VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2017 Bc. Michal Daněk

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

VIRTUÁLNÍ PRIVÁTNÍ SÍTĚ NA BÁZI TECHNOLOGIE MPLS
MPLS BASED VIRTUAL PRIVATE NETWORKS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Michal Daněk

VEDOUCÍ PRÁCE
SUPERVISOR
doc. Ing. Vít Novotný, Ph.D.

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Telekomunikační a informační technika**
Ústav telekomunikací

Student: Bc. Michal Daněk ***ID:*** 150435
Ročník: 2 ***Akademický rok:*** 2016/17

NÁZEV TÉMATU:

Virtuální privátní sítě na bázi technologie MPLS

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou technologie MPLS a jejím využitím pro poskytování virtuálních privátních sítí se dvěma či více vzdálenými pobočkami. V závislosti na dostupném vybavení pracoviště navrhněte laboratorní úlohu pro předmět Architektura sítí, sestavte a zprovozněte pracoviště, a k úloze vypracujte návod.

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: 1.2.2017 ***Termín odevzdání:*** 24.5.2017

Vedoucí práce: doc. Ing. Vít Novotný, Ph.D.
Konzultant:

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

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

ABSTRAKT

Diplomová práce se zabývá architekturou sítě na bázi technologie multiprotokolového přepojování podle návěští (MPLS). Dále její využití pro bodové či více bodové spoje ať už na úrovni síťové nebo spojové vrstvy. Praktická část práce je zaměřena na návrh laboratorní úlohy, jejíž náplní je konfigurace technologie virtuální privátní LAN služby (VPLS). Tato technologie emuluje mnohabodové spojení na úrovni spojové vrstvy.

KLÍČOVÁ SLOVA

Cisco, GNS3, LDP, MPLS, návěští, VPLS

ABSTRACT

Master thesis deals with architecture of network based on multiprotocol label switching technology (MPLS). Work also describes use of this technology for point to point or multipoint connections based on network or data link layer. The practical part is focused on design of laboratory task which is aimed to configuration of virtual private LAN service (VPLS). This technology emulates multipoint connection based on the data link layer.

KEYWORDS

Cisco, GNS3, LDP, MPLS, label, VPLS

DANĚK, Michal. *Virtuální privátní sítě na bázi technologie MPLS*. Brno, 2017, 73 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: doc. Ing. Vít Novotný, CSc.

Vysázeno pomocí balíčku `thesis` verze 2.63; `http://latex.feec.vutbr.cz`

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Virtuální privátní sítě na bázi technologie MPLS“ jsem vypracoval(a) samostatně pod vedením vedoucího diplomové práce 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(ka) uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil(a) autorská práva třetích osob, zejména jsem nezasáhl(a) nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom(a) 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, CSc. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci. Také bych rád poděkoval své rodině, která mi umožnila studium na fakultě elektrotechniky a komunikačních technologií a po celou dobu mi byla oporou.

Brno ....

podpis autora

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic

http://www.six.feec.vutbr.cz

PODĚKOVÁNÍ

Výzkum popsaný v této diplomové práci 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

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OP Výzkum a vývoj
pro inovace

OBSAH

Úvod **12**

1 Teoretická část **13**
1.1 MPLS 13
1.1.1 Základní charakteristika 14
1.1.2 Termíny a architektura sítě 15
1.1.3 MPLS záhlaví 17
1.1.4 Distribuce návěští 24
1.1.5 Vyhledání okolních LSR 25
1.2 Virtuální privátní sítě 27
1.2.1 Přehled a klasifikace VPN 27
1.2.2 MPLS L3 VPN 28
1.2.3 MPLS L2 VPN 30

2 Praktická část **34**
2.1 Motivace úlohy 34
2.2 Návrh laboratorní úlohy 34
2.2.1 Výběr simulačního prostředí 34
2.2.2 Síťové systémy 35
2.2.3 Hypervisor 36
2.2.4 Laboratorní síť - návrh 36
2.2.5 Laboratorní síť - konfigurace 38
2.2.6 Cíl laboratorní úlohy 47

3 Závěr **50**

Literatura **51**

Seznam symbolů, veličin a zkratek **53**

Seznam příloh **55**

A Příprava prostředí pro úlohu **56**
A.1 VMware Workstation 56
A.2 GNS3 56

B Laboratorní úloha - Implementace služby Virtual Private LAN Service **60**
B.1 Teoretický úvod 60

B.1.1 MPLS 60
B.1.2 BGP 62
B.1.3 VPLS 62
B.1.4 Topologie 63
B.1.5 Postup řešení 63

C Laboratorní úloha - Přílohy **71**
C.1 Topologie - popis rozhraní 71
C.2 Úloha - řešení potíží 71

D Obsah přiloženého DVD **73**

SEZNAM OBRÁZKŮ

1.1 Umístění MPLS v ISO/OSI modelu. 14
1.2 MPLS doména. 15
1.3 Řídicí a datová rovina. 16
1.4 Ukázka výstupu ze síťového analyzátoru. 18
1.5 Záhlaví MPLS v detailu. 19
1.6 Operace s návěštím. 20
1.7 MPLS doména. 21
1.8 MPLS páteřní síť bez použití BGP. 22
1.9 Detailní výpis LDP zprávy. 26
1.10 Přehled VPN. 27
1.11 L3 VPN síte. 29
1.12 Emulace LAN. 31
2.1 Koncept GNS3 prostředí. 35
2.2 Topologie laboratorní sítě. 37
2.3 VPLS síť z pohledu zákazníka. 38
A.1 Připojení R1 do Internetu. 58
A.2 Volba síťové karty. 59
B.1 Emulace LAN. 61
B.2 Umístění MPLS v ISO/OSI modelu. 61
B.3 Topologie laboratorní sítě. 63
B.4 Směrovač připraven. 64
B.5 Kontrola funkčnosti směrování. 64
B.6 Rozhraní nakonfigurovaná pro MPLS. 65
B.7 Detaily LDP relací. 67
B.8 Kontrola BGP relace. 67
B.9 Kontrola funkce VPLS. 69
B.10 Ověření dostupnosti poboček. 70
C.1 Popisky rozhraní směrovačů 71
C.2 Problém s klientem Putty. 72
C.3 Problém s rozhraními na PE. 72

SEZNAM TABULEK

1.1 Rezervovaná návěští. 17
1.2 Mapování bitů DSCP do pole TC. 18
1.3 Ilustrace stohování návěští. 19
2.1 IP adresy jednotlivých rozhraní 49
B.1 Detaily PC. 70

SEZNAM VÝPISŮ

2.1 Nastavení názvu zařízení. 39
2.2 Nastavení IP adresy. 39
2.3 Nastavení OSPF. 39
2.4 Ověření nastavení rozhraní v OSPF. 40
2.5 Aktivace MPLS na rozhraní. 40
2.6 MPLS rozhraní. 40
2.7 Ukázka přiřazených návěští protokolem LDP. 41
2.8 Konfigurace BGP na hraničním směrovači. 42
2.9 Konfigurace BGP na RR1. 43
2.10 Konfigurace VPLS na PE1. 44
2.11 Konfigurace přepínače. 45
2.12 Konfigurace PC. 46
2.13 Konfigurace R1. 48
B.1 Konfigurace MPLS na PE1. 65
B.2 Konfigurace BGP na hraničním směrovači. 66
B.3 Konfigurace VPLS na PE1. 68

ÚVOD

Digitální svět se v posledních několika dekádách hodně změnil. Namísto regionálních poboček tak hodně společností přemyslí nad globálním trhem a logistice. Společnosti mají více poboček, které jsou rozprostřeny po celé republice či světě. Je zde jeden fakt, který všechny tyto společnosti spojuje. Jedná se o fakt, že všechny společnosti potřebují vybudovat rychlou, bezpečnou a spolehlivou infrastrukturu bez ohledu na jejich umístění. Není tomu tak dlouho, kdy jmenovatelem využití spolehlivé komunikace byly pronajaté linky, jejichž údržba i pronájem byly velmi nákladné. S přibývajícím počtem různorodých technologií se zvyšovala komplexnost sítí a často musely být budovány dvě či více sítí bok po boku jež se lišily pouze přenosovou technologií. Řešení jejich spojení nabídla technologie víceprotokolového přepojování paketů MPLS.

Diplomová práce se skládá z teoretické a praktické části. Teoretická část obsahuje základní popis technologie MPLS, architekturu sítě a protokol pro vytváření a distribuci návěští LDP. Dále jsou rozebrány koncepty virtuálních sítí, jejichž základem je technologie MPLS. Jedná se o směrované sítě, jejichž princip spočívá ve využití směrových protokolů (BGP), ale také o sítě, které jsou schopny přenášet (tunelovat) přímo celé nezměněné rámce mezi zákaznickými pobočkami. Může se jednat o jednobodové či mnohabodové sítě. Obecný přístup k řešení datových služeb ve větších společnostech tak může být rozdělen na dvě skupiny. V té první se bude jednat o sítě využívající směrových protokolů, kde bude nutná výměna směrových informací s hraničními směrovači poskytovatele. Do druhé skupiny se řadí spojení na úrovni spojové vrstvy.

Praktická část je zaměřena na návrh laboratorní úlohy, jejíž tématem je konfigurace Virtual Private LAN Service (VPLS), která vytváří ze sítě poskytovatele jednu všesměrovou doménu, která je dedikovaná pouze danému zákazníkovi a jeho data jsou oddělena od dat jiných zákazníků. Pro zákazníka se pak síť poskytovatele chová jako jeden velký přepínač a to i přesto, že jsou jednotlivé pobočky geograficky vzdáleny. V úloze je využit protokol BGP pro automatické objevování hraničních směrovačů a signalizace je provedena pomocí protokolu LDP.

V příloze se nachází mimo jiné hlavně postup přípravy laboratorní úlohy a její samotné vypracování.

1 TEORETICKÁ ČÁST

1.1 MPLS

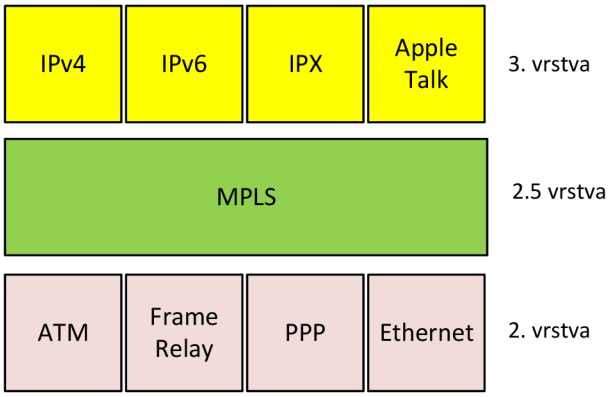
Technologie multiprotokolového přepojování podle návěští MPLS (Multi Protocol Label Switching) byla standardizována v roce 2001 (RFC 3031) a postupem času si vydobyla svoje jedinečné postavení v páteřních sítích poskytovatelů připojení. Principem této technologie je předřazení krátkého návěští (angl. label) před každý paket vstupující do páteřní sítě, na jehož základě se dále rozhoduje o přepojení dané datové jednotky [1].

Původním záměrem při tvorbě technologie MPLS byla redukce počtu prohledávání směrové tabulky. Hlavní impulz přichází již v září roku 1993, kdy bylo standardizováno tzv. „beztřídní směrování“ CIDR (Classless Inter-Domain Routing). Beztřídní směrování, které určuje masku sítě počtem bitů, nikoliv příslušností IP adresy ke třídě IP adres mělo za následek více nepromyšlených důsledků. A právě jedním z důsledků byla nutnost procházení směrové tabulky a vyhledání tzv. nejdelší shody síťového prefixu (z angl. longest match). Problém to byl proto, že se procházení směrové tabulky v dané době velmi těžce implementovalo. Původní implementace byly čistě softwarové (např. algoritmus PATRICIA), později optimalizovaná technika CEF (Cisco Express Forwarding) nicméně i přes tyto dílčí optimalizace trvalo mnoho let než procházení směrových tabulek bylo prováděno čistě na hardwarové úrovni zákaznických obvodů ASIC (Application Specific Integrated Circuit) v patřičně krátkém čase. V čase, kdy technologie MPLS byla vytvořena, byla řešením právě pro tento problém. Uzly páteřní sítě tak již nemusely zdlouhavě prohledávat směrové tabulky, pouze přepojovaly datové jednotky na základě kratšího identifikátoru - návěští. Postupem času však moderní ASIC obvody prakticky vyřešily původní problém náročnosti procházení směrových tabulek. Jejich výkon již dostačuje k desítkám nebo i stovkám milionů cyklů procházení směrové tabulky v jediné sekundě. Nabízí se otázka, proč se stále zajímat o MPLS?

Pravděpodobně jako nejvýznamnější důvod je schopnost implementace kontroly, kde a jak je datový provoz směrován. Tato schopnost se skrývá pod zkratkou TE (Traffic Engineering). Dále ale také schopnost doručit data transportních služeb (Frame-Relay, ATM, VPLS, aj.), stejně jako služby směrovaných sítí IP, a to přes sdílenou paketově přepojovanou infrastrukturu. Za zmínku stojí také zlepšení pružnosti sítě reagovat na případné výpadky.

1.1.1 Základní charakteristika

Zatímco tradiční směrování paketů se uzel od uzlu provádí přiřazením paketu k určité třídě FEC (Forwarding Equivalent Class) dle prefixu cílové adresy sítě, u MPLS se toto přiřazení k dané FEC provede pouze jednou. Při doručení paketu na hraniční směrovač se provede prohledání směrové tabulky stejně jako tomu bylo v tradičním konceptu směrování, nicméně dále už se před paket přiřadí tzv. návěští a to na vstupu do MPLS domény (na hraničním směrovači). Další uzly v doméně už se paket po paketu přepojují na základě návěští a neprohledávají znovu směrovou tabulku. Pod pojmem FEC se skrývá tok paketů, které budou odeslány stejnou cestou napříč MPLS doménou. Návěští má neměnnou délku a má pouze lokální význam (lokální význam mezi dvěma přilehlými směrovači). Při srovnání s konvenčními směrovými protokoly, které pracují na třetí vrstvě ISO/OSI modelu, je MPLS zařazené na pomezí druhé a třetí vrstvy. Toto zařazení je zobrazeno na Obr. 1.1. Koncept MPLS striktně dělí řídicí a datovou rovinu. Řídicí rovina (angl. control plane) je realizována pomocí směrových protokolů a mechanizmů, které vytvářejí a distribuují návěští mezi směrovači. Datová rovina (angl. data plane) je zodpovědná za samotné přepojování datových jednotek.



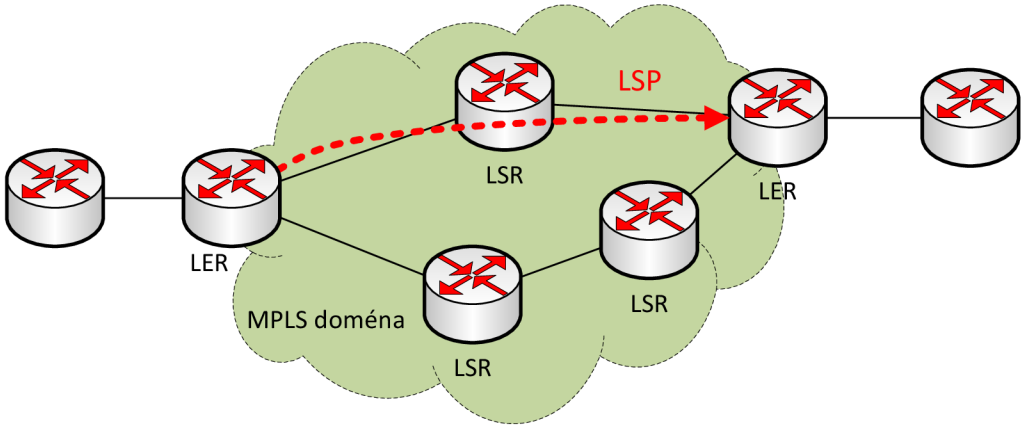
Obr. 1.1: Umístění MPLS v ISO/OSI modelu.

Z Obr. 1.1 je zřejmé, že technologie MPLS není závislá na přenosové technologii spojové vrstvy a zároveň může sama přenášet jakýkoliv protokol vrstvy síťové (IPv4, IPv6, aj.).

1.1.2 Termíny a architektura sítě

K popisu MPLS sítě bude nutné vymezit následující důležité pojmy:

- LSR (Label Switching Router) - Je to obecný pojem pro jakýkoliv směrovač v síti, na kterém je spuštěna technologie MPLS.
- LER (Label Edge Router) - Jedná se o směrovač, na kterém běží MPLS, s tím rozdílem, že se jedná o hraniční uzel v doméně.
- LSP (Label Switched Path) - Cesta napříč MPLS doménou.
- LDP (Label Distribution Protocol) - Protokol, který vytváří návěští a zajišťuje jejich distribuci.
- LFIB (Label Forwarding Information Base) - Přepojovací tabulka návěští.
- LIB (Label Information Base) - Tabulka návěští.



Obr. 1.2: MPLS doména.

Část sítě, která využívá technologii MPLS, je nazvána MPLS doménou, která je zobrazena na Obr. 1.2. Mezi základní prvky, ze kterých se doména skládá, patří směrovače LSR, které si budují přepojovací tabulku LFIB. Potřebné informace pro přepojování si směrovače vyměňují za pomoci protokolu pro distribuci návěští LDP, jehož funkce je závislá na směrovacích informacích získaných pomocí některého z IGP (Internal Gateway Protocol) protokolů. Cesta LSP je sestavena tak, že si postupně všechny LSR směrovače vytvářejí vazbu mezi příchozím a odchozím návěštím pro danou adresu sítě. LSP je tedy trasa od vstupu datové jednotky do MPLS domény, až po její opuštění. LSP je zde uvažována jako jednosměrný tunel, kterým prochází pakety od vstupu do domény po její opuštění [1], což umožňuje například rozklad zátěže v obou směrech přes různé spoje.

