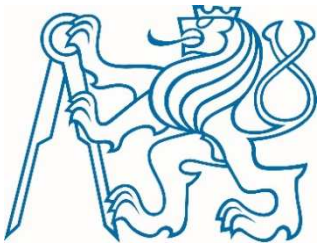


ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra telekomunikační techniky

Simulátory síťového prostředí

Network Environment Simulators

květen 2016

Bakalant: **Daniel Rantoš**

Vedoucí práce: **Ing. Pavel Bezpalec, Ph.D.**

Čestné prohlášení

Prohlašuji, že jsem zadanou bakalářskou práci zpracoval sám s přispěním vedoucího práce a používal jsem pouze literaturu v práci uvedenou. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé bakalářské práce nebo její části se souhlasem katedry.

V Praze dne 27. 5. 2016

……..……

Podpis bakalanta

České vysoké učení technické v Praze
Fakulta elektrotechnická

katedra telekomunikační techniky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: **Daniel Rantoš**

Studijní program: Komunikace, multimédia a elektronika
Obor: Síťové a informační technologie

Název tématu: **Simulátory síťového prostředí**

Pokyny pro vypracování:

Podrobně analyzujte možnosti dostupných simulátorů síťového prostředí. Zaměřte se zejména na možnost propojení simulované sítě s reálnými síťovými prvky. Svá zjištění doprovoďte experimentem. Vytvořte výukové pracoviště s podklady pro laboratorní výuku.

Seznam odborné literatury:

[1] Banks, J. at al.: *Discrete-Event System Simulation, 5th edition*. Prentice Hall 2009. ISBN: 978-0-13606-212-7.
[2] GNS3 2007-2015 [cit. 2015-11-27] Dostupné na http://www.gns3.com [on-line].

Vedoucí: Ing. Pavel Bezpalec, Ph.D.

Platnost zadání: do konce letního semestru 2016/2017

L.S.

prof. Ing. Boris Šimák, CSc.
vedoucí katedry

prof. Ing. Pavel Ripka, CSc.
děkan

V Praze dne 21. 12. 2015

Anotace

Tato bakalářská práce se zabývá analýzou a možnostmi propojení simulátorů síťového prostředí s reálnými síťovými prvky. Jako reálné i virtuální síťové prvky byly použity zařízení od výrobců Cisco a Huawei. Dále bylo vytvořeno testovací pracoviště a čtyři laboratorní úlohy, ve kterých byl kladen důraz právě na využití propojení simulované a reálné sítě. Jednotlivé úlohy, tématicky zaměřené na RIPv2, Inter-VLAN Routing, OSPF a MPLS VPN, jsou rozděleny do několika částí: zadání s topologií, rozbor a postupný návod. Dále je v příloze uvedena celá konfigurace. Laboratorní úlohy byly realizovány v simulátoru sítí GNS3.

Klíčová slova

GNS3, Packet Tracer, eNSP, RIPv2, Inter-VLAN Routing, OSPF, MPLS VPN, Cisco, Směrovač, Přepínač

Summary

This bachelor thesis analyzes the possibilities of interconnection and network environment simulators with real network elements. As the real and virtual elements has been used equipment from company Cisco and Huawei. Further were created test departments and four laboratory excercises in which the emphasis is being placed on using simulated and real interconnection networks. Individual tasks thematically focused on RIPv2, Inter-VLAN Routing, OSPF a MPLS VPN are divided into several parts: entered with topology, analysis and gradual instructions. Entire configuration is mentioned in the attachement. The laboratory experiments were conducted in a simular's network GNS3.

Index Terms:

GNS3, Packet Tracer, eNSP, RIPv2, Inter-VLAN Routing, OSPF, MPLS VPN, Cisco, Router, Switch

Poděkování

Děkuji vedoucímu práce Ing. Pavlu Bezpalcovi, Ph.D. za velmi užitečnou metodickou pomoc a cenné rady při zpracování této bakalářské práce.

Dále bych chtěl poděkovat celé mé rodině včetně přítelkyně za podporu, trpělivost a povzbuzování při psaní této práce.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

V dnešní době je velmi důležité každou změnu v síti podrobně testovat a analyzovat. Nevhodný zásah v podobě např. špatně nastaveného směrovače, může vést k nestabilitě sítě popřípadě i k výpadkům. Simulátory síťového prostředí nám pomáhají těmto problémům předcházet, jelikož většina z nich umožňuje podrobně napodobit (simulovat) a analyzovat reálné situace.

Využijí je tedy IT technici, ale i studenti a učitelé, protože ušetří nemalé prostředky, které by byly zapotřebí na koupi reálných zařízení. Jedni z nejznámějších simulátorů jsou Paket Tracer od společnosti Cisco sloužící pro výukové účely v Cisco Networking Academy nebo GNS3.

Nespornou výhodou některých simulátorů je možnost propojení simulované sítě s reálnou. Otevírají se nám nové možnosti testování. Jsme schopni k již běžící síti připojit síť simulovanou a sledovat chování obou sítí.

Cílem této práce je otestovat možnosti propojení simulované sítě se sítí reálnou v několika simulátorech síťového prostředí, vytvořit testovací pracoviště a s důrazem na toto propojování vytvořit vzorové laboratorní úlohy. Výhodou tohoto řešení je, že student se naučí pracovat jak se simulačním softwarem, tak i s reálným hardwarem. Samotné úlohy jsou rozděleny na zadání včetně topologie, rozboru a postupu řešení. S vedoucím práce bylo dohodnuto, že laboratorní úlohy budou vytvořeny v prostředí simulačního softwaru GNS3.

1 Simulátory síťového prostředí

Pro analýzu propojení simulované a reálné sítě byly zvoleny tři simulátory. Dva z nich pocházení od světoznámých výrobců aktivních síťových prvků - Cisco a Huawei. Jako třetí byl zvolen simulátor GNS3, který je vyvíjen pod licencí GPLv3 [1]. Tomuto nástroji je věnována větší pozornost, jelikož v něm jsou realizovány laboratorní úlohy.

V této kapitole se se všemi třemi simulátory seznámíme a v závěru shrneme jejich vlastnosti.

1.1 GNS3

GNS3 (Graphic Network Simulator) je grafický simulační software datových sítí. Na rozdíl např. od Cisco Paket Traceru je tento software open-source a tedy i zdarma. Slouží jako grafická nadstavba k emulátoru Dynamips, který je také open-source a který nám zajišťuje emulaci síťových prvků, jako jsou např. Cisco směrovače, PIX firewally, Juniper směrovače a další, nicméně neumí emulovat Cisco přepínače. Jediné tedy, co při využívání tohoto nástroje není zdarma, jsou operační systémy (IOS) od firmy Cisco, které jsou potřeba, protože Dynamips emuluje pouze hardware a software tedy IOS musíme dodat jako je v případě emulace operačních systémů. [2]

GNS3 je velice využívaný nástroj pro přípravu k Cisco certifikacím, jako je např. CCNA. Dá se ale využít k testování provozu a chování zařízení (např. při kybernetickém útoku) jelikož jeho velkou předností je možnost propojení simulované sítě se sítí reálnou skrze síťovou kartu počítače. Další velkou předností je, že můžeme virtualizovaný počítač ve VirtualBoxu nebo VMWaru přímo připojit k simulované síti.

Projekt GNS3 má velice rozšířenou komunitu lidí, kteří tvoří podporu, a tak jsou vždy ochotni poradit na oficiálním fóru. Též najdeme mnoho videií s návody na webu YouTube [3]. Podporované operační systémy jsou Microsoft Windows, Linux a Apple Mac OS.

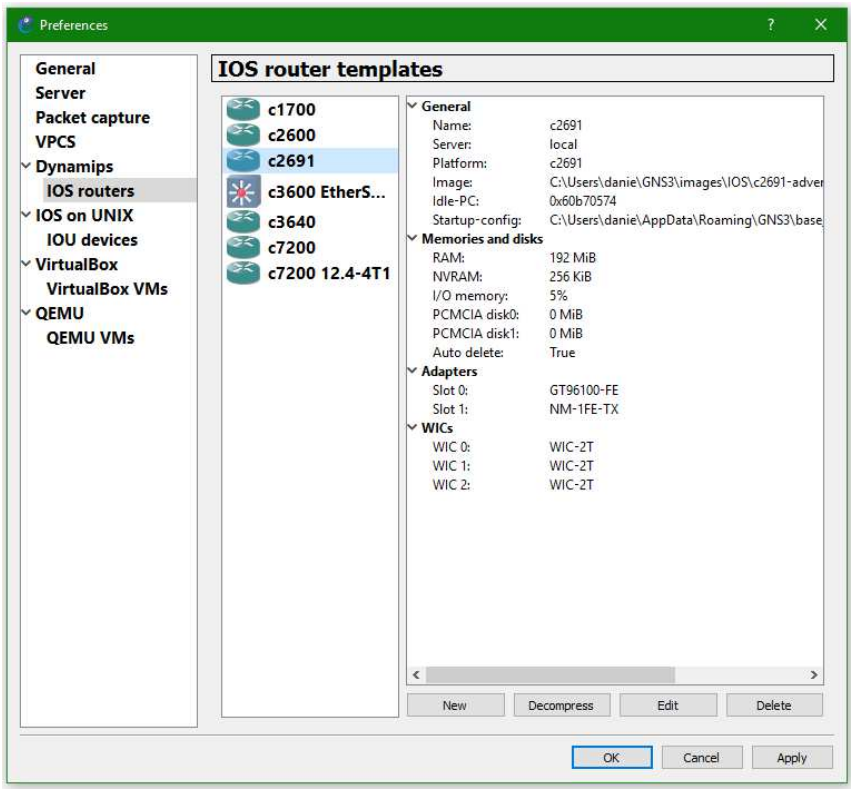
1.1.1 Instalace a základní nastavení

Pro stažení instalačního balíčku musíme navštívit stránku společnosti GNS3 Technologies Inc. [4] a zaregistrovat se. Po provedení registračního procesu nám bude umožněno stáhnout instalátor, který obsahuje vše, co budeme pro simulaci sítě potřebovat. Během instalace si ovšem můžeme vybrat, jestli se má instalovat vše nebo jen něco. Dokumentaci k instalaci, která obsahuje popis instalace na všech podporovaných OS, najdeme též na stránkách společnosti [4], samozřejmě vše v angličtině. [5]

1.1.2 Přidání nového směrovače

Před přidáním nového směrovače do prostředí GNS3 si připravíme image IOS. Existuje mnoho verzí, které jsou určené pro různé typy zařízení. Software podporuje následující řady směrovačů: c1700, c2600, c3600, c3700, c7200. Přidání směrovače provedeme následujícím postupem [6]:

- Spustíme program GNS3
- v horní liště zvolíme „Edit“ a z rozevíracího seznamu „Preferences“ – zobrazí se okno s nastavením
- Zvolíme záložku Dynamips a vybereme IOS routers viz Obr. 1
- V dolní části okna klikneme na New a následně vybere cestu k IOS, který chceme nahrát.
- Program by měl sám rozpoznat zařízení, které náleží k tomuto IOS a doplnit název
- Následuje nastavení velikost RAM a Flash
- Dále můžeme přidat moduly - ať už ethernetové či sériové
- V závěru nastavíme tzv. Idle-PC, toto je velice důležité a sníží to značně vytížení procesoru, lze popřípadě změnit v nastavení zařízení



Obr. 1 Dialog pro přidání nového Cisco směrovače včetně seznamu již přidaných

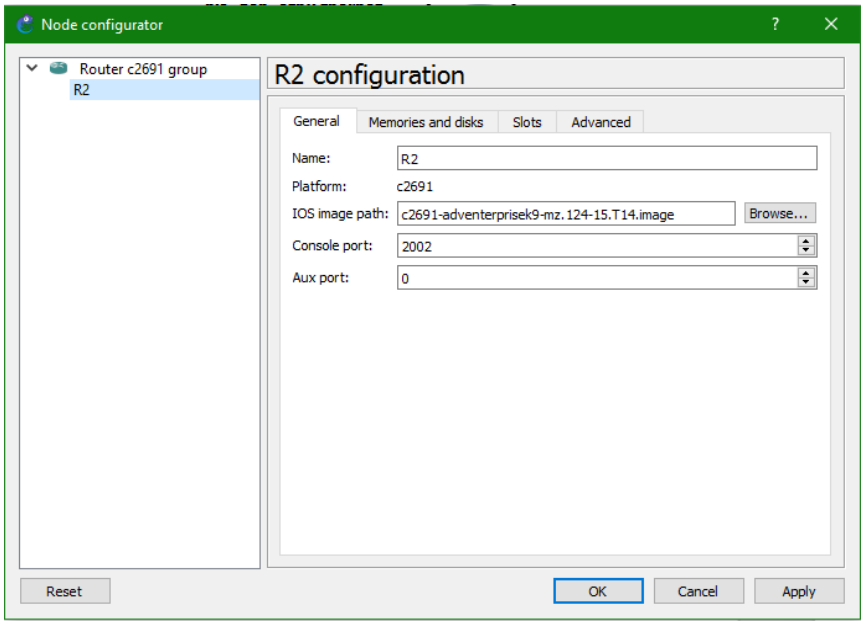
1.1.3 Vytvoření projektu a topologie

Po spuštění GNS3 se nám zobrazí dialog pro vytvoření nového projektu nebo otevření dříve uloženého. Pojmenujeme nový projekt, zvolíme cestu, kam se má uložit a klikneme na „OK“.

