VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2016

Bc. Martin Karlík

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

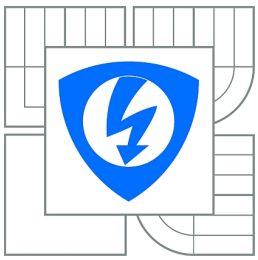
ROZBOR PROTOKOLŮ CISCO SÍTÍ
PROTOCOLS ANALYSIS OF CISCO NETWORKS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Martin Karlík**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Vladislav Škorpil, CSc.**
SUPERVISOR

BRNO 2016



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Martin Karlík	***ID:***	136535
Ročník:	2	***Akademický rok:***	2015/2016

NÁZEV TÉMATU:

Rozbor protokolů CISCO sítí

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se se specifiky CISCO sítí a s používanými protokoly MPLS, EIGRP, OSPF, Multicast - sparse mode/dense mode. Ve volně dostupném simulačním prostředí GNS3 navrhněte, analyzujte a realizujte minimálně dvě laboratorní úlohy, ve kterých implementujete vybrané z výše uvedených protokolů, popřípadě jiné relevantní protokoly.

DOPORUČENÁ LITERATURA:

[1] CISCO, firemní dokumentace 2006 – 2015
[2] KABELOVÁ, A., DOSTÁLEK, L. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.
[3] PUŽMANOVÁ,R. Moderní komunikační sítě A-Z. Computer Press, Brno 2007.
[4] GNS3, http://www.gns3.com/

Termín zadání:	1.2.2016	***Termín odevzdání:***	25.5.2016

Vedoucí práce: doc. Ing. Vladislav Škorpil, CSc.
Konzultanti diplomové práce:

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

UPOZORNĚNÍ:

ABSTRAKT

Bc.Karlík, Martin

Ústav telekomunikací, Fakulta elektrotechniky a komunikačních technologií, Vysoké učení technické v Brně.

Rozbor protokolov CISCO sietí

Táto diplomová práca je venovaná CISCO sieťam a protokolom ako OSPF, EIGRP, MPLS, BGP, IPv4, IPv6, Multicast – sparse / dense mode. Úlohou bolo preštudovať tieto porotokoly a vo voľne dostupnom simulačnom prostredí GNS3 navrhnúť a realizovať tri laboratórne úlohy zo zameraním sa na vybrané z vyššie uvedených protokolov. Navrhnuté laboratórne úlohy sa venujú protokolom MPLS, OSPF a EIGRP. V práci je použitý CISCO smerovač 3745.

KĽÚČOVÉ SLOVÁ

OSPF, EIGRP, MPLS, BGP, Ipv4, Ipv6, CISCO, GNS3, multicast

ABSTRACT

Bc.Karlík, Martin

Department of Telecommunications, Faculty of Electrical Engineering and Communication, Brno University of Technology.

Protocols analysis of cisco networks

This diploma thesis is focused on CISCO networks and protocols like OSPF, EIGRP, MPLS, BGP, Ipv4, Ipv6, Multicast – sprase / dense mode. The task was study of those protocols and design and implement three lab excercises with choosen of those protocols by using free network simulator GNS3. Designed lab excercises are focused on MPLS, OSPF and EIGRP. In this excercise is used CISCO router 3745.

KEY WORDS

OSPF, EIGRP, MPLS, BGP, Ipv4, Ipv6, CISCO, GNS3, multicast

KARLÍK, M. Rozbor protokolov CISCO sietí. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2016. 104 s. Vedoucí diplomové práce doc.Ing. Vladislav Škorpil, CSs.

PREHLÁSENIE

Prehlasujem, že som svoju diplomovú prácu na tému „Rozbor protokolov CISCO sietí“ vypracoval samostatne pod vedením vedúceho diplomovej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenéj diplomovej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto ddiplomovej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia S11 a nasledujúcich autorského zákona č. 121/2000Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), vo znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhé, hlavy VI. diel 4 Trestného zákonníka č.40/2009 Sb.

Brno ....

(podpis autora)

POĎAKOVANIE

Rád by som sa poďakoval vedúcemu diplomovej práce pánovi doc.Ing. Vladislavovi Škorpilovi, CSs za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Brno ....
(podpis autora)

Faculty of Electrical Engineering
and Communication

Brno University of Technology
Technicka 12, CZ-61600 Brno, Czechia

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

Výzkum popsaný v této diplomové práci byl realizovaný v laboratořích podpořených projektem Centrum senzorických, informačních a komunikačních systémů (SIX); registrační číslo CZ.1.05/2.1.00/03.0072, operačního programu Výzkum a vývoj pro inovace.

OBSAH

Zoznam obrázkov

Zoznam tabuliek

Úvod

Komunikácia a počítačové siete sú v súčasnosti všade okolo nás a stali sa našou každodennou súčasťou a používame ich každodenne či už vedome alebo nevedome. Pri súčasnom vzostupe doby „Internet of Things“ sú poznanie a porozumenie týchto dvoch entít pre budúcich inžinierov ale aj laikov o to dôležitejšie. Keďže reálny hardvér na ktorom by sa dali simulovať, implementovať a učiť rôzne techniky, technológie a topológie je pridrahý vznikli sieťové simulačné programy. Tieto programy sú používané na rôzne simulácie sieťových technológií či už v školách pri výuke na demonštrovanie vlastností daných komunikačných technológií alebo v rôznych telekomunikačných spoločnostiach kde sa využívajú na testovanie technológie alebo topológie pred uvedením do produkcie.

Jeden s takýchto simulačných programov je aj GNS3 (Graphical Network Simulator 3), ktorý je využívaný aj v tejto diplomovej práci. Práca je zameraná na teoretický rozbor sieťových protokolov MPLS, OSPF, EIGRP, PIM sparse / dense mode, IPv4, IPv6, BGP, návrh a implementáciu laboratórnych úloh, ktoré sa venujú protokolom OSPF, MPLS a EIGRP.

Prvá kapitola sa venuje smerovaniu a smerovacím protokolom OSPF a EIGRP,
Druhá kapitola pojednáva o smerovacom protokole BGP. Tento protokol sa využíva na smerovanie dát medzi autonómnymi systémami.

Tretia a štvrtá kapitola sa venuje protokolom IPv4 a IPv6. Protokol IPv6 sa v súčasnej dobe stáva čoraz viac používanejší.

V piatej kapitole je teoreticky rozobraný protokol MPLS, ktorý predstavuje revolučnú techniku v smerovaní dát v sieti na základe návestí.

Šiesta kapitola stručne popisuje multicast. Siedma kapitola sa venuje sieťovému operačnému systému IOS od spoločnosti CISCO. V laboratórnych úlohách je použitý CISCO smerovač 3745. Spoločnosť CISCO je v súčasnosti lídrom na trhu zo sieťovými technológiami.

Kapitola číslo osem popisuje sieťový simulátor GNS3, ktorý je použitý v tejto práci.

Deviata kapitola obsahuje navrhnuté laboratórne úlohy, v ktorých sú implementované vybrané s vyššie uvedených prtokolov. Aj keď je úloha tvorená formou krok za krokom, vyžaduje sa od študenta aby chápal základné princípy danej problematiky, pretože nie sú vypísané všetky potrebné príkazy. Návody k laboratórnym

úlohám sa nachádzajú v prílohe diplomovej práce.

1 Smerovanie a smerovacie protokoly

Smerovanie je proces, ktorý používa smerovač na doručenie paketov v sieti z bodu A do bodu B. Smerovač smeruje pakety na základe cieľovej IP adresy, ktorú získa z IP paketu a smerovacích pravidiel, ktoré sa nachádzajú v smerovacej tabuľke smerovača. Poznáme dva typy smerovania a to [30]:

- **Statické smerovanie** – smerovacia tabuľka je konfigurovaná administrátorom.

- **Dynamické smerovanie** – záznamy v smerovacej tabuľke smerovač získa od iných smerovačov prostredníctvom smerovacích protokolov.

1.1 Protokol OSPF

Protokol OSPF (Open Shortest Path First) je otvorený IGP (Interior Gateway Protocol) link – state protokol špecifikovaný v RFC 2328. Link – state protokoly si vytvoria tabuľku topológie siete tzv. Link – state database. Z link – state databázy sa prostredníctvom Djikstrovho SPF (Shortest Path First) algoritmu vypočíta SPF strom, z tohto stromu sa následne vyberajú cesty, ktoré sa uložia do smerovacej tabuľky. Cesty sú vyberané na základe metriky – ceny , ktorá je odvodzovaná od prenosovej rýchlosti linky. Administratívna vzdialenosť OSPF protokolu je 110 [28]. Existujú dve varianty protokolu OSPF a to OSPFv2 pre IPv4 protokol a OSPFv3 pre IPv6 protokol. OSPF protokol si udržuje tri databázy, ktoré sú používané k vytvoreniu troch tabuliek:

- **Adajacency databaze → Neighbor table** – Tabuľka susedných smerovačov obsahuje zoznam všetkých smerovačov, ktoré sú priamo pripojené k danému smerovaču. Táto tabuľka je unikátna pre každý smerovač.

- **Link – State databaze → Topology table** – Obsahuje zoznam všetkých smerovačov v danej sieti (topológiu). Všetky smerovače v rovnakej oblasti majú identickú link – state databázu.

- **Forvarding database → Routing table** – Smerovacia tabuľka obsahuje zoznam ciest do iných sietí. Smerovacia tabuľka je unikátna pre každý smerovač.

1.1.1 Výpočet metriky

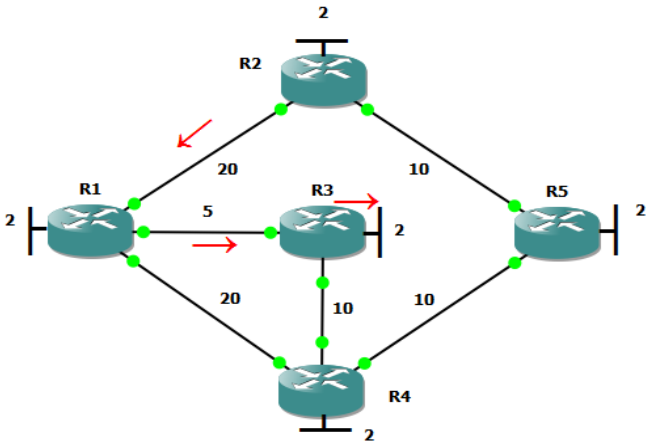
OSPF protokol vypočítava metriku z prenosovej rýchlosti daného portu. Ako referenčnú hodnotu používa rýchlosť 100 Mb/s. Vzorec pre výpočet metriky je, že sa vydelí referenčná hodnota hodnotou daného portu, tabuľka č.1. Ale ak je prenosová rýchlosť väčšia ako referenčná tak výsledná metrika je vždy 1 [28].

Štandard	Prenosová rýchlosť	Metrika
T1	1.554Mb/s	64
E1	2.048Mb/s	48
Ethernet	10Mb/s	10
Fast Ethernet	100Mb/s	1
Gigabit Ethernet	1Gb/s	1
10Gb Ethernet	10Gb/s	1

Tabuľka 1: Štandardy a OSPF metrika.

1.1.2 Djikstrov Algoritmus

OSPF používa Djikstrov algoritmus na zostavenie SFP stromu z ktorého sa následne vyberajú cesty do smerovacej tabuľky. Djikstrov algoritmus hľadá najkratšiu cestu v grafe a to na základe hodnôt jednotlivých hrán grafu, ktoré spájajú jednotlivé vrcholy grafu [28, 27]. Na obrázku č.1 môžeme vidieť príklad grafu kde smerovače predstavujú vrcholy grafu a spoje medzi smerovačmi predstavujú hrany grafu hodnota spoja predstavuje metriku danej linky. Smerovač R2 zvolí cestu k smerovaču R3 cez smerovač R1 a to pretože suma hodnôt jednotlivých ciest je najnižšia. [10]



Obrázok 1: Princíp Djikstrovho algoritmu.