Architektura MPLS

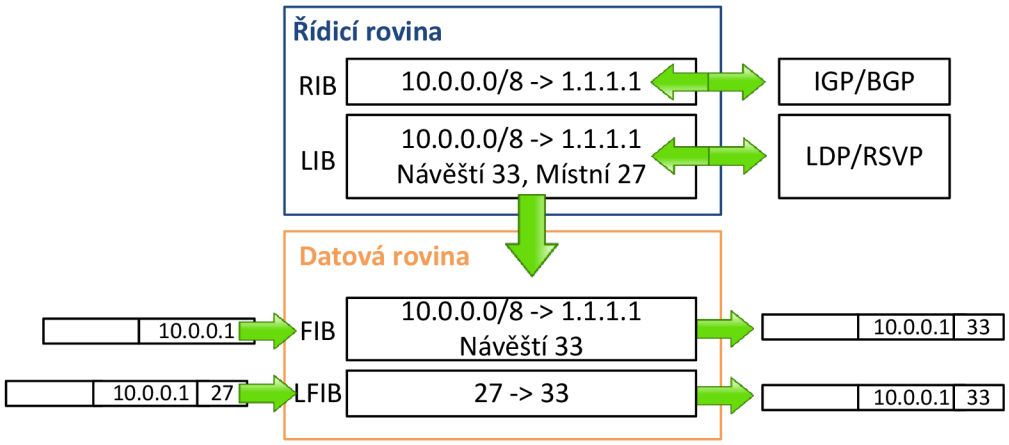
Architektura striktně odděluje řízení a samostatné přepojování datových jednotek:

- Mezi základní části řídicí roviny patří:
  - Směrové protokoly IGP.
  - Směrová tabulka RIB (Routing Information Base.
  - Tabulka návěští LIB.
- Datová rovina se skládá z:
  - Přepojovací tabulka FIB.
  - Přepojovací tabulka návěští LFIB.

Řídicí rovina má za úkol výměnu směrových informací (pomocí směrových protokolů) na úrovni třetí vrstvy ISO/OSI modelu a dále se stará o vytváření a výměnu návěští pomocí příslušných protokolů:

- TDP (Tag Distribution Protocol) - Starší Cisco proprietární protokol.
- LDP (Label Distribution Protocol) - Novější standardizovaný protokol.[1]
- RSVP-TE (Resource Reservation Protocol - Traffic Engineering) - Umožňuje řízení provozu (angl. traffic engineering).

Samotné přepojování paketů pak zajišťuje datová rovina viz Obr. 1.3 níže. Obrázek



Obr. 1.3: Řídicí a datová rovina.

mimo rovin znázorňuje operace vložení a výměnu návěští. Tedy případ, kdy je paket již opatřen MPLS návěštím (paket vchází do LFIB) ale i případ, ve kterém je třeba samotný paket opatřit návěštím (paket vchází do FIB).

[1]Pro upřesnění, LDP v MPLS terminologii vystupuje jako obecný termín zastřešující všechny protokoly které jsou určeny pro práci s návěštím ale i jako jeden z jejich představitelů.

1.1.3 MPLS záhlaví

Záhlaví MPLS paketu se nachází za záhlavím spojové vrstvy a je následováno záhlavím síťové vrstvy. Jeho celková délka je 32 bitů a skládá z následujících čtyř částí:

1. Návěští - o délce 20 bitů. Hodnota návěští je celé kladné číslo v rozsahu 0 až 1,048,575 nicméně prvních 16 hodnot bylo rezervováno z rozsahu pro normální užívání a mají speciální význam. Jsou uvedeny v Tab. 1.1 níže:

Tab. 1.1: Rezervovaná návěští.

Hodnota návěští	**Význam**
0	Explicitní IPv4 nulové návěští.
1	Analogické využití „Router Alert Option“ jako v IP paketu.
2	Explicitní IPv6 nulové návěští.
3	Implicitní nulové návěští.
4 až 15	Rezervováno pro budoucí použití.

   Použitím nulového explicitního návěští návěští nezmizí, ale je ignorováno. Je to z důvodu zachování TC bitů - tedy zachování možnosti dále klasifikovat datový provoz pro QoS. Jak implicitní, tak explicitní návěští jsou generována posledním směrovačem směrem ke svým sousedům. Implicitní nulové návěští je výchozí a má za úkol oznámit předposlednímu směrovači, aby odesílal pouze IP pakety bez MPLS záhlaví. Tato technika byla pojmenována jako PHP (Penultimate Hop Popping) a její význam tkví ve zredukování prováděných operací hraničním směrovačem. PHP má ovšem také nevýhodu - jelikož MPLS záhlaví není přenášeno, také hodnota TC bitů je ztracena (QoS)[3].

2. TC - Traffic Class, tři bity (20 až 22) využité dnes výhradně pro QoS. Mapování jednotlivých tříd DSCP do MPLS zprávy, tedy do pole TC je přehledně zaznamenáno v Tab. 1.2. Dřívější pojmenování TC bitů bylo jako experimentální (EXP) [2]. Svého času totiž nikdo nevěděl, k čemu budou v budoucnosti použity.

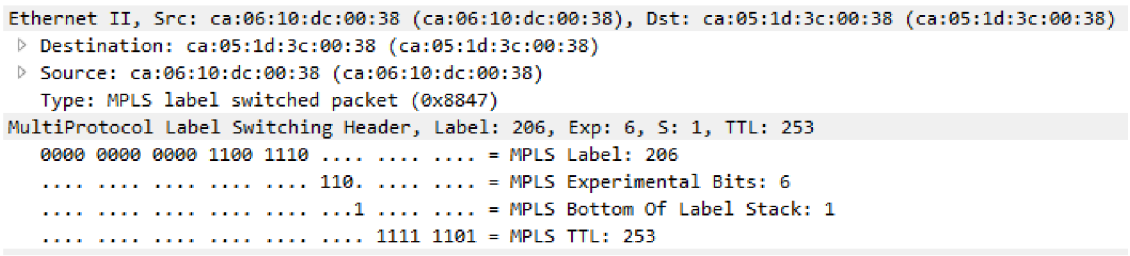
3. BS - Bottom of Stack (23) indikující dno zásobníku (může být více záhlaví za sebou a je třeba odlišit které je poslední).

4. TTL - Time to Live (24-31) má stejný význam jako u paketu, tedy zabraňuje nekonečnému putování paketu sítí snižováním o jedničku s každým skokem. Při dosažení nulové hodnoty je paket zahozen.

Tab. 1.2: Mapování bitů DSCP do pole TC.

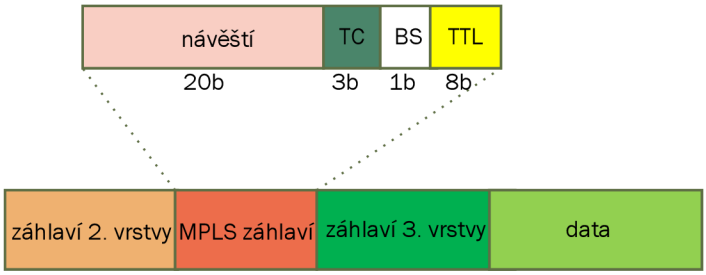
Pojmenování DiffServ třídy	**DSCP**	**TC**
EF	101110	111
AF4	100010	110
AF3	011010	101
AF2	010010	100
AF1	001010	011
BE	000000	010

Na Obr. 1.4 lze vidět, jakým způsobem je v Ethernetovém rámci na druhé vrstvě odlišeno, že bude následovat MPLS záhlaví (type 0x8847). Bohužel vývojáři analyzátoru Wireshark prozatím neupravili pole pro QoS (Traffic Class) a na Obr. 1.4 je uveden původní název, tedy Experimental Bits. Zároveň lze vidět i všechny výše jmenované části MPLS záhlaví. V případě použití technologie ATM, je návěští umís-



Obr. 1.4: Ukázka výstupu ze síťového analyzátoru.

těno do pole VPI/VCI v jeho hlavičce. Zbytek MPLS hlavičky (TC, BS, TTL) je umístěno do datového pole ATM buňky. Tento mód je nazván jako tzv. Cell mode MPLS. Druhou možností pro ostatní L2 technologie je jednoduché vložení MPLS záhlaví mezi záhlaví 2. a 3. vrstvy, což je pro přehlednost znázorněno na Obr. 1.5. V tomto případě se jedná o tzv. frame mode MPLS.



Obr. 1.5: Záhlaví MPLS v detailu.

Stohování návěští

Stohování návěští (angl. label stack) reprezentuje sekvenci MPLS záhlaví řazené za sebou. Některé MPLS aplikace totiž mohou vyžadovat k jejich práci více než pouze jedno návěští[2].

Tab. 1.3: Ilustrace stohování návěští.

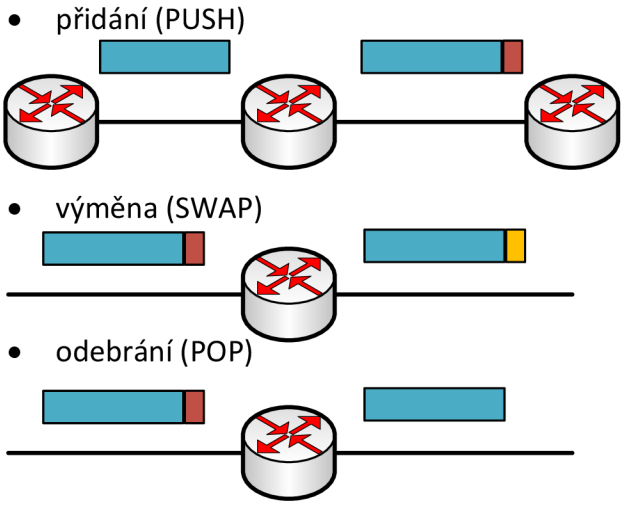
návěští	TC	**0**	TTL
návěští	TC	**0**	TTL
		....	
návěští	TC	**1**	TTL

V Tab. 1.3 je znázorněno, jakým způsobem se stohují návěští ve spojitosti s „BS“ bitem, který jak již bylo řečeno, ukazuje na dno zásobníku. Návěští jsou zpracována odshora, a tedy poslední návěští na dně zásobníku má nastaveno BS bit na hodnotu 1.

Operace s návěštím

Na vstup do MPLS domény přichází datová jednotka a je třeba k ní předřadit návěští pomocí operace přidání (angl. push). Po přidání návěští a odeslání k dalšímu uzlu je třeba provést výměnu (angl. swap), a to z důvodu lokální platnosti návěští. Obdobně, pokud již datová jednotka má návěští, a je na hraničním směrovači a chystá se opustit doménu, bude provedena operace odebrání (angl. pop) návěští. Všechny tři vyjmenované situace jsou zachyceny na Obr. 1.6.

[2]Ve většině literatury se autoři odkazují pouze na to, že je použito více návěští). Ve skutečnosti však jsou vždy použity celá záhlaví opakovaně, nikoliv pouze návěští. Pro zjednodušení v této práci bude taktéž použit termín návěští.

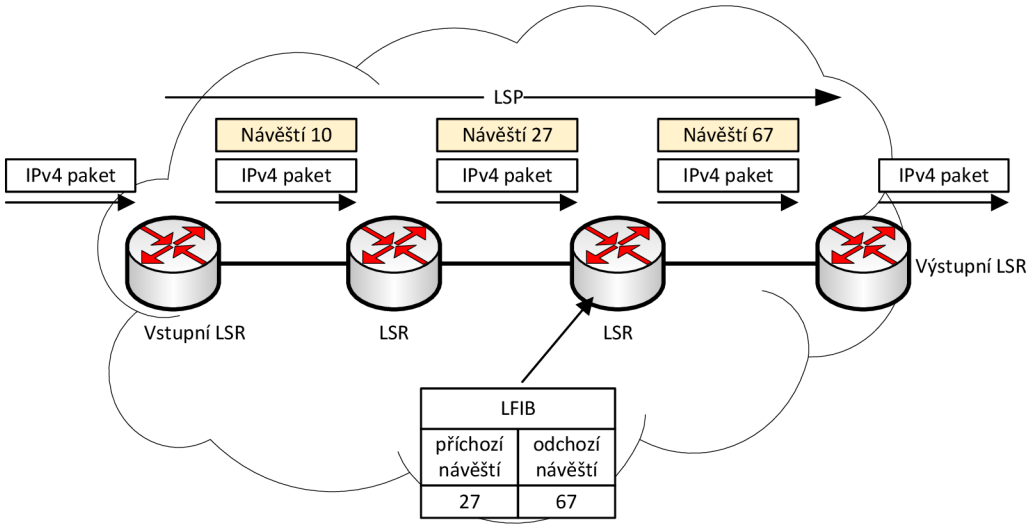


Obr. 1.6: Operace s návěštím.

Přepojování paketů řízené návěštím

Pro bližší popis přepojování datové jednotky MPLS doménou je potřeba uvést operace, které jsou během ní vykonány. Na Obr. 1.7 je znázorněn IPv4 paket vstupující na hraničním LSR směrovači do MPLS domény. Hraniční směrovač prozkoumá přijatý paket a už ze záhlaví druhé vrstvy rozpozná, že se jedná o IP paket (typ 0x0800) nikoliv MPLS paket. Směrovač prohledá směrovou tabulku a zkontroluje, zdali je k dané FEC již přiřazeno nějaké návěští. Pokud existuje mapování dané FEC/návěští, potom je vloženo (push) návěští a dále zpracováno dle LFIB jako paket obsahující návěští. V tomto případě existuje mapování FEC na návěští, návěští 10 bylo připojeno k paketu a následně odesláno na sousední LSR směrovač. Sousední směrovač opět již z druhé vrstvy rozpozná MPLS paket, a rovnou může prohledat přepojovací tabulku LFIB. Na základě prohledání LFIB je nalezena hodnota odchozího návěští 27, provedena funkce výměny návěští (swap) a paket odeslán dalšímu uzlu. Další uzel postupuje stejně jako předchozí, tedy prohledá přepojovací tabulku LFIB a na základě nálezu provede výměnu návěští a odeslání hraničnímu směrovači. Hraniční směrovač při výstupu z MPLS domény návěští odstraní a paket může pokračovat směrem k cíli.

V případě že LSR přijme paket s návěštím, pro které on sám nemá žádné mapování v přepojovací tabulce návěští, paket musí být zahozen. Směrovač by mohl pokračovat v odebrání návěští a směrování pouze na základě směrové tabulky. Tímto



Obr. 1.7: MPLS doména.

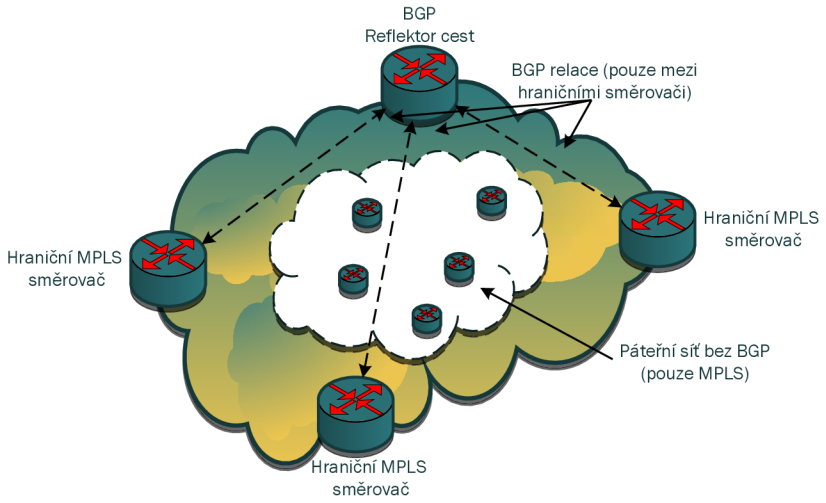
však může vzniknout směrová smyčka, ve které se tak pakety mohou zacyklit. Taktéž jsou zahazovány pakety, pro které LSR nemá odchozí návěští a to ze stejného důvodu.

Výhody MPLS

Technika přepojování návěští s sebou přináší mnohé výhody, které mohou být klíčové při návrhu sítě:

- Použití jednotné infrastruktury: MPLS může přenášet nejen protokoly síťové vrstvy IPv4, IPv6 ale i rámce technologií spojové vrstvy. Například Ethernet, HDLC, PPP, aj. Zjednodušeně řečeno, MPLS je jednoduchá metoda přepojování více protokolů(technologií) pomocí jedné sdílené sítě.
- Páteřní síť bez nutnosti použití BGP (Border Gateway Protocol): Pokud síť poskytovatele má přenášet data, každý směrovač musí prohledat směrovou tabulku vzhledem k cílové IP adrese každého paketu, aby tak určil další skok (odchozí rozhraní). Pokud jsou pakety odesílány do externích sítí ležících mimo síť poskytovatele, tyto externí sítě musí být přítomny ve směrové tabulce každého směrovače. BGP pak distribuuje jak zákaznické prefixy, tak i ty internetové. Jelikož však MPLS funguje na základě návěští a nezajímá se v páteřní síti o cílovou IP adresu, znamená to, že páteřní směrovače nadále nepotřebují znát všechny cílové IP adresy. Páteřní směrovače tudíž nepotřebují dále používat BGP, viz Obr. 1.8. Samozřejmostí je, že hraniční směrovače musí znát

všechny sítě a vstupní pakety označit návěštím a tedy i používat BGP, ale dále při směrováním paketu sítí poskytovatele se použije pouze návěští samotné [4]. Pro zajištění plné dostupnosti v rámci autonomního systému se pak využívá spojově stavových protokolů, a to z důvodu jejich znalosti celkové topologie [4].



Obr. 1.8: MPLS páteřní síť bez použití BGP.

- Vícebodová komunikace: Je možné realizovat nejen dvoubodové spoje (angl. point to point), ale také více bodové (angl. multipoint).

- Optimální tok dat: při využití MPLS sítě jsou data přepojována napřímo, tedy optimálně mezi všemi připojenými pobočkami. V porovnání s překryvnými sítěmi, kde by se pro dosažení optimálního toku muselo zajistit plné propojení (angl. full mesh).

- Traffic Engineering (TE): základní myšlenkou je optimalizace využití síťové infrastruktury. Ať už například využít doposud nevyužitých záložních linek (např.: směrový protokol vybral jinou linku jako linku s nejlepší cenou, nejkratší vzdáleností, aj.).