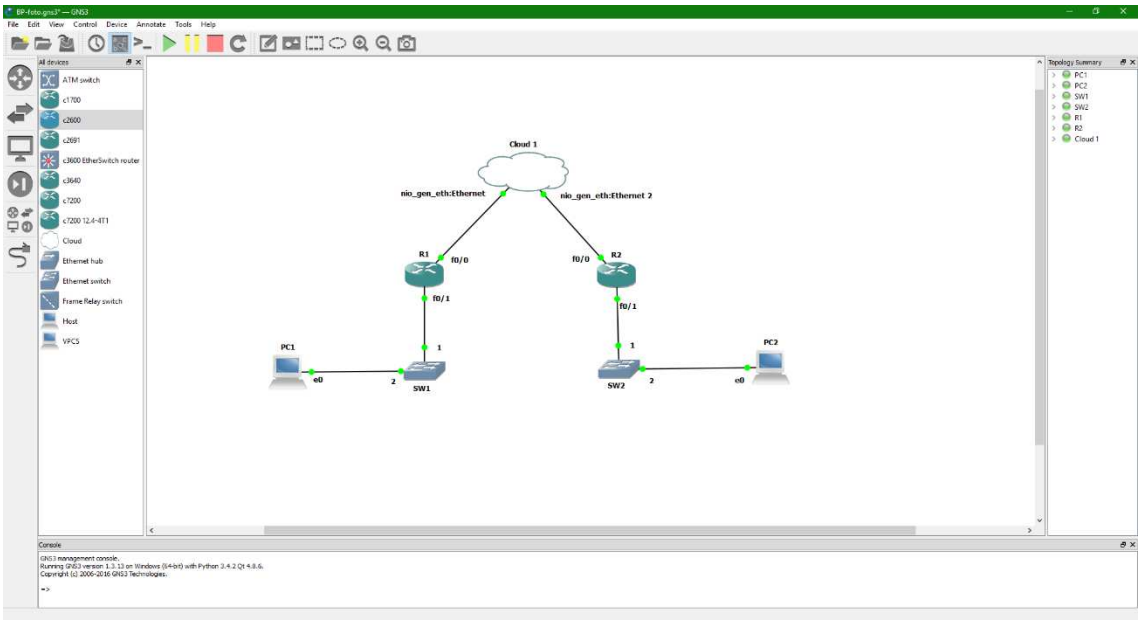
Topologii vytvoříme následujícím postupem:

- Na levé straně hlavního okna programu máme řadu ikon s motivem zařízení, které daná ikona seskupuje – směrovače, přepínače, koncová zařízení – PC, firewally, pak je zde ikonka která nám zobrazí seznam všech zařízení dohromady a ikona s motivem kabelu s koncovkou, kterou využijeme při spojování zařízení – viz Obr. 2
- Zařízení přidáme tak, že ho přetáhneme ze seznamu do vedlejšího okna, kde vytváříme topologii.
- Propojení zařízení s jiným probíhá tak, že klikneme na ikonu propojení (motiv kabel s koncovkou) klikneme na zařízení, zvolíme port a následně klikneme na druhé zařízení a také zvolíme port. Tím se nám zařízení propojí.
- Dále jsou možnosti vytváření popisků a jiné grafické úpravy včetně zobrazení připojených portů.
- Síťové prvky se nastavují standardně pomocí konzole, jako to známe z reálných sítí ovšem některá nastavení jako je např. název, velikost pamětí či rozšiřující karty zařízení lze nastavit i v grafickém režimu – viz Obr. 3
- Zařízení typu Cloud je most mezi simulovanou sítí a reálnou sítí – viz Obr. 5

Obr. 2 Ikony seskupující zařízení stejného typu



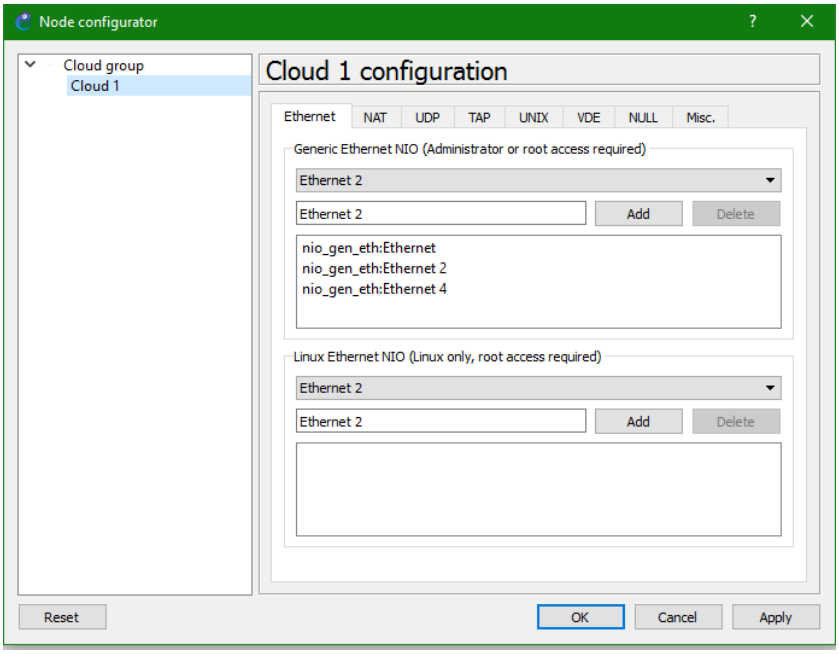
Obr. 3 Konfigurace směrovače z grafického prostředí



Obr. 4 Příklad topologie vytvořenou v GNS3

1.1.4 Nástroj Cloud

GNS3 umožňuje propojit simulovanou síť se sítí reálnou. Tato funkce je docílena pomocí nástroje Cloud, které nám vytváří most mezi reálnou a simulovanou sítí. Na Obr. 5 vidíme nastavení Cloudu, ve kterém vybereme fyzické síťové adaptéry počítače, přes které chceme, aby simulovaná síť komunikovala s reálnou, a naopak a následně připojíme virtuální zařízení ke Cloudu stejným způsobem, jako při vytváření topologie. Toto je veliká výhoda oproti Cisco Packet Traceru, který tuto funkci neumožňuje.



Obr. 5 Konfigurace nástroje Cloud

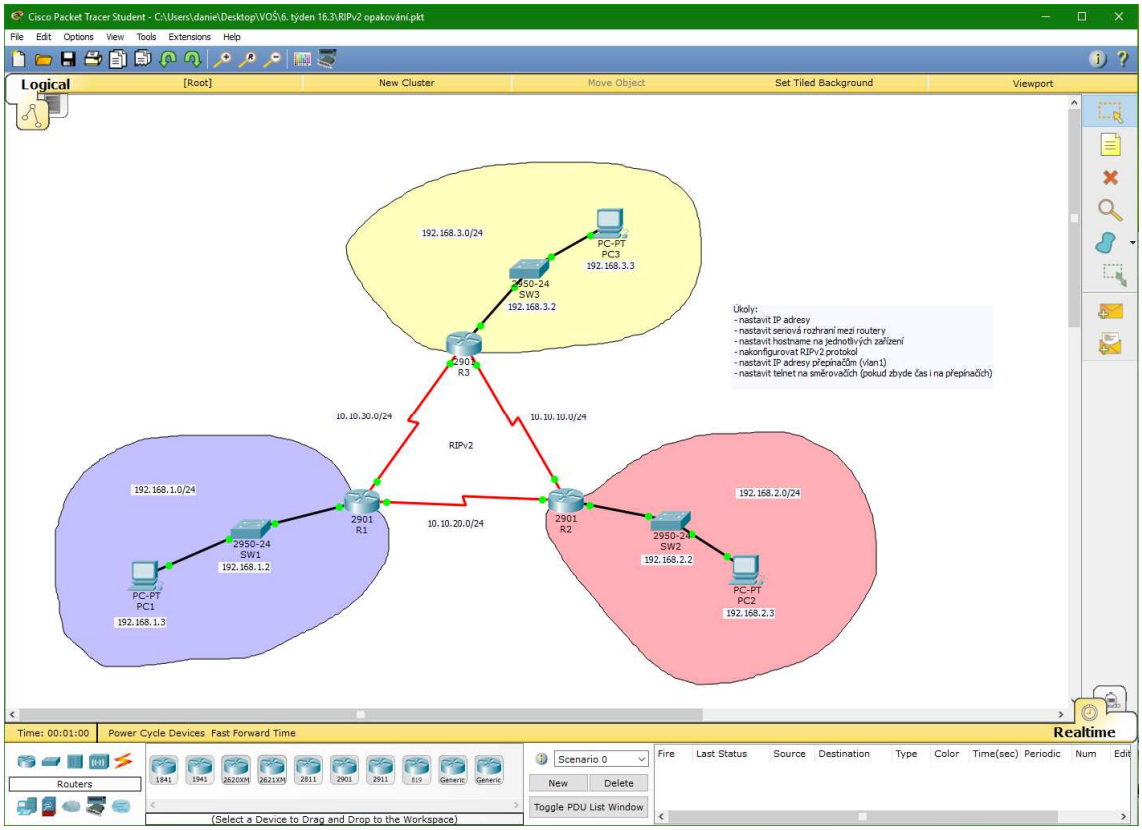
Pro správný a spolehlivý chod této funkce je nutné, aby byl GNS3 spuštěn jako správce, jinak není možné přistupovat k síťovým kartám hostujícího operačního systému přímo v programu. Zvolená síťová karta musí být v promiskuitním režimu a při vlastním provozu se chová transparentně. [7]

1.2 Cisco Packet Tracer

Packet Tracer je nástroj pro simulaci datových sítí od společnosti Cisco Systems, Inc. [8]. Je navržen tak, aby nenáročnou a zároveň profesionální formou umožnil vzdělání v oblasti datových sítí a zvýšil interakci mezi studenty a instruktory.

Umožňuje velice podrobnou simulaci datových sítí s velikou škálou zařízení a nastavení doprovázené intuitivní grafickou reprezentací. Jeho značnou nevýhodou je, že nepodporuje propojení s reálnou sítí. Tento software se hojně využívá ve výukových kurzech CCNA, CCNP apod. vzhledem k tomu, že do veliké míry nahrazuje fyzická zařízení, ovšem ne všechna nastavení, která umožnují fyzická zařízení, jsou Packet Tracerem podporována. Jelikož je tento software velmi populární, už kvůli rozšíření produktů od firmy Cisco Systems, najdeme pro něj mnoho výukových materiálů od návodů až po připravené výukové LABy.