1.1.3 OSPF oblasti

Pre minimalizovanie požiadavkov na výkon operačnej pamäte a procesora OSPF môže rozdeliť topológiu na oblasti [28]. Výhodou rozdelenia topológie na oblasti je že sa minimalizujú záznamy v smerovacej tabuľke a dopad zmeny topológie sa obmedzí len na danú oblasť. Detailné informácie o oblasti sa nešíria za jej hranice. Všetky oblasti musia mať priame spojenie na Oblasť jadra. Typy oblastí:

- **Oblasť jadra** (Area 0) označuje sa aj ako tranzitná oblasť.
- **Štandardné** oblasti:

Stub oblasť – Oblasť do ktorej sa neposielajú správy typu LSA4 a LSA5. Táto oblasť je výhodná vtedy ak pre danú oblasť nieje podstatné aké externé siete existujú a cez aký ASBR (Autonomous System Broder Router) smerovač sú dostupné [28]. Stub oblasť nemá informácie o externých sieťach ani o ASBR smerovačoch, neobsahuje ASBR smerovač.

Totally stuby oblasť – Je to oblasť do ktorej sa nepostielajú LSA3, LSA4 a LSA5. Tento typ oblasti sa používa ak oblasť má jediný ABR. Oblasť nemá informácie o ASBR smerovačoch a externých sieťach [28].

Not – so – stuby oblasť – Táto oblasť má charakter Stub oblasti avšak vyžaduje ASBR smerovač [28].

1.1.4 Smerovače v OSPF

OSPF definuje špeciálne typy smerovačov a to DR (Designated Router) a BDR (Backup Designated Router). DR smerovač plní funkciu centrálneho smerovacieho bodu pre výmenu smerovacej informácie. Ostatné smerovače zasielajú smerovacie informácie na tento smerovač a ten ich zase rozposiela ostatným smerovačom na segmente a do iných segmentov. DR sa volí dynamicky pre každú jednu IP sieť. BDR smerovač je záložný DR smerovač v prípade výpadku smerovača, ktorý plní funkciu DR. Smerovače, ktoré neplnia funkciu DR ani BRD sa nazývajú DROTHERS [28].

Ďalším typom smerovačov, ktoré sú definované v OSPF je ABR (Area Border Router) a ASBR (Autonomous System Boundary Router). ABR smerovač je

smerovač, ktorý je na rozhraní viacerých oblastí, každý ABR smerovač musí byť členom oblasti jadra. ASBR smerovač je smerovač na rozhraní autonómneho systému, plní funkciu filtrátoru a sumarizátoru informácií do OSPF domény [28].

1.1.5 OSPF pakety

Smerovače v OSPF doméne komunikujú prostredníctvom OSPF paketov, ktoré sú zasielané na IP adresu 224.0.0.5 [28] . Typy OSPF paketov:

• **Hello** – Slúži na objavovanie susedných smerovačov a vytváranie susedstva medzi smerovačmy. Ďalej sa tento paket využíva pri voľbe DR/BDR smerovača. Prenáša informácie, ktoré musia medzi dvojicou susedných smerovačou spĺňať isté kritériá:

Číslo oblasti a jej typ musia byť zhodné.

Adresa spoločnej siete a maska musia byť zhodné.

Hello a Dead interval musia byť zhodné.

Hello paket sa posiela každých 10 sekúnd na sieťach typu broadcast a Point – to – Poin, na sieťach typu NBMA a Point – to – Multipoint sa posiela každých 30 sekúnd [28] .
Dead interval je vždy implicitne 4 krát väčší ako hello interval [28].

• **DDP** – Database description paket, slúži pre synchronizáciu databáz medzi smerovačmy. Smerovače komunikujú týmito paketmi vo fáze synchronizácie topologických databáz, kedy si vytvárajú zoznam položiek topologickej databázy, ktoré sú u suseda novšie respektíve tie, ktoré smerovač vôbec nemá [28] .

• **LSR** – Link State Request, žiadosť o konkrétnu položku topologickej databázy od suseda .

• **LSU** – Link State Update, využíva sa na prenos samotnej topologickej informácie.

• **LSAck** – Link State Acknowledgement, slúži pre potvrdenie úspešného prijatia paketu iného typu.

1.1.6 Hlavička OSPF protokolu

Naobrázku č.2 môžeme vidieť 32 bitov dlhú OSPF hlavičku.

Bity	0 -7	8 -15	16 -31
	Verzia	Typ	Dĺžka paketu
	ID smerovača		
	ID oblasti		
	Kontrolný súčet		Typ Autentifikácie
	Autentifikácia		
	Dáta		

Obrázok 2: Hlavička OSPF protokolu

Verzia (1B) – udáva verziu OSPF protokolu.

Typ (1B) – špecifikuje typ OSPF paketu.

Dĺžka paketu (2B) – určuje veľkosť OSPF paketu vrátane hlavičky.

ID smerovača (4B) – obsahuje ID smerovača, ktorý zaslal daný paket.

ID oblasti (4B) – číslo oblasti do ktorej patrý paket, paket môže patriť len do jednej oblasti.

Kontrolný súčet (2B) - kontrolný súčet celého paketu.

Typ Autentifikácie (2B) - určuje použitý typ autentifikácie.

Autentifikácia (8B) - autentifikačné dáta.

1.1.7 LSA správy

LSA (Link State Advertisement) je dátová štruktúra posielaná v LSA paketoch. Popisuje stav rozhrania smerovača, jeho metriku, môže tiež niesť informácie o segmente siete alebo informácie o celej oblasti. Každá LSA správa je tvorená hlavičkou a dátovou časťou. Údaje v hlavičke určujú typ LSA správy (pole LS type), identifikujú smerovač, ktorý zaslal dané LSA [28] . Typy LSA:

• **LSA1** je posielaná každým smerovačom. Popisuje stav jeho rozhrania a k nemu priradenú metriku. Šíri sa len v rámci oblasti.

• **LSA2** je odosielaná len zo smerovača typu DR. Popisuje všetky smerovače pripojené k jednému segmentu siete. Taktiež sa šíri len v rámci oblasti.

• **LSA3** je posielaná hraničným smerovačom oblasti (ABR). Sumarizovane propaguje všetky siete za danú oblasť a prípadne tiež defaultnú cestu. Tento typ LSA je posielaný z jednotlivých oblastí do oblasti 0 a naopak.

• **LSA4** je podobná Network Summary LSA, popisuje cestu k smerovači ASBR.

• **LSA5** je vysielaná z ASBR a popisuje externé cesty re - distribuované do OSPF AS. Šíria sa do všetkých oblastí okrem stub oblasti.

• **LSA6** typ správy, ktorý sa využíva pre multicastové aplikácie.

• $\left[\left((K1)\frac{K2*Bandwith}{Bandwith+256-Load}+(K3*Delay)\right)\frac{K5}{K4+Reliability}\right]*256$ **LSA7** je vysielaná ASBR smerovačom v oblasti typu NSSA. Šíri sa len v rámci tejto oblasti a na ABR smerovači je konvertovaná na správu typu LSA5.

$$(Bandwith+Delay)*256$$

1.2 Protokol EIGRP

Protokol EIGRP (Enhanced Interior Gateway Routing Protocol) je CISCO proprietárny IGP protokol. Je vylepšením protokolu IGRP, oproti svojmu prechodcovy je napríklad rýchlejší pri konvergencií a zasiela len tzv. triggered updates. [13] Je označovaný za distance – vector protokol, aj keď sa dá povedať že je to hybridný protokol, ktorý pre výpočet metriky danej cesty využíva prvky špecifické pre link – state protokoly. Pre výpočet najlepšej cesty do cieľovej siete a zabezpečeniu bez slučkového prostredia využíva algoritmus s názvom DUAL (Diffusing Update Algorithm), niekedy sa označuje ako DUAL FSM (DUAL Finite – State Machine) [14]. Metrika je počítaná na základe K hodnôt. Je to classless protokol, ktorý využívá CIDR a VLMS. Tento protokol tak ako OSPF zostavuje susedstvá zo susednými smerovačmi pomocou hello paketov, aby boli dva smerovače schopné zostaviť susedstvo tak z pohľadu EIGRP musia rozhrania byť v rovnakom EIGRP autonómnom systéme a musia mať rovnaké K hodnoty [6]. EIGRP podporuje rôzne protokoly ako IP, IPX a AppleTalk. EIGRP je schopný rovnomerného aj nerovnomerného loadbalancingu. Protokol si zostavuje dve tabuľky, tabuľku susedov – neighbor table a tabuľku topologickú – topology table. Protokol má dafaultne nastavenú automatickú sumarizáciu sietí, toto však v prípade použitia nekontinuálneho adresného priestoru je nežiadúce, pretože v sumarizovanej adrese sa budú nachádzať aj sieťe, ktoré niesu použité, alebo, ktoré nechceme aby boli smerované do danej destinácie. Preto je zvykom že sa táto funkcia hneď na začiatku konfigurácie vypne. Administratívna vzdialenosť EIGRP je 90 [6].

Neighbor table – tabuľka susedov: je to tabuľka, ktorá obsahuje záznamy o smerovačoch s ktorými bolo nadviazané EIGRP susedstvo. Do tabuľky sa ukladá IP adresa suseda a rozhranie cez ktoré je suesed pripojený.

Topology table – topologická tabuľka: obsahuje záznamy o všetkých cieľových sieťach oznamovaných smerovačmi v EIGRP AS.

1.2.1 Výpočet metriky

EIGRP vypočítáva kompozitnú metriku na základe parametrov danej linky. Medzi tieto parametre patrí:

Delay – oneskorenie [10μs].

Bandwith – šírka pásma [kb/s].

Reliability – spoľahlivosť [1 – 255, 255 je najspolahlivejšie].

Load – zátaž [1- 255, 255 je najvyťaženejší].

Ďalej sú tu takzvané K hodnoty, ktoré sú zahrnuté do výpočtu a ktoré môže užívateľ meniť, a tak ovplivňovať metriku danej cesty, a tak ovplivniť smerovanie. Premenné K majú hodnotu 0 alebo 1, celkovo je päť K hodnôt. Defaultné nastavenie je K1 = K3 = 1, K2 = K4 = K5 = 0. Vzorec pre výpočet metriky je nasledovný [6]:

Keďže K2, K4 a K5 su 0, tak sa nám vzorec vpodstate zjednoduší na [6]:

Takže metrika je dafaultne počítaná zo šírky pásma a oneskorenia danej linky. EIGRP používá pojmy ako successor, feasible successor, reported distance, feassible distance a feasibility condition, ich definícia je nasledovná:

Successor – je to cesta k cieľovej sieti, ktorá sa vloží do smerovacej tabuľky smerovača. Pre danú sieť môže exitovať viacero successorov avšak počet ciest, ktoré sa vložia do smerovacej tabuľky je obmedzený, defaultne je to 4.

Feasible successor – je to druhá najlepšia cesta do cielovej siete, slúži ako záložná cesta v prípade výpadku successor cesty. Neukladá sa do smerovacej tabuľky, ukladá sa do topologickej tabuľky.

Reported distance – je to celková najnižšia metrika do cieľovej siete, je zasielaná susedmy.

Feasible distance – je to reported distance + cena k dosiahnutiu suseda, ktorý zaslal danú RD.

Feasibility condition – je to podmienka pre vytvorenie smerovacieho aparátu bez slučiek. Je využitá pri voľbe successoru a fesible successoru, a udáva ak RD < FD pre danú destináciu tak táto destinácia leží na ceste bez slučiek [13][14][15].

1.2.2 EIGRP pakety

Protokol EIGRP zasiela svoje pakety na multicastovú adresu 224.0.0.10. Typy paketov v EIGRP:

Hello – slúži pre objavovanie susedov, zistenie nefunkčných susedov, je zasielaný periodicky každých 5s, čo je dafaultné nastavenie. Hold time interval pre hello paket je trojnásobok hello intervalu teda 15s [18] [20].

ACK – Slúži pre potvrdzovanie, je to v podstate hello paket bez dát.

Query – Tento paket je zasielaný pri prechode smerovača do aktívneho stavu.

Reply – Je odpoveďou na query.

Update – Prenáša informácie o cestách, na základe jeho obsahu sa zostavuje topologická tabuľka.

1.2.3 Hlavička EIGRP protokolu

Na obrázku č.3 môžeme vidieť hlavičku EIGRP protokolu, je dlhá 32 bitov.

Bity	0 -7	8 - 15	16 -23	24 - 31
	Verzia	Opkód	Kontrolný súčet	
	Príznaky			
	Sekvenčné číslo			
	ACK			
	Číslo autonómneho systému			
	TLV			

Obrázok 3: Hlavička EIGRP protokolu

Verzia (4b) – udáva verziu EIGRP protokolu.

Opkód (4b) – je to štvor bitové pole, ktoré udáva typ EIGRP správy, 1 = Update, 3 = Query, 4 = Reply, 5 = Hello, 6 = IPX SA, 10 = SIA Query, 11 = SIA Reply.