Jak již bylo v zmíněno v kapitole 1.1 v dnešní době zákaznických obvodů ASIC již výkonnost přepojování na základě návěští není hlavním argumentem ve prospěch této technologie. Toto platilo v dobách dřívějších, kde veškeré operace probíhaly nad procesory CPU (Central Processing Unit) bez využití ASIC. Hodně záleží od daného výrobce, jakým způsobem MPLS implementoval. Například na konferenci MikroTik

User Meeting v roce 2009 byl prezentován výkon směrovače Mikrotik RB1000 při využití MPLS a klasického směrování. Zde se ukázalo, že při využití MPLS byl výkon téměř dvojnásobný a zároveň srovnatelný s výkonem přepínače [6].

1.1.4 Distribuce návěští

Jak již bylo řečeno, základem MPLS jsou označené pakety návěštím a každý LSR musí provést výměnu návěští před přepojení paketu. Což znamená, že v každém případě návěští musí být distribuována [7]. Toho je možné dosáhnout dvěma způsoby. Buď vytvořit zcela nový protokol, který bude určený pouze pro distribuci návěští, nebo návěští distribuovat pomocí existujícího směrového protokolu. V případě úpravy existujících směrových protokolů by bylo nutné upravit všechny. Lepším přístupem tedy bude vytvořit nový protokol pro distribuci návěští. Tím se směrování stane nezávislým a nový protokol bude schopen spolupracovat se všemi směrovými protokoly. To je přesný důvod, proč byl LDP vytvořen: přenáší (distribuuje) mapování návěští na FEC napříč MPLS doménou. LDP vystupuje jako obecný pojem pro protokol sloužící k výměně návěští, ale název LDP také nese přímo jeden z konkrétních představitelů [3]. Jedinou výjimkou je směrový protokol BGP. Protože přenáší externí prefixy je považován za efektivnější, aby nesl také návěští spolu s prefixy. Druhým důvodem je, že je jako jediný používaný mezi autonomními systémy, a tedy sám o sobě se stává důvěryhodnějším [4].

Label Distribution Protocol

Pro doručení paketu po LSP napříč MPLS doménou všechny LSR musí podporovat protokol LDP. V momentě, kdy všechny LSR mají návěští pro danou FEC, pakety mohou být doručeny. Operace s návěštími jsou všem LSR známé a pro každý FEC záznam jsou konkrétní operace uloženy v LFIB. LFIB je přepojovací tabulka, která je plněna mapováním FEC na návěští, které pocházejí z tabulky návěští LIB. LIB je plněna například záznamy přijatými od sousedních uzlů pomocí LDP, BGP, statickým mapováním. Jedna z dalších možností je RSVP protokol, který distribuuje prefixy pouze pro MPLS traffic engineering. Protože BGP nese návěští pouze pro BGP prefixy, RSVP taktéž pouze pro traffic engineering - pro distribuci návěští interních směrových protokolů zbývá již pouze LDP. Tudíž všechny přímo připojené směrovače musí vzájemně navázat LDP relaci a to pomocí TCP/UDP zpráv na portu 646. Následně využijí tuto navázanou relaci k výměně mapování FEC na návěští. Čtyři hlavní funkce LDP protokolu jsou:

1. Vyhledání okolních LSR používající LDP.
2. Navázání a udržování relace.
3. Propagování návěští.
4. Notifikace.

K realizaci výše uvedených funkcí LDP využívá tyto zprávy:

[3] LDP v tomto případě označuje přímo již samotný protokol k výměně návěští nikoliv obecný termín pro všechny protokoly.

- Hello zpráva - tyto zprávy jsou vyměňovány mezi uzly jako část objevovacího procesu okolních uzlů.
- Inicializační zpráva - zpráva je vyměňována jako část ustavení relace mezi dvěma směrovači využívající LDP protokol.
- KeepAlive zpráva - LSR odesílá tyto zprávy, které jsou částí mechanismu monitorující integritu LDP relace.
- Adresní zpráva - LSR odesílá adresní zprávu, ve které oznamuje přilehlým směrovačům IP adresy jeho rozhraní.

1.1.5 Vyhledání okolních LSR

LSR používající protokol LDP periodicky odesílají tzv. hello zprávy, a to všemi rozhraními, která jsou k tomu určena a oznamují tak svoji přítomnost v doméně. Hello zprávy využívají jako transportní protokol UDP na portu 646 a jsou odesílány na skupinovou IP adresu 224.0.0.2 (všechny směrovače na sítí). Směrovač, který přijímá tyto zprávy na určitém rozhraní, je tedy informován tímto prostřednictvím o přítomnosti jiných směrovačů používajících taktéž LDP protokol. Hello zprávy obsahují tzv. hold časovač, který určuje maximální hodnotu stáří, po kterou směrovače udržují aktivní již navázanou relaci bez přijetí jakékoliv další LDP zprávy. Pro úplnost je nutné zmínit tzv. cílené LDP (angl. targeted LDP), které nevyužívají skupinovou, adresu ale jsou odesílány cíleně na jednu adresu. Toho se využívá pro další MPLS aplikace jako je např. technologie VPLS která bude popsána dále.

Navázání a udržování relace

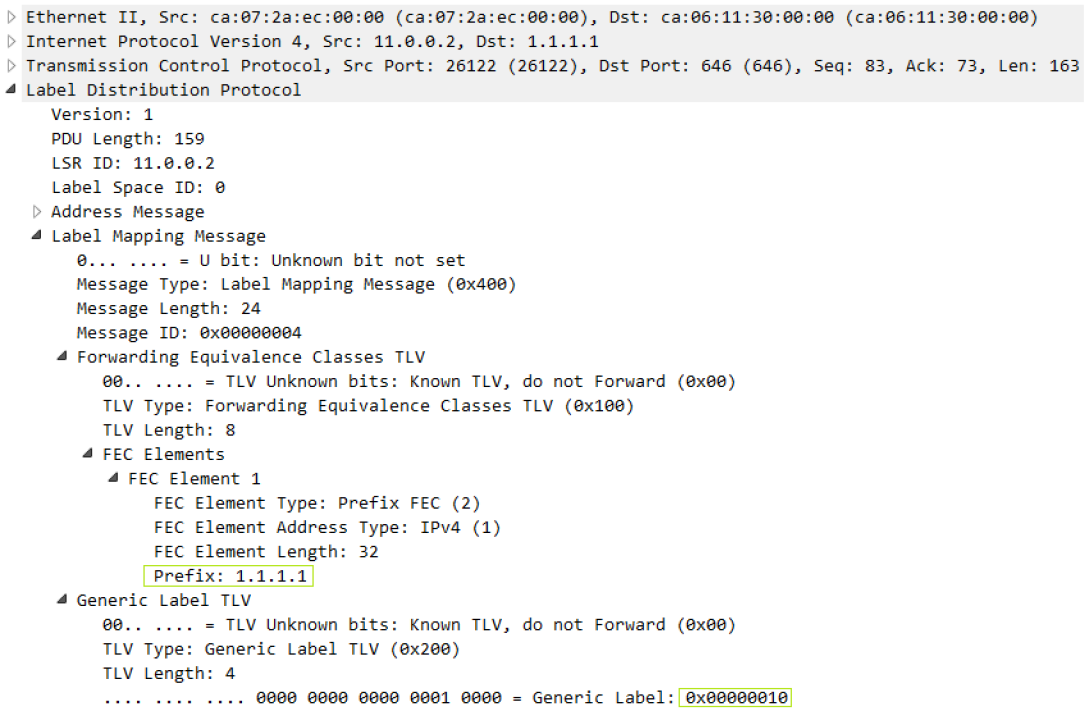
Pokud se dva směrovače „najdou“ za pomoci LDP hello zpráv, pokusí se mezi sebou sestavit LDP relaci. LSR se pokusí otevřít TCP relaci vzhledem k druhému LSR a to na portu 646. Pokud je TCP spojení navázáno, oba LSR si vzájemně vyjednají parametry LDP spojení výměnou tzv. inicializační zprávy. Mezi vyjednávané parametry patří:

- Hodnoty časovačů.
- Metoda distribuce návěští.
- Virtual path identifier (VPI)/virtual channel identifier (VCI) rozsahy pro návěštím řízené ATM.
- Data-link connection identifier (DLCI) rozsahy pro Frame Relay.

V případě že se dva přilehlé směrovače shodnou na společných parametrech pro navázání LDP spojení, budou mezi sebou udržovat TCP relaci. V opačném případě se pokusí relaci vytvořit znovu. Po tom co byla LDP relace navázaná je udržována přijetím jakékoliv LDP zprávy a nebo navíc periodickým příjmem LDP tzv. keepalive zprávy. S každou LDP zprávou je keepalive časovač pro danou relaci vynulován.

Propagování návěští

Propagace návěští je hlavním úkolem LDP protokolu. Každý LSR vytváří návěští ke všem prefixům, které má ve směrové tabulce a dále tato mapování návěští na prefix rozesílá na okolní LSR směrovače. LDP tedy slouží převážně k distribuci návěští a jeho funkce je závislá na plné dostupnosti uzlů napříč MPLS doménou, a to buď za pomoci IGP protokolů nebo staticky nastavených směrových záznamů. Na Obr. 1.9 je detailně zobrazen obsah zprávy LDP protokolu. Vyznačen je přenášený prefix a hodnota návěští (šestnáctkově).



Obr. 1.9: Detailní výpis LDP zprávy.

Charakter návěští

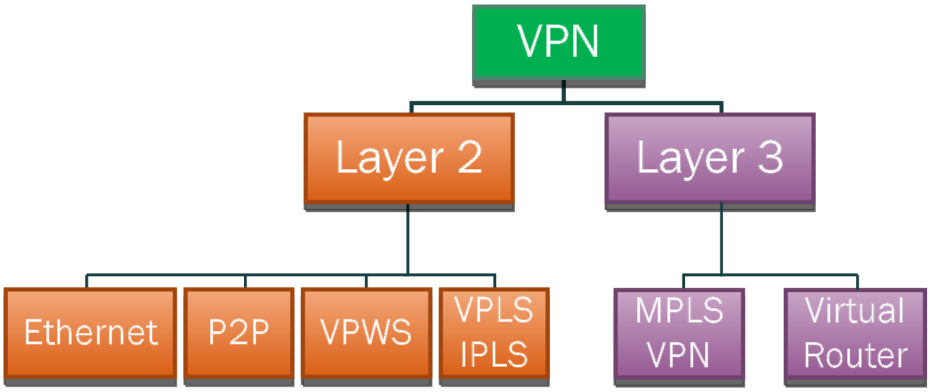
Charakter návěští může být dvojího druhu. LSR mohou vytvářet návěští, která mají buď globální význam (per-platform space), nebo význam pouze v rámci jednoho rozhraní (per-interface label space). Globální význam znamená, že návěští je unikátní vzhledem k dané FEC a není použito na žádném jiném rozhraní. Návěští s významem v rámci rozhraní jsou unikátní pouze v rámci daného rozhraní (tedy jiné rozhraní musí používat rozdílné návěští pro stejnou FEC).

1.2 Virtuální privátní sítě

VPN síť je privátní síťová infrastruktura (síť podniková) založená na sdílené síťové infrastruktuře (síť poskytovatele). Pojem „virtuální“ zde vyjadřuje fakt, že se nejedná o fyzicky propojenou síť na bázi pronajatých fyzických okruhů. Pod pojmem „privátní“ si lze představit, že síť je zcela izolována od ostatních sítí v rámci sdílené infrastruktury poskytovatele. Pokud se jedná o MPLS VPN, oddělení se zde dosáhne z podstaty konceptu technologie a není nutné používat a udržovat často velmi složité distribuční listy či případně další filtry.

1.2.1 Přehled a klasifikace VPN

Virtuální privátní sítě lze klasifikovat z pohledu referenčního modelu ISO/OSI, tedy z pohledu, na které z vrstev je daný VPN koncept založen. Koncepty jsou přehledně shrnuty na Obr. 1.10. První možností je tzv. L2 (Layer 2) VPN, která poskytuje funkcionalitu srovnatelnou se spojovou vrstvou - tedy např. přenos Ethernetového rámce MPLS doménou a druhou možností je tzv. L3 (Layer 3) VPN poskytující funkcionalitu, kterou nabízí síťová vrstva - směrování paketů. Ve spojení s MPLS



Obr. 1.10: Přehled VPN.

VPN se liší označování uzlů v páteřní síti. Hraniční směrovač poskytovatele je nazván jako tzv. provider edge (PE) směrovač, stejně je pak odvozen název pro směrovač na straně zákazníka tzv. customer edge (CE). Směrovač nacházející se uvnitř páteřní sítě (pozor, ne hraniční) je nazván jako tzv. provider (P) směrovač. Dále zde figuruje velmi obecný pojem tzv. attachement circuits (AC), který označuje konkrétní síťovou

technologii. AC se stará o připojení CE k PE a to pomocí technologií Frame Relay, ATM, Ethernet, VLAN, PPP, aj.

1.2.2 MPLS L3 VPN

V MPLS L3 VPN konceptu sítě si hraniční směrovače poskytovatele PE vyměňují směrovací informace přímo se směrovači zákazníka CE. PE jsou pak propojeny pomocí MPLS páteřní sítě. PE uzly využívají techniku VRF (Virtual Routing and Forwarding), pomocí které se pak vytváří oddělené směrové tabulky pro každého zákazníka a umožňují tak použití shodných IP adresních rozsahů pro různá VRF. Dále je potom využito protokolu BGP pro distribuci VPN prefixů i s nimi spojených návěští mezi různými PE směrovači. VPN prefixy jsou známé pouze pro PE směrovače. Tedy znalost VPN (příslušnost k VRF) leží pouze na hraničních směrovačích MPLS VPN sítě, což dělá tento koncept dobře škálovatelný. Tento druh privátních sítí je velmi rozšířený. Možnou nevýhodou však může být, že směrování je spravováno poskytovatelem nikoliv zákazníkem.

Virtual Routing and Forwarding (VRF)

Virtual Routing and Forwarding představuje techniku pro vytvoření oddělených směrových tabulek na PE uzlu pro jednotlivé zákazníky a jejich VPN (pouze na PE uzlu, na CE nemá význam). Každá VRF instance musí obsahovat svoje RD a jeden či více RT. RD je možné specifikovat jak pro vložení (import), tak pro výstup (export) z nebo do daného VRF. Pomocí importu/exportu lze využívat například sdílené služby, které poskytovatel služeb může nabízet (pošta, dns, proxy, aj.).

Virtual Private Routed Network VPRN

V případě VPRN se jedná o model komunikace více bodů na více bodů (multipoint to multipoint) a stěžejní část práce zde zastoupí směrování. Distribuce prefixů je zajištěna pomocí víceprotokolového BGP (Multiprotocol BGP - MP-BGP). VPRN používá MPLS mechanismus se dvěma návěštími. Jednu „venkovní“ značku, která zajišťuje průchod paketu skrze MPLS síť a druhá „vnitřní“, která identifikuje příslušnost k dílčí virtuální směrové tabulce VRF. VPRN síť je znázorněna na Obr. 1.11.

Route Distinguisher (RD)

VPN prefixy jsou propagovány napříč MPLS VPN sítí pomocí MP-BGP. Problém vzniká, když BGP přenáší zákaznické prefixy přes síť poskytovatele, tedy prefixy musí být unikátní. Pokud více zákazníků používá shodné adresní rozsahy směrování

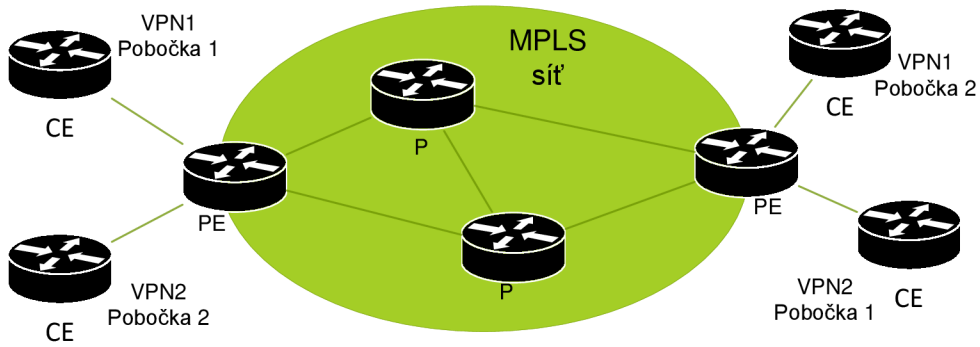
nebude fungovat. Řešením tohoto problému je koncept tzv. Route Distinguisher (RD), který zajistí, že adresní prefixy budou unikátní. RD je 64 bitů dlouhé číslo zapisované ve dvou formátech: ASN:nn nebo IP:nn, kde ASN znamená číslo autonomního systému a za nn může být dosazeno unikátní číslo vyhrazené pro konkrétní síť či IP adresa. Myšlenka je taková, že každý prefix bude posílán spolu s RD, čímž se zajistí unikátnost i přes to, že zákazníci poskytovatele budou využívat překrývající se adresní rozsahy. IPv4 prefix a RD jsou po jejich spojení souhrnně nazvány jako VPNv4 o délce 96 bitů. RD tedy pouze zajistí unikátnost prefixu, ale neukazuje ke kterému VRF prefix patří.

Route Target (RT)

V případě existence pouze RD by mezi sebou nemohly komunikovat uzly v různých VPN sítích jednoduše proto, že by jejich RD nesouhlasily (musí být rozdílné z jejich podstaty) a nebylo by možné VPNv4 prefixy zařadit do správného VRF. Zde nastupuje tzv. Route Target (RT), který říká do jakého VRF se má prefix zařadit. Je přenášený jako jeden z atributů BGP (extended community).

Propagace VPN prefixů v MPLS VPN síti

PE přijímá IP prefixy od CE pomocí některého z IGP protokolů nebo pomocí BGP. Tyto prefixy jsou přiřazeny k dané VRF. V případě existence více VRF bude použito to, které je na dané rozhraní přiřazeno. Je jim přiřazen RD, čímž se z nich stávají VPNv4 prefixy, které jsou následně vloženy do MP-BGP. BGP se dále postará o distribuci těchto VPNv4 prefixů na všechny PE uzly v MPLS VPN síti. Na PE uzlech, tyto VPNv4 prefixy jsou zbaveny RD a vloženy do VRF jako IPv4 prefixy.