Tento software je zdarma pro instruktory, studenty a absolventy programu Cisco Networking Academy. [9]



Obr. 6 Prostředí simulačního softwaru Packet Tracer

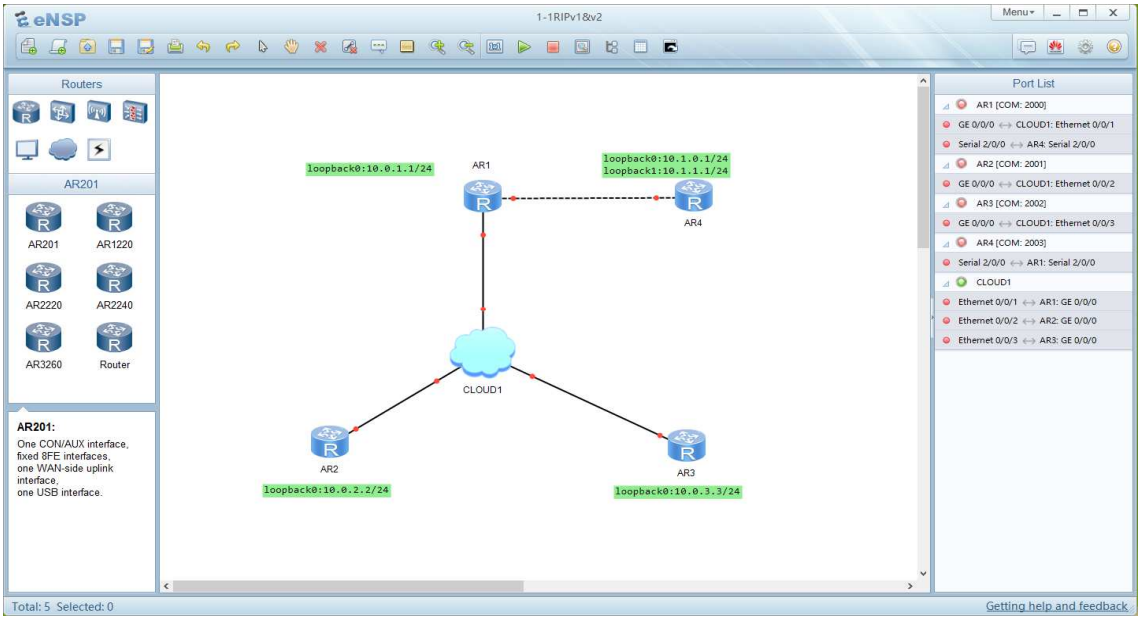
1.3 Huawei eNSP

eNSP (Enterprise Network Simulation Platform) je simulační nástroj od firmy Huawei Technologies Co. Ltd. [10]. Tato firma je největším světovým výrobcem telekomunikačních zařízení. Je tedy pochopitelné, že bylo třeba vytvořit software, ve kterém lze tato zařízení testovat.

Umožňuje simulovat datové sítě pouze se zařízeními Huawei, ovšem pokud je potřeba testovat rozsáhlé sítě ve které jsou i zařízení jiných výrobců, lze propojit eNSP např. s GNS3, které umožňuje emulovat zařízení Cisco a Juniper, pomocí nástroje Cloud. Cloud pracuje obdobně, jako v případě simulátoru GNS3, a proto už tu jeho činnost popisovat nebudeme.

Síťové prvky od firmy Huawei se konfigurují velice obdobně jako zařízení od firmy Cisco, a proto není velký problém pro IT administrátory konfigurovat zařízení od obou výrobců. V Tab. 1 najdeme srovnání některých příkazů.

eNSP je po registraci na webových stránkách společnosti Huawei k dispozici zdarma. [11]



Obr. 7 Prostředí simulačního softwaru eNSP

Příkaz Cisco	**Příkaz Huawei**
configure terminal	system
hostname *hostname*	sysname *sysname*
interface *interface-name*	interface *interface-name*
ip address *ip-address mask*	ip address *ip-address mask*
router rip	rip
no auto-summary	undo summary
ip router	ip route-static
show ip route	display ip routing-table
show running-configuration	display current-configuration
erase	delete
exit	quit

Tab. 1 Porovnání příkazů pro nastavení zařízení od společnosti Cisco a Huawei

1.4 Porovnání

Každý z výše uvedených simulátorů má své klady i zápory, v Tab. 2 najdeme přehledné porovnání funkcí.

Z tabulky vyplývá, že nejvíce kladů má simulátor GNS3. Ovšem pro realizaci simulací v tomto nástroji je třeba, abychom disponovali obrazy operačního systému pro síťové prvky od firmy Cisco popřípadě Juniper, jelikož GNS3 zařízení emuluje a chová se tedy obdobně jako VirtualBox nebo VMWare.

Další problém by se mohl jevit v tom, že ho nevyvíjí přímo výrobce zařízení a mohly by vznikat nedostatky se správným odladěním simulovaných zařízení. Toto je vyřešeno tím, že jako jediný z testované trojice síťové prvky nesimuluje, ale emuluje a tím je zajištěna velmi dobrá napodobenina reálného zařízení.

Cisco Packet Tracer nedisponuje žádnou z testovaných funkcí nicméně vzhledem k tomu, že je určen primárně pro studenty a instruktory programu Cisco Networking Academy, je pro tyto účely dostačující. Na druhou stranu, součástí instalace je nejvíce vzorových topologií.

	GNS3	Cisco Packet Tracer	Huawei eNSP
Propojení s reálnou sítí	Ano	Ne	Ano
Přidání vlastních zařízení	Ano	Ne	Ne
Emulace zařízení	Ano	Ne	Ne
Propojení s VM přímo v simulátoru	Ano	Ne	Ne
Dostupnost	Zdarma*	Zdarma**	Zdarma***
Velikost po instalaci	130 MB	167 MB	1,44 GB
Vyvíjen výrobcem zařízení	Ne	Ano	Ano
Vzorové topologie (obsažené v instalaci)	Ne	Ano	Ano

* Zdarma po registraci, je nutné disponovat operačními systémy pro síťové prvky

** Zdarma pro studenty a instruktory programu Cisco Networking Academy

*** Zdarma po registraci

Tab. 2 Porovnání vlastností síťových simulátorů

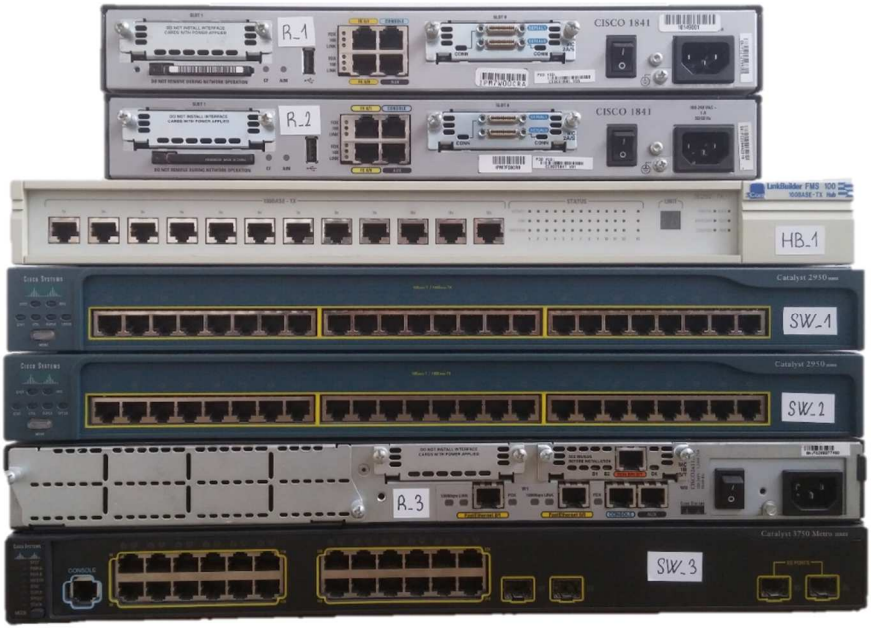
2 Výukové pracoviště

V rámci testování možností spojení simulované a reálné sítě bylo vytvořeno výukové pracoviště skládající se ze zařízení od firmy Cisco a 3Com viz Obr. 8. Konkrétně jde o dva směrovače řady 1841, jeden směrovač řady 2611XM, dva přepínače řady 2950 a jeden přepínač řady 3750. V případě potřeby analýzy komunikace je přítomen i hub od firmy 3Com.

Ve směrovačích Cisco 1841 jsou dostupné přídavné karty typu WIC-2A/S, které slouží k propojení zařízení sériovou linkou.

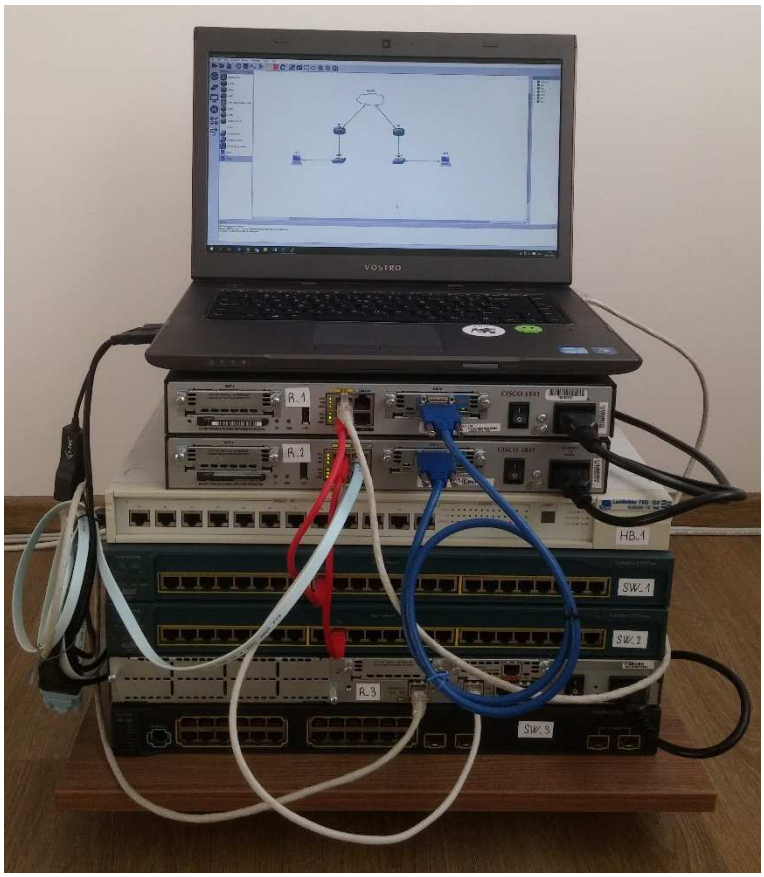
Pro instalaci simulačních programů byl použit notebook DELL Vostro 3560 s jednou integrovanou síťovou kartou a jednou externí síťovou kartou. Operační systém byl zvolen Windows 10. Vzhledem k tomu, že poslední verze GNS3 (1.4.5) doporučuje, aby software běžel ve virtuálním počítači, byla zvolena starší verze (1.3.13), která je bez této funkcionality.

Jednotlivé úlohy využívají pouze jeden směrovač Cisco 1841, nicméně každou lze modifikovat tak, aby byly využity další fyzické prvky. Záleží pouze na tom, do jaké míry chceme využít reálnou/simulovanou síť. Stejně tak lze většinu úloh realizovat celé buď v simulovaném prostředí, nebo v reálném.



Obr. 8 Výukové pracoviště

Na Obr. 9 vidíme, jak by mohlo spojení simulované sítě s reálnou například vypadat. V případě analýzy komunikace lze mezi dva směrovače zapojit hub a např. programem WireShark [12] odchytávat a analyzovat komunikaci.



Obr. 9 Příklad zapojení výukového pracoviště

Pro prvotní konfiguraci zařízení od společnosti Cisco propojíme PC a směrovač nebo přepínač modrým konzolovým (rollover) kabelem zapojeným do rozhraní s názvem „CONSOLE“ a na PC bude využit program PuTTY podporující sériovou konektivitu. Tento kabel má na straně jedné konektor RJ-45 a na druhé RS-232. Nastavení programu najdeme na Obr. 10.