Kontrolný súčet (3B) – kontrolný súčet pre celý paket.

Príznaky (4B) – používajú sa len dva príznaky, a to pri zostavovaní nového susedstva alebo pri použití cisco proprietárneho multicasstového RTP prtokolu.

Sekvenčné číslo (4B) – identifikuje sekvenčné číslo RTP protokolu.

ACK (4B) – je to potvrdenie na prijatý paket, obsahuje jeho sekvenčné číslo.

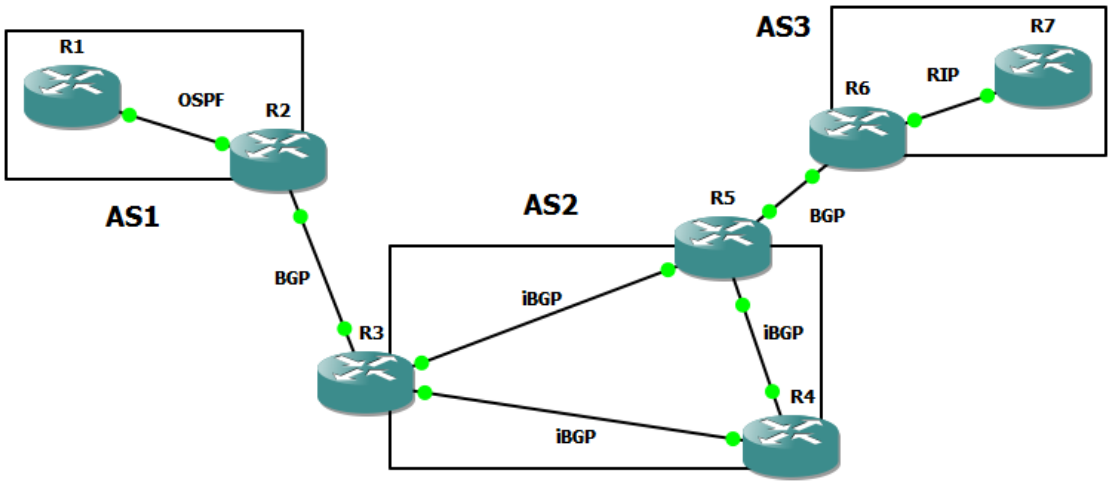
Číslo autonómneho systému (4B) – identifikátor EIGRP domény.

TLV (Type/Lengh/Value 4B) – je to 32 bitové pole, ktoré prenáša informácie o cestách a taktiež aj informácie využívané algoritmom DUAL. Existuje niekoľko typov TLV a to nasledovné [18][19]:

Všeobecné TLV:
0x0001 – EIGRP parametre – K hodnoty a hold time interval.
0x0002 – MD5 autentifikačné dáta.
0x0003 – Sekvencia. Používaná RTP protokolom.
0x0004 – Softvérové verzie IOS a EIGRP.
0x0005 – Nasledovná musticast sekvencia. Používané RTP protokolom.
0x0006 – EIGRP stub parametre.
IP TLVs:
0x0102 – IP interná cesta.
0x0103 – IP externá cesta.

2 Protokol BGP

BGP (Boder Gateway Protokol) – je chrbticový path – vector externý smerovací protokol určený k výmene smerovacích informácií medzi autonómnymi systémamy o sieťach, ktoré tieto autonómne systémy obsahujú. Autonómny sytém je sieť alebo skupina sietí , ktoré maju spoločnú správu a smerovaciu politiku, obrázok č.4.Samotné autonómne systemy používajú vnútorné smerovacie protokoly ako RIP či OSPF. Informácie si predávajú hraničné smerovače tzv. border gateway smerovače pomocou protokolu TCP na porte číslo 179 [2], tieto smerovače sa označujú aj jako „peer“ a samotný prenos informácií ako „peering“. BGP je classless protokol, takže podpoduje prenos informácií o sietach z neimplicitnou maskou. Najnovšia verzia protokolu BGP je 4 (RFC 4271) [3]. Varianta iBGP (internal BGP) slúži pre prenos informácií v rámci jedného autonómneho systému, a to v situácií kedy je potrebné preniest informácie medzi viacerými hraničnými smerovačmy daného AS.



Obrázok 4: Použitie protokolu BGP.

Protokol BGP si v pamäti smerovača vytvára svoju smerovaciu tabuľku Loc – RIB (Local Routing Information Base), táto tabuľka je oddelená od hlavnej smerovacej tabuľky smerovača kde sú záznamy od iných smerovacích prtokolov [2]. Pre každý susedný smerovač s ktorým má nadviazané BGP susuedstvo si udržuje tabuľku Adj – RIB – In (Adjacent Routing Information Base, Incomming), ktorá obsahuje NLRI záznamy oz daného suseda. Ďaľšiu tabuľku, ktorú si udržuje je Adj – RIB – Out (Adjacent Routing Information Base, Outgoing), kde sa nachádzajú NLRI správy pripravené k odoslaniu konkrétnemu susedovy. BGP sa pri smerovaní rozhoduje

na základe týchto parametrov:

• **Počet prechádzaných AS, parameter AS_PATH.**

Administrátorom definované parametre [3]:

- ***Weight (váha).***
- ***Local preference (miestna preferencia).***
- ***Multi Exit Diskriminator (výstupný diskriminátor).***

2.1.1 Hlavička BGP protokolu

Obrázok č.5 nám ilustruje hlavičku BGP protokolu.

Bity	0 - 15	16 - 17	18	ľubovolné
0	Marker	Dĺžka	Typ	Dáta

Obrázok 5: Hlavička BGP protokolu.

Marker (16B) – pole pre kompatibilitu zo staršími verziami BGP prtotokolu.

Dĺžka (2B) – celková dĺžka správy v bajtoch vrátane hlavičky, maximálna dĺžka je 4096 a minimálna je 19 bajtov.

Typ (1B) – obsahuje kód ktorý udáva typ prenášanej správy. Poznáme 4 typy správ:

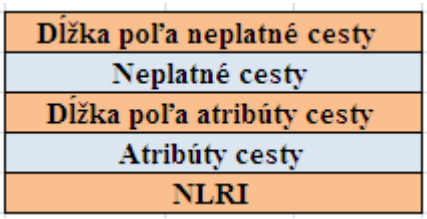
- ***Open*** – je úvodná inicializačná správa zasielaná po utvorení TCP spojenia, prenáša informácie o AS . Táto správa musí byť potvrdená správou typu keep – alive.
- ***Update*** – Obsahuje aktualizáciu smerovacích informácií, označuje sa tiež ako NLRI update.
- ***Notification*** – Správa, ktorá sa používa k zrušeniu TCP spojenia.
- ***KeepAlive*** – Táto správa sa posiela každým 60s a smerovač pomocou nej oznamuje, že je stále aktívny a pracuje.

Dáta – nepovinná časť.

Čerpané bolo zo zdrojov [2], [3], [4].

2.2 Správa NLRI

NLRI (Network Layer Reachability Information Update), (obrázok č.6) je správa, ktorá prenáša aktualizácie smerovacích informácií protokolu BGP. Táto správa je odosielaná len pri zmene dostupnosti siete alebo sietí a pri zmenách topológie. Formát správy NLRI môžeme vidieť na obrázku [22].



Obrázok 6: Správa NLRI.

Dĺžka poľa neplatné cesty (2B) – Pole obsahuje informácie o neplatných cestách. Ak niesú prenášané žiadne cesty tak toto pole má veľkosť 0B.

Neplatné cesty – Je to pole premenlivej veľkosti a obsahuje zoznam ciest do ktorých už daný smerovač nieje schopný smerovať pakety.

Dĺžka poľa atribúty cesty (2B) – Ak je hodnota tohoto poľa 0B tak nasledujúce pole (atribúty cesty) neprenáša žiadne daľšie informácie.

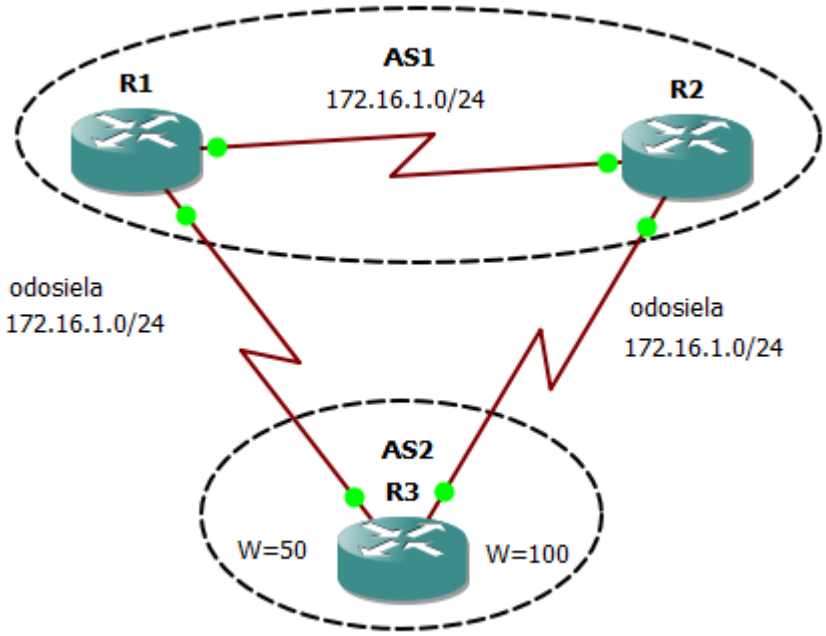
Atribúty cesty – Pole, ktoré prenáša atribúty danej cesty a skladá sa z troch podčastí a to:

- ***typ atribútu.***
- ***dlžka atribútu.***
- ***hodnota atribútu.***

NLRI (*Network Layer Reachability Information*) – Toto pole je premenlivej dĺžky a môže obsahovať jednu alebo viac informácií NLRI [22].

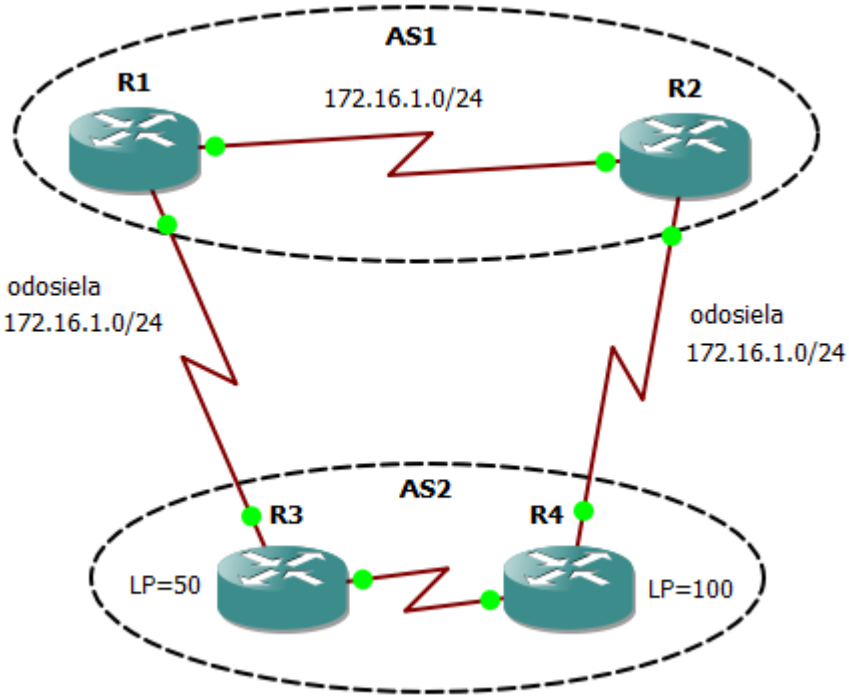
2.2.1 Atribúty cesty

Weight – tento atribút je definovaný spoločnosťou CISCO a slúži k výberu cesty k danému cieľu podľa najvyššej hodnoty weight. Tento atribút sa nešíri mimo daný smerovač. Na obrázku č.7 vidíme princíp atributu weight, smerovač R3 zvolý cestu cez R2 [2].