Obr. 1.11: L3 VPN síťe.

Přeposílání paketů v MPLS VPN síti

Jak již bylo popsáno dříve, pakety nemohou být přeposílány čistě jako IP pakety mezi pobočkami, a to proto, že P uzly je neumí směrovat. P uzly nemají žádné informace o příslušnosti k VRF atd. MPLS to vyřešilo za pomocí označení paketu návěštím a odeslání ze vstupního PE na výstupní ve spolupráci s LDP protokolem. Jak PE směrovač na vzdálené straně pozná, do kterého VRF paket umístit? Tato informace není v IP záhlaví a nemůže být odvozena z IGP návěští, jelikož toto je použito výhradně k přeposlání paketu přes síť poskytovatele. Řešením je zde přidat další návěští a návěští stohovat. Toto druhé návěští ukazuje, do kterého VRF již samotný paket patří. To znamená, že všechny zákaznické pakety jsou přeposílány se dvěma návěštími: IGP návěští jako vrchní (průchodem MPLS doménou je s každým P uzlem změněno) a spodní VPN návěští (identifikuje na posledním uzlu v MPLS doméně příslušnost k VRF a zůstává neměnné). Rekapitulací je, že VRF-VRF provoz využívá dvou návěští. IGP návěští je zde zajištěno protokolem LDP a VPN návěští bylo přeneseno mezi dvěma PE za pomoci MP-BGP.

1.2.3 MPLS L2 VPN

Typy L2 VPN sítí jsou rozlišovány jejich charakteristikou poskytované služby. Dle levé části VPN podstromu z Obr. 1.10 existují celkem čtyři druhy technologií, nad kterými lze L2 VPN realizovat. Ethernet a například tunelování 802.1Q přes 802.1Q k vytvoření VPN stejně tak jako fyzické bodové spoje P2P nebudou dále uvažovány. Prostor se zde dostává technologiím Virtual Private Wire Service (VPWS) a Virtual Private LAN service (VPLS), které využívají tzv. pseudowires [9].

Pseudowire

Pseudowire (PW) poskytují zapouzdření a emulaci služeb napříč paketově přepojovanou páteřní síť a umožňuje tak přenos datových jednotek různých technologií spojové vrstvy a to včetně například TDM toků (E1/T1). Pseudowire je virtuální relace (spoj) navázaná mezi dvěma PE uzly. Zatímco AC (Attachment Circuit) je využit pro přenos rámce mezi CE a PE, PW je využito pro přenos rámce mezi dvěma PE. Jinak řečeno napříč páteřní sítí. Sestavení, údržba a stavové informace daného PW jsou udržovány dvěma PE, které jsou koncovými body pro daný PW nikoliv však páteřními směrovači (P uzly). Pseudowire mohou být typu:

- Bod - bod,
- Vícebodové.

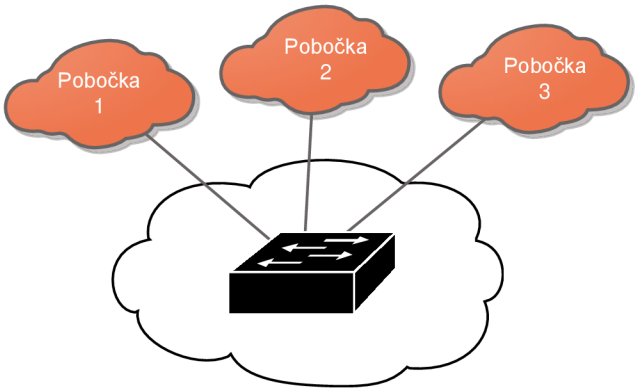
V konceptu point-to-point jsou PW vždy považovány za obousměrné. V případě vícebodových variant jsou PW vždy považovány za jednosměrné.

Virtual Private Wire service VPWS

VPWS poskytují služby spojové vrstvy přes MPLS k vytvoření připojení typu bod-bod, které spojují pobočky zákazníků do VPN. Tyto L2 VPN poskytují alternativu k dvoubodovým VPN sítím, které byly dříve dostupné přes ATM nebo Frame Relay páteřní sítě [9].

Virtual Private LAN service VPLS

VPLS je jednou z klíčových aplikací založených na MPLS. Jak již název napovídá, účelem VPLS je poskytnout privátní vícebodovou službu typu Ethernet. Dá se tedy říct že, VPLS je emulace lokální sítě LAN nad MPLS jak je zobrazeno na Obr. 1.12. Sítě využívající VPLS jsou spíše regionálního charakteru a využívají výhody, že celý adresový prostor případně i směrování a další funkce jsou výlučně ve správě zákazníka. Dojde tak k minimalizaci potřeby interakce mezi zákazníkem a poskytovatelem. Zákaznici tak mají možnost bezprostředních změn v jejich síti, což může ušetřit ve výsledku drahocenné hodiny nebo i dny. Časem však může nastat otázka, do jaké míry bude síť rozšiřitelná. Jedná se o to, že s každým dalším zařízením v takové sítí roste všesměrová doména (angl. broadcast domain).



Obr. 1.12: Emulace LAN.

VPLS má svoje místo v prostředí poskytovatelů připojení jako způsob, jak doručit mnohabodovou transparentní službu na úrovni spojové vrstvy přes Ethernet infrastrukturu pomocí MPLS. Čím je VPLS tak zvláštní? Klíč je v MPLS. Jsou známé různé přístupy, kterými mohou poskytovatelé připojení doručit služby přes infrastrukturu založenou na Ethernetu, ale ne všechny vyhovují jejich požadavkům v ohledech rozšiřitelnosti, spolehlivosti a pružnosti. MPLS se stalo urychlovačem,

který může z Ethernetové infrastruktury vytvořit vhodný nástroj pro poskytovatele připojení. Naproti tomu sítě poskytovatelů založené pouze na virtuálních sítích VLAN nebo na technice více násobného označkování (802.1Q přes 802.1Q, také Q in Q) postupem času ukázaly, že neposkytují to, co by se od nich očekávalo [8].

Architektura VPLS

Klasický VPLS model vyžaduje v páteřní síti plné propojení (angl. full mesh) LSP (pseudowires) mezi všemi PE směrovači, které jsou využity v dané VPLS instanci (v rámci sítě jednoho zákazníka). Pro VPLS síť s n pobočkami musí být sestaveno n*(n-1)/2 PW mezi PE směrovači, což s sebou přináší velkou režii [11]. V neprospěch velkých sítí se přičítá fakt, že je třeba provádět zmnožení paketů na PE pro každý PW (mnohabodová komunikace). Z toho důvodu byl zaveden hierarchický model, označovaný jako H-VPLS, který má za úkol snížení replikační a signalizační režie a umožnit tak nasazení technologie ve velkém měřítku. Na Obr. 1.12 je ilustrace sítě VPLS z pohledu zákazníka. Jedná se tedy o transparentní službu a z pohledu zákazníka se MPLS síť chová jako přepínač.

Jako možnou výhodu lze také zmínit, že v roli CE zařízení v architektuře VPLS nemusí vystupovat pouze směrovač, ale může být použit také přepínač.

Řídicí rovina VPLS

Existují dvě hlavní funkce řídicí roviny VPLS:

- Auto-objevování (angl. autodiscovery) ostatních směrovačů účastnících se stejných VPN sítí v rámci páteřní sítě.
- Sestavení a ukončení pseudowire tunelů ze kterých se daná VPLS instance skládá. Sestavování a ukončování tunelů se souhrnně nazývá signalizace (angl. signalling).

Existují dvě možnosti jak byla implementována signalizace, obě byly standardizovány. Jedná se o tyto standardy:

- RFC4761 – signalizace VPLS založená na BGP.
- RFC4762 – signalizace VPLS založená na LDP.

Obě výše jmenované implementace jsou identické z pohledu přepojování datových jednotek (z pohledu datové roviny). Liší se v řídicí rovině a to zejména v protokolu, který využívají k signalizaci a sestavení výše zmíněných pseudowires, tedy BGP nebo LDP [12].

Datová rovina VPLS

Datová rovina zajišťuje hlavně zapouzdřování Ethernetových rámců, přijatých od zákaznických zařízení a zajišťuje jejich přepojování. Rámce, které přicházejí ze zákaznických poboček jsou rozděleny do tzv. servisních instancí (angl. service instance)

a jsou asociovány k příslušné přepojovací tabulce, která se váže k rozhraní, ze kterého byly přijaty. Pakety jsou přepojeny v dané servisní instanci dle jejich cílové MAC adresy tak, jako je tomu v lokálních sítích. Pod pojmem servisní instance se skrývá pravidlo, které určuje dle čeho se rozliší, která data patří do kterých servisních instancí. Takovým pravidlem může být například číslo sítě VLAN. Dalšími funkcemi datové roviny je například učení MAC adres, jejich stárnutí, zaplavování všech okolních PE směrovačů pakety, pro které není známá cílová MAC adresa, aj. [12]. Do jedné servisní instance je tedy možné připojit více poboček daného zákazníka, které jsou ukončeny na stejném hraničním směrovači.

IP-Only LAN Service IPLS

IPLS je modifikovanou verzí VPLS, avšak možné využití je pouze pro IP provoz. Původní záměr pro IPLS bylo alternativní řešení pro PE směrovače, které měly problém s učením MAC adres. Avšak tento problém s novějšími zařízeními přestal existovat a IPLS tak zůstalo v pozadí [10].

2 PRAKTICKÁ ČÁST

V teoretické části byla popsána funkce MPLS a některé hlavní další služby s jejich popisem. Praktická část diplomové práce je zaměřena na návrh laboratorní úlohy se zaměřením na službu VPLS. V následujících kapitolách bude popsáno, jakým způsobem byla úloha vytvořena, co je potřeba pro její běh a také dále samotná konfigurace směrovačů. Kompletní zadání laboratorní úlohy je uvedeno ve zvláštní příloze.

2.1 Motivace úlohy

Motivací pro následující laboratorní úlohu je nejen seznámení studentů s MPLS technologií a poskytovanými službami, ale celkově si od úlohy slibuji, že student, který laboratorní úlohu absolvuje, si propojí jednotlivé souvislosti, které z ní vyplývají. Mám na mysli propojení mezi protokoly, jejich vzájemnou spolupráci, ale také získání vlastních praktických zkušeností.

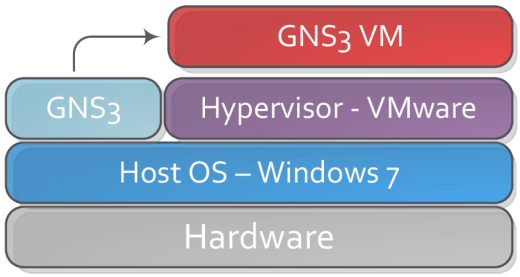
2.2 Návrh laboratorní úlohy

2.2.1 Výběr simulačního prostředí

Existuje nepřeberné množství různých typů síťových simulátorů, např. VIRL, Boson Netsim, Packet Tracer, Eve-ng, Imunes, Mininet, Netkit, aj. Ze všech těchto typů se jeví jako nejlepší volba simulátor od firmy Cisco, který je znám pod zkratkou VIRL (Virtual Internet Routing Lab). Jedná se totiž o jednotnou platformu, na které by se dala úloha provést a obejít tak veškeré problémy, které potencionálně přinášejí jiná řešení. Bohužel, po rozhovoru s autorem knihy (virlbook.com) zabývající se prostředím VIRL, Jackem Wangem, jsem se dozvěděl, že VPLS služba není plně implementována (pouze řídicí rovina, nikoliv datová) v tomto virtuálním prostředí. Znamenalo by to tedy pouze teoretickou možnost konfigurace služby VPLS, bez výsledného přepojování paketů simulovanou sítí. Konečnou volbou tak bylo prostředí grafického simulátoru GNS3 (Graphical Network Simulator 3), které poskytuje uživatelsky přívětivé grafické prostředí. V pozadí simulátoru GNS3 se dá využít mnoho různých komponent nejen pro emulaci síťových systémů. Ke konečné volbě prostředí GNS3 přispěla i moje předchozí zkušenost a znalost tohoto prostředí.

Simulátor GNS3 může emulovat síťové systémy více způsoby. Jedním z nich je emulace na počítači za pomoci softwaru Dynamips, což je řešení, které vytvořil Christophe Fillot v roce 2005 určené pouze pro emulaci směrovačů Cisco (navíc

pouze vybrané verze IOS). Další z možností, dokonce doporučovanou možností vývojáři simulátoru, je použít koncept typu klient-server, tedy nikoliv emulace přímo pomocí Dynamips, ale na speciálně upraveném serverovém systému GNS3 VM. Koncept je takový, že za pomocí simulátoru GNS3 se vytvoří pouze grafická topologie a samotné síťové systémy pak jsou spouštěny na serverové části v pozadí (která ale může být spouštěna lokálně). Simulátor GNS3, nainstalovaný přímo na počítači se chová jako klient a využívá zdroje serverové části GNS3 VM tak, jak je naznačeno šipkou na Obr. 2.1. Využití serverové části je označováno vývojáři jako stabilnější řešení, z toho důvodu bylo využito i pro tuto úlohu.



Obr. 2.1: Koncept GNS3 prostředí.

2.2.2 Síťové systémy

V úloze budou použity tři odlišné typy síťových systémů, plnící tyto funkce:

- Hraniční směrovač PE; funkce: MPLS + VPLS logika, připojení zákaznických poboček (Platforma Cisco CSR1000V - IOS XE).
- Směrovač páteřní sítě P; funkce: MPLS, přepopojování paketů (Platforma Cisco 7206VXR - IOS)
- Přepínač SW; funkce: Trunk + přístupové rozhraní, připojení pobočky k páteřnímu směrovači + připojení zařízení (Platforma IOS on Unix)

Síťový systém pro hraniční směrovače jsem zvolil Cisco Cloud Services Router 1000V (CSR1000V), zástupce systémů IOS XE. Jedná se čistě o virtuální platformu, jejíž využití je směřováno do virtuálních sítí (angl. cloud). V rámci hledání vhodného systému pro službu VPLS v daném prostředí GNS3 se zdá, že platforma CSR1000V je jedinou možností. Vzhledem k mým předchozím zkušenostem s konfigurací směrovačů Cisco jsem nehledal podobné funkce virtuálních systémů u jiných výrobců.

Pro směrovače v páteřní síti byl zvolen systém IOS, určený pro směrovače typu Cisco 7206VXR. Jedná se totiž o doporučovaný systém z hlediska stability samotnými vývojáři simulátoru GNS3.

Přepínač (angl. switch) lze v GNS3 implementovat více způsoby. Vybral jsem ten nejstabilnější. Jedná se o využití IOU systému. Další možností je např. využití přepínacího modulu NM-16ESW na směrovači typu C3640, nicméně tuto možnost jsem po pár dnech testování vyloučil. Chování této platformy v simulátoru bylo velmi nepředvídatelné (např. nekomunikující rozhraní, rozhraní nejdou zapnout, směrovač po zapnutí nenabíhá, aj.)

2.2.3 Hypervisor

Pro prvotní testování jsem využíval pro běh směrovačů CSR1000v hypervisor od Oracle - Virtualbox (také prvotně vše spouštěno pouze lokálně, bez využití GNS3 VM). Jelikož simulátor GNS3 umožňuje přímé vložení jakéhokoliv virtuálního stroje, využíval jsem z počátku tuto možnost pro platformu CSR1000v. Vytvořil jsem jeden virtuální směrovač ve Virtualbox, naklonoval a klony vložil přímo do GNS3. Po spuštění topologie v GNS3 se tyto klony spustily na pozadí simulátoru a bylo možné konfigurovat co bylo třeba. Podařilo se mi tímto způsobem za pomocí Virtualboxu zprovoznit funkční VPLS topologii. Vše fungovalo správně, ale pouze do bodu, když jsem chtěl přenášet přes MPLS doménu provoz různých virtuálních sítí VLAN (Virtual Local Area Network). Tedy, přenos více virtuálních sítí od zákazníka přes MPLS doménu např. na jinou pobočku. V momentě, kdy jsem nastavil na hraničním směrovači aby přijímal i jiné než neoznačkované rámce (VLAN), přestal přes něj procházet provoz. Bohužel po vyzkoušení snad všech možností jsem zjistil, že sám Virtualbox (ve spojení s GNS3) má problémy s přenosem značkovaných rámců VLAN. Podrobnější dokumentace této problematiky prakticky neexistuje. Na webových stránkách vývojářů (forums.virtualbox.org) lze dohledat, že se tímto problémem už někdo v minulosti zabýval, avšak ani doporučované využití např. Paravirtualised adaptéru oproti síťové kartě Intel PRO/1000 tento problém nevyřešilo.

Přes všechny okolnosti popsané výše jsem dospěl k využití hypervisoru od VMware Workstation. Při použití VMware Workstation vše fungovalo jak mělo a problém s přenosem provozu více VLAN byl odstraněn.

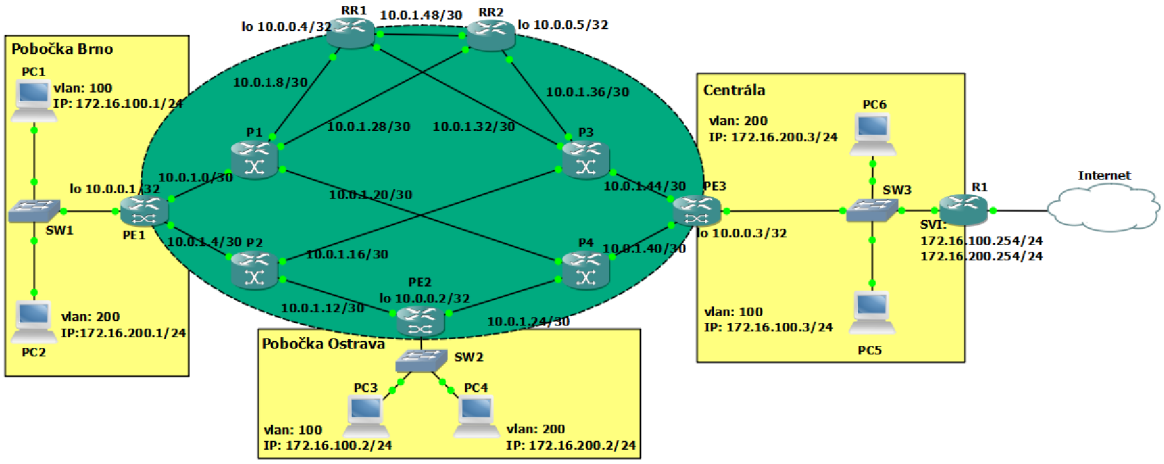
2.2.4 Laboratorní síť - návrh

Laboratorní síť se skládá ze dvou celků, které jsou na Obr. 2.2 odděleny zelenou a žlutou barvou. Zelená část obsahuje prvky páteřní sítě:

- PE1-PE3: Hraniční směrovače.
- P1-P4: Páteřní směrovače.