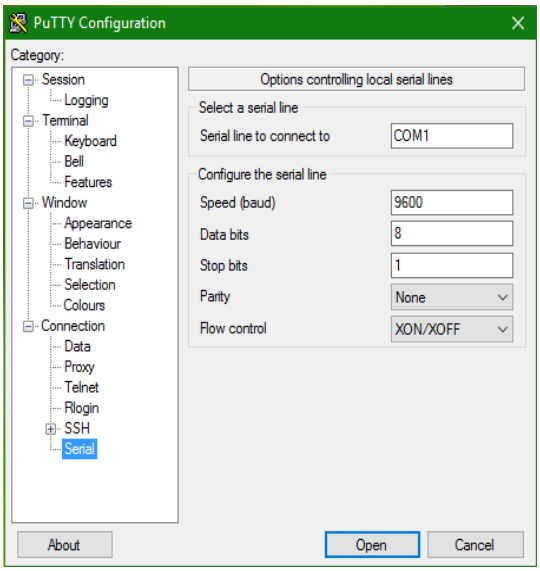
Konfigurace směrovače probíhá shodně v reálném i simulovaném prostředí díky tomu, že GNS3 zařízení emuluje.

Pro správnou funkci propojení sítí je zapotřebí správně nastavit síťová rozhraní na PC. Především jde o zapnutí promiskuitního režimu. Tento režim nám zajistí, že síťové rozhraní bude přijímat i pakety, které nejsou určené přímo pro něj a může tedy s nimi i pracovat. Pokud by byl promiskuitní režim vypnutý, síťová karta by filtrovala provoz a k operačnímu systému by se dostaly pouze pakety, které jsou určené jen pro dané rozhraní a žádné jiné. V praxi by to například znamenalo, že by při dynamickém routování nefungovala výměna routovacích tabulek mezi směrovači v reálné a simulované síti, jelikož by probíhala filtrace paketů nesoucí tuto informaci a síťová karta by tyto pakety zahazovala. [13]

Dále je zapotřebí, aby bylo GNS3 spuštěno jako správce, kvůli tomu, aby mělo plný přístup k síťovým rozhraním.

V případě, že požadujeme, aby se skrze síťové rozhraní přeposílaly ethernetové rámce rozšířené o číslo virtuální sítě (VLAN) dle standartu 802.1q (úloha Inter-VLAN Routing), je důležité, abychom v systémovém registru nalezli položku HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\00nn kde nn číslo síťového rozhraní a zkontrolovali, zda obsahuje položku MonitorModeEnabled a její hodnota je 1. V případě že položka neexistuje, vytvoříme ji. [14]

Tím zajistíme, že síťová karta nebude v ethernetovém rámci odstraňovat informaci o přiřazení paketu do VLAN sítě.



Obr. 10 Nastavení programu PuTTY pro komunikaci se směrovačem Cisco

Obr. 11 Konzolový kabel pro konfiguraci zařízení Cisco [22]

3 Laboratorní úlohy

V této kapitole se nacházejí čtyři laboratorní úlohy, které jsou seřazené od nejjednodušší po složitější. V každé z nich je kladen důraz na využití propojení mezi reálnou a simulovanou sítí. Jednotlivé úlohy obsahují zadání s topologií, rozbor a postup řešení. Témata jednotlivých úloh jsou:

- RIPv2
- Inter-VLAN Routing
- OSPF Single Area
- MPLS VPN

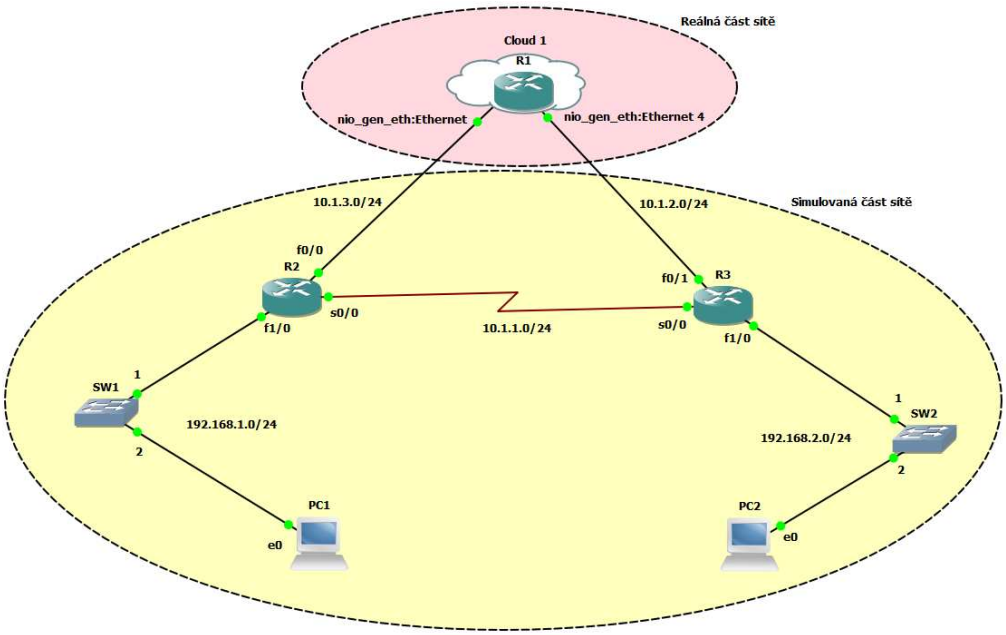
3.1 Úloha – RIPv2

Tato úloha se zabývá implementací dynamického routovacího protokolu RIPv2 v simulované síti, kde jeden směrovač typu Cisco 1841 je fyzický.

3.1.1 Zadání a topologie

Zadání:

- V prostředí simulačního softwaru GNS3 a jednoho reálného směrovače realizujte dynamické směrování protokolem RIPv2
- Uvažujte topologii dle Obr. 12
- Funkčnost zkontrolujte příkazem ping z **PC1** i **PC2** a to se zapojenou sériovou linkou mezi **R2** a **R3** i bez ní



Obr. 12 Topologie k úloze RIPv2

Zařízení	Rozhraní	IP adresa	Gateway	DTE/DCE
PC1	e0	192.168.1.2	192.168.1.1	-
PC2	e0	192.168.2.2	192.168.2.1	-
R1	f0/0	10.1.3.1	-	-
	f0/1	10.1.2.1	-	-
R2	f0/0	10.1.3.2	-	-
	f1/0	192.168.1.1	-	-
	s0/0	10.1.1.1	-	DTE
R3	f0/1	10.1.2.2	-	-
	f1/0	192.168.2.1	-	-
	s0/0	10.1.1.2	-	DCE

Tab. 3 Tabulka IP adres k úloze RIPv2

3.1.2 Rozbor úlohy

V této úloze budeme nastavovat 2 virtuální a jeden fyzický směrovač. Směrovače **R2** a **R3** budou spojeny sériovým kabelem a **R2** bude zdroj taktu. **R1** (Cisco 1841) bude připojen k **R2** a **R3** přes fyzická síťová rozhraní hostitelského počítače a dále pomocí nástroje Cloud připojeny do simulované sítě. Pro připojení **R1** k fyzickým síťovým rozhraním hostitele využijeme ethernetové porty FE 0/0 a FE 0/1 viz Obr. 13. Jako emulovaná zařízení použijeme dva směrovače typu Cisco 2961, dva ethernetové přepínače a dva virtuální počítače (VPCS). Na všech směrovačích bude zajištěna výměna routovacích tabulek protokolem RIPv2.

Obr. 13 Využívaná rozhraní směrovače Cisco 1841 v úloze RIPv2

Routovací protokol RIPv2

RIPv2 (Routing Information Protocol version 2) je směrovací protokol umožňující směrovačům výměnu routovacích tabulek a tím reagovat na změny topologie sítě.

RIP se řadí do skupiny distance-vector protokolů využívající Bellmanův-Fordův algoritmus pro určení nejkratší cesty v síti. Metrikou směrování je počet skoků (směrovačů) k cílové síti. Tento počet je omezen na 15, 16 hopů je bráno jako nekonečná vzdálenost a využívá se pro označení nepoužitelných tras.

V dnešní době již není vhodné tento protokol nasazovat vzhledem ke svému omezení vůči ostatním směrovacím protokolům jako je OSPF nebo EIGRP. Pro tuto laboratorní úlohu je však zcela dostačující. [15]

3.1.3 Postup řešení

Na Obr. 12 vidíme rozdělení na simulovanou a reálnou část sítě. Nejprve nastavíme simulovanou část a až poté část reálnou.

IP adresy přidělíme a nastavíme zařízením dle **Tab. 3**

PC1:

Pro nastavení IP adresy zadáme příkaz:

```
PC1> ip 192.168.1.2/24 192.168.1.1
```

Správnost nastavení zkontrolujeme příkazem:

```
PC1> show
```

Totéž zopakujeme pro **PC2**.

R2:

Příklad konfigurace síťového rozhraní na Cisco směrovači.

```
R2# configure terminal
R2(config)# interface fastethernet0/0
R2(config-if)# ip address 10.1.3.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
```

Obdobným způsobem nastavíme i ostatní rozhraní na směrovači **R2**. U sériového rozhraní nesmíme zapomenout na příkaz `clock rate`, který určuje hodinový takt sériové linky.

Nastavení a zapnutí RIP protokolu

Pro správnou funkci RIP protokolu postačí, aby byly zadány přímo připojené sítě k směrovači. Následně jsou informace o připojených sítí distribuovány směrem k ostatním směrovačům. [16]

```
R2(config)# router RIP
R2(config-router)# version 2
R2(config-router)# no auto-summary
R2(config-router)# network 10.1.3.0
R2(config-router)# network 192.168.1.0
R2(config-router)# network 10.1.1.0
R2(config-if)# exit
```

R3:

Stejným způsobem jako **R2** nastavíme i **R3**, pouze u sériového rozhraní nezadáváme příkaz `clock rate` , protože **R3** pouze poslouchá, takt poskytuje **R2**.

Pro kontrolu funkčnosti protokolu použijte příkaz:

```
R1# show ip rip database
```

Z výpisu je zřejmé, že směrovač je obeznámen se všemi sítěmi v této úloze:

```
Router#show ip rip database
10.0.0.0/8    auto-summary
10.1.1.0/24
    [1] via 10.1.2.2, 00:00:45, FastEthernet0/1
    [1] via 10.1.3.2, 00:00:40, FastEthernet0/0
10.1.2.0/24    directly connected, FastEthernet0/1
10.1.3.0/24    directly connected, FastEthernet0/0
192.168.1.0/24    auto-summary
192.168.1.0/24
    [1] via 10.1.3.2, 00:00:40, FastEthernet0/0
192.168.2.0/24    auto-summary
192.168.2.0/24
    [1] via 10.1.2.2, 00:00:45, FastEthernet0/1
```

Tento příkaz použijte pro kontrolu i na zbylých směrovačích.

Nyní jsou nakonfigurovány všechny prvky sítě a můžeme začít zkoušet komunikaci mezi **PC1** a **PC2**.

Klikněte pravým tlačítkem myši na spojení mezi **R2** a **R3** a zvolte „Start capture“. Otevře se nám WireShark a okamžitě nám začne odchytávat veškerou komunikaci mezi těmito směrovači.

Do konzole PC1 zadejte příkaz `ping` a adresu **PC2**.

Ve WireSharku můžeme pozorovat ICMP pakety, kterými se **PC1** a **PC2** dorozumívají. Jak bylo řečeno v úvodu, protokol RIPv2 využívá k určení optimální cesty počet směrovačů od zdroje k cíli. Sériová linka mezi **R2** a **R3** je opravdu nejkratší cesta od **PC1** k **PC2** a tudíž RIPv2 zvolil správnou cestu.