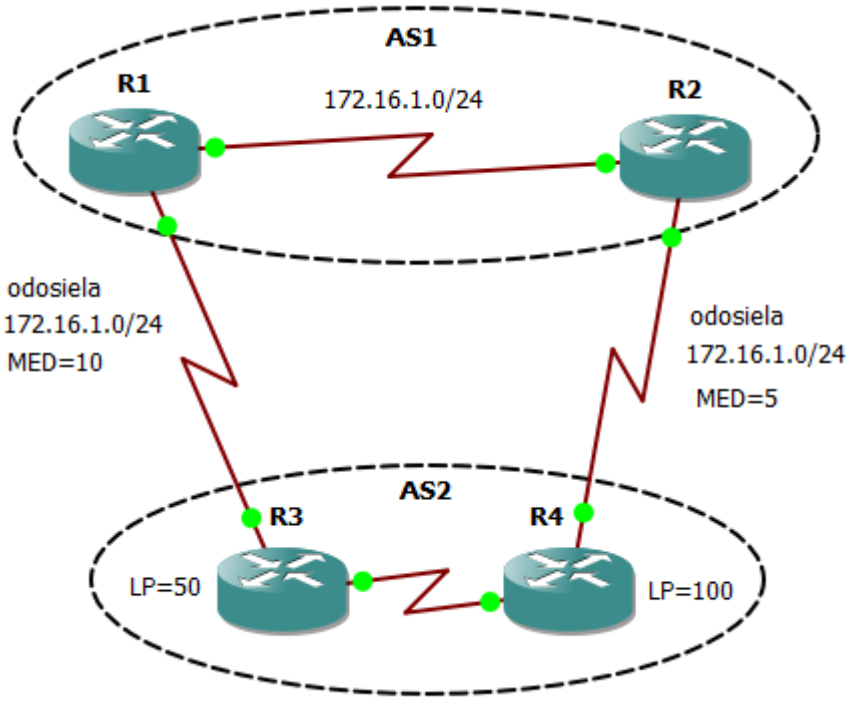
Obrázok 7: Atribút weight BGP protokolu.

Local preference – tento atribút na rozdiel od predchádzajúceho definuje preferovanú cestu v rámci celého AS. Ak existuje viacej ciest z daného AS do cieľa vyberie sa cesta s najväčšou hodnotou local preference, obrázok č.8. Na obrázku vidíme že preferovaná cesta do AS 1 bude cesta medzi smerovačom R4 a R2 [2].



Obrázok 8: Atribút local preference BGP protokolu.

Multi – Exit Diskriminator – Tento atribút ovplivňuje okolité AS pri výbere cesty do daného AS poprípade za daný AS (obrázok č.9). Na obrázku smerovač R1 odosiela sieť 172.16.1.0/24 s MED =10 a smerovač R2 s MED = 5. U atribútu MED je preferovaná menšia hodnota, preto sa zvolí cesta z AS2 do AS1 ako cesta medzi smerovačom R4 a R2. Dôležité je, že hodnota MED sa porovnáva len na linkách, ktoré vychádzajú z rovnakého AS [2].



Obrázok 9: Parameter multi – exit diskriminator BGP protokolu.

Origin – Tento atribút nám hovorý odkiaľ sa informácia o ceste v BGP vzala. Može nadobudnút tri hodnoty: IGP (cesta pochádza z IGP protokolu), EGP (cesta pochádza z externého smerovacieho protokolu EGP) a INCOMLETE (pôvod cesty nieje známy) [2].

AS_PATH – Atribút, ktorý obsahuje reťazec čísiel AS, cez ktoré sa dostaneme k danej sieti. Vyberajú sa tie cesty, ktoré majú kratší AS_PATH. Každy AS cez ktorý daná cesta prechádza pridá svoje číslo na začiatok atribútu AS_PATH [2].

Next hop – Tento BGP atribút je IP adresa, ktorá je využívaná k dosiahnutiu smerovača, ktorý informáciu o ceste do AS zaslal [2].

3 Protokol IPv4

Protokol IPv4 pracuje podľa modelu ISO/OSI na úrovni sieťovej vrstvy. Je to komunikačný protokol, ktorý je nespojovo orientovaný, to znamená, že pred vyslaním paketu sa nenadväzuje virtuálne spojenie medzi komunikujúcimi uzlami. Pracuje na princípe best effort – prioritou je samotné doručenie správy, patrí medzi nespoľahlivé protokoly pretože negarantuje doručenie správ a ich korektnosť, túto funkciu zabezpečujú protokoly vyšších vrstiev (TCP, UDP) [12].

3.1 Adresovanie v IPv4

Protokol IPv4 používa 32 bitové IP adresy. Adresa sa zapisuje po 4 blokoch v decimálnom formáte oddelených bodkami, každý blok obsahuje 8 bitov - oktet. Napr. 192.168.1.1. Iný zápis môže mať podobu napríklad 192.168.1.0/24 , toto je takzvaný slash formát, ktorý nám udáva počet bitov masky siete. IP adresy sa delia na triedy: A, B, C, D a E (tabuľka č.2). Triedy sa od seba odlišujú počtom sietí a počtom koncových staníc, ktoré môžu byť v danej sieti. IP adresy sa ďalej delia na classfull a classless, clasfull adresy majú implicitnú masku. Classless siete využívajú techniku CIDR (Clasless Inter-Domain Routing). Ďalšie delenie IP adries je na verejné IP adresy, ktoré sú smerovateľné v Internete a privátne IP adresy, ktoré sú určené pre LAN siete a niesu smerovateľné v Internete [12] [7].

Trieda	1. Oktet	Implicitná maska	Počet sietí	Počet použitelných IP adries
A	0 – 127	255.0.0.0	128	16777214
B	128 – 191	255.255.0.0	16383	65534
C	192 – 223	255.255.255.0	2097150	254
D	224 - 239	240.0.0.0	Skupinové adresy	16777214
E	240 – 255	240.0.0.0	Experimentálne adresy	16777214

Tabuľka 2: Triedy IP adries as ich vlastnosti

3.2 IPv4 Paket

Na obrázku č.10 môžeme vidieť hlavičku IPv4 paketu, minimálna dĺžka IPv4 hlavičky je 160 bitov [11] [6].

Bity	0-3	4 - 7	8-15	16 - 18	19 - 31
0	Verzia IP	Dĺžka záhlavia	Typ služby	Celková dĺžka (hlavička + dáta)	
32	Identifikácia			Príznaky	Posunutie
64	TTL		Protokol	Kontrolný súčet záhlavia	
96	Zdrojová IP adresa				
128	Cieľová IP adresa				
160	Voliteľné položky				
160/192+	Dáta				

Obrázok 10: Hlavička IPv4 paketu.

Verzia IP (4b) – Slúži pre identifikáciu verzie IP protokolu, v prípade IPv4 pole obsahuje hodnotu 4.

Dĺžka záhlavia (4b) – Udáva veľkosť záhlavia, minimálna dĺžka je 20 bajtov a maximálna 60 bajtov.

Typ služby (8b) – Pole sa využíva pri QoS a udáva prioritu paketu.

Celková dĺžka (16b) – Udáva celkovú veľkosť paketu, hlavička + dáta.

Identifikácia (16b) – Každý paket obsahuje jedinečný identifikátor podľa, ktorého sa identifikujú pakety, ktoré patria k sebe ak bola vykonaná fragmentácia.

Príznaky (3b) – Slúži pre riadenie fragmentácie, keď je bit DF (Don´t Fragment) nastavený na 1, je zakázaná fragmentácia. Ak je bit MF (More Fragments) nastavený na 1 udáva že nasleduje ďalší fragment. Posledný bit sa nevyužíva.

Posunutie (13b) – Udáva na akej pozícií v pôvodnom pakete začína tento fragment, prijímacia strana je na základe tohto poľa schopná znova poskladať fragmentovaný paket.

TTL (8b) – Doba života. Toto pole je ochranou proti zacykleniu paketu v sieti. Každým priechodom smerovača sa hodnota TTL zmenší o 1. Ak je 0 tak sa paket

zahodí. Hodnota TLL je v rozmedzí 0 – 255.

Protokol (8b) – Určuje protokol vyššej vrstvy ktorému sa majú predať dáta po doručení do cieľa. Pole môže obsahovať napríklad hodnoty: UDP 17, TCP 6, EGP 8.

Kontrolný súčet záhlavia (16b) – Slúži k overeniu či nedošlo k poškodeniu paketu pri prenose sieťou, kontrola je vykonávaná pomocou CRC (Cyklická redundantná kontrola) na každom smerovači. Počíta sa z hlavičky a ak nesúhlasí paket je zahodený.

Zdrojová IP adresa (32b) – V poli je uložená IP adresa odosielateľa IP paketu.

Cieľová IP adresa (32b) – V poli je uložená IP adresa príjemcu IP paketu.

Voliteľné položky (32b) – Rôzne rozširujúce informácie a požiadavky.

Dáta – Obsahuje ďalšie zapuzdrené protokoly.

4 Protokol IPv6

Protokol IPv6 je nástupca protokolu IPv4, taktiež je to nespojovo orientovaný protokol, ktorý patrí do tretej vrstvy modelu ISO/OSI.IPv6 bol vyvinutý kvôli nedostatku IP adries ktoré ponúka IPv4. IPv4 ponúka viac ako 4 miliardy adries zatiaľčo IPv6 2^{128} adries. IPv6 obsahuje ďalšie výhody oproti IPv4 a to [11] [22]:

- **Možnosť autentifikácie a kryptografické zabezpečenie.**
- **Mechanizmy pre priame zabezpečenie QoS.**
- **Zjednodušenie formátu záhlavia – menej povinných položiek.**
- **Podpora hierarchického smerovania – redukovanie počtu záznamov v smerovacej tabuľke.**
- **Zníženie hodnoty oneskorenia pri spracovaní paketu v smerovači – neprepočítava sa CRC a nenastáva fragmentácia.**
- **Mobilita staníc.**
- **Nové protokoly ICMPv6 a DHCPv6.**
- **Možnosť väčšej teoretickej dĺžky paketu až 4GB tzv. jumbo pakety.**
- **Jednotná adresná schéma pre celý internet a privátne siete.**
- **Tri druhy adries – individuálne, skupinové a výberové.**
- **Natívna podpora multicastových prenosov.**

Čerpané bolo zo zdroja [11] a [22].

4.1 Adresovanie v IPv6

V IPv6 sú definované tri druhy adresovania, ktoré sa líšia svojím správaním [11] [22].

Individuálne (unicast) – Adresy identifikujúce jednotlivé sieťové rozhrania.

Skupinové (multicast) – Tieto adresy sú určené pre adresovanie skupín. Pakety odoslané na tieto adresy by maly byť doručené všetkým členom skupiny. Tieto adresy zastupujú aj broadcast adresy, ktoré v IPv6 niesu definované.

Výberové (anycast) – Určené taktiež pre skupinu adresátov ale rozdiel je v tom, že pakety sa posielajú iba jednému jej členovi a spravidla tomu, ktorý je najbližšie.

4.1.1 Zápis adries IPv6

Adresy protokolu IPv6 sa zapisujú ako 8 skupín po 4 hexadecimálnych čísliciach oddelených dvojbodkou napríklad [22]:

F0A0:CDF1:0000:0000:0000:0000:A1D2:789F

Ak adresa obsahuje súvislí blok núl tak sa dá použiť skrátený zápis:

F0A0:CDF1::A1D2:789F

Znak „::“ sa smie použiť v zápise len raz. Podobne ako u IPv4 adries je definovaný prefix, ktorý predstavuje adresu siete alebo podsiete. Zápis je nasledovný:

F0A0:CDF1::A1D2:789F/64

4.1.2 Typy adries IPv6

Vrámci IPv6 sú definované špeciálne podtypy adries, tie sú nasledovné:

Lokálna slučka – már rovnaký význam ako v protokole IPv4 umožňuje stanici komunikovať samej zo sebou. Rozdiel oproti IPv4 je ten, že sa jedná o jedinú IP adresu a nie o celý rozsah ako pri IPv4 [22].

Lokálne linkové adresy (fe80::/10) – Má rovnaký význam ako adresy 169.254.0.0/16 u IPv4 protokolu [22]. Jedná sa o adresy s lokálnou platnosťou v rámci danej linky. Tieto adresy sú nastavené u každého aktívneho rozhrania. Pakety s touto adresou

neprejdú cez žiadny smerovač, majú lokálny dosah. Stanica si túto adresu vytvorí automaticky sama a to je jej hlavná výhoda, je vždy k dispozícií. Adresy sú využívané pri komunikácii medzi stanicami cez prepínač. Ďalej sú využívané pri výmene správ medzi klientom a serverom v protokole automatickej konfigurácie DHCPv6.