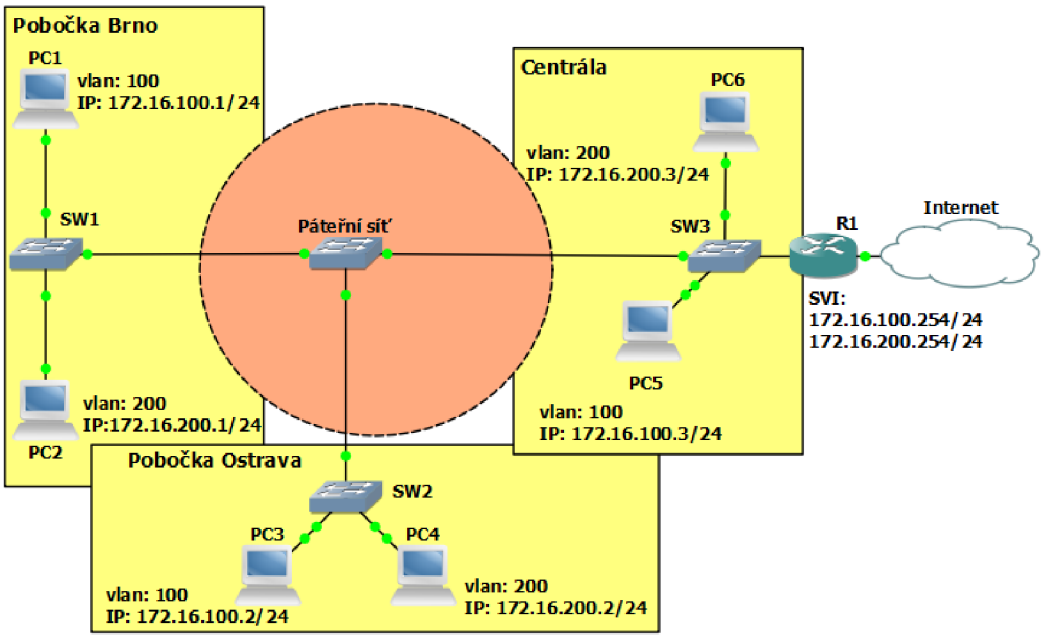
- RR1-RR2: Reflektory směrových informací RR (Route Reflector).

Síť jsem navrhl s ohledem na redundanci linek i směrovačů. Prakticky jako jediné zranitelné místo lze označit hraniční směrovače. Pro zajištění dostupnosti v rámci páteřní sítě byl zvolen směrový protokol OSPF (Open Short Path First). V páteřních sítích poskytovatelů připojení se využívají s výhodou směrové protokoly spojově stavové (angl. link-state) a to z důvodu jejich znalosti celé topologie. Pro přenos stavových informací mezi hraničními směrovači je určen směrový protokol BGP. Z důvodu lepší škálovatelnosti jsem využil konceptu reflektoru cest, dále jen RR. V tomto konceptu nenavazují hraniční směrovače relaci přímo každý s každým, ale využívají tzv. route reflector směrovače. Takže hraniční směrovač navazuje pouze dvě relace na každý z reflektorů namísto navazování relací s každým dalším hraničním směrovačem jednotlivě. Využitím RR jsem obešel nutnost plného propojení (angl. full mesh) v interní BGP síti. RR směrovače jsou využité v páru z důvodu redundance [5].



Obr. 2.2: Topologie laboratorní sítě.

Žlutě vyznačené celky označují jednotlivé pobočky, které jsou spojeny pomoci sítě poskytovatele do virtuální L2 sítě. Z pohledu zákazníka se pak celá páteřní síť chová jako jeden L2 přepínač viz Obr. 2.3. Mezi hraničními směrovači a přepínači na pobočkách je nastaven režim tzv. trunk, který je určen pro přenos více sítí VLAN. Z přepínačů směrem k jednotlivým PC už provoz není značkován a jedná se tedy o klasické přístupové rozhraní. Popis, do které z VLAN je PC připojen je umístěn vždy vedle samotného PC, včetně IP adres. Konvence IP adresace zde odpovídá ve třetím oktetu - číslu dané VLAN. PC1 je tedy umístěn do VLAN 100 a třetí oktet začíná taktéž stejnou číslovkou 100 - IP adresa je pak 172.16.100.1.



Obr. 2.3: VPLS síť z pohledu zákazníka.

2.2.5 Laboratorní síť - konfigurace

Před započetím samotné konfigurace je třeba zvolit IP adresaci v síti. Pro propoje mezi jednotlivými směrovači byla vyhrazena síť 10.0.1.0/24, která byla rozdělena na menší celky obsahující každý dvě IP adresy. První bude vypadat následovně: 10.0.1.0/30. Hraniční směrovače PE1 až PE3 a směrovače RR1, RR2 mají navíc nakonfigurované tzv. smyčková rozhraní (angl. loopback interface), která se s výhodou dají použít, pokud existuje v páteřní síti k danému směrovači více jak jedna cesta. Smyčkové rozhraní zůstává vždy aktivní a tím pádem i BGP relace zůstávají zachovány do té doby, dokud IGP (Internal Gateway Protocol) protokol zná alespoň jednu cestu, jak se k danému smyčkovému rozhraní dostat. Pro smyčková rozhraní (angl.loopback interface) byla vyhrazena síť 10.0.0.0/24, kde první rozhraní nacházející se na směrovači PE1 bude mít adresu 10.0.0.1/32. Jejich rozdělení je uvedeno na Obr. 2.2. Seznam smyčkových rozhraní pro jednotlivé směrovače je uveden v Tab. 2.1:

V následující části bude popsána konfiguraci jednotlivých směrovačů. Vždy bude uveden příklad konfigurace pouze na jednom ze zařízení. Kompletní zálohované konfigurační soubory jsou uloženy na přiloženém DVD.

Konfigurace názvu zařízení

Každému zařízení je dobré pro přehlednost nastavit vlastní název, čehož lze dosáhnout pomocí příkazu **hostname** z konfiguračního režimu:

Výpis 2.1: Nastavení názvu zařízení.

```
Router#configure terminal // vstup do konfig. režimu
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)#hostname PE1
PE1(config)#
```

Konfigurace IP adres

Bez IP adres by nebylo komunikace, proto je nastavím jako první, příklad uveden opět na směrovači PE1. Seznam IP adres všech zařízení je uveden v Tab.2.1.

Výpis 2.2: Nastavení IP adresy.

```
PE1(config)#interface GigabitEthernet3
PE1(config-if)#ip address 10.0.1.1 255.255.255.252
PE1(config-if)#no shutdown
```

Po nastavení IP adresy je navíc nutné samotné rozhraní aktivovat. Ve výchozím nastavení je totiž administrativně vypnuto. Zapnutí docílíme pod daným rozhraním příkazem **no shutdown**.

Konfigurace směrového protokolu OSPF

Směrový protokol OSPF v páteřní síti slouží k zajištění plné dostupnosti všech rozhraní jednotlivým směrovačům. Jeho konfigurace je možná více způsoby. Já využívám způsob (Výpis 2.3), kdy je každému rozhraní specifikováno, že se má účastnit směrování OSPF. První číslice 1 značí číslo procesu a druhé číslo oblasti (area 0). V této úloze jsou všechny směrovače členy oblasti 0. Tímto způsobem je třeba spe-

Výpis 2.3: Nastavení OSPF.

```
PE1(config)#interface GigabitEthernet3
PE1(config-if)#ip ospf 1 area 0
```

cifikovat všechna rozhraní, která je třeba mít dosažitelné v rámci páteřní sítě. V případě směrovače PE1 se bude jednat o rozhraní: GigabitEthernet3, GigabitEthernet4, interface Loopback0. Kontrolu lze provést příkazem zobrazeným na Výpise 2.4. Z daného výpisu lze vidět všechna rozhraní, která jsou zahrnuta do OSPF procesu, případně jejich IP adresy. Po konfiguraci směrového protokolu OSPF lze přikročit

Výpis 2.4: Ověření nastavení rozhraní v OSPF.

```
PE1#show ip ospf interface  brief
Interface PID Area  IP Address/Mask Cost  State Nbrs F/C
Lo0       1   0       10.0.0.1/32    1     LOOP   0/0
Gi4       1   0       10.0.1.1/30    1     DR     1/1
Gi3       1   0       10.0.1.5/30    1     DR     1/1
```

ke konfiguraci MPLS.

Konfigurace MPLS

Základní konfigurace pro účel této úlohy je velmi jednoduchá. Jeden příkaz aktivuje vše potřebné - aktivuje samotnou technologii MPLS, ale také protokol pro distribuci a tvorbu návěští LDP. Tento příkaz se podobně jako při konfiguraci OSPF spouští pod daným fyzickým rozhraním viz Výpis 2.5. Ověření aktivovaných roz-

Výpis 2.5: Aktivace MPLS na rozhraní.

```
PE1(config)#interface gigabitEthernet 3
PE1(config-if)#mpls ip
```

hraní pro MPLS lze provést příkazem **show mpls interfaces** (Výpis 2.6).

Výpis 2.6: MPLS rozhraní.

```
PE1#show mpls interfaces
Interface          IP    Tunnel   BGP Static Operational
GigabitEthernet3   Yes (ldp) No        No   No      Yes
GigabitEthernet4   Yes (ldp) No        No   No      Yes
```

Případně lze také zobrazit již přiřazená návěští k jednotlivým prefixům směrové tabulky pomocí příkazu **show mpls ldp bindings** viz Výpis 2.7. Na výpise lze vidět, jaká návěští jsou přiřazena konkrétnímu prefixu 10.0.0.1/32, jež je zároveň umístěn na daném směrovači (proto je jeho návěští imp-null, tedy nulové).

Výpis 2.7: Ukázka přiřazených návěští protokolem LDP.

```
PE1#show mpls ldp bindings
  lib entry: 10.0.0.1/32, rev 2
        local binding:  label: imp-null
        remote binding: lsr: 10.0.1.29:0, label: 28
        remote binding: lsr: 10.0.1.17:0, label: 30
        remote binding: lsr: 10.0.0.2:0, label: 23
        remote binding: lsr: 10.0.0.3:0, label: 16

(zobrazen pouze první záznam)
```

Konfigurace BGP na hraničním směrovači PE1

Konfigurace směrového protokolu je zcela identická na všech hraničních směrovačích. Jak již bylo popsáno, BGP relace je navazována pouze s reflektory cest, které jsou stejné pro jakýkoliv hraniční směrovač. Konfigurace je uvedena a komentována ve Výpise B.2. Číslo AS (Autonomous System) je pro celou doménu zvoleno 100.

Konfigurace BGP na Route Reflektoru RR1

Konfigurace BGP na RR se v zásadě neliší od konfigurace hraničních směrovačů (klientů RR). Navíc má specifikováno, aby přeposílal směrové informace, které přijme od okolních směrovačů na ty ostatní (příkazem route-reflector-client). Dále jsem zde využil možnosti tzv. peer-group. Jedná se o definici skupiny zařízení se stejnými parametry, z důvodu lepší správy a přehlednosti konfigurace. Byla tedy vytvořena peer-group s názvem RR1, pod kterou jsou nastaveny parametry (remote-as, update-source). Dále je třeba do této skupiny přiřadit všechny hraniční směrovače viz Výpis 2.9.

Výpis 2.8: Konfigurace BGP na hraničním směrovači.

```
%vstup do konfiguračního režimu
PE1#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.

%spuštění protokolu bgp, číslo AS je 100
PE1(config)#router bgp 100

%nastavení IP adres route reflektorů spolu s jejich AS
PE1(config-router)#neighbor 10.0.0.4 remote-as 100

%explicitní volba zdrojového rozhraní - loopback 0
PE1(config-router)#neighbor 10.0.0.4 update-source Lo 0

PE1(config-router)#neighbor 10.0.0.5 remote-as 100
PE1(config-router)#neighbor 10.0.0.5 update-source Lo 0
%vstup do konfigurace adresní rodiny pro vpls
PE1(config-router)#address-family l2vpn vpls

%aktivování komunikace se na zvolené směrovače RR
PE1(config-router-af)#neighbor 10.0.0.4 activate

%instrukce pro bgp odesílat jak standardní tak
%rozšířené komunity
PE1(config-router-af)#neighbor 10.0.0.4 send-comunity both

PE1(config-router-af)#neighbor 10.0.0.5 activate
PE1(config-router-af)#neighbor 10.0.0.5 send-comunity both
```

Výpis 2.9: Konfigurace BGP na RR1.

```
%vstup do konfigurace BGP
RR1(config)#router bgp 100

%vytvoření peer-group
RR1(config-router)#neighbor RR1 peer-group

%specifikace AS pro objekt peer-group
RR1(config-router)#neighbor RR1 remote-as 100

%specifikace zdrojového rozhraní pro objekt peer-group
RR1(config-router)#neighbor RR1 update-source Loopback0

%přidání ostatních směrovačů do peer-group RR1
RR1(config-router)#neighbor 10.0.0.1 peer-group RR1
RR1(config-router)#neighbor 10.0.0.2 peer-group RR1
RR1(config-router)#neighbor 10.0.0.3 peer-group RR1

%nastavení bgp peeringu se sousedním RR2
R1(config-router)#neighbor 10.0.0.5 remote-as 100
R1(config-router)#neighbor 10.0.0.5 update-source Loop0

%definice adresní rodiny l2vpn vpls
RR1(config-router)#address-family l2vpn vpls

%nastavení směrovačů jako klientů tohoto RR
RR1(config-router-af)#neighbor RR1 route-reflector-client

%aktivace komunikace mezi směrovači
RR1(config-router-af)#neighbor 10.0.0.1 activate
RR1(config-router-af)#neighbor 10.0.0.2 activate
RR1(config-router-af)#neighbor 10.0.0.3 activate
```

Konfigurace VPLS na hraničních směrovačích

Konfigurace VPLS se skládá prakticky ze tří bodů, jedná se o vytvoření:

- Virtuální instance VFI (Virtual Forwarding Instance).
- Virtuální domény (angl. bridge domain).
- Servisní instance (angl. service instance).

Výpis 2.10: Konfigurace VPLS na PE1.

```
PE1#configure terminal
%vytvoreni instance VFI, definice vpn id, autodiscovery,
%signaling, vpls-id
PE1(config)#l2vpn vfi context VFI
PE1(config-vfi)#vpn id 100
PE1(config-vfi)#autodiscovery bgp signaling ldp
PE1(config-vfi-autodiscovery)#vpls-id 100

%vytvoreni virtualni domeny (virtualniho switche)
PE1(config)#bridge-domain 300
%pripojeni jednotlivych rozhrani do domeny
PE1(config-bdomain)#member GigabitEthernet 1
service-instance 100
PE1(config-bdomain)#member vfi VFI

%konfigurace pristupoveho rozhrani
PE1(config)#interface gigabitEthernet 1
PE1(config-if)#description LAN_pobocka1

%pomoci servisní instance se vytvori pravidlo,
%ktere definuje typ provozu ktery do ni muze vstoupit
PE1(config-if)#service instance 100 ethernet
PE1(config-if-srv)#encapsulation dot1q any
%nakonec nesmime opomenout opet aktivovat rozhrani
PE1(config-if)#no shutdown
```

Servisní instance je zde nakonfigurována tak, aby vyhověla všem příchozím rámcům (VLAN 1-4094) a to klíčovým slovem any. V produkční síti by se tento přístup pravděpodobně zcela neuplatnil. Hraničnímu směrovači by byla předřazena přístupová nebo distribuční vrstva, která by pravděpodobně využívala techniky dvojitého značkování dle 802.1ad nebo například techniku Mac in Mac dle 802.1ah.

Konfigurace přepínačů SW na pobočkách

Na každé zákaznické pobočce se nachází přepínač (označení SW1-SW3), který je přímo připojen k hraničnímu směrovači a to pomocí rozhraní typu trunk, které je schopno přenášet více VLAN. Dále jsou do každého přepínače připojeny dva počítače, každý do jiné VLAN (používají se VLAN 100 a 200). Jak již bylo řečeno, je na přepínačích třeba nastavit dvě přístupová rozhraní a jeden trunk viz Výpis 2.11. Při nastavování rozhraní Ethernet0/0 je nutné dodržet pořadí, tedy prvně zvolit typ

Výpis 2.11: Konfigurace přepínače.

```
%nastaveni nazvu zarizeni
Switch(config)#hostname SW1
%vstup do konfigurace rozhrani pripojeneho k PE1
SW1(config)#interface Ethernet 0/0
%popis rozhrani
SW1(config-if)#description PE1
%volba zapouzdreni ramcu
SW1(config-if)#switchport trunk encapsulation dot1q
%prepnuti do modu trunk
SW1(config-if)#switchport mode trunk
%nasleduje nastaveni rozhrani pro PC1 a PC2
SW1(config-if)#interface Ethernet0/1
%volba modu pro koncove stanice
SW1(config-if)#switchport mode access
%prirazeni k vlan 100 a nasledne 200
SW1(config-if)#switchport access vlan 100
SW1(config-if)#interface Ethernet0/2
SW1(config-if)#switchport access vlan 200
SW1(config-if)#switchport mode access
```

zapouzdření a až poté bude umožněno přepnutí módu na trunk. Rozhraní Ethernet0/3, které připojuje směrovač R1 k přepínači SW3 musí být nakonfigurované jako trunk. Na směrovači jsou ukončené rozhraní obou vlan sítí a je zde mezi nimi možné směrování.