Nyní smažte sériové spojení mezi **R2** a **R3** a vyčkejte přibližně 30 sekund, než se obnoví routovací tabulky. Poté opět vyzkoušejte komunikaci mezi **PC1** a **PC2**. Pokud Vám **PC2** odpoví, RIPv2 je nakonfigurován správně a je schopný reagovat na změny v topologii sítě.

Můžete si ještě ověřit, kudy paket putuje naší sítí příkazem:

```
PC1> trace 192.168.2.2
```

Dostanete výpis vstupních portů zařízení, která paket zpracovávala:

```
PC1> trace 192.168.2.2

trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop

 1   192.168.1.1    10.533 ms  9.010 ms  9.009 ms

 2   10.1.3.1       19.017 ms  19.580 ms  19.010 ms

 3   10.1.2.2       29.019 ms  28.023 ms  29.612 ms

 4   *192.168.2.2         39.029 ms (ICMP type:3, code:3, Destination port
unreachable)
```

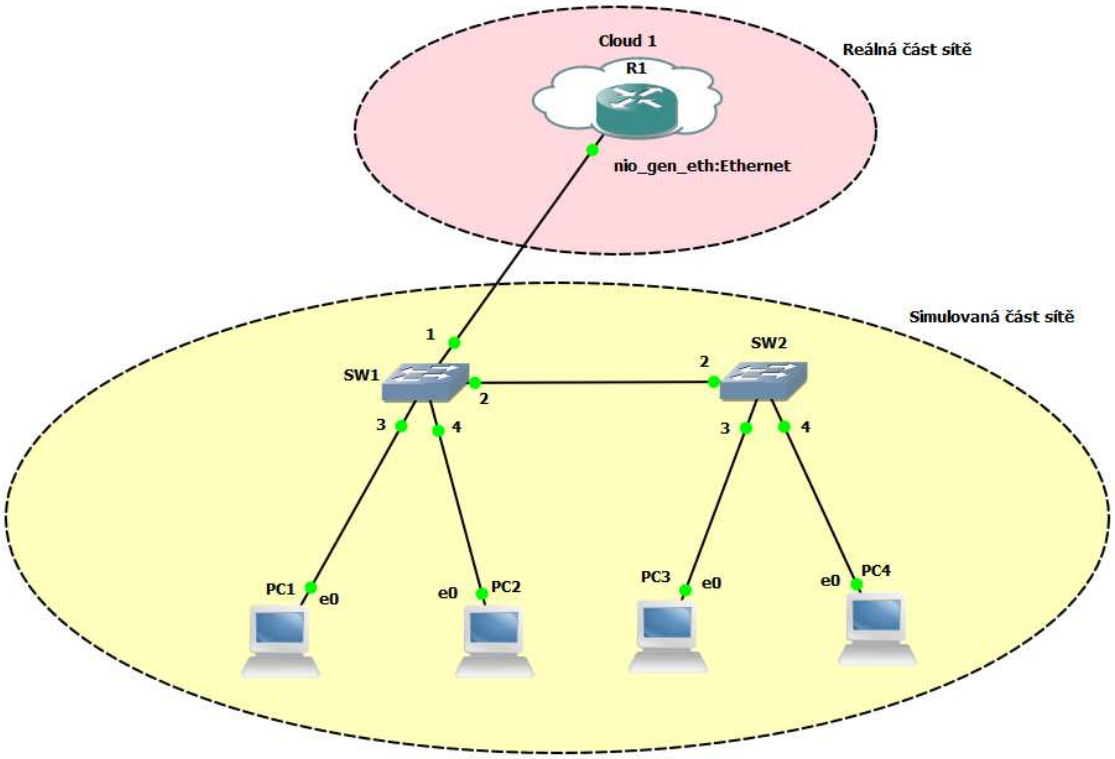
3.2 Úloha – Inter-VLAN Routing

Tato laboratorní úloha se zabývá virtuálními LAN sítěmi a komunikací mezi nimi. Jako fyzický směrovač bude použit Cisco 1841.

3.2.1 Zadání a topologie

Zadání:

- V prostředí simulačního softwaru GNS3 a jednoho reálného směrovače realizujte komunikaci mezi dvěma virtuálními sítěmi
- Uvažujte topologii dle Obr. 14
- Funkčnost ověřte příkazem ping z PC1 na PC4 i opačně



Obr. 14 Topologie k úloze Inter-VLAN Routing

Zařízení	Rozhraní	IP adresa	Gateway	VLAN
PC1	e0	192.168.10.2	192.168.10.1	10
PC2	e0	192.168.20.2	192.168.20.1	20
PC3	e0	192.168.10.3	192.168.10.1	10
PC4	e0	192.168.20.3	192.168.20.1	20
R1	f0/0.1	192.168.1.1	-	-
	f0/0.10	192.168.10.1	-	10
	f0/0.20	192.168.20.1	-	20

Tab. 4 Tabulka IP adres k úloze Inter-VLAN Routing

3.2.2 Rozbor úlohy

V této úloze budeme nastavovat dva virtuální přepínače a jeden fyzický směrovač, který bude zajišťovat routing mezi VLAN sítěmi. Směrovač **R1** (Cisco 1841) bude připojen k přepínači přes fyzické síťové rozhraní hostitelského počítače a dále pomocí nástroje Cloud připojen do simulované sítě. Pro připojení **R1** k fyzickému síťovému rozhraní hostitele využijeme ethernetový port FE 0/0 viz Obr. 15. Jako emulovaná zařízení použijeme dva ethernetové přepínače a čtyři virtuální počítače (VPCS). Dva počítače budou ve VLAN síti 10 a dva ve VLAN síti 20

Obr. 15 Využívaná rozhraní směrovače Cisco 1841 v úloze Inter-VLAN Routing

Virtuální LAN síť (VLAN)

V dnešní době se virtuální LAN sítě hojně používají. Podstata spočívá v tom, že na jednom nebo více fyzických zařízení (přepínače) dokážeme vytvořit více LAN sítí, které jsou sice virtuální, nicméně chovají se jako obyčejné LAN sítě.

VLANy mezi s sebou mohou a taky nemusí komunikovat. Jestliže potřebujeme, aby mezi sebou komunikovali, spojíme je ve směrovači (stejně jako standartní LAN sítě). K tomuto účelu se používají virtuální rozhraní (Sub-interfaces).

Pokud chceme, aby přepínače mezi sebou komunikovali a přenášely mezi sebou informace o virtuálních LAN sítích, musíme na portech, kterými jsou spojeny, aktivovat trunk režim. Port v režimu trunk nám umožní přenášet informace o více virtuálních sítích, kdežto režim access je určen pouze pro komunikaci v jedné virtuální síti. [17]

3.2.3 Postup řešení

Na Obr. 14 vidíme rozdělení na simulovanou a reálnou část sítě. Nejprve nastavíme simulovanou část a až poté část reálnou.

IP adresy přidělíme a nastavíme zařízením dle Tab. 4

PC1:

Pro nastavení IP adresy zadáme příkaz:

```
PC1> ip 192.168.10.2/24 192.168.10.1
```

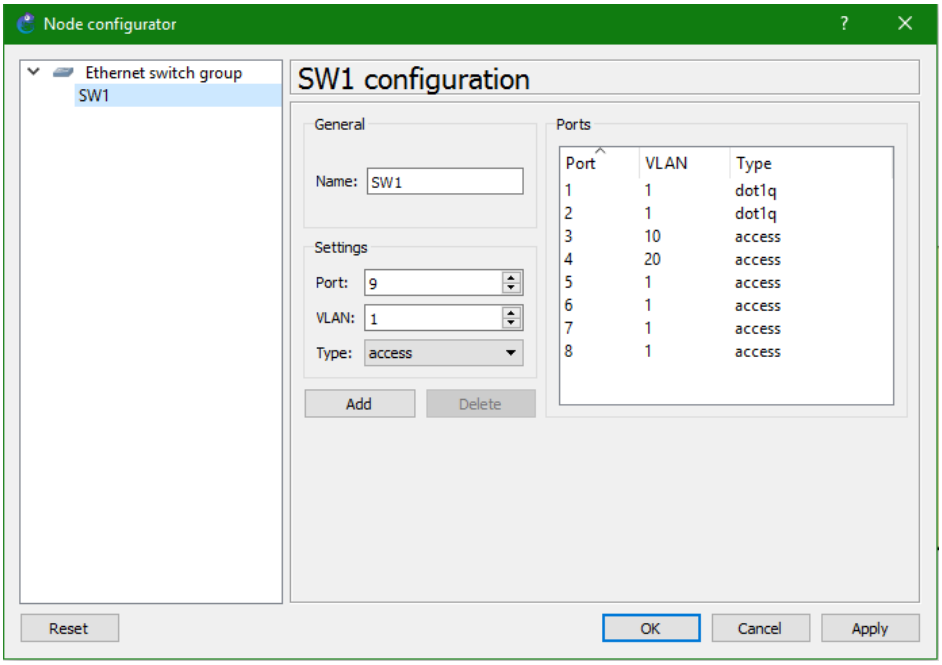
Správnost nastavení zkontrolujeme příkazem:

```
PC1> show
```

Stejným způsobem nastavíme i **PC2**, **PC3** a **PC4**

SW1:

Klikneme pravým tlačítkem na ikonu přepínače a zvolíme „Configure“. Přepínač nastavíme podle Obr. 16



Obr. 16 Nastavení přepínače v úloze Inter-VLAN Routing

Nastavení znamená, že porty 1 a 2 je nastaveny pro zapouzdření (enkapsulaci) ethernetových rámců dle standardu IEEE 802.1Q. Tento standard přidá do hlavičky ethernetového rámce informaci o tom, do jaké VLANy rámec patří. Porty 3, 4 jsou přístupové porty pro PC1 a PC2 a definují nám, do které VLANy daný PC patří.

SW2:

Přepínač **SW2** bude nastaven shodně jako **SW1**. Port č. 1 nastavovat nemusíme, jelikož není připojen k žádnému zařízení.

Nyní si můžeme ověřit příkazem `ping` například z **PC1** na **PC2**, že sítě mezi sebou nekomunikují, jelikož není nastaven směrovač **R1**:

```
PC1> ping 192.168.20.2

host (192.168.10.1) not reachable
```

V tuto chvíli máme nastavenou simulovanou část sítě a přejde ke konfiguraci reálného směrovače **R1**. Pro každou virtuální LAN musíme vytvořit sub-interface, nastavit zapouzdřování 802.1Q a přiřadit IP adresu. Po vytvoření se sub-interface chová stejně, jako fyzický interface.

Před tím, než nastavíte IP adresu virtuálnímu rozhraní, musíte nastavit typ enkapsulace.

Nastavení virtuálních rozhraní pro jednotlivé virtuální LAN sítě:

```
R1# configure terminal
R1(config)# interface fastethernet0/0
R1(config-if)# no shutdown
R1(config-if)# interface fastethernet0/0.1
R1(config-subif)# encapsulation dot1q 1 native
R1(config-subif)# ip address 192.168.1.1 255.255.255.0
R1(config-subif)# interface fastethernet0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# interface fastethernet0/0.20
R1(config-subif)# encapsulation dot1q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# exit
```

Následujícím příkazem zkontrolujeme nastavení:

```
Router# show vlans
```

Příkazem `ping` otestujeme správnost nastavení.