Lokálne unikátne adresy (fc::/7) – Sú generované lokálne. U týchto adries sa predpokladá že nie sú smerované v internete, majú lokálnu platnosť. Môžu byť použité v prípade keď sa viacero LAN sietí tvári ako jedna LAN sieť. Jedná sa o podobu privátnych adries z IPv4 [22].

Skupinové adresy (ff00::/8) – Slúžia predovšetkým k distribúcií multimediálneho obsahu, ako je zvuk a obraz a to v reálnom čase. Adresa je štrukturovaná na nasledujúce časti. Prvých 8 bitov sú vždy jednotky ďaľšie štyri bitu sú určité voľby, ďalšie štyri bity definujú platnosť adresy a ostatných 112 bitov je vyhradených pre adresu skupiny [22].

Globálne individuálne adresy – sú adresy pre bežné použitie. Principiálne zastupujú verejné IPv4 adresy. Tieto adresy majú pevne danú štruktúru [22] (obrázok č.11).

48 bitov	16 bitov	64 bitov
Globálny smerovací prefix	Identifikátor podsiete	Identifikátor rozhrania
Verejná topológia	Miestna topológia	Lokálna sieť

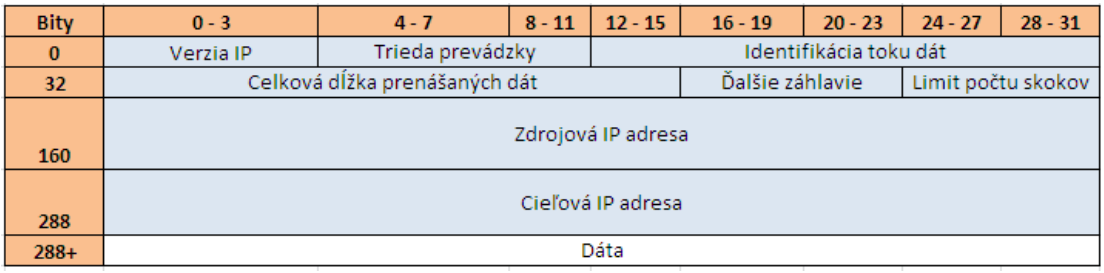
Obrázok 11: Štruktúra IPv6 adresy.

- **Globálny smerovací prefix** – Odpovedá adrese IPv4.
- **Identifikátor podsiete** – Je určený k identifikácií podsietí v rámci celej siete.
- **Identifikátor rozhrania** – Je určený k odlíšeniu koncových staníc v lokálnej sieti.

Výberové adresy – Tieto adresy sú určené pre identifikáciu skupiny staníc. Pakety zaslané na tieto adresy budú doručené najbližšiemu zariadeniu. Najbližšie zariadenie sa určí zo smerovacieho protokolu [22].

4.2 IPv6 Paket

Celková dĺžka záhlavia (obr.č.12) je 40 B a je pevné daná na rozdiel od IPv4 protokolu kde bola dĺžka záhlavia premenná. Záhlavie IPv6 je dvojnásobnej veľkosti. Štruktúra základného záhlavia IPv6 paketu je znázornená na obrázku 12, [22].



Obrázok 12: Hlavička IPv6 paketu.

Verzia IP (4b) – Toto pole udáva verziu IP protokolu, v tomto prípade je hodnota 6.

Trieda prevádzky (8b) – Toto pole umožňuje nastaviť prioritu paketu.

Identifikácia toku dát (20b) – Označuje tok dát, zjednodušuje smerovanie tak, že pakety, ktoré spolu súvisia majú túto hodnotu nastavenú rovnako a smerovač tak môže pakety poslať rovnakou cestou ako predchádzajúce. Hodnota 0 značí že paket nepatrí k žiadnemu toku.

Celková dĺžka prenášaných dát (16b) – Udáva veľkosť prenášaných dát cez hlavičky. Maximálna dĺžka môže byť 64kB.

Ďalšie záhlavie (8b) – Pole odkazuje na protokol vyššej vrstvy.

Limit počtu skokov (8b) – Toto pole odpovedá poľu TTL v IPv4 protokole. Maximálny počet skokov, ktoré smie paket absolvovať.

Zdrojová IP adresa (128b) – IP adresa odosielateľa paketu.

Cieľová IP adresa (128b) – IP adresa príjemcu paketu.

5 Protokol MPLS

MPLS (Multi Protokol Label Switching) je mechanizmus smerovania sieťovej prevádzky medzi uzlami siete na základe návestia (Label) pevnej dĺžky a nie IP adries. Tým sa vynecháva prehľadávanie smerovacích tabuliek a proces je tak oveľa rýchlejší. Návestie neidentifikuje koncové body ako IP adresa ale virtuálne spoje medzi smerovačmi. Ako z názvu vyplýva MPLS môže zapúzdrovať a prenášať rôzne smerovacie protokoly. Hlavnou výhodou MPLS je odstránenie závislosti na technológií linkovej vrstvy ako ATM, Frame Relay, SONET alebo Ethernet. MPLS pracuje na rozhraní 2 a tretej vrstvy modelu ISO/OSI a preto sa často označuje ako vrstva 2,5. Obrázok č.13 znázorňuje hlavičku protokolu MPLS [8], [24].

Bity	1 - 19	20 - 22	23	24 - 31
0	Návestie	EXP: Experimentální (QoS a ECN)	S	TTL

Obrázok 13: Hlavička MPLS protokolu.

Návestie (20b) – číselná hodnota, ktorá predstavuje cieľovú adresu.

EXP (3b) – pole slúži pre experimentálne účely pre QoS (Quality of Service) a ECN (Explicit Congestion Notification) čo predstavuje ochranu proti zahltení siete.

S (1b) – pole, ktorého hodnota označuje posledné návestie.

TTL (8b) – doba života.

5.1 Smerovače v MPLS

LSR (Label Switch Router) – Niekedy sa označuje aj ako tranzitný smerovač alebo aj P – smerovač (Provider) a jeho úloha je prepínanie rámcov na základe návestia a taktiež vykonávajú zmeny návestia medzi jednotlivými skokmi v MPLS sieti. Tieto smerovače sa nachádzajú vnútri MPLS siete. Ak LSR prijme paket, tak podľa návestia obsiahnutého v hlavičke paketu vyhľadá v smerovacej tabuľke cestu kam sa má daný paket poslať a zároveň nové návestie, ktoré nahradí pôvodné [25].

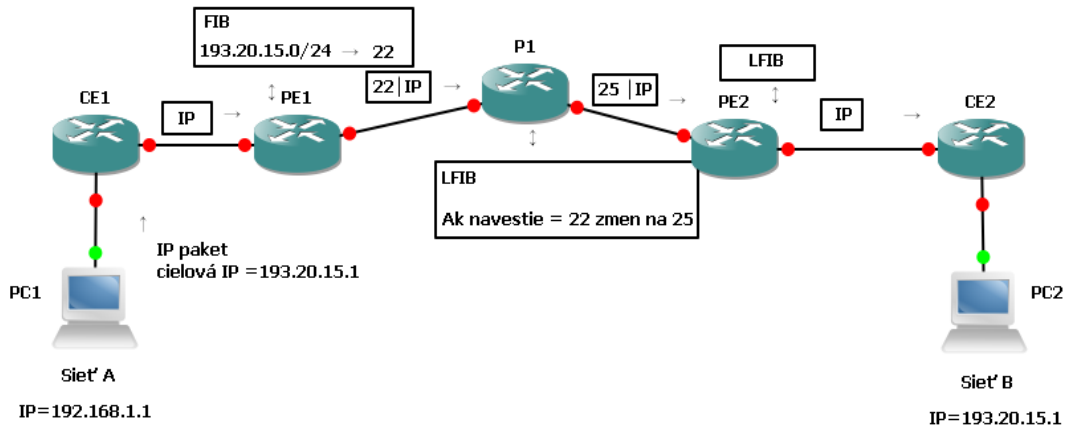
LER (Label Edge Router) – Je to hraničný smerovač, ktorý sa nachádza na hranici MPLS siete a predstavuje vstupný a výstupný bod. Paketom, ktoré prichádzajú do

MPLS siete pridáva návestie a paketom, ktoré opúštajú MPLS sieť ho zase odoberá. Pakety, ktoré opúšťajú MPLS sieť sú potom smerované ďalej podľa štandardných smerovací pravidiel IP protokolu [25].

CE (Customer Edge) – Smerovač, ktorý je na hranici siete zákazníka. Tento smerovač nieje členom MPLS domény.

5.2 Princíp MPLS

Príklad MPLS siete môžeme vidieť na obrázku č. 14, [8], [25].



Obrázok 14: Princíp MPLS protokolu.

1. Stanica 1 vygeneruje paket a odošle paket bez návestia s cieľovou IP adresou 193.20.15.1.

2. Smerovač CE1, ktorý nieje členom MPLS domény odošle paket bez návestia bežnými pravidlami pre smerovanie, teda podľa cieľovej IP.

3. Paket bez návestia príde na smerovač PE1, ktorý už patrí do MPLS domény. Do paketu doplní nové návestie s hodnotou 22 a odošle ho ďalej.

4. Upravený paket s návestím príde na smerovač P1, ktorý prepíše hodnotu návestia na 25 a paket odošle ďalej.

5. Paket s novím návestím príde na smerovač PE2, ktorý odstráni návestia a paket odošle na smerovač CE2.

6. Smerovač CE2 príjme paket a predá ho koncovej stanici PC2. CE2 taktiež nieje členom MPLS domény.

Pri zasielaní paketov využívajú smerovače P a PE databázy FIB a LFIB, tieto databázy obsahujú potrebné informácie k návestiam, informácie o odchodzom rozhraní a ďalšom skoku.

FIB – Slúži pre príchodzie pakety bez návestia. Cisco IOS hľadá zhodu cieľovej IP adresy paketu s najlepším prefixom vo FIB databáze [8].

LFIB – slúži pre príchodzie pakety s návestím. Tu Cisco IOS porovnáva návestia v príchodzom pakete zo zoznamom návestí v LFIB a paket sa odošle podľa takto nájdenej položky v databáze [8].

6 Multicast

Multicast je technika prenosu dát, kde je jeden zdroj dát a veľa koncových staníc, ktoré príjimajú dáta zo zdroja. Multicastový prenos je veľmi efektívny čo sa týka zaťaženia prenosovej kapacity site, pretože sa vysiela len jedna kópia dát, a tá sa podľa potreby kopíruje k jednotlivým členom multicastovej skupiny. Kopírovanie dát vykonávajú smerovače a prepínače, ktoré musia multicastový prenos podporovať. Smerovače si udržujú tabuľku multicastových skupín, ktoré majú byť vysielané koncovým staniciam. Aby koncová stanica mohla prijímať multicastový prenos, musí byť prihlásená do multicastovej skupiny. Toto zabezpečuje protokol IGMP (Internet Group Management Protokol) [1], [2].

6.1 Multicastové adresy IPv4

Pre účlely multicastu bola v IPv4 vyhradená celá trieda D s rozsahom 224.0.0.0 až 239.255.255.255 [22]. Tento rozsah sa ešte ďalej delí, vid tab č.3.

Rozsah IP adries	Popis
224.0.0.0 – 224.0.0.255	Použitie v rámci lokálnej siete
224.0.1.0 – 238.255.255.255	Použitie v rámci internetu
239.0.0.0 – 239.255.255.255	Určené pre privátne použitie

Tabuľka 3: Rozdelenie multicastových adries IPv4.

6.2 Protokol IGMP

Tento protokol súži pre komunikáciu medzi smerovačmi a koncovými stanicami, jeho úlohou je umožnenie pripojenia koncovým staniciam do multicastovej skupiny. Platnosť správ tohoto protokolu je obmedzená len na lokálnu sieť a nie sú smerovateľné v Internete. IGMP protokol existuje v troch verziách, v súčasnosti sa používa verzia 2 definovaná v RFC 2236 [22].

6.2.1 IGMPv2

Verzia 2 protokolu IGMP je v súčastnosti najpoužívanejšia a oproti svojmu predchodcu prináša výhodu v podobe správy, ktorá umožňuje okamžité opustenie multicastovej skupiny. Výhoda tejto správy je v situáciách kedy sa členstvo koncových staníc v multicastovej skupine rýchlo mení. Na obrázku č.15 môžeme vidieť hlavičku protokolu

IGMPv2 [22].