Konfigurace PC na pobočkách

Počítače jsou z důvodu paměťové náročnosti realizovány pomocí Cisco směrovačů a jsou určeny pouze pro základní diagnostiku pomocí nástroje ping či zobrazení ARP (Address Resolution Protocol) tabulky. Úloha celkově zabírá dost paměti RAM,

z toho důvodu nejsou vyžity jako koncové stanice reálné operační systémy. Jedinou konfigurací je zde nastavení adresy IP, MAC adresy a názvu zařízení viz Výpis 2.12. Každý PC má pozměněnou MAC adresu, z důvodu jejich lepší identifikace při finálním ověřování v laboratorní úloze. PC1 má první dva oktety nulové, a další dva jsou vyplněny jedničkami, čímž lze jednoduše rozpoznat v ARP tabulce MAC adresu patřící danému PC1. Konfigurace dále zahrnuje určení výchozí brány pro komunikaci mezi sítěmi VLAN nebo do Internetu. Navíc byl nastaven i dns server pro možnost získání odezvy ze serverů v Internetu bez znalosti jejich IP adresy.

Výpis 2.12: Konfigurace PC.

```
%vstup do konfiguracniho rezimu
Router#configure terminal

%nastaveni nazvu zarizeni
Router(config)#hostname PC1

%vstup do konfiguracniho rezimu rozhani Fa 0/0
PC1(config)#interface FastEthernet 0/0

%nastaveni IP adresy na rozhrani
PC1(config-if)#ip address 172.16.100.1 255.255.255.0

%nastaveni MAC adresy
PC1(config-if)#mac-address 0000.1111.1111

%aktivace rozhrani
PC1(config-if)#no shutdown

%deaktivace smerovani
PC1(config)#no ip routing

%nastaveni vychozi brany, na R1
PC1(config)#ip default-gateway 172.16.100.254

%nastaveni dns serveru
PC1(config)#ip name-server 8.8.8.8
```

Konfigurace R1

Směrovač R1 je určen jednak ke směrování mezi virtuálními sítěmi VLAN 100 a 200 ale také pro přístup do Internetu. Přístupu do Internetu je docíleno tak, že symbol mraku v topologii zprostředkuje připojení k fyzické síťové kartě počítač. R1 má tedy rozhraní Fa0/1 připojeno do školní sítě, odkud pomocí DHCP protokolu dostává IP adresu. Dále bylo nutné využít techniky překladu adres (NAT) a to mezi pobočkami (sítě 172.16.X.0/24) a IP adresou která je přiřazena směrovači R1 na venkovním rozhraní.

2.2.6 Cíl laboratorní úlohy

Kompletní konfigurace jednotlivých prvků byla popsána výše. Laboratorní úloha bude simulovat situaci, kdy se poskytovatel připojení rozhodl rozšířit stávající páteřní síť o jeden hraniční směrovač - PE1. Směrovač bude obsahovat pouze základní nastavení a zprovoznění hraničního uzlu bude hlavním úkolem úlohy (OSPF, MPLS, BGP, VPLS). Vypracovaný návod je uveden v příloze. V přílohách se také nachází postup jak zprovoznit celé prostředí spolu s poznámkami, jak řešit případné problémy, které mohou nastat v prostředí GNS3.

Výpis 2.13: Konfigurace R1.

```
%vytvoreni pod-rozhrani pro vlan sit 100
R1(config)#interface FastEthernet0/0.100

%definice cisla vlan a typu zapouzdreni
R1(config-if)#encapsulation dot1Q 100

%nastaveni IP adresy
R1(config-if)#ip address 172.16.100.254 255.255.255.0

%k prekladu IP adres je nutne urcit vnitrni
%a venkovni rozhrani
R1(config-if)#ip nat inside

%obdobne je tomu pro vlan 200
R1(config-if)#interface FastEthernet0/0.200
R1(config-if)#encapsulation dot1Q 200
R1(config-if)#ip address 172.16.200.254 255.255.255.0
R1(config-if)#ip nat inside

% WAN rozhrani do Internetu
R1(config-if)#interface FastEthernet0/1
%IP adresa ziskana dynamicky pomoci dhcp
R1(config-if)#ip address dhcp
%definice venkovniho rozhrani pro NAT
R1(config-if)#ip nat outside

%pomoci pristupovych seznamu ACL
%vymezime site, ktere se budou ucastnit prekladu NAT
%jedna se o lokalni site ve vlan 100 a 200
R1(config)#access-list 10 permit 172.16.100.0 0.0.0.255
R1(config)#access-list 10 permit 172.16.200.0 0.0.0.255

%konfigurace prekladu NAT
%preklad vnitrnich adres na venkovni
%prekladaji se adresy vyhovujici access listu 10
%na IP adresu wan rozhrani Fa 0/1
%klicovym slovem overload definujeme preklad portu PAT
R1(config)#ip nat inside source list 10 interface
FastEthernet0/1 overload
```

Tab. 2.1: IP adresy jednotlivých rozhraní

uzel	**rozhraní**	**IP adresa**	**maska**
PE1	GigabitEthernet3	10.0.1.1	255.255.255.252
PE1	Loobpack0	10.0.0.1	255.255.255.255
PE1	GigabitEthernet4	10.0.1.5	255.255.255.252
PE2	GigabitEthernet3	10.0.1.14	255.255.255.252
PE2	Loopback0	10.0.0.2	255.255.255.255
PE2	GigabitEthernet4	10.0.1.25	255.255.255.252
PE3	GigabitEthernet3	10.0.1.46	255.255.255.252
PE3	Loopback0	10.0.0.3	255.255.255.255
PE3	GigabitEthernet4	10.0.1.42	255.255.255.252
P1	FastEthernet0/0	10.0.1.2	255.255.255.252
P1	FastEthernet0/1	10.0.1.9	255.255.255.252
P1	FastEthernet1/0	10.0.1.21	255.255.255.252
P1	FastEthernet1/1	10.0.1.29	255.255.255.252
P2	FastEthernet0/0	10.0.1.6	255.255.255.252
P2	FastEthernet0/1	10.0.1.13	255.255.255.252
P2	FastEthernet1/0	10.0.1.17	255.255.255.252
P3	FastEthernet0/0	10.0.1.45	255.255.255.252
P3	FastEthernet0/1	10.0.1.34	255.255.255.252
P3	FastEthernet1/0	10.0.1.18	255.255.255.252
P3	FastEthernet1/1	10.0.1.38	255.255.255.252
P4	FastEthernet0/0	10.0.1.41	255.255.255.252
P4	FastEthernet0/1	10.0.1.26	255.255.255.252
P4	FastEthernet1/0	10.0.1.22	255.255.255.252
RR1	FastEthernet0/0	10.0.1.33	255.255.255.252
RR1	Loopback 0	10.0.0.4	255.255.255.255
RR1	FastEthernet0/1	10.0.1.10	255.255.255.252
RR1	FastEthernet1/0	10.0.1.49	255.255.255.252
RR2	FastEthernet0/0	10.0.1.30	255.255.255.252
RR2	Loopback0	10.0.0.5	255.255.255.255
RR2	FastEthernet0/1	10.0.1.37	255.255.255.252
RR2	FastEthernet1/0	10.0.1.50	255.255.255.252

3 ZÁVĚR

Diplomová práce se ve větší míře zabývala technologií multiprotokolového přepojování na základě návěští (MPLS). Byl popsán princip funkce, základní architektura a prvky sítě, ze kterých se síť skládá. Dále byly popsány techniky, které umožňují vytvoření virtuálních privátních sítí a to jak na síťové, tak na spojové vrstvě ISO/OSI modelu.

Pro praktickou část diplomové práce a návrh laboratorní úlohy byla vybrána technologie VPLS, která využívá pro svůj běh MPLS sítě. I přes značné problémy, které se naskytly při vytváření laboratorní úlohy se ji podařilo zdárně vytvořit. Laboratorní úloha vytvořená ve virtualizovaném prostředí tak funkčně prakticky plnohodnotně nahrazuje reálné prostředí a není tak nutné budovat nákladnou laboratoř obsahující fyzická zařízení. Cílem vytvořené laboratorní úlohy měla být praktická ukázka výše zmíněných technologií a jejího možného využití.

LITERATURA

[1] Andersson, L., Asati, R. *Multiprotocol Label Switching Architecture* [online]. Leden 2001, Dostupné z URL: <https://tools.ietf.org/html/rfc3031>.

[2] Andersson, L., Asati, R. *Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP"Field Renamed to "Traffic Class"Field* [online]. Únor 2009, Dostupné z URL: <https://tools.ietf.org/html/rfc5462>.

[3] Rosen, E., Tappan, D., Fedorkow, G., Cisco Systems, Inc., Rekhter, Y., Juniper Networks, Farinacci, D., Li, T., Procket Networks, Inc., Conta, A. *MPLS Label Stack Encoding* [online]. Leden 2001, Dostupné z URL: <https://tools.ietf.org/html/rfc3032>.

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

[5] BEIJNUM, Iljitsch van *BGP. 1st ed.* Sebastopol, CA: O'Reilly, c2002, xiv, 272 p. ISBN 05-960-0254-8.

[6] *MikroTik RouterOS Introduction to MPLS* [online]. 2009, MUM Czech Republic 2009]. Dostupné z URL: <http://mum.mikrotik.com/presentations/CZ09/MPLS.pdf>.

[7] L. Andersson, Ed., Acreo AB, I. Minei, Ed., Juniper Networks, B. Thomas, Ed., Cisco Systems, Inc. *LDP Specification* [online]. Říjen 2009, Dostupné z URL: <https://tools.ietf.org/html/rfc5036>.

[8] Juniper Networks, Inc. *DEMYSTIFYING H-VPLS* [online]. 2010, Dostupné z URL: <https://www.juniper.net/us/en/local/pdf/app-notes/3500116-en.pdf>.

[9] L. Andersson, Ed., Acreo AB, E. Rosen, Ed., Cisco Systems, Inc., *Framework for Layer 2 Virtual Private Networks (L2VPNs)* [online]. Září 2006, Dostupné z URL: <https://tools.ietf.org/html/rfc4664>.

[10] H. Shah, Cinea Corp., E. Rosen, Juniper Networks, F. Le Faucheur, G. Heron, Cisco Systems, Inc. *LDP Specification* [online]. Leden 2015, Dostupné z URL: <https://tools.ietf.org/html/rfc7436>.

[11] M. Lasserre, Ed., V. Kompella, Ed., Alcatel-Lucent. *LDP Specification* [online]. Leden 2007, Dostupné z URL: <https://tools.ietf.org/html/rfc4762>.

[12] K. Kompella, Ed., Y. Rekhter, Ed., Juniper Networks. *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling* [online]. Leden 2007, Dostupné z URL: <https://tools.ietf.org/html/rfc4761>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

AC	Attachment Circuit
ARP	Address Resolution Protocol
AS	Autonomous System
ASIC	Application Specific Integrated Circuit
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BS	Bottom of Stack
CE	Customer Edge
CEF	Cisco Express Forwarding
CIDR	Classless Inter-Domain Routing
CPU	Central Processing Unit
CSR	Cloud Services Router
DLCI	Data Link Connection Identifier
FEC	Forwarding Equivalent Class
FIB	Forwarding Information Base
GNS3	Graphical Network Simulator 3
HDLC	High Level Data Link Control
IGP	Internal Gateway Protocol
IOS	Internetwork Operating System
IP	Internet Protocol
LAN	Local Area Network
LDP	Label Distribution Protocol
LFIB	Label Forwarding Information Base
LIB	Label Information Base
LER	Label Edge Router
LSP	Label Switched Path
LSR	Label Switching Router
MP	Multi Protocol
MPLS	Multi Protocol Label Switching
OSPF	Open Short Path First
PE	Provider Edge
PHP	Penultimate Hop Popping
PPP	Point to Point Protocol
PW	Pseudowire
RD	Route Distinguisher
RIB	Routing Information Base
RSVP-TE	Resource Reservation Protocol - Traffic Engineering

RR	Route Reflector
RT	Route Target
TC	Traffic Class
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TDP	Tag Distribution Protocol
TE	Traffic Engineering
TTL	Time to Live
UDP	User Datagram Protocol
VCI	Virtual Circuit Identifier
VFI	Virtual Forwarding Instance
VIRL	Virtual Internet Routing Lab
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VPI	Virtual Path Identifier
VPLS	Virtual Private LAN Service
VPRN	Virtual Private Routed Network
VPWS	Virtual Private Wire Service
VRF	Virtual Routing and Forwarding

SEZNAM PŘÍLOH

A Příprava prostředí pro úlohu **56**
A.1 VMware Workstation 56
A.2 GNS3 56

B Laboratorní úloha - Implementace služby Virtual Private LAN Service **60**
B.1 Teoretický úvod 60
B.1.1 MPLS 60
B.1.2 BGP 62
B.1.3 VPLS 62
B.1.4 Topologie 63
B.1.5 Postup řešení 63

C Laboratorní úloha - Přílohy **71**
C.1 Topologie - popis rozhraní 71
C.2 Úloha - řešení potíží 71

D Obsah přiloženého DVD **73**

A PŘÍPRAVA PROSTŘEDÍ PRO ÚLOHU

Tato kapitola popisuje instalaci a nastavení celého prostředí pro vytvoření laboratorní úlohy. Úloha byla vytvořena v prostředí MS Windows 7 (64 bit). K jejímu běhu je třeba mít na počítači 16 GB paměti RAM (systém potřebuje zhruba 2 GB, úloha 13 GB a 1 GB je rezerva). Nejnáročnější na paměť jsou směrovače CSR1000V, kdy každý z nich vyžaduje pro spuštění oficiálně nejméně 3 GB operační paměti. Dá se systém spustit i s 2,7 GB ale vzhledem k tomu, že se pak může chovat různě nedoporučuji to.

A.1 VMware Workstation

Po spuštění instalačního souboru VMware-workstation-full-12.5.4-5192485.exe není potřeba žádné speciální volby. Stačí instalátorem projít a využít pouze voleb Next a na konci Finish. Po nainstalování programu Workstation bude třeba naimportovat do něj virtuální stroj (serverová aplikace) GNS3 VM:

1. Otevřít aplikaci VMware Workstation
2. File - Open: Vybrat z adresáře GNS3.VM.VMware.Workstation.1.5.3 soubor GNS3 VM.ova.
   Při importu je důležité dodržet název virtuálního stroje GNS3 VM tak jak je uvedený při importu. V opačném případě se nespojí s prostředím GNS3, které bude nainstalováno dále. Po naimportování je třeba ve vlastnostech virtuálního stroje změnit velikost paměti na 13000 MB. Po změně paměti je možné VMware zavřít.

A.2 GNS3

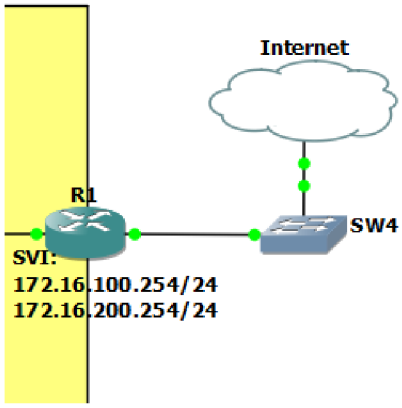
Po spuštění instalačního souboru GNS3-1.5.3-all-in-one.exe není opět nutné žádných speciálních voleb. Jediné, co odznačuji při výběru komponent k instalaci jsou: SolarWinds, VPCS, TightVNC. Nebudou totiž využity. Instalátor vyžaduje připojení k Internetu, protože některé komponenty stahuje.
Po nainstalování spusťte GNS3 simulátor. Ihned po startu se zobrazí Setup Wizard pro výběr serverové části. Ponechejte volbu Local GNS3 VM, dále zvolte virtualizační software VMware. Pokud jste v kroku importování GNS3 VM nezměnili jméno, předvyplní se jméno tohoto virtuálního stroje v okně VM name. RAM size upravte na 13000 MB. Dále jen potvrďte.
Jelikož se při startu programu GNS3 spouští paralelně i VMware Workstation/GNS3

VM, je dobré spouštět Workstation skrytě. Toto lze nastavit v GNS3 - Edit/Preferences/Server GNS3 VM záložka, zaškrtnout volbu Start VM in headless mode.