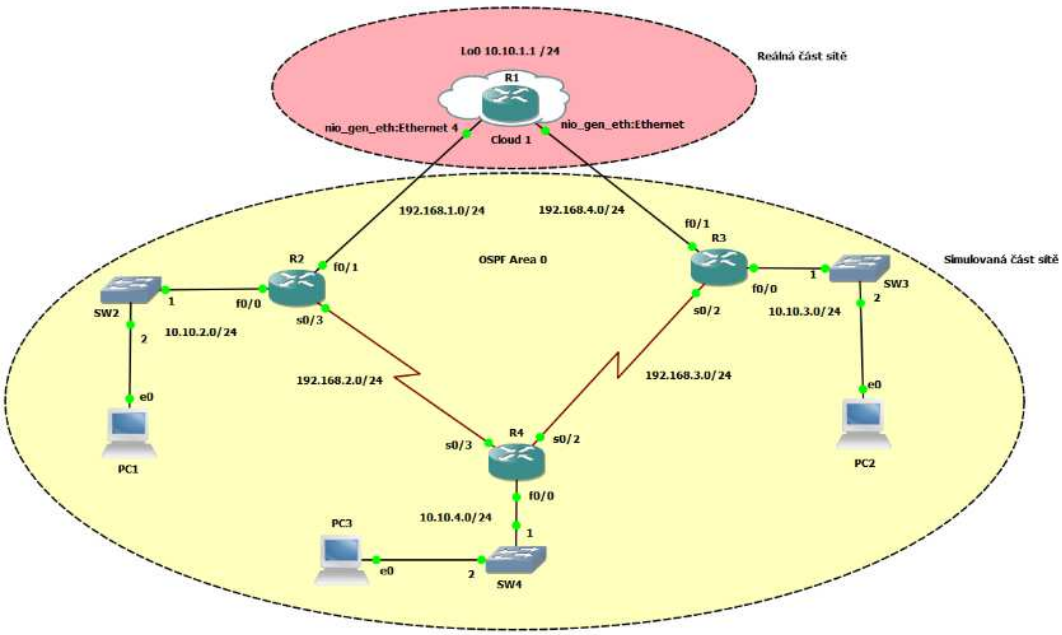
3.3 Úloha – OSPF Single Area

V této úloze se budeme zabývat implementací routovacího protokolu OSPF Single Area v síti obsahující 3 virtuální směrovače Cisco 2951 a jeden fyzický směrovač Cisco 1841.

3.3.1 Zadání a topologie

Zadání:

- V prostředí simulačního softwaru GNS3 a jednoho reálného směrovače realizujte dynamické směrování protokolem OSPF
- Všechny sítě umístěte do oblasti (Area) 0
- Uvažujte topologii dle Obr. 17
- Správnou funkčnost směrování ověřte několikrát příkazem ping a trace. Před zadáním příkazů vždy odstraňte jiné spojení mezi směrovači.



Obr. 17 Topologie k úloze OSPF Single Area

3.3.2 Rozbor úlohy

V této úloze budeme nastavovat tři virtuální a jeden fyzický směrovač. Směrovače **R2** a **R3** budou spojeny sériovým kabelem s **R4**, který bude pro obě spojení poskytovat zdroj taktu. **R1** (Cisco 1841) bude připojen k **R2** a **R3** přes fyzická síťová rozhraní hostitelského počítače a dále pomocí nástroje Cloud připojeny do simulované sítě. Pro připojení **R1** k fyzickým síťovým rozhraním hostitele využijeme ethernetové porty FE 0/0 a FE 0/1 viz Obr. 18.

Zařízení	Rozhraní	IP adresa	Gateway	DTE/DCE
PC1	e0	10.10.2.2	10.10.2.1	-
PC2	e0	10.10.3.2	10.10.3.1	-
PC3	e0	10.10.4.2	10.10.4.1	
R1	f0/0	192.168.1.1	-	-
	f0/1	192.168.4.1	-	-
	Lo0	10.10.1.1	-	
R2	f0/0	10.10.2.1	-	-
	f0/1	192.168.1.2	-	-
	s0/3	192.168.2.1	-	DTE
R3	f0/0	10.10.3.1	-	-
	f0/1	192.168.4.2	-	-
	s0/2	192.168.3.1	-	DTE
R4	f0/0	10.10.4.1	-	-
	s0/2	192.168.3.2	-	DCE
	s0/3	192.168.2.2	-	DCE

Tab. 5 Tabulka IP adres k úloze OSPF Single Area

Jako emulovaná zařízení použijeme tři směrovače typu Cisco 2961, tři ethernetové přepínače a tři virtuální počítače (VPCS). Na směrovači **R1** bude nakonfigurováno rozhraní Loopback 0, které budeme využívat pro ověření funkčnosti routování místo přepínače a počítače. Na všech směrovačích bude zajištěna výměna routovacích tabulek protokolem OSPF.

Obr. 18 Využívaná rozhraní směrovače Cisco 1841 v úloze OSPF Single Area

Routovací protokol OSPF

Protokol OSPF (Open Shortest Path First) můžeme zařadit do skupiny směrovacích protokolů IGP - Interior Gateway Routing Protocols. Je tedy určen k použití uvnitř autonomního systému.

Tento protokol je představitelem směrovacích směrovacích protokolů typu Link State. Směrovací protokoly se stavem linky vytváření v paměti směrovače topologii celé sítě, která se označuje jako Link State Database (LSDB). Nad touto databází společně s algoritmem Shortest Path First (SPF) provádí směrovač výpočty k nalezení nejvýhodnější cesty do jednotlivých sítí.

OSPF je schopen pracovat i ve velikých sítích (oproti RIPv2). Této funkce je docíleno tím, že OSPF síť můžeme rozdělit do několika oblastí (Areas). Mezi jednotlivé oblasti se posílají pouze sumární informace. Výpočet SPF se také provádí pouze v jednotlivých oblastech. Změna topologie v jedné oblasti tedy nezpůsobí výpočet SPF v ostatních oblastech.

Metrikou tohoto protokolu pro určení nejvhodnější cesty do jiné sítě je „cena“ (cost). Je to číslo od 1 do 65565. Každé rozhraní směrovače má přiřazenou cenu. Čím menší číslo, tím lepší je metrika a cesta bude více preferována. [18] [15]

$$cena = \frac{1000000}{\text{šířka pásma } [bit/s]}$$

3.3.3 Postup řešení

Na Obr. 17 vidíme rozdělení na simulovanou a reálnou část sítě. Nejprve nastavíme simulovanou část a až poté část reálnou.

IP adresy přidělíme a nastavíme zařízením dle Tab. 5

PC1:

Pro nastavení IP adresy zadáme příkaz:

```
PC1> ip 10.10.2.2/24 10.10.2.1
```

Správnost nastavení zkontrolujeme příkazem:

```
PC1> show
```

Totéž zopakujeme pro **PC2** i **PC3**.

R2:

Příklad konfigurace síťového rozhraní na Cisco směrovači.

```
R2# configure terminal
R2(config)# interface fastethernet0/0
R2(config-if)# ip address 10.10.2.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
```

Obdobným způsobem nastavíme i ostatní rozhraní na směrovači **R2**. Vzhledem k tomu, že zdroj taktu poskytuje **R4**, příkaz `clock rate` u sériového rozhraní nezadáváme.

Nastavení a zapnutí OSPF protokolu

U protokolu OSPF musíme nakonfigurovat všechny přímo připojené sítě, inverzní masku těchto sítí a oblast, do které sítě patří. Inverzní maska (Wildcard mask) je speciální zápis síťové masky. Jedná se o opak ke klasické masce. Místo jedniček v binárním zápise se v tomto případě počítají nuly. Například ke klasické masce 255.255.255.0 odpovídá inverzní maska 0.0.0.255. [16]

```
R2(config)# router ospf 1
R2(config-router)# network 10.10.2.0 0.0.0.255 area 0
R2(config-router)# network 192.168.1.0 0.0.0.255 area 0
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
R2(config-if)# exit
```

R3:

Směrovač **R3** nastavíme shodně jako **R2**, pouze změníme IP adresy a přímo připojené sítě.

R4:

V případě směrovače **R4** bude nastavení probíhat shodně jako u **R2** a **R3**. Dle Tab. 5 poskytuje hodinový takt sériovým linkám **R2-R4** a **R3-R4**. V nastavení příslušného rozhraní musíme nastavit přikazem `clock rate` takt hodin, jinak nám spojení nebude fungovat.

V tuto chvíli je dokončena konfigurace simulované sítě a nyní bude konfigurována část reálná. Směrovač **R1** bude nastaven shodně jako **R2**, **R3** a **R4**. Rozhraní Loopback 0 nastavíme následujícím způsobem:

```
R2(config)# interface loopback0
R2(config-if)# ip address 10.10.1.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
```

Pro kontrolu funkčnosti protokolu a zjištění, zda má směrovač přístup ke všem sítím, použijte příkaz:

```
R4# show ip route
```

```
R4#show ip route
O    192.168.4.0/24 [110/128] via 192.168.3.1, 00:00:09, Serial0/2
     10.0.0.0/24 is subnetted, 4 subnets
O       10.10.1.0 [110/129] via 192.168.3.1, 00:00:09, Serial0/2
                  [110/129] via 192.168.2.1, 00:00:09, Serial0/3
O       10.10.2.0 [110/65] via 192.168.2.1, 00:00:09, Serial0/3
O       10.10.3.0 [110/65] via 192.168.3.1, 00:00:09, Serial0/2
C       10.10.4.0 is directly connected, FastEthernet0/0
O    192.168.1.0/24 [110/128] via 192.168.2.1, 00:00:09, Serial0/3
C    192.168.2.0/24 is directly connected, Serial0/3
C    192.168.3.0/24 is directly connected, Serial0/2
```

Z výpisu je zřejmé, že směrovač je obeznámen se všemi sítěmi v této úloze. Příznak „o“ značí, že síť byla přidána dynamickým směrovacím protokolem OSPF.

Nyní příkazy `ping` a `trace` otestujeme správné nastavení sítě. Vyzkoušejte i rozpojení některých spojení a pomocí příkazu `trace` sledujte, jak se změní cesta paketu od zdroje k cíli.

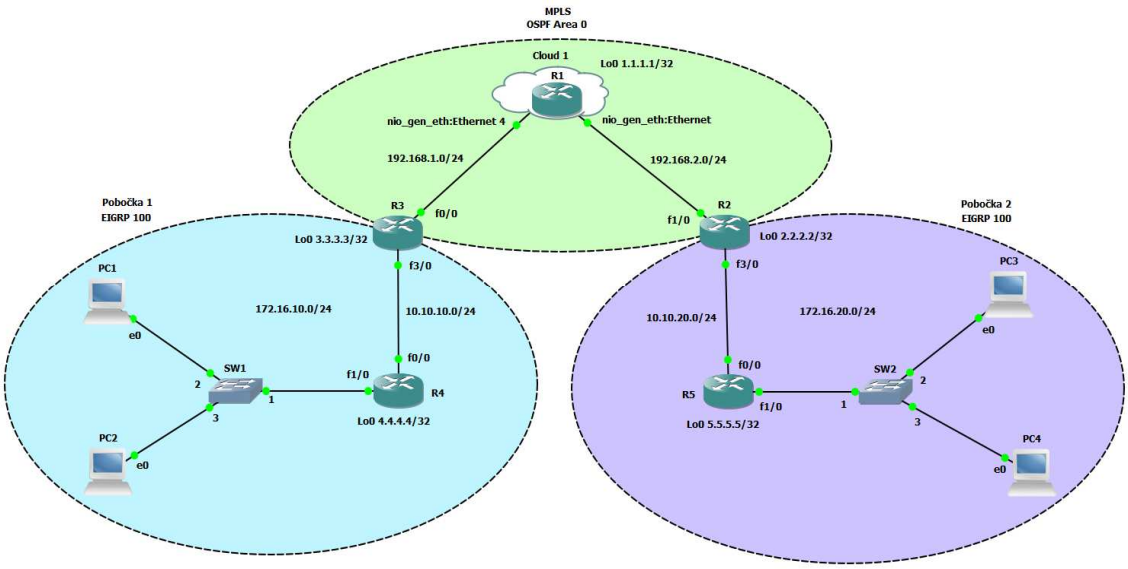
3.4 Úloha – MPLS VPN

Tato úloha se zabývá nastavením sítě MPLS (Multi-Protocol Label Switching) včetně propojení dvou vzdálených sítí pomocí VPN (Virtual Private Network). [19]

3.4.1 Zadání a topologie

Zadání:

- V prostředí simulačního softwaru GNS3 a jednoho reálného směrovače nakonfigurujte síť MPLS
- Technologií VPN propojte dvě pobočky jedné firmy
- Uvažujte topologii dle Obr. 19
- Správnou funkčnost sítě ověřte příkazem ping z pobočky 1 do pobočky 2 a opačně. Příkazem trace sledujte cestu paketu.