Bity	0 - 7	8-15	16 - 31
0	Typ správy	Časový limit odozvy	Kontrolný súčet
32	Adresa skupiny		

Obrázok 15: Hlavička protokolu IGMPv2.

Typ správy – toto pole nesie údaj o type prenášanej správy. Typy správ môžu byť:

• ***Membership query*** **–** Táto správa predstavuje dotaz na zistenie prijímaných multicastových skupín koncovými stanicami na lokálnej sieti.

• ***Version 2 Membership report*** – Týmto typom správy koncová stanica ohlasuje záujem o pripojenie do multicastovej skupiny.

• ***Version 1 Membership report*** – Táto správa je z prvej verzie protokolu IGMP a používa sa z dôvodu kompatibility a súbehu oboch verzií protokolu.

• ***Leave Group*** – Opustenie skupiny.

• **Časový limit odozvy** – Táto správa je zasielaná koncovým staniciam smerovačom, a obsahuje časový limit v desatinách sekundy pre zaslanie odozvy (membership report) na správu membership query.

• **Kontrolný súčet** – Zabezpečenie paketu, počíta sa z dátovej časti paketu.

• **Adresa skupiny** – Pole nesie informáciu o adrese multicastovej skupiny.

6.3 Protokol PIM

Protokol PIM (Protokol Independent Multicast) je najpoužívanejším protokolom pre smerovanie multicastových prenosov, ktorého úlohou je vytvorenie distribučného stromu či už zdielaného alebo najkratšej cesty. Na zistenie topológie siete využíva informácie od štandardných unicastových smerovacích protokolov. Z názvu je jasné, že tento protokol je nezávislí na unikastovom smerovacom protokole a tak môže bežať nad EIGRP, OSPF alebo RIP protokolom [1]. Protokol PIM má dva režimy a to:

- **PIM Sparse mode.**
- **PIM Dense mode.**

6.3.1 PIM Sparse mode

Pri tejto technike sa predpokladá, že multicast nebude v sieti prevažovať, takže sieť nieje zaplavovaná multicastovým prenosom. Ak chce člen nejakej vetvy siete odoberať multicastový prenos musí zažiadať o členstvo v mulsticastovej skupine pomocou správy PIM join a pre ukončenie odberu musí poslať správu PIM prune. Platí, že správa PIM join sa musí zasielať periodicky. Sparse mode je založený na distribučnom strome zdielaného typu [1] [21].

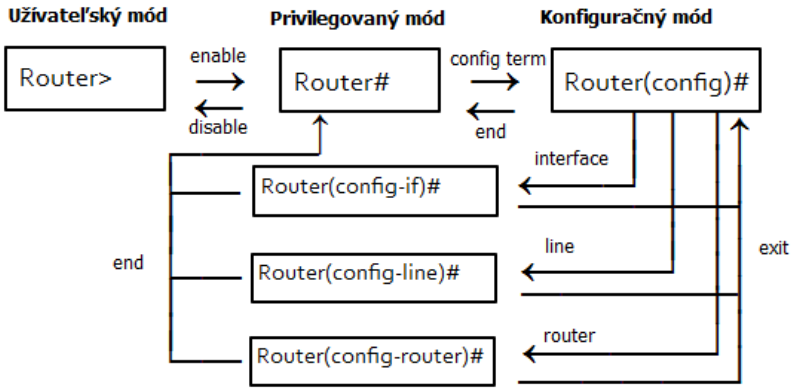
6.3.2 PIM Dense mode

Pri použití módu Sprase sa predpokladá, že v sieti sa nachádza veľa príjemcov multicastového prenosu a sieť je na začiatku zaplavená multicastovým prenosom, v tých segmentoch siete kde sa príjemcovia nenachádzajú je prenos potlačený smerovačmi. Tento mechanizmus funguje tak, že smerovač vetvy v ktorej sa nenachádza žiadny príjemca multicastového prenosu odošle správu susednému smerovaču a prenos do tejto vetvy je zastavený. Tieto správy sú zasielané periodicky každé 3 minúty [1], [22].

7 CISCO IOS

Cisco IOS (Internetwork Operating System) je operačný systém používaný na smerovačoch a prepínačoch spoločnosti Cisco Systems. Tento operačný systém predstavuje balíček smerovacích, prepínacích, prepojovacích a telekomunikačných funkcií. Jednotlivé zariadenia sú konfigurované cez príkazový riadok (IOS CLI), ktorý ponúka užívateľom niekoľko módov (obrázok č.16) a podľa toho v ktorom móde sa užívateľ nachádza má k dispozícií určitú sadu príkazov a určité práva.
Módy CISCO IOS CLI:

- **Konfiguračný mód** – poskytuje príkazy pre zmenu systémovej konfigurácie, "`(config)#`" .
- **Konfiguračný mód rozhrania** – poskytuje príkazy pre zmenu konfigurácie špecifického rozhrania,"`(config-if)#`" .
- **Privilegovaný mód** – umožňuje prístup k úplným informáciám o zariadení a jeho konfigurácií, umožňuje aj reštart zariadenia, "`#`" .
- **Užívateľský mód** – tento mod je východzí a má najmenej možností, ">" .



Obrázok 16: Módy CISCO IOS.

Čerpané bolo zo zdroja [5].

8 Grafický sieťový simulátor GNS3

GNS3 je voľne dostupný softvér pre simuláciu sietí, jednoduchých ale aj komplexných. Pre emulovanie Cisco IOS operačného systému používa Dynamips emulačný softvér. Toto prostredie dokáže emulovať širokú radu smerovačov, prepínačov a zariadení určených pre ochranu siete, na to sa používajú ďalšie emulátory, ktoré sú popísané v ďalšej kapitole. GNS3 sa využíva pri testovaní topológii a konfigurácií pred samotným uvedením do produkcie ale najme pre edukačné účely. To využívajú najme študenti pripravujúci sa na CISCO certifikáciu. Prostredie využíva niekoľko svetových špičkových spoločností ako napríklad: Exxon, Walmart, AT&T, NASA. Toto simulačné prostredie je veľmi obľúbené vďaka svojej prehľadnosti a jednoduchosti [16], [17], [29].

8.1 Emulátory v GNS3

GNS3 používa rôzne typy emulátorov pre simulovanie rôznych zariadení od rôznych výrobcov a platforiem (tabuľka č.3). Na obrázku môžeme vidieť zoznam emulátorov, ktoré podporuje GNS3 [16], [17].

Dynamips	Emulácia CISCO smerovačov
Virtual Box	Emulácia Vyatta a Juniper smerovačov, Linuxových a Windowsových koncových staníc
Qemu	Emulácia Vyatta a Juniper smerovačov, ASA firewallow a Linuxovích koncových staníc
Pemu	Emulácia PIX firewallow, je to variácia Qemu

Tabuľka 4: Emulátory v GNS3.

Kedže v tejto práci sa budeme venovať simulácií CISCO sietí tak je pre nás najdôležitejší Dynamis emulátor, ktorý dokáže emulovať CISCO IOS. Tento emulátor je kompatibilný s operačnými systámamy jako Linux a Windows. Úloha dynamipsu spočíva v prekladaní inštrukcií IOS operačného systému, ktoré sú určené pre procesory tipu MIPS (Microprocessor Without Interlocked Pipeline Stages) na inštrukcie, ktoré sú kompatibiliné s procesormi Intel a AMD používaných v bežných počítačoch.

Nevýhoda Dynamipsu a GNS3 je, že nedokáže plnohodnotne simulovať prepínače a to z dvôvodu, že sa nedajú emulovať špeciálne procesory tipu ASIC (Application Specific Integrated Circuit), ktoré tieto zariadenia používajú. Tento problém sa rieši

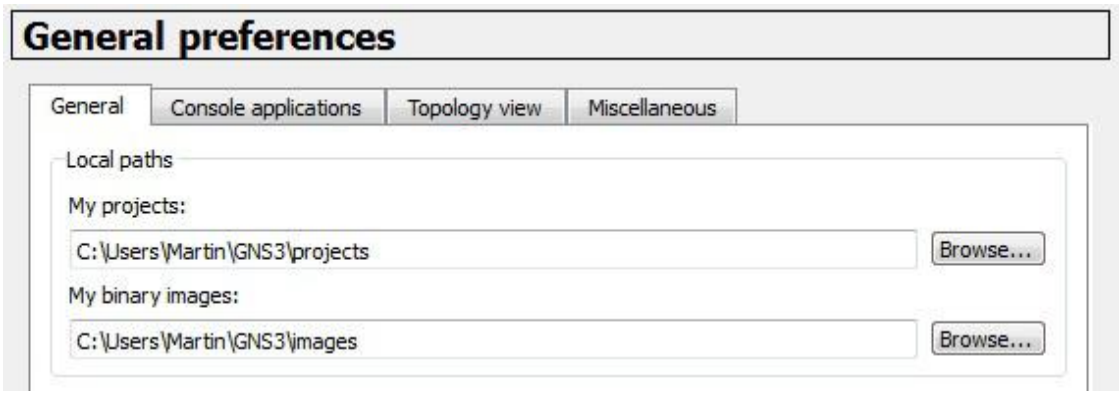
prostredníctvom smerovača, ktorému osadíme modul EtherSwitch a takto prispôsobený smerovač využívame ako prepínač. Avšak takto upravený smerovač nám nikdy neposkytne funkcie plnohodnotného prepínača [16], [17], [29].

9 Praktická realizácia

Laboratórne úlohy sú tvorené vo verzií GNS3 1.3.10, operačný systém na, ktorom boli úlohy tvorené je Windows 7 64bit. GNS3 si môžeme stiahnuť na stránke https://www.gns3.com/software/download, je nutné sa najskôr registrovať. IOS pre daný typ smerovača si môžeme stiahnuť napríklad tu: http://srijit.com/working-cisco-ios-gns3/.

9.1 Nastavenie prostredia GNS3

Všetky dôležité nastavenia sa vykonávajú cez položku Edit v ľavom hornom rohu. Následne z kontextového menu vyberieme položku preferences zobrazí sa nám okno s nastavením ciest ukladania projektov a cesta k IOS imidžom (obrázok č.17).

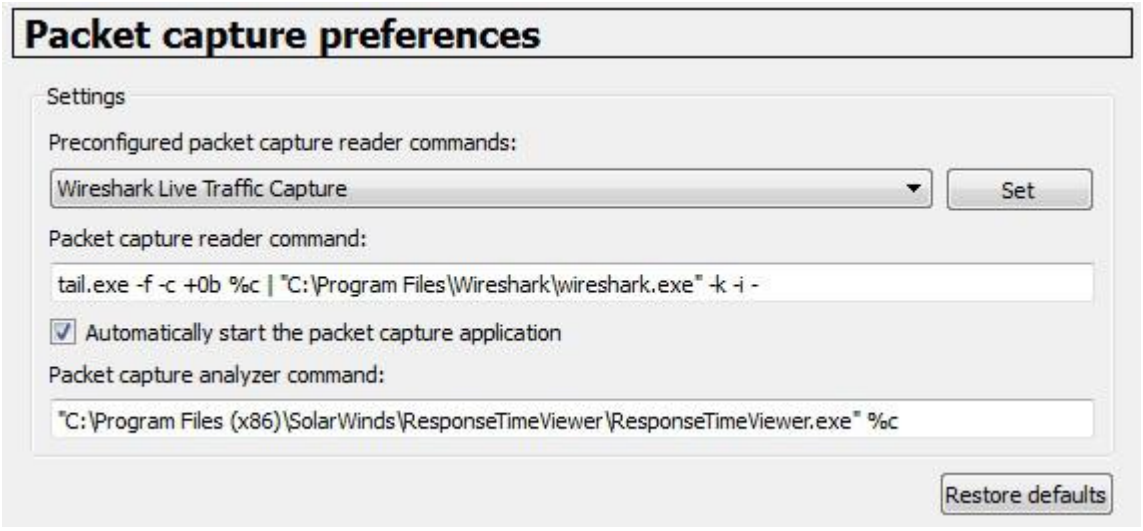


Obrázok 17: GNS3 Všeobecné nastavenia.

Tu si každý študent nastaví svoj vlastný adresár. Záložky Console applications, Topology view a Miscellaneous, nemeníme a ponecháme im defaultné nastavenia.