Vložení síťových systémů do GNS3

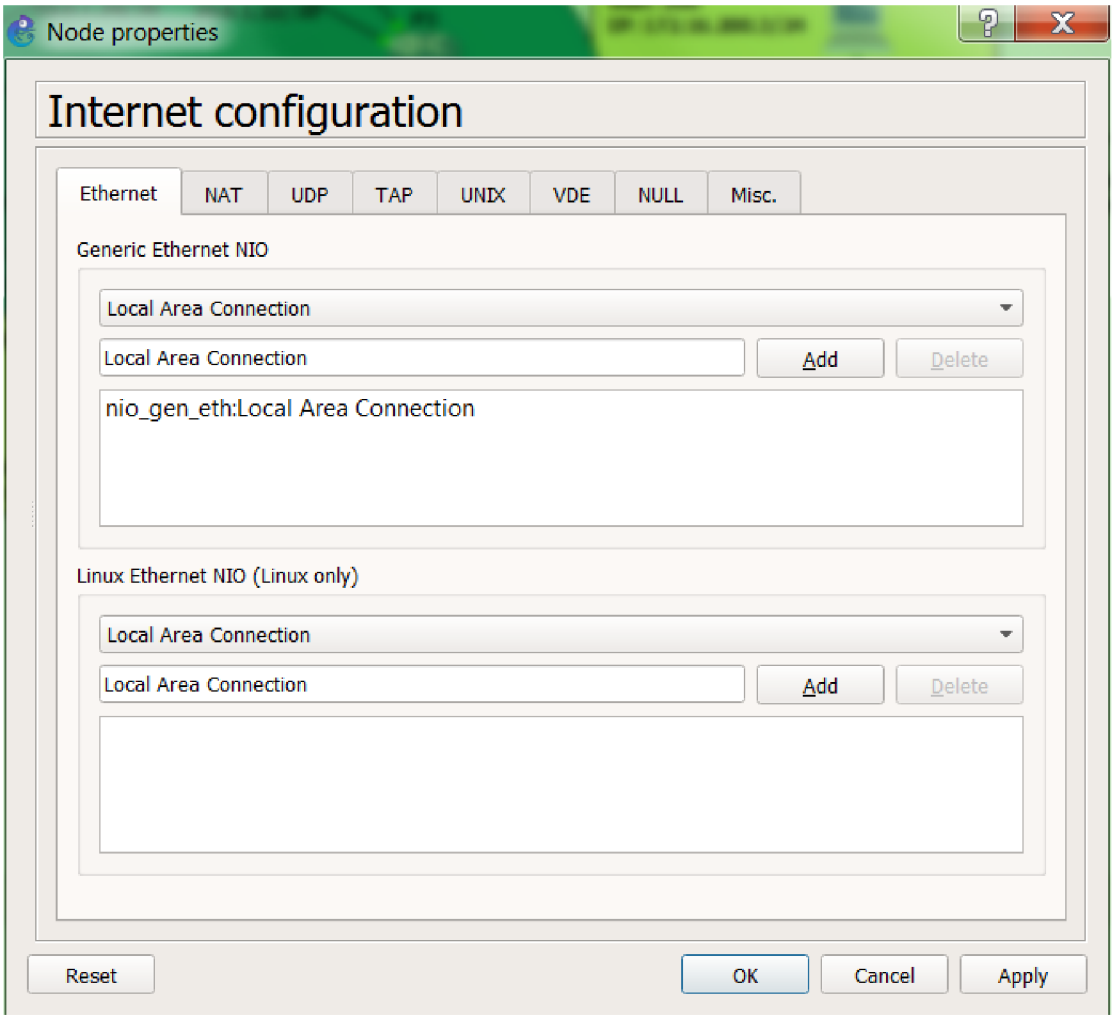
1. Vložení systému pro páteřní směrovače:
   - V simulátoru zvolte File/Import appliance, zvolte soubor cisco-csr1000v.gns3a, dále ponechte volbu Run the appliance on the GNS3 VM, dále vyberte verzi 16.4.1 a stiskněte import, vyberte soubor csr1000v-universalk9.16.04.01-serial.qcow2.
   - Importování tohoto typu systému je třeba provést 3x za sebou, tedy opakovat první bod ještě 2x. Při opakovaném vložení budete upozorněni, že jméno systému již existuje a vyzve vás ke změně. Po druhé jsem přidal za název -2 a po třetí -3. K využívání více kusů daného směrovače by měl stačit import pouze jednoho zařízení a dále ji jen množit. Nicméně tento způsob se jevil jako nestabilní a z tohoto důvodu se vkládá stejný systém 3x.
2. Vložení systému pro přepínače:
   V GNS3 zvolte Edit/Preferences/IOU Devices a dále zvolte New pro vytvoření nového zařízení. Zde zvolte název např prepinac, Image/New Image, Type L2, dále browse a zvolte i86bi-linux-l2-adventerprisek9-15.1a.bin. Tímto byl vložen systém pro emulaci přepínače.
3. Vložení systému Cisco 7206VXR pro páteřní směrovače a PC:
   Opět volba z prostředí GNS3 Edit/Preferences/Dynamips/IOS Routers dále New pro přidání nového zařízení, New Image/Browse a zvolit c7200-adventerprisek9-mz.152-4.S2.image. Do slotu 0 vložit modul C7200-IO-2FE a do slotu 1 vložit modul PA-2FE-TX.

Po vytvoření všech potřebných zařízení se z levé části simulátoru dají vkládat jednotlivá zařízení. Dále jsem vložil všechna potřebná zařízení a propojil je pomocí nástroje Add a link, který se taktéž nachází na levé straně. Po propojení všech zařízení je možné přistoupit ke konfiguraci jednotlivých prvků. Nejdříve je třeba všechny zařízení zapnout (zelená ikona "přehrát"z horní lišty). Po naběhnutí zařízení je možné pokračovat s jejich konfigurací. Vypracovaná topologie se nachází v adresáři vpls/untitled.gns3. Poslední poznámku v tématu přípravy topologie bych chtěl věnovat připojení R1 do Internetu. Na Obr. A.1 lze vidět, že připojení není přímé. Přímé připojení R1 do mraku Internet není možné (gns3 to neumožní), z toho důvodu je mezi tyto dva prvky vložen přepínač bez jakékoliv konfigurace. Aby to lépe vypadalo, SW4 byl překryt mrakem Internet (kliknout pravým tlačítkem myši na ikonku Internet: Raise one layer, a na SW4 lowe one layer). Následující Obr. A.2 ukazuje



Obr. A.1: Připojení R1 do Internetu.

volbu fyzické síťové karty v počítači. Tuto volbu lze vyvolat kliknutím pravého tlačítka myši na mrak a dále v poli Generic Ethernet NIO zvolením názvu síťové karty (Add, Ok).



Obr. A.2: Volba síťové karty.

B LABORATORNÍ ÚLOHA - IMPLEMENTACE SLUŽBY VIRTUAL PRIVATE LAN SERVICE

Cíl

Cílem úlohy je seznámit se s funkcí technologie MPLS a konkrétně s jednou s jejich služeb - VPLS a jejich konfigurací. Úloha si dále klade za cíl pochopení spolupráce a význam jednotlivých protokolů používaných v páteřní síti. Náplní úlohy bude konfigurace hraničního směrovače. Pro úlohu je využito prostředí simulátoru sítí GNS3 a jejím úkolem bude konfigurace hraničního směrovače PE1.

Úkoly

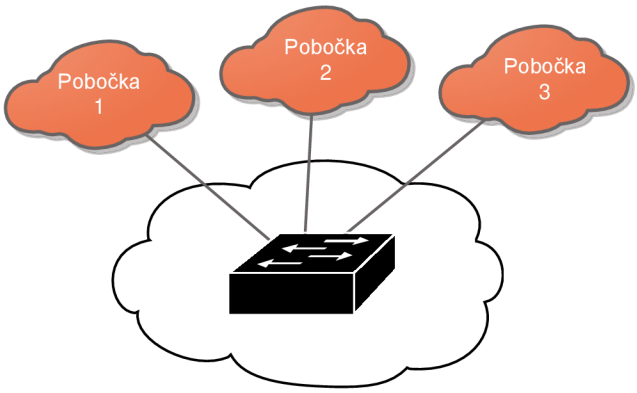
1. Ověření plné dostupnosti dostupnosti v rámci páteřní sítě (ověření funkce OSPF)
2. Nastavení MPLS, ověření funkce
3. Nastavení BGP, ověření funkce
4. Nastavení služby VPLS, ověření funkce

B.1 Teoretický úvod

Technologie VPLS (Virtual Private LAN Service) poskytuje způsob, jakým mohou poskytovatelé služeb doručit zákazníkovi vícebodovou LAN komunikaci založenou na Ethernetu přes MPLS síť. Technologie umožňuje spojení geograficky vzdálených poboček do jedné všesměrové domény (angl. broadcast domain), čímž vzniká virtuální privátní síť VPN. Z pohledu zákazníka se pak síť poskytovatele chová jako jeden velký přepínač viz Obr. B.1.

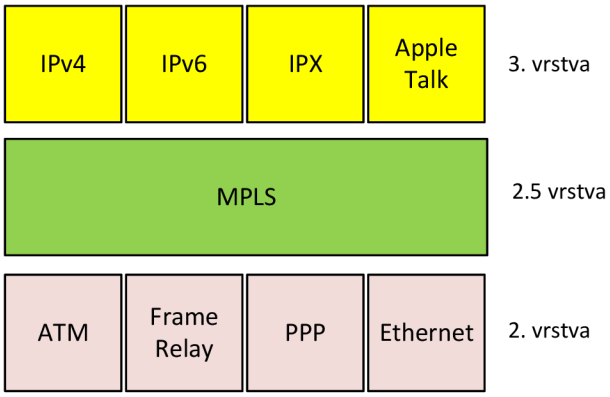
B.1.1 MPLS

Technologie multiprotokolového přepojování podle návěští MPLS (Multi Protocol Label Switching) byla standardizována v roce 2001 (RFC 3031) a postupem času si vydobyla svoje jedinečné postavení v páteřních sítích poskytovatelů připojení. Principem této technologie je předřazení krátkého návěští (angl. label) před každý paket procházející páteřní sítí, na jehož základě se dále rozhoduje o přepojení dané datové jednotky. Návěští má neměnnou délku a má pouze lokální význam (lokální význam mezi dvěma přilehlými směrovači). Při srovnání s konvenčními směrovými protokoly, které pracují na třetí vrstvě ISO/OSI modelu, je MPLS zařazené na pomezí druhé a třetí vrstvy. Toto zařazení je zobrazeno na Obr. B.2. Koncept MPLS striktně dělí řídicí a datovou rovinu. Řídicí rovina (control plane) je realizována pomocí směrových protokolů a mechanizmů, které vytvářejí a distribuují návěští mezi směrovači.



Obr. B.1: Emulace LAN.

Datová rovina (data plane) je zodpovědná za samotné přepojování datových jednotek. Z Obr. 1.1 je zřejmé, že technologie MPLS není závislá na přenosové technologii



Obr. B.2: Umístění MPLS v ISO/OSI modelu.

spojové vrstvy a zároveň může sama přenášet jakýkoliv protokol vrstvy síťové (IPv4, IPv6, aj.).

K distribuci návěští mezi jednotlivými uzly lze použít protokol LDP (Label Distribution Protocol) nebo např. RSVP-TE (Resource Reservation Protocol - Traffic Engineering). Protokol RSVP je navíc schopen řízení datového provozu TE (Traffic Engineering). V této úloze bude využit protokol LDP, protože zde není technika řízení provozu využita.

B.1.2 BGP

Směrový protokol BGP (Border Gateway Protocol) může být využit jak pro směrování mezi autonomními systémy AS (Autonomous System) tak i pro přenos informací uvnitř AS. V této úloze je BGP využito k automatickému objevování dalších hraničních směrovačů PE, které jsou připojeny do stejné VPN. Jedná se konkrétně o více-protokolové rozšíření BGP-MP (Multi-Protocol) umožňující distribuci VPN ID a dalších specifických informací k dané VPN. Automatické objevování hraničních směrovačů a jejich připojených VPN velmi ulehčuje jejich správu. Při instalaci nového zákazníka jsou pak změny distribuovány dynamicky. Stejně tak tomu je i při odpojení zákazníka (VPN) z daného hraničního směrovače. Další z nástrojů k usnadnění konfigurace a škálovatelnosti páteřní sítě je tzv. reflektor cest RR (Route Reflector). Jelikož pro protokol BGP platí pravidlo, že pokud se jedná o komunikaci v rámci jednoho autonomního systému (náš případ), musí mezi sebou všechny směrovače navázat sousedství. Toto je možné dodržovat v sítích, kde je malé množství směrovačů, nicméně s postupným rozšiřováním sítě se to stává nemožným (na každém ze směrovačů by bylo třeba ručně nastavit relaci na nový směrovač). Řešením je tedy využít zmíněný reflektor cest. V tomto konceptu musí každý hraniční směrovač navázat relaci pouze s RR, který bude rozesílat přijaté směrovací informace ostatním směrovačům. Z důvodu redundance jsou zde vyžity reflektory dva (RR1, RR2).

B.1.3 VPLS

VPLS je jednou z klíčových aplikací založených na MPLS. Jak již název napovídá, účelem VPLS je poskytnout privátní vícebodovou službu typu Ethernet. Dá se tedy říct že, VPLS je emulace lokální sítě LAN nad MPLS.

VPLS má svoje místo v prostředí poskytovatelů připojení jako způsob, jak doručit mnohabodovou transparentní službu na úrovni spojové vrstvy přes Ethernet infrastrukturu pomocí MPLS. Čím je VPLS tak zvláštní? Klíč je v MPLS. Jsou známy různé přístupy, kterými mohou poskytovatelé připojení doručit služby přes infrastrukturu založenou na Ethernetu, ale ne všechny vyhovují jejich požadavkům v ohledech rozšiřitelnosti, spolehlivosti a pružnosti.

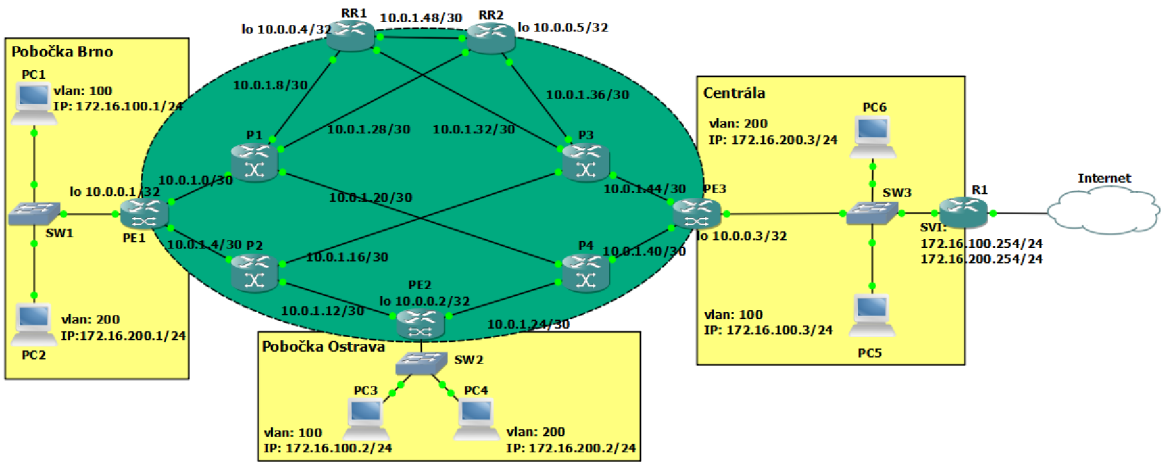
Architektura VPLS

Klasický VPLS model vyžaduje v páteřní sítí plné propojení (full mesh) LSP (pseudowires) mezi všemi PE směrovači, které jsou využity v dané VPLS instanci (v rámci sítě jednoho zákazníka). Pro n VPLS instanci musí být sestaveno n*(n-1)/2 PW mezi PE směrovači, což s sebou přináší velkou režii. V neprospěch velkých sítí se přičítá

fakt, že je třeba provádět zmnožení paketů na PE pro každý PW (mnohabodová komunikace). Z toho důvodu byl zaveden hierarchický model označovaný jako H-VPLS, který má za úkol snížení replikační a signalizační režii a umožnit tak nasazení technologie ve velkém měřítku. Na Obr. B.1 je ilustrace sítě VPLS z pohledu zákazníka. Jedná se tedy o transparentní službu a z pohledu zákazníka se MPLS síť tváří jako přepínač. Jako možnou výhodu lze také zmínit, že v roli CE, v architektuře VPLS nemusí vystupovat pouze směrovač, ale může být použit také přepínač.

B.1.4 Topologie

Topologie laboratorní úlohy se skládá z páteřní sítě (vyznačeno zeleně) a tří připojených poboček k páteřní síti (žlutě). Na páteřních směrovačích PE je implementována veškerá logika, která zastřešuje funkci technologie VPLS. Páteřní směrovače P se starají pouze o přepojování paketů označených návěštím. Z důvodu lepší škálovatelnosti sítě jsou využity reflektory cest (RR1, RR2). BGP sousedství se pak nenavazuje na přímo mezi hraničními směrovači, ale vždy pouze mezi daným hraničním směrovačem a reflektorem cest. Úloha reflektoru je přijímat směrové informace a dále je distribuovat k ostatním hraničním směrovačům. Každá z poboček pak obsahuje přepínač (SW1-SW3), ke kterému jsou připojeny dva počítače, každý v jiné virtuální síti VLAN. Spoje mezi přepínačem SW, a hraničním směrovačem jsou z pohledu směrovače nastaveny jako tzv. trunk rozhraní jejichž úlohou je přenášet více VLAN.



Obr. B.3: Topologie laboratorní sítě.

B.1.5 Postup řešení

Spusťte z plochy počítače odkaz simulátoru GNS3. Ihned po spuštění simulačního prostředí se objeví okno, kde bude napsáno: Starting the GNS3 VM. Provádí se spuš-

tění serverové části simulačního programu, vyčkejte cca 20 sekund až okno zmizí. Poté budete vyzvání k otevření projektu, zvolte z plochy adresář vpls/untitled.gns3. Po načtení topologie stiskněte zelené tlačítko "play", které spustí všechna zařízení. Většina zařízení je připravena prakticky okamžitě. Jedinou výjimkou jsou PE směrovače, jejichž načtení může trvat 5-10 minut. Doporučuji otevřít konzoli na směrovači PE1 (kliknout pravým tlačítkem na daný objekt, zvolit console). Otevře se konzole, nyní je třeba vyčkat, dokud systém nebude připraven (systém se bude jevit jako zamrzlý, nic nemusí být vidět chvíli). Moment, kdy je systém připraven k práci lze rozpoznat dle výpisů do konzole viz Obr B.4. Jakmile uvidíte výpisy do konzole obsahující časové značky stejně jako na obrázku, znamená to, že směrovač je připraven pro další konfiguraci.

```
*Apr  7 13:01:10.829: %VUDI-6-EVENT: [serial numb
*Apr  7 13:01:10.902: %SMART_LIC-6-AGENT_READY: S
*Apr  7 13:01:11.044: %IOS_LICENSE_IMAGE_APPLICAT
*Apr  7 13:01:19.315: %VXE_THROUGHPUT-6-LEVEL: Th
*Apr  7 13:01:19.316: %VXE_THROUGHPUT-2-LOW_THRO
```

Obr. B.4: Směrovač připraven.

Ověření plné dostupnosti dostupnosti v rámci páteřní sítě

Směrovač PE1 obsahuje pouze základní nastavení IP adres a směrového protokolu OSPF. Než budete pokračovat, je dobré se ujistit, že se všechna zařízení načetla správně a že není problém s komunikací. Toto ověření lze provést pomocí programu ping ze směrovače PE1 na ostatní dva hraniční směrovače PE2 (IP: 10.0.0.2) a PE3 (IP: 10.0.0.3). K dalšímu postupu je nutné, aby odpovídaly. Pokud nedostanete odpověď z některého z nich, podívejte se do přílohy na řešení problémů.

```
PE1#ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/18/20 ms
PE1#ping 10.0.0.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/39/75 ms
```

Obr. B.5: Kontrola funkčnosti směrování.