Obr. 19 Topologie k úloze MPLS VPN

3.4.2 Rozbor úlohy

V této úloze budeme nastavovat čtyři virtuální a jeden fyzický směrovač. Směrovače **R2** a **R3** budou hraničními směrovači mezi MPLS sítí a pobočkovými sítěmi. **R1** (Cisco 1841) bude připojen k **R2** a **R3** přes fyzická síťová rozhraní hostitelského počítače a dále pomocí nástroje Cloud připojeny do simulované sítě. Pro připojení **R1** k fyzickým síťovým rozhraním hostitele využijeme ethernetové porty FE 0/0 a FE 0/1 viz Obr. 20. Jako emulovaná zařízení použijeme čtyři směrovače typu Cisco 3640, dva ethernetové přepínače a čtyři virtuální počítače (VPCS). Na všech směrovačích bude nakonfigurováno rozhraní Loopback 0, kterým se bude směrovač identifikovat v síti.

Zařízení	Rozhraní	IP adresa	Gateway	DTE/DCE
PC1	e0	172.16.10.2	172.16.10.1	-
PC2	e0	172.16.10.3	172.16.10.1	-
PC3	e0	172.16.20.2	172.16.20.1	-
PC4	e0	172.16.20.3	172.16.20.1	-
R1	f0/0	192.168.2.1	-	-
	f0/1	192.168.1.1	-	-
	Lo0	1.1.1.1	-	-
R2	f1/0	192.168.2.2	-	-
	f3/0	10.10.20.1	-	-
	Lo0	2.2.2.2	-	-
R3	f0/0	192.168.1.2	-	-
	f3/0	10.10.10.1	-	-
	Lo0	3.3.3.3	-	-
R4	f0/0	10.10.10.2	-	-
	f1/0	172.16.10.1	-	-
	Lo0	4.4.4.4	-	-
R5	f0/0	10.10.20.2	-	-
	f1/0	172.16.20.1	-	-
	Lo0	5.5.5.5	-	-

Tab. 6 Tabulka IP adres k úloze MPLS VPN

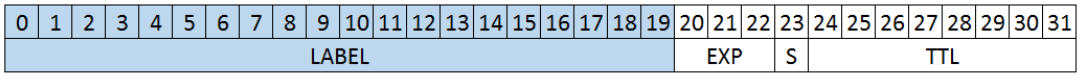
V úloze se využívají tři směrovací protokoly – OSPF, EIGRP a BGP. Protokolem OSPF probíhá směrování uvnitř MPLS sítě. Protokol EIGRP zde slouží jako směrovací protokol obou poboček. BGP protokol je nastaven pro přenos řídících informací pobočkového routovacího protokolu EIGRP.

Obr. 20 Využívaná rozhraní směrovače Cisco 1841 v úloze MPLS VPN

Technologie MPLS

MPLS (Multi-Protocol Label Switching) vzniklo jako snaha spojit nejlepší vlastnosti sítí IP a ATM. Pakety jsou na vstupu do sítě označeny značkou (label). Směrovače se v síti MPLS nezajímají o obsah IP hlavičky, ale právě o label, který je primárně určen k určení dalšího bodu směrování. Tyto směrovače označujeme jako LSR (Label Switch Router).

Label je součástí 32 bitového MPLS záhlaví a může být paketu přidělena dle cílové adresy a QoS parametrů, multicastové adresy nebo příslušnosti k VPN zákazníka. Celé MPLS záhlaví znázorňuje Obr. 21



Obr. 21 Záhlaví MPLS

Protokol MPLS bývá označován jako protokol 2+ vrstvy OSI modelu. Jeho záhlaví je součástí rámce druhé vrstvy a nachází se mezi záhlavím rámce (ethernet, PPP, ATM či Frame-Relay) a transportovaným IP paketem.

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) je dynamický směrovací protokol vyvinutý společností Cisco jako proprietární protokol. V roce 2013 byl zveřejněn jako volně dostupný standart. Patří do skupiny distance-vector protokolů (obdobně jako RIP).

EIGRP je využíván ke směrování v rámci jednoho autonomního systému. Na rozdíl od ostatních známých směrovacích protokolů posílá pouze přírůstkové aktualizace routovacích tabulek, což snižuje nároky jak na zařízení, tak na síť. [20] [15]

BGP

Border Gateway Protocol (BGP) je dynamický směrovací protokol využívaný pro směrování mezi autonomními systémy (AS). Patří do rodiny protokolů Exterior Gateway Protocols - vnější směrovací protokoly. Pomocí BGP si hraniční směrovače vyměňují informace o sítích v jednotlivých autonomních systémech a také o tom, přes které AS se lze do jednotlivých sítí dostat. [21] [15]

3.4.3 Postup řešení

Na Obr. 19 vidíme rozdělení na síť MPLS a pobočkové sítě. Nejdříve nakonfigurujeme síť MPLS společně s fyzickým směrovačem a až poté pobočkové sítě.

IP adresy přidělíme a nastavíme zařízením dle Tab. 6

R1:

Příklad konfigurace síťového rozhraní na Cisco směrovači.

```
R1# configure terminal
R1(config)# interface fastethernet0/0
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

Pro identifikaci směrovače v síti nastavíme rozhraní Loopback 0

```
R1(config)# interface loopback0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# ip ospf network point-to-point
R1(config-if)# no shutdown
```

Správnou konfiguraci IP adres ověříme příkazem

```
R1# show ip interface brief
```

Routování dynamickým protokolem OSPF

```
R1(config)# router ospf 1
R1(config-router)# network 1.1.1.1 0.0.0.0 area 0
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
R1(config-if)# exit
```

MPLS zapneme příkazem

```
R1(config-if)# mpls IP
```

Tento příkaz musíme zadat u **každého** síťového rozhraní, který se nachází v síti MPLS.

Kontrola, zda je MPLS zapnuto na všech požadovaných rozhraní

```
R1# show mpls interfaces
Interface              IP           Tunnel   Operational
FastEthernet0/0        Yes (ldp)    No       Yes
FastEthernet1/0        Yes (ldp)    No       Yes
```

Identifikace směrovače v síti podle adresy rozhraní Loopback 0

```
R1# mpls ldp router-id Loopback0
```

Konfigurace **R2** a **R3** bude probíhat obdobně, pouze s několika rozdíly:

- V konfiguraci OSPF nebudeme zadávat síť, která je připojená k rozhraní fa3/0 jelikož tato síť už je v pobočkové části topologie
- Aby se nešířily informace protokolem OSPF přes rozhraní fa3/0 do pobočkové sítě, zadáme příkaz

```
R2(config-router)# passive-interface fa3/0
```

Nyní máme nastavenou síť MPLS a přistoupíme ke konfiguraci rozhraní MPLS VPN

Vytvoříme vrf (Virtual Routing and Forwarding) a nazveme ho „FIRMA“. Provedeme nastavení RD (Route Distinguisher) a Route-target. Toto vrf přiřadíme rozhraní, ke kterému je připojena pobočka. Konfigurace je shodná na **R2** i **R3**

```
R2(config)# ip vrf FIRMA
R2(config-vrf)# rd 100:1
R2(config-vrf)# route-target both 1:100
R2(config)# interface fa3/0
R2(config-if)# ip vrf forwarding FIRMA
```

POZOR! Během přiřazování vrf k rozhraní se vymaže IP adresa na daném rozhraní, je tedy potřeba jí nastavit znovu.

V případě, že budete chtít vyzkoušet komunikaci z **R3** na **R4** popřípadě z **R2** na **R5**, nelze to udělat pouze příkazem `ping`.

```
R2# ping vrf FIRMA 10.10.20.2
```

Konfigurace EIGRP na **R4** i **R5** bude probíhat shodně, pouze zadáme příslušné sítě.

```
R4(config)# router eigrp 100
R4(config-router)# network 10.10.10.0 0.0.0.255
R4(config-router)# network 172.16.10.0 0.0.0.255
R4(config-router)# network 4.4.4.4 0.0.0.0
R4(config-router)# no auto-summary
R1(config-if)# exit
```

EIGRP na **R2** a **R3**

```
R2(config)# router eigrp 1
R2(config-router)# address-family ipv4 vrf FIRMA
R2(config-router-af)# autonomous-system 100
R2(config-router-af)# network 10.10.20.0 0.0.0.255
R2(config-router-af)# no auto-summary
```

Kontrola EIGRP sousedství

```
R2#sh ip eigrp vrf FIRMA neighbors
IP-EIGRP neighbors for process 100
H   Address     Interface   Hold  Uptime    SRTT   RTO   Q    Seq
                            (sec)           (ms)         Cnt  Num
0   10.10.20.2  Fa3/0       13    02:42:05  1254   5000  0    3
```

Konfiguraci protokolu BGP provedeme **pouze** na **R2** a **R3**, jelikož slouží ke komunikaci mezi autonomními systémy

```
R2(config)# router bgp1
R2(config-router)# neighbor 3.3.3.3 remote-as 1
R2(config-router)# neighbor 3.3.3.3 update-source loopback 0
R2(config-router)# address-family vpnv4
R2(config-router-af)# neighbor 3.3.3.3 activate
R2(config-router-af)# neighbor 3.3.3.3 send-community extended
```

Při konfiguraci BGP na směrovači **R3**, použijte místo příkazu

```
R2(config-router-af)# neighbor 3.3.3.3 send-community extended
```

příkaz

```
R3(config-router-af)# neighbor 2.2.2.2 send-community both
```

Nyní už nám zbývá pouze nastavit redistribuci routovacích cest mezi BGP a EIGRP a naopak.

```
R2(config)# router eigrp 1
R2(config-router)# address-family ipv4 vrf FIRMA
R2(config-router-af)# redistribute bgp 1 metric 1500 400 20 20 1500
R2(config)# router bgp 1
R2(config-router)# address-family ipv4 vrf FIRMA
R2(config-router-af)# redistribute eigrp 100
```

```
R2(config)# router bgp1
R2(config-router)# neighbor 3.3.3.3 remote-as 1
R2(config-router)# neighbor 3.3.3.3 update-source loopback 0
R2(config-router)# address-family vpnv4
R2(config-router-af)# neighbor 3.3.3.3 activate
R2(config-router-af)# neighbor 3.3.3.3 send-community extended
```

Provedeme kontrolu routovacích cest mezi oběma pobočkami

```
R3# show ip route vrf FIRMA
```

A pokud je vše správně nastaveno, měli bychom dostat následující výpis:

```
R2#sh ip route vrf FIRMA
Routing Table: FIRMA
Gateway of last resort is not set
     4.0.0.0/32 is subnetted, 1 subnets
B       4.4.4.4 [200/156160] via 3.3.3.3, 00:08:45
     5.0.0.0/32 is subnetted, 1 subnets
D       5.5.5.5 [90/156160] via 10.10.20.2, 00:10:14, FastEthernet3/0
     172.16.0.0/24 is subnetted, 2 subnets
D       172.16.20.0 [90/30720] via 10.10.20.2, 00:10:14, FastEthernet3/0
B       172.16.10.0 [200/30720] via 3.3.3.3, 00:08:45
     10.0.0.0/24 is subnetted, 2 subnets
B       10.10.10.0 [200/0] via 3.3.3.3, 00:08:45
C       10.10.20.0 is directly connected, FastEthernet3/0
```

Vidíme, že existují cesty z pobočky 2 na pobočku 1. Totéž zkontrolujeme i na **R3**.

Na závěr otestujeme příkazem `ping` komunikaci mezi oběma pobočkami.

