hodnotu 0?
5. Je možné tunelovat provoz ostatních protokolů (OSPF, STP, CDP,…) přes VPLS?

Seznam zkratek:

AS	Autonomus System
ATM	Asynchronus Transport Machine
AToM Any	Transport over MPLS
BGP	Border Gateway Protocol
BoS	Bottom of Stack
C	Customer
CE	Customer Edge
EoMPLS	Ethernet over MPLS
FEC	Forwarding Equivalence Classes
FR	Frame-relay
HDLC	High-Level Data Link Control
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
LDP	Label Distribution Protocol
LFIB	Label Forwarding Information Base
LLDP	Link Layer Discovery Protocol
LSP	Label Switched Path
LSR	Label Switching Router
MPLS	Multi-Protocol Label Switching
MPLS	VPN MPLS Virtual private Network
OSPF	Open Shortest Path First
P	Provider
PPP	Point-to-Point Protocol
PE	Provider Edge
QoS	Quality of Services
RIP	Routing Information Protocol
STP	Spanning Tree Protocol
TTL	Time to Live
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

VPLS	Virtual Private LAN Services
VPN	Virtual Private Netork