9.1.1 Nastavenie zachytávania paketov

Podrobnú analýzu paketov môžeme vykonávať pomocou programu Wireshark Tento program je súčasťou prostredia GNS3. Prepneme sa do položky Packet capture z ľavého menu (obrázok č.18).

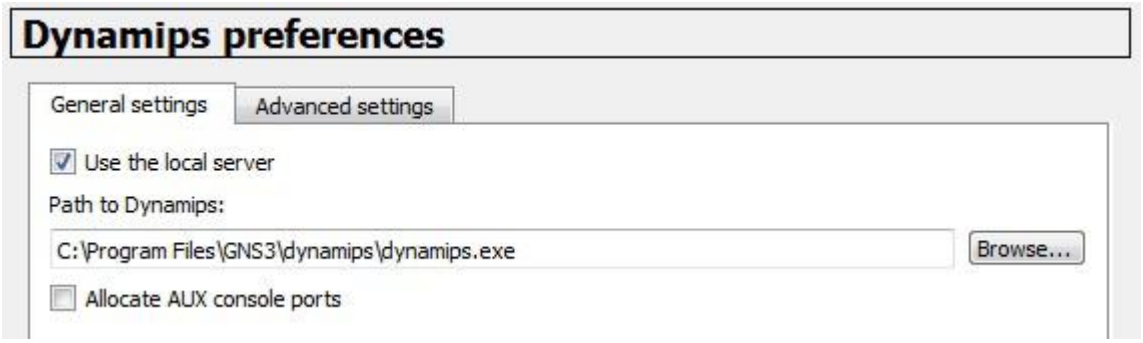


Obrázok 18: GNS3 Nastavenie zachytávania prevádzky.

Tu zvolíme možnosť Wireshark Live Traffic Capture. Ostatné položky sa doplnia automaticky.

9.1.2 Nastavenie Dynamips

Prepneme sa do položky Dynamips v ľavom menu.Tu sa prepneme do Advanced settings (obrázok č.19 a č. 22). A zvolíme všetky možnosti, ktoré nám okno ponúka.



Obrázok 19: GNS3 Nastavenie Dynamips 1.

Obrázok 20: GNS3 Nastavenie Dynamips 2.

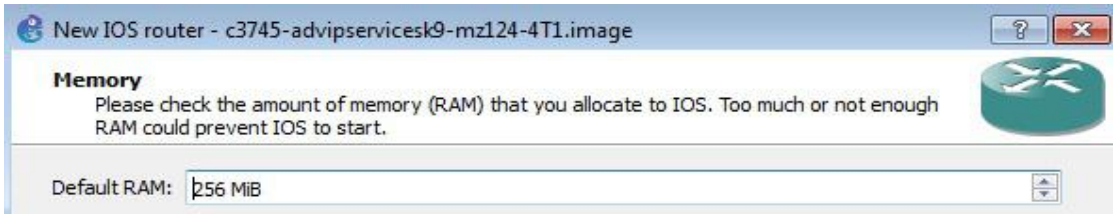
9.1.3 Import IOS imidžu

Súbory operačných systémov smerovačov, ktoré chceme používať rozbalíme aby mali príponu .image a uložíme do zložky, ktorá je popísaná v kapitole 9.1.

Každý IOS image je určený pre konkrétny typ smerovača a priradíme ho danému typu smerovača nasledovne. Vľavom menu zvolíme Dynamips → IOS routers. Ďalej zvolíme New, tu vyberieme náš IOS Imidž, klikneme na Next, tu zvolíme model smerovača (Platform) pre daný IOS (obrázok č. 21).

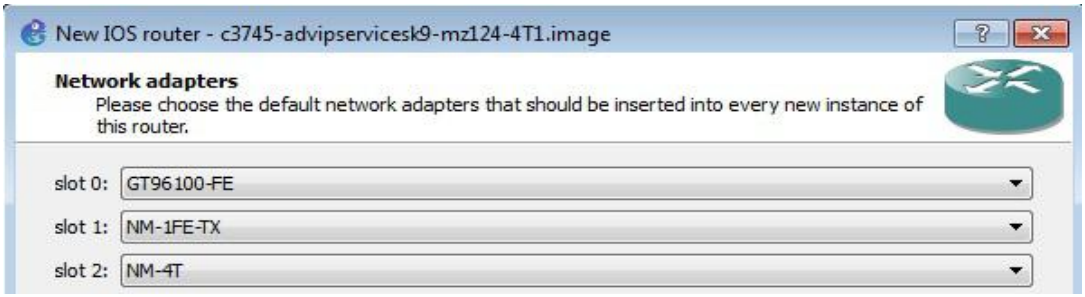
Obrázok 21: GNS3 Import ISO imidžu.

Ďalej klikneme na Next, tu sa nám zobrazí okno s nastavením výpočetných zdrojov pre daný smerovač, GNS3 mám ponúka defaultnú hodnotu na základe typu smerovača (obrázok č.22).



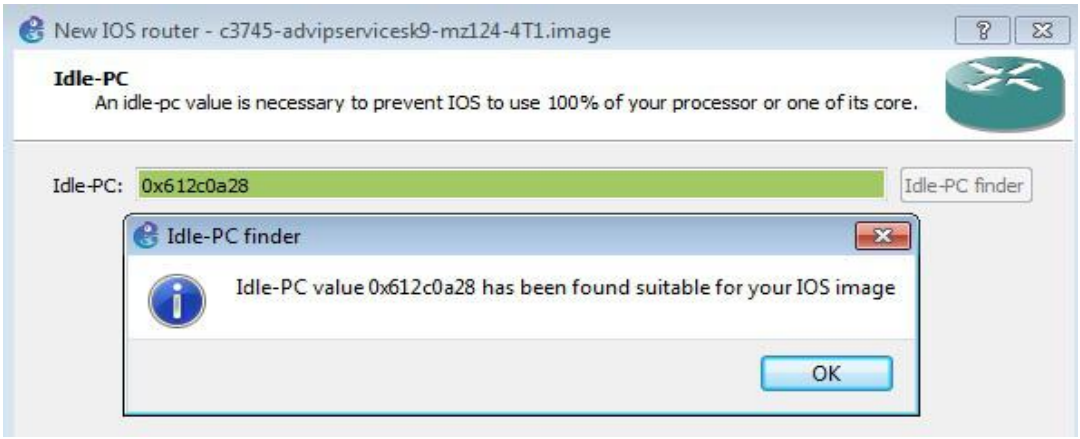
Obrázok 22: GNS3 Nastavenie RAM.

Ponecháme tam defaultnú hodnotu a klikneme na Next. V ďalšom okne si vyberieme, ktoré hardvérové moduly bude náš smerovač obsahovať. Zvolíme moduly GT96100-FE, NM-1FE-TX a NM-4T (obrázok č.23).



Obrázok 23: GNS3 Nastavenie hardvérových modulov.

Ďalej klikneme na Next. V tomto okne sa nastavuje hodnota Idle-PC, klikneme na Idle-PC finder a GNS3 nám vygeneruje optimálnu hodnotu. Táto hodnota je dôležitá pre optimálny chod a využívánie výpočtových prostriedkov fyzickej stanice na ktorej beží symulátor GNS3 (obrázok č.24).



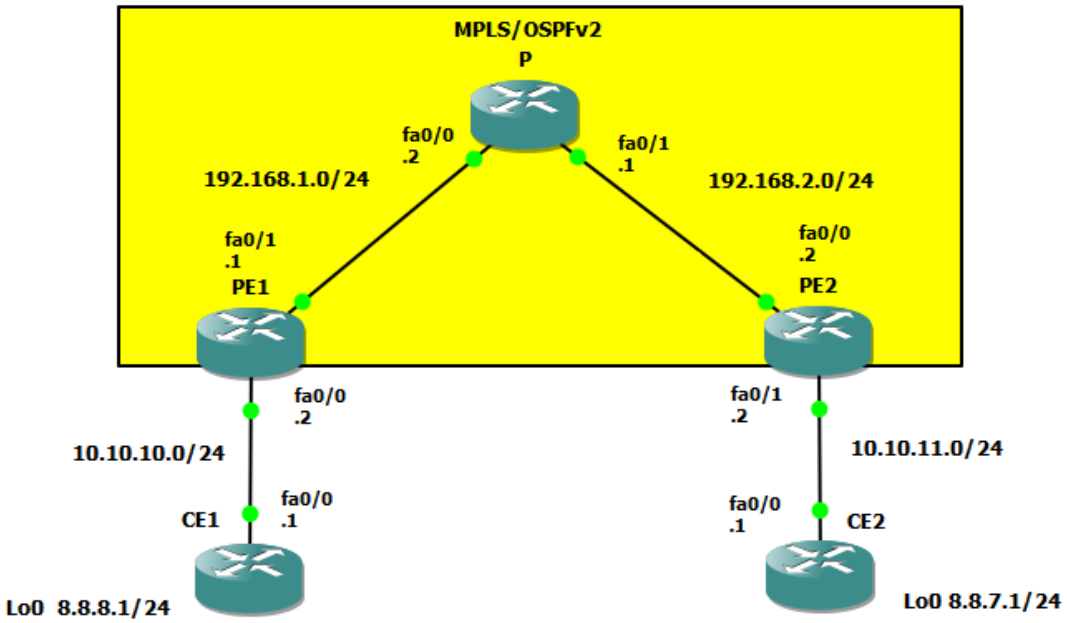
Obrázok 24: GNS3 Nastavenie hodnoty Idle-PC.

V poslednom kroku likneme na OK a na Finish, prostredie je týmto nastavné.

9.2 Laboratórne úlohy

9.2.1 Laboratórna úloha 1

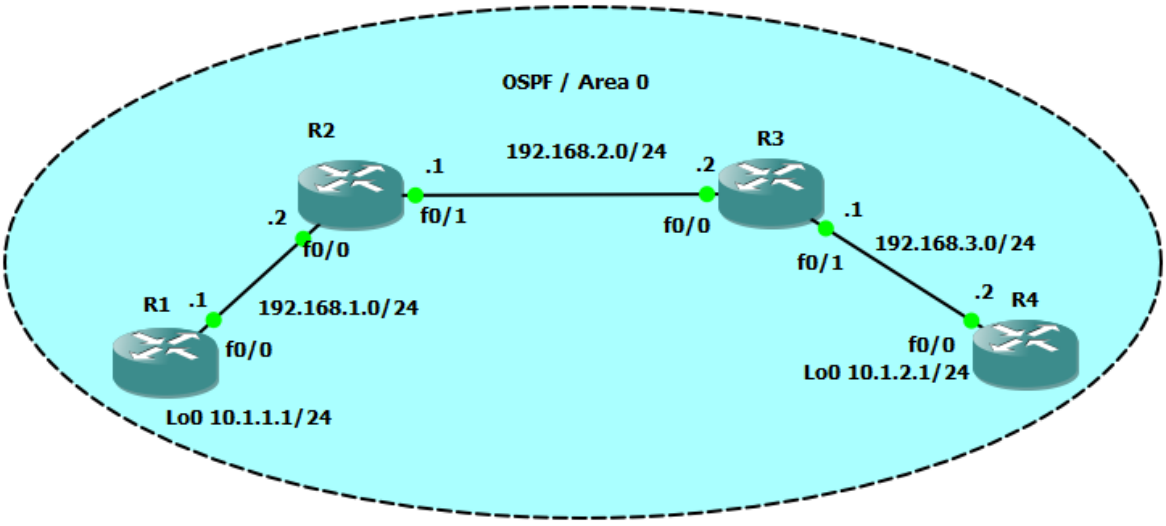
Na obrázku č. 25 môžeme vidieť topológiu laboratórnej úlohy č. 1. Táto úloha je zameraná na konfiguráciu protokolu MPLS so smerovacím protokolom OSPF. Úloha začína teoretickým úvodom, ktorý zoznamuje s protokolom MPLS. Ďalej nasledujú štyri úlohy. V prvej sa konfiguruje smerovací protokol OSPF a adresy. V druhej časti sa konfiguruje samotný MPLS protokol. Tretia časť sa venuje autentizácií v MPLS. Posledná štvrtá časť je samostatná úloha, ktorá sa zaoberá prepojením IPv6 koncových oblastí cez IPv4 jadro, kedy sa medzi smerovačmi PE1 – CE1 a PE2 – CE2 nakonfiguruje IPv6 protkol. Úlohou je sfunkčniť komunikáciu medzi týmito oblasťami cez IPv4 jadro mopocou metódy 6PE. Úlohu nasleduje jej riešenie, ktoré je určené pre vyučujúceho. Úloha je zakončená kontrolnými otázkami, ktoré slúžia na overenie získaných znalostí z danej problematiky protokolu MPLS.