```
PC3> ping 172.16.10.2

84 bytes from 172.16.10.2 icmp_seq=1 ttl=59 time=71.047 ms

84 bytes from 172.16.10.2 icmp_seq=2 ttl=59 time=79.552 ms

84 bytes from 172.16.10.2 icmp_seq=3 ttl=59 time=79.552 ms

84 bytes from 172.16.10.2 icmp_seq=4 ttl=59 time=79.058 ms

84 bytes from 172.16.10.2 icmp_seq=5 ttl=59 time=79.552 ms
```

4 Vyhodnocení

Cílem této práce bylo analyzovat možnosti propojení simulátorů síťových prostředí s reálnou sítí. Pro tyto účely byly zvoleny tři simulační nástroje - GNS3, Cisco Packet Tracer a Huawei eNSP, kterým se podrobně věnuje první kapitola. Jako nejvhodnější se pro tyto účely jeví GNS3, ve kterém jsou realizovány laboratorní úlohy. Jeho nevýhoda je v tom, že pro realizaci simulace je zapotřebí, abychom disponovali obrazy operačních systémů pro síťové prvky. Na rozdíl od Cisco Packet Traceru a Huawei eNSP totiž GNS3 síťové prvky nesimuluje, ale emuluje a tudíž se zařízení chovají obdobně, jako virtualizované počítače. Huawei eNSP umožňuje také propojení simulované a reálné sítě, ovšem vzhledem k tomu, že ho vyvíjí společnost Huawei, lze simulace provádět pouze na zařízeních od tohoto výrobce. Cisco Packet Tracer neumožňuje propojení. V Tab. 2 najdeme přehledné porovnání a výsledky této analýzy.

Dále bylo vytvořeno výukové pracoviště složené z aktivních síťových prvků od společnosti Cisco a 3com. Toto pracoviště je podrobně popsáno a vyobrazeno v kapitole 2. K němu lze připojit libovolný počítač nejlépe se dvěmi síťovými rozhraními a nainstalovaným softwarem GNS3. Pomocí nástroje Cloud je GNS3 propojen s reálnými síťovými prvky.

Společně s výukovým pracovištěm vznikly i čtyři laboratorní úlohy zaměřené na směrování, přepínaní a technologii MPLS VPN. V těch úlohách je kladen důraz na využití propojení mezi simulovanou a reálnou sítí a v případě potřeby lze tyto úlohy snadno modifikovat např. využitím více fyzických zařízení.

Literatura

[1] *A Quick Guide to GPLv3* [online]. b.r. [cit. 2016-05-05]. Dostupné z: http://www.gnu.org/licenses/quick-guide-gplv3.html

[2] VYSTRČIL, Martin. *M-linux: Cisco network – simulace* [online]. b.r. [cit. 2016-04-29]. Dostupné z: http://m-linux.cz/2014/02/cisco-network-simulace/

[3] *YouTube, LLC* [online]. b.r. [cit. 2016-02-24]. Dostupné z: https://www.youtube.com/

[4] *GNS3 Technologies Inc.* [online]. b.r. [cit. 2016-02-19]. Dostupné z: https://gns3.com/

[5] *Dokumentace k programu GNS3* [online]. b.r. [cit. 2016-04-29]. Dostupné z: https://www.gns3.com/support/docs/quick-start-guide-for-windows-us

[6] VYSTRČIL, Martin. *M-linux: GNS3 – úvodní nastavení* [online]. b.r. [cit. 2016-04-29]. Dostupné z: http://m-linux.cz/2014/02/gns3-uvodni-nastaveni/

[7] *COMPUTERWORLD: Test: Možnosti Cisco emulátoru sítí GNS3* [online]. b.r. [cit. 2016-04-29]. Dostupné z: http://computerworld.cz/testy/test-moznosti-cisco-emulatoru-siti-gns3-5632

[8] *Cisco Systems, Inc.* [online]. b.r. [cit. 2016-04-30]. Dostupné z: http://www.cisco.com/

[9] *Cisco Networking Academy* [online]. b.r. [cit. 2016-04-29]. Dostupné z: https://www.netacad.com/

[10] *Huawei Technologies Co. Ltd.* [online]. b.r. [cit. 2016-04-30]. Dostupné z: http://www.huawei.com/en/

[11] *Huawei: eNSP Download* [online]. b.r. [cit. 2016-04-30]. Dostupné z: http://support.huawei.com/enterprise/toolNewInfoAction!toToolDetail?contentId=TL1000000015

[12] *Wireshark* [online]. b.r. [cit. 2016-04-30]. Dostupné z: https://www.wireshark.org/

[13] VAVREČKOVÁ, Šárka. ÚSTAV INFORMATIKY, FPF SU OPAVA. *Nástroje pro analýzu počítačových sítí* [online]. b.r., 4.12.2014 [cit. 2016-04-30]. Dostupné z: http://vavreckova.zam.slu.cz/obsahy/analyzadat/ad_07_site2.pdf

[14] *GNS3 Forum: Issues connecting to real network* [online]. b.r. [cit. 2016-04-29]. Dostupné z: http://forum.gns3.net/topic7653.html

[15] ODOM, Wendell, Rus HEALY a Naren MEHTA. *Směrování a přepínání sítí: autorizovaný výukový průvodce*. Vyd. 1. Brno: Computer Press, 2009, 879 s. Samostudium. ISBN 9788025125205.

[16] HUCABY, Dave a Steve MCQUERRY. *Konfigurace směrovačů Cisco: [autorizovaný výukový průvodce : podrobný přehled příkazů, protokolů a nastavení]*. Vyd. 1. Brno: Computer Press, 2004, 632 s. Samostudium. ISBN 8072269518.

[17] BOUŠKA, Petr. *VLAN - Virtual Local Area Network* [online]. 2007 [cit. 2016-05-02]. Dostupné z: http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

[18] GRYGÁREK, Petr. KATEDRA INFORMATIKY FEI, VŠB-TU OSTRAVA. *Směrovací protokol OSPF* [online]. b.r. [cit. 2016-04-30]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/OSPF/ospf.html

[19] *GNS3Vault: Basic MPLS VPN* [online]. b.r. [cit. 2016-04-28]. Dostupné z: http://gns3vault.com/mpls/basic-mpls-vpn/

[20] *Wikipedia: Enhanced Interior Gateway Routing Protocol* [online]. Wikimedia Foundation, b.r. [cit. 2016-04-30]. Dostupné z: https://en.wikipedia.org/wiki/Enhanced_Interior_Gateway_Routing_Protocol

[21] GRYGÁREK, Petr. KATEDRA INFORMATIKY FEI, VŠB-TU OSTRAVA. *Směrovací protokol BGP* [online]. b.r. [cit. 2016-04-30]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/BGP/BGP.html

[22] *Rollover cable* [online]. b.r. [cit. 2016-05-14]. Dostupné z: http://www.aliexpress.com/item/NEW-100pcs-lot-1-5M-RJ45-to-serial-9-hole-RJ45-serial-cable-RS232-cable-rollover/32389285163.html

Seznam příloh

A. Konfigurace úloh

Zde jsou uvedeny běžící konfigurace (running-config) jednotlivých směrovačů z každé úlohy.

A.1 Úloha - RIPv2

R1:

```
hostname R1
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 10.1.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.2.1 255.255.255.0
 duplex auto
 speed auto
!
router rip
 version 2
 network 10.0.0.0
 no auto-summary
!
end
```

R2:

```
hostname R2
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 10.1.3.2 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 10.1.1.1 255.255.255.0
 clock rate 64000
!
interface FastEthernet1/0
 ip address 192.168.1.1
255.255.255.0
 duplex auto
 speed auto
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
!
end
```

R3:

```
hostname R3
!
no ip domain lookup
!
interface Serial0/0
 ip address 10.1.1.2 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.1.2.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 192.168.2.1
255.255.255.0
 duplex auto
 speed auto
!
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.2.0
 no auto-summary
!
end
```

A.2 Úloha - Inter-VLAN Routing

R1:

```
hostname R1
!
no ip domain lookup
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 192.168.1.1
255.255.255.0
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1
255.255.255.0
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1
255.255.255.0
!
end
```

A.3 Úloha - OSPF Single Area

R1:

```
hostname R1
!
no ip domain lookup
!
interface Loopback0
 ip address 10.10.1.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.1.1
255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.4.1
255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 10.10.1.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area
0
 network 192.168.4.0 0.0.0.255 area
0
!
end
```

R2:

```
hostname R2
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 10.10.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.2
255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/3
 ip address 192.168.2.1
255.255.255.0
!
router ospf 1
 log-adjacency-changes
 network 10.10.2.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area
0
 network 192.168.2.0 0.0.0.255 area
0
!
end
```

R3:

```
hostname R3
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 10.10.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.4.2
255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/2
 ip address 192.168.3.1
255.255.255.0
!
router ospf 1
 log-adjacency-changes
 network 10.10.3.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area
0
 network 192.168.4.0 0.0.0.255 area
0
!
end
```

R4:

```
hostname R4
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 10.10.4.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/2
 ip address 192.168.3.2
255.255.255.0
 clock rate 64000
!
interface Serial0/3
 ip address 192.168.2.2
255.255.255.0
 clock rate 64000
!
router ospf 1
 log-adjacency-changes
 network 10.10.4.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area
0
 network 192.168.3.0 0.0.0.255 area
0
!
end
```

A.4 Úloha - MPLS VPN

R1:

```
hostname R1
!
no ip domain lookup
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 ip address 192.168.1.1
255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet1/0
 ip address 192.168.2.1
255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 1.1.1.1 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area
0
 network 192.168.2.0 0.0.0.255 area
0
!
mpls ldp router-id Loopback0
!
end
```

R2:

```
hostname R2
!
no ip domain lookup
!
ip vrf FIRMA
 rd 100:1
 route-target export 1:100
 route-target import 1:100
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet1/0
 ip address 192.168.2.2
255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet3/0
 ip vrf forwarding FIRMA
 ip address 10.10.20.1
255.255.255.0
 duplex auto
 speed auto
!


router eigrp 1
 no auto-summary
 !
 address-family ipv4 vrf FIRMA
  redistribute bgp 1 metric 1500
400 20 20 1500
```

```
  network 10.10.20.0 0.0.0.255
  no auto-summary
  autonomous-system 100
 exit-address-family
!
router ospf 1
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 192.168.2.0 0.0.0.255 area
0
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 3.3.3.3 remote-as 1
 neighbor 3.3.3.3 update-source
Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community
both
 exit-address-family
 !
 address-family ipv4 vrf FIRMA
  redistribute eigrp 100
  no synchronization
 exit-address-family
!
mpls ldp router-id Loopback0
!
end
```

R3:

```
hostname R3
!
no ip domain lookup
!
ip vrf FIRMA
 rd 100:1
 route-target export 1:100
 route-target import 1:100
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 ip address 192.168.1.2
255.255.255.0
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet3/0
 ip vrf forwarding FIRMA
 ip address 10.10.10.1
255.255.255.0
 duplex auto
 speed auto
!
router eigrp 1
 no auto-summary
 !
 address-family ipv4 vrf FIRMA
  redistribute bgp 1 metric 1500
400 20 20 1500
```

```
  network 10.10.10.0 0.0.0.255
  no auto-summary
  autonomous-system 100
 exit-address-family
!
router ospf 1
 log-adjacency-changes
 network 3.3.3.3 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area
0
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source
Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community
both
 exit-address-family
 !
 address-family ipv4 vrf FIRMA
  redistribute eigrp 100
  no synchronization
 exit-address-family
!
mpls ldp router-id Loopback0
!
end
```

R4:

```
hostname R4
!
no ip domain lookup
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.10.10.2
255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 172.16.10.1
255.255.255.0
 duplex auto
 speed auto
!
router eigrp 100
 network 4.4.4.4 0.0.0.0
 network 10.10.10.0 0.0.0.255
 network 172.16.10.0 0.0.0.255
 no auto-summary
!
end
```

R5:

```
hostname R5
!
no ip domain lookup
!
interface Loopback0
 ip address 5.5.5.5 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.10.20.2
255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 172.16.20.1
255.255.255.0
 duplex auto
 speed auto
!
router eigrp 100
 network 5.5.5.5 0.0.0.0
 network 10.10.20.0 0.0.0.255
 network 172.16.20.0 0.0.0.255
 no auto-summary
!
end
```