Konfigurace MPLS

MPLS se je třeba nastavit na rozhraních Gi3 a Gi4 (popis rozhraní je uveden na Obr C.1 umístěný v příloze), které jsou připojeny k ostatním směrovačům páteřní sítě. Základní konfigurace se provede příkazem **mpls ip** pod každým ze jmenovaných rozhraní výše. Tímto se zároveň aktivuje i protokol pro tvorbu a distribuci

Výpis B.1: Konfigurace MPLS na PE1.

```
%vstup do globalniho rezimu
PE3>enable
%prepnuti se do konfiguracniho rezimu
PE3#configure terminal
%konfiguracni rezim
PE3(config)#
%vstup do konfigurace rozhrani pripojeneho k P1
PE1(config)#interface GigabitEthernet 3
%zapnuti mpls
PE1(config-if)#mpls ip
```

návěští LDP. Kontrolu konfigurace lze provést pomocí příkazů **show mpls interfaces** a **show mpls ldp neighbors**. Na Obr B.6 lze vidět, jak by měl vypadat výsledek, tedy obě rozhraní jsou součástí MPLS domény. Dále lze zobrazit sousední

```
PE1#show mpls interfaces
Interface              IP            Tunnel   BGP Static Operational
GigabitEthernet3       Yes (ldp)     No       No  No     Yes
GigabitEthernet4       Yes (ldp)     No       No  No     Yes
```

Obr. B.6: Rozhraní nakonfigurovaná pro MPLS.

směrovače, se kterými je navázána LDP relace. Z pohledu směrovače PE1 by se relace měla navázat s oběma páteřními směrovači P1, P2 viz Obr B.7. Na Obr B.7 lze vidět IP adresu sousedního směrovače (Peer LDP Ident) a také například jak dlouho je relace mezi nimi navázána (Up time).

Konfigurace BGP

Nyní je třeba sestavit BGP sousedství mezi hraničním směrovačem PE1 a dvěma reflektory cest RR1, RR2. Směrovače RR jsou již přednastaveny. Zbývá tedy dokončit konfigurace na hraničním směrovači PE1. Postup s komentáři je zobrazen ve Výpise B.2.

Výpis B.2: Konfigurace BGP na hraničním směrovači.

```
%vstup do konfiguračního režimu
PE1#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.

%spuštění protokolu bgp, číslo AS je 100
PE1(config)#router bgp 100

%nastavení IP adres route reflektorů spolu s jejich AS
PE1(config-router)#neighbor 10.0.0.4 remote-as 100

%explicitní volba zdrojového rozhraní - loopback 0
PE1(config-router)#neighbor 10.0.0.4 update-source Lo 0

PE1(config-router)#neighbor 10.0.0.5 remote-as 100
PE1(config-router)#neighbor 10.0.0.5 update-source Lo 0
%vstup do konfigurace adresní rodiny pro vpls
PE1(config-router)#address-family l2vpn vpls

%aktivování komunikace se na zvolené směrovače RR
PE1(config-router-af)#neighbor 10.0.0.4 activate

%instrukce pro bgp odesílat jak standardní tak
%rozšířené komunity
PE1(config-router-af)#neighbor 10.0.0.4 send-comunity both

PE1(config-router-af)#neighbor 10.0.0.5 activate
PE1(config-router-af)#neighbor 10.0.0.5 send-comunity both
```

```
PE1#show mpls ldp neighbor
    Peer LDP Ident: 10.0.1.29:0; Local LDP Ident 10.0.0.1:0
        TCP connection: 10.0.1.29.61959 - 10.0.0.1.646
        State: Oper; Msgs sent/rcvd: 191/182; Downstream
        Up time: 01:11:46
        LDP discovery sources:
          GigabitEthernet3, Src IP addr: 10.0.1.2
        Addresses bound to peer LDP Ident:
          10.0.1.2        10.0.1.9        10.0.1.29       10.0.1.21
    Peer LDP Ident: 10.0.1.17:0; Local LDP Ident 10.0.0.1:0
        TCP connection: 10.0.1.17.43993 - 10.0.0.1.646
        State: Oper; Msgs sent/rcvd: 188/179; Downstream
        Up time: 01:08:34
        LDP discovery sources:
          GigabitEthernet4, Src IP addr: 10.0.1.6
        Addresses bound to peer LDP Ident:
          10.0.1.6        10.0.1.17       10.0.1.13
    Peer LDP Ident: 10.0.0.2:0; Local LDP Ident 10.0.0.1:0
        TCP connection: 10.0.0.2.20741 - 10.0.0.1.646
        State: Oper; Msgs sent/rcvd: 60/60; Downstream
        Up time: 00:31:14
        LDP discovery sources:
          Targeted Hello 10.0.0.1 -> 10.0.0.2, active, passive
 --More--
```

Obr. B.7: Detaily LDP relací.

Kontrolu, zda se BGP relace navázala lze provést pomocí příkazu **show ip bgp summary**, jehož výsledek by měl být mimo časové údaje shodný s Obr B.8. Ve výpise lze spatřit IP adresy RR, se kterými jste již nakonfigurovali relaci, číslo AS (shodně 100 pro všechny) a dále čas po jaký je relace ustavena. Pokud vidíte text namísto časového údaje, znamená to chybu v konfiguraci a je třeba ji překontrolovat dle Výpisu B.2.

```
PE1#show ip bgp summary
BGP router identifier 10.0.0.1, local AS number 100
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.4        4          100      50      55        1    0    0 00:46:32        0
10.0.0.5        4          100      42      47        1    0    0 00:37:26        0
```

Obr. B.8: Kontrola BGP relace.

Konfigurace VPLS na směrovači PE1

Konfigurace VPLS se skládá prakticky ze tří bodů, jedná se o vytvoření:

- Virtuální instance VFI (Virtual Forwarding Instance).
- Virtuální domény (angl. bridge domain).
- Servisní instance (angl. service instance).

Výpis B.3: Konfigurace VPLS na PE1.

```
PE1#configure terminal
%vytvoreni instance VFI, definice vpn id, autodiscovery,
%signaling, vpls-id
PE1(config)#l2vpn vfi context VFI
PE1(config-vfi)#vpn id 100
PE1(config-vfi)#autodiscovery bgp signaling ldp
PE1(config-vfi-autodiscovery)#vpls-id 100
%návrat do globálního konf. režimu
PE1(config-vfi-autodiscovery)#exit
PE1(config-vfi)#exit
PE1(config)#
%vytvoreni virtualni domeny (virtualniho prepinace)
PE1(config)#bridge-domain 300
%pripojeni jednotlivych rozhrani do domeny
PE1(config-bdomain)#member GigabitEthernet 1
service-instance 100
PE1(config-bdomain)#member vfi VFI
%konfigurace zakaznickeho rozhrani
PE1(config)#interface gigabitEthernet 1
%pomoci servisní instance se vytvori pravidlo,
%ktere definuje typ provozu ktery do ni muze vstoupit
PE1(config-if)#service instance 100 ethernet
PE1(config-if-srv)#encapsulation dot1q any
%nakonec nesmime opomenout opet aktivovat rozhrani
PE1(config-if)#no shutdown
```

Prvním krokem je vytvoření vfi kontextu, ve kterém se specifikují detaily identifikující danou vpls síť a také protokol pro automatické objevování stejných vpn sítí na jiných směrovačích, signalizační protokol LDP. Nově vytvořený kontext je třeba připojit do tzv. bridge domain (virtuální přepínač) spolu s rozhraním, kde je připojena síť zákazníka (GigabitEthernet 1). Posledním krokem je vytvoření servisní

instance, ve které lze specifikovat jaké virtuální sítě LAN budou přenášeny. Servisní instance je zde nakonfigurována tak, aby vyhověla všem příchozím rámcům (VLAN 1-4094) a to klíčovým slovem any. Posledním krokem je ujištění, že rozhraní zákazníka nebylo administrativně vypnuté. Ověření funkčnosti provedeme tentokrát jak na směrovači, tak ze strany síťových zařízení na pobočkách.

```
PE1#show vfi
Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No

VFI name: VFI, state: up, type: multipoint, signaling: LDP
  VPN ID: 100, VPLS-ID: 100:300
  RD: 100:100, RT: 100:100,
  Bridge-Domain 300 attachment circuits:
  Neighbors connected via pseudowires:
  Peer Address     VC ID        Discovered Router ID    S
  10.0.0.3         100          10.0.0.3                Y
  10.0.0.2         100          10.0.0.2                Y
```

Obr. B.9: Kontrola funkce VPLS.

Na Obr B.9 lze vidět výsledek kontroly pomocí příkazu **show vfi**. Zobrazený výstup je výsledkem funkce auto objevování okolních směrovačů účastnících se stejných VPN sítí pomocí BGP. Všimněte si, že jste nikde přesně nespecifikovaly při konfiguraci směrovače PE1, se kterými směrovači má navázat spojení. Stalo se to na základě toho, že jsme specifikovaly VPN a VPLS ID. Jelikož zde využíváme protokol BGP, ten tuto informaci rozdistribuoval mezi ostatní směrovače. Protože ostatní směrovače využívají stejné VPN a VPLS ID, navázaly pak mezi sebou spojení na základně těchto shodujících se parametrů. Finálním testem bude ověření dostupnosti připojení mezi pobočkami. Otevřete si konzoli PC1 a proveďte ping na jiný počítač ze stejné sítě VLAN a dále i z té druhé VLAN. Dále prověřte ARP tabulku na PC1, ze kterého jste ověřovali dostupnost ostatních PC. Uvidíte přímo fyzické adresy daných PC (v rámci stejné VLAN), však nikoliv MAC adresu hraničního směrovače viz Obr B.10. Směrovač R1 poskytuje směrování mezi sítěmi VLAN ale také poskytuje připojení do Internetu takže můžete směřovat odezvu i na veřejné portály (seznam.cz).

Tab. B.1: Detaily PC.

PC	VLAN	IP	MAC
PC1	100	172.16.100.1	0000.1111.1111
PC2	200	172.16.200.1	0000.2222.2222
PC3	100	172.16.100.2	0000.3333.3333
PC4	200	172.16.200.2	0000.4444.4444
PC5	100	172.16.100.3	0000.5555.5555
PC6	200	172.16.200.3	0000.6666.6666

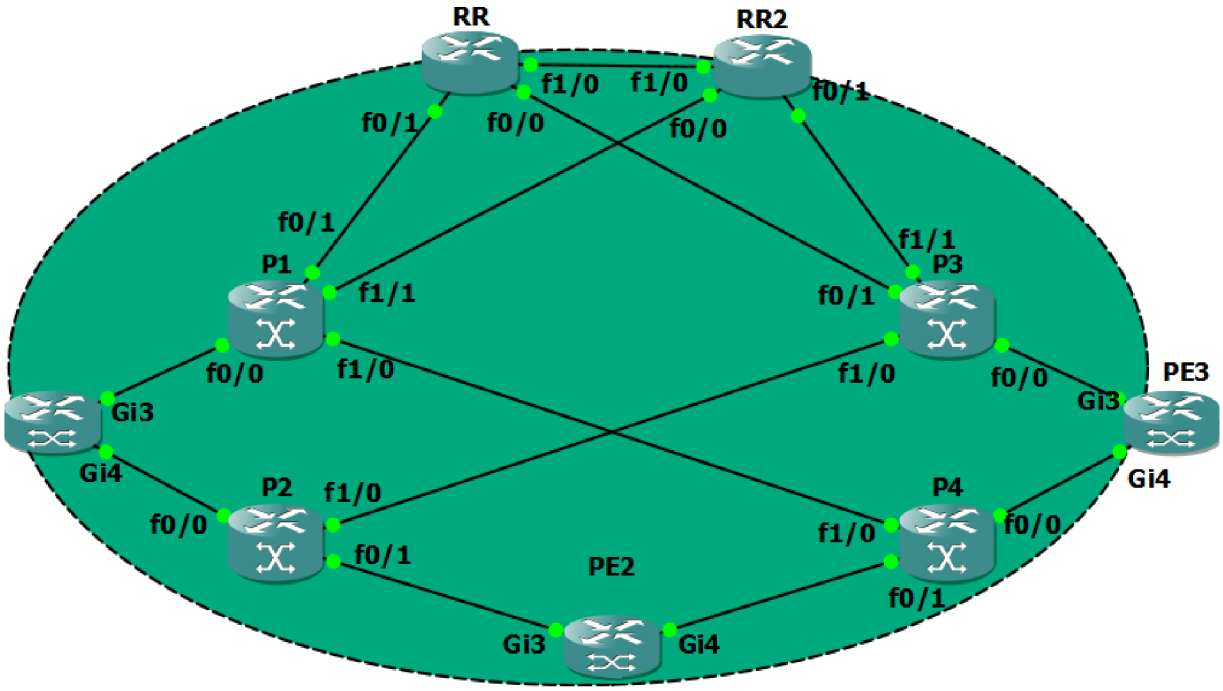
```
PC2#ping 172.16.200.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.200.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/258/1060 ms
PC2#ping 172.16.200.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.200.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 72/79/92 ms
PC2#sh ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.200.1            -   0000.2222.2222  ARPA   FastEthernet0/0
Internet  172.16.200.2            0   0000.4444.4444  ARPA   FastEthernet0/0
Internet  172.16.200.3            0   0000.6666.6666  ARPA   FastEthernet0/0
PC2#ping seznam.cz
Translating "seznam.cz"...domain server (8.8.8.8) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 77.75.77.39, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/75/100 ms
```

Obr. B.10: Ověření dostupnosti poboček.

C LABORATORNÍ ÚLOHA - PŘÍLOHY

C.1 Topologie - popis rozhraní

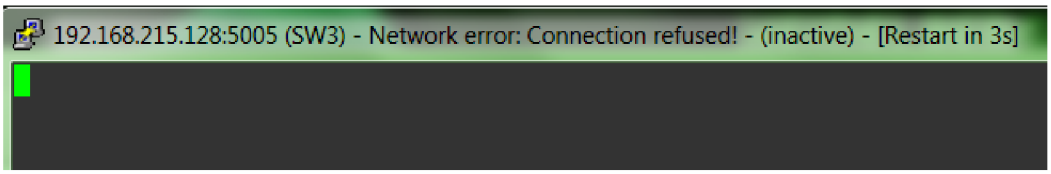


Obr. C.1: Popisky rozhraní směrovačů

C.2 Úloha - řešení potíží

Tato kapitola obsahuje nejčastější problémy, se kterými se lze během vypracování laboratorní úlohy setkat. V případě, že bude třeba vypnout z jakéhokoliv důvodu program GNS3 a opět jej zapnout, bude nutné ve správci úloh ručně ukončit vmware. Ten se totiž po ukončení GNS3 sám nevypne. Je třeba najít proces vmware-vmx.exe a ukončit jej. Jmenované problémy níže se stávají pouze na páteřních směrovačích PE.

1. Putty klient ukazuje v záhlaví hlášku **Connection refused** viz Obr C.2. Jediným řešením je zapnout a vypnout dané zařízení (ne všechny!). Klikněte pravým tlačítkem myši na dané zařízení a zvolte Stop a následně Start. Konzolové okno Putty zavřete a otevřete znovu.
2. Rozhraní (interfaces) na jednom z hraničních směrovačů jsou ve stavu down / down (ne admin down) viz Obr C.3. V tomto případě opět pomůže pouze vypnout



Obr. C.2: Problém s klientem Putty.

a zapnout daný uzel. Klikněte pravým tlačítkem na dané zařízení, zvolte Stop a následně Start.

```
PE3#show interfaces description
Interface                      Status         Protocol Description
Gi1                            down           down     LAN
Gi2                            down           down
Gi3                            down           down
Gi4                            down           down
Lo0                            up             up
pw100001                       up             up
```

Obr. C.3: Problém s rozhraními na PE.

3. Jeden z hraničních směrovačů se načte ve výchozím nastavení, což lze poznat tak, že nemá svoje jméno, ale jmenuje se např. pouze **Router**. Řešení je nahrát do běžící konfigurace (running-config) tu startovací (startup-config) konfiguraci. To se provede příkazem **copy running startup** a enter v globálním režimu. V případě, že nahráváte znovu konfiguraci, bude nutné dodatečně aktivovat rozhraní. To se provede z konfiguračního režimu skupinovým příkazem **interface range Gi 1-4** a dále příkazem **no shutdown**. Tímto způsobem se aktivují všechna čtyři rozhraní naráz (klíčové slovo range).

D OBSAH PŘILOŽENÉHO DVD

Na přiloženém DVD se nachází pět adresářů. Jejich obsah je uveden níže vždy s komentářem, co který z nich obsahuje.

- `/` ..... kořenový adresář přiloženého DVD
  - `konfigurace` ..... Konfigurace všech zařízení
    - `P1-startup-config.cfg`
    - `P2-startup-config.cfg`
    - `P3-startup-config.cfg`
    - `P4-startup-config.cfg`
    - `PC1-startup-config.cfg`
    - `PC2-startup-config.cfg`
    - `PC3-startup-config.cfg`
    - `PC4-startup-config.cfg`
    - `PC5-startup-config.cfg`
    - `PC6-startup-config.cfg`
    - `PE1-startup-config.cfg`
    - `PE2-startup-config.cfg`
    - `PE3-startup-config.cfg`
    - `R1-startup-config.cfg`
    - `RR1-startup-config.cfg`
    - `RR2-startup-config.cfg`
    - `SW1-startup-config.cfg`
    - `SW2-startup-config.cfg`
    - `SW3-startup-config.cfg`
  - `vpls` ..... Vypracovaný projekt do GNS3
    - `project-files`
    - `screenshot.png`
    - `untitled.gns3`
  - `systemy` ..... Adresář obsahující síťové systémy
    - `c7200-adventerprisek9-mz.152-4.S2.image`
    - `cisco-csr1000v.gns3a`
    - `csr1000v-universalk9.16.04.01-serial.qcow2`
    - `i86bi-linux-l2-adventerprisek9-15.1a.bin`
  - `instalacni` ..... Instalační soubory
    - `GNS3-1.5.3-all-in-one.exe`
    - `VMware-workstation-full-12.5.4-5192485.exe`
  - `GNS3.VM.VMware.Workstation.1.5.3` ..... GNS3 Virtual Machine
    - `GNS3 VM.ova`