Obrázok 25: Topológia Laboratórnej úlohy 1.

9.2.2 Laboratórna úloha 2

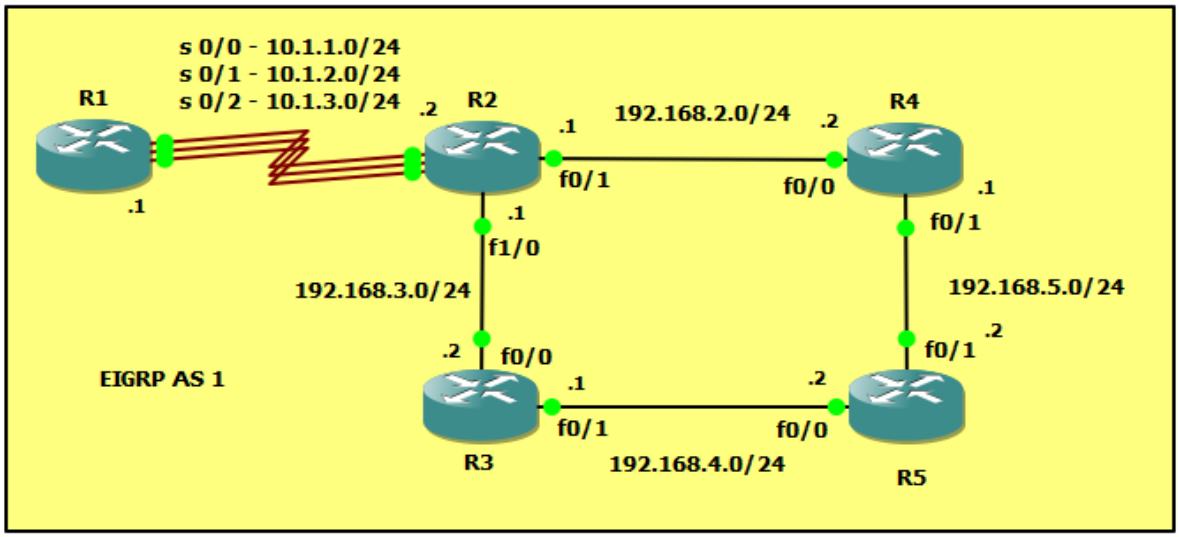
Úloha je zameraná na praktické vlastnosti protokolu OSPF. Laboratórna úloha má šesť častí. V prvej sa konfigurujú adresy, dalšia časť sa venuje konfigurácií OSPF protokolu a popisuje voľbu DR smerovača. Tretia časť sa zaoberá ovplivnením výberu DR/BDR smerovača, zmenou odosielanej masky v smerovacích updejtoch, časovačom a autentizáciou v OSPF protokole. Tieto try čiastkové úlohy sa vykonávajú v konfigurácií ktorú vidíme na obrázku č. 26, toto je základná konfigurácia, ktorá sa v daľších častiach mení. V štvretj časti sa zaoberáme sumarizáciou a rozosielaním defaultnej cesty. Pre zejdnodušenie sú použité len smerovače R1 a R2. Oblasť 0 je len medzi týmito smerovačmi. Na R2 je nakonfigurovaná oblasť 11 do ktorej patria loop-back rozhrania, obr. č. 29. Piata časť laboratórnej úlohy sa venuje technike virtuálnej linky a konfirugácií viacerých oblastí v rámci topológie. Technika virtuálnej linky slúži na prepojenie oblastí, ktoré niesu priamo prepojené s oblaťou 0 práve s touto oblasťou. Ďalej sa táto časť venuje podrobnému rozboru OSPF databázy. Posledná časť je samostatná uloha, v ktorej sa vyžaduje aby študenti prišli na zmenu konfigurácie, ktorá zabezpečí že smerovač R4 bude vo svojej smerovacej tabuľke obsahovať len defaultnú cestu zasielanú smerovačom R1. Úlohu nasleduje jej riešenie, ktoré je určené pre vyučujúceho. Laboratórna úloha je zakončená kontrolnými otázkami.



Obrázok 26: Topológia laboratórnej úlohy 2

9.2.3 Laboratórna úloha 3

Na brázku č. 27 vidíme topológiu laboratórnej úlohy č. 3, táto úloha je zameraná na vlastnosti protkolu EIGRP a redistribúciu medzi OSPF a EIGRP. Úloha sa skladá zo šiestich častí, v prvej sa konfigurujú adresy. V druje časti sa konfiguruje protokol EIGRP, táto časť obsahuje rozbor EIGRP databázy. Ďaľšia časť sa venuje autentizácií v EIGRP, nedesruptivnou zmenou hesla a zmenou časovačov. Štvrtá časť sa zaoberá failoverom liniek medzi smerovačmi R1 a R2, ďaľej úpravou metriky a load – balancingom. Predposledná časť sa zaoberá redistribúciou medzi smerovacím protokolom EIGRP a OSPF, kedy sa na rozhraniach fa0/0 smerovača R4 a fa0/1a Lo0 na smerovači R5 nakonfiguruje protokol OSPF. Posledná časť je samostatná úloha zameraná na riadenie toku dát zmenou parametru delay vo výpočte metriky. Nasleduje riešenie samostatnej úlohy, ktoré je určené pre vyučujúceho a slúži na kontrolu riešenia študentov tejto samostatnej úlohy. Úloha je zakončená kontrolnými otázkami z problematiky EIGRP protokolu.



Obrázok 27: Topológia laboratórnej úlohy 3

10 ZÁVER

Táto diplomová práca je zameraná na teoretický rozbor protokolov OSPF, EIGRP, MPLS, BGP, IPv4, IPv6 a Multicastu. Ďalej je práca zameraná na sieťové simulačné prostredie GNS3 v ktorom sú navrhnuté a implementované tri laboratórne úlohy, ktorých hlavné zameranie je na praktické vlastnosti a použitie protokolov MPLS, OSPF a EIGRP s využitím protokolov IPv4, IPv6 a BGP. V úlohách je použitý CISCO smerovač 3745. Úlohy majú niekoľko častí v ktorých sa konfigurujú rôzne praktické vlastnosti daných protokolov, sú písané formou kuchárky teda krok za krokom. Avšak každá úloha obsahuje samostatnú časť, ktorá obsahuje len zadanie a študenti si zo zadaným problémom musia poradiť sami. Za zadaním problému nasleduje jeho riešenie, ktoré je určené len pre vyučujúceho. Každá laboratórna obsahuje obrázok topológie a je zakončená niekoľkými otázkami z danej problematiky na ktoré by študenti maly byť schopný odpovedať po absolvovaní úlohy. Každá úloha obsahuje výpisy z príkazového riadku smerovačov kde sú zobrazené, vysvetlené a okomentované rôzne nastavenia, paramatre a databázy daných protokolov.

Prvá laboratórna úloha sa zaoberá protokolom MPLS, obsahuje jeho základnú konfiguráciu a konfiguráciu autentizácie v MPLS. V tejto časti sa študenti zoznámily s praktickými vlastnosťami tohto protokolu. Samostatná časť úlohy sa zaoberá použitím protokolu IPv4 na koncových smerovačoch, ktoré komunikujú naprieč IPv4 jadrom pomocou metódy 6PE.

Druhá laboratórna úloha je zameraná na protokol OSPF. Obsahuje základnú konfiguráciu, konfiguráciu autentizácie, ovplinenie výberu DR a BDR smerovača, konfiguráciu virtuálnej linky, sumarizáciu na ABR smerovači. Úloha obsahuje podrobný rozbor OSPF topologickej databázy. Samostatná časť úlohy sa zaoberá zmenou typu oblasti na totally stuby a dopad tejto zmeny na obsah smerovacej tabuľky.

V tretej laboratórnej úlohe sa konfiguruje protokol EIGRP. Úloha obsahuje kofiguráciu autentizácie, nedisruptívnu zmenu hesla na linke, fail-over liniek, rovnomerný a nerovnomerný loadbalancing, úpravu metriky, zmenu časovačov a časť je venovaná redistribúcií smerovacích informácií medzi OSPF a EIGRP. Úloha taktiež obsahuje rozbor EIGRP topologickej databázy. Samostatná časť úlohy sa zaoberá riadením toku dát zmenou parametru delay vo výpočte metriky.

Študenti by maly byť schopný každú úlohu zvládnuť v časovom rámci dve hodiny.

11 LITERATÚRA

[1] 2005_08_21_36977_2.htm. *Multicast* . [online]. 22.9.2015 [cit. 2015-11-29]. Dostupné z: *http://www.net130.com/CMS/Pub/network/network_protocal/2005_08_21_36977_2.html*

[2] BGP Case Studies. CISCO. *Configuration Example and TechNotes* [online]. 2008 [cit. 2015-11-29]. Dostupné z: http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html.

[3] Border Gateway Protocol (BGP). CISCO. *Internetworking Technology Handbook* [online]. 2010 [cit. 2015-11-29]. Dostupné z: http://docwiki.cisco.com/wiki/Border_Gateway_Protocol.html.

[4] Border Gateway Protocol. CISCO. *Docwiki.cisco* [online]. 2009 [cit. 2015-11-29]. Dostupné z: http://docwiki.cisco.com/wiki/Border_Gateway_Protocol.

[5] Cisco IOS softver. CISCO NETWORKING ACADEMY. *Cisco Academy Aspone* [online]. 2008 [cit. 2015-11-29]. Dostupné z: http://cisco-academy.aspone.cz/cisco-ios-softver.html

[6] Cisco Routing 2 – EIGRP – Enhanced Interior Gateway Routing Protocol. *http://www.samuraj-cz.com.* [online]. 29.03.2009 [cit. 2016-04-05]. Dostupné z: *http://www.samuraj-cz.com/clanek/cisco-routing-2-eigrp-enhanced-interior-gateway-routing-protocol/*

[7] Configuring IPv4 Addresses. CISCO. *IP Addressing: IPv4 Addressing Configuration Guide, Cisco IOS XE Release 3S* [online]. 2008 [cit. 2015-11-29]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_ipv4/configuration/xe-3s/ipv4-xe-3s-book/configuring_ipv4_addresses.html

[8] Configuring Basic MPLS Using OSPF. CISCO. *CISCO* [online]. 2005 [cit. 2015-11-29]. Dostupné z: http://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13736-mplsospf.html

[9] Configuring BGP. CISCO. *Cisco IOS IP Configuration Guide, Release 12.2* [online]. 2008 [cit. 2015-11-29]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfbgp.html.

[10]Configuring OSPF. CISCO. *IP Routing: OSPF Configuration Guide, Cisco IOS Release 12.4T* [online]. 2005 [cit. 2015-11-29]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios-

xml/ios/iproute_ospf/configuration/12-4t/iro-12-4t-book/iro-cfg.html

[11] Configuring IPv6 Routing. CISCO. Catalyst 3750 Software Configuration Guide, Release 12.2(55)SE [online]. 2008 [cit. 2015-11-29]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750/swipv6.html

[12] DOSTÁLEK, Libor a Alena Kabelová. Velký průvodce protokoly TCP/IP a systémem DNS, 2. aktualizované vydání. Praha: Computer Press, 2000. ISBN 80-7226-323-4.

[13] EIGRP. *http://cisco-academy.aspone.cz.* [online]. 2008 [cit. 2016-04-05]. Dostupné z: *http://cisco-academy.aspone.cz/eigrp.html*

[14] EIGRP Neighbor, Routing and Topology Tables. *http://www.certiology.com.* [online]. [cit. 2016-04-05]. Dostupné z: *http://www.certiology.com/tutorials/eigrp-tutorial/eigrp-neighbor-and-topology-table-explained.html*

[15] Enhanced Interior Gateway Routing Protocol. *http://www.cisco.com.* [online]. 5.1.2015 [cit. 2016-04-05]. Dostupné z: *http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html*

[16] GNS3 Initial Configuration. PLURALSIGHT. GNS3 Tutorial [online]. 2014 [cit. 2015-11-29]. Dostupné z: http://blog.pluralsight.com/gns3-initial-configuration

[17] Hardware emulated by GNS3. GNS3. GNS3 Jungle [online]. 2014 [cit. 2015-11-29]. Dostupné z: https://community.gns3.com/docs/DOC-1708

[18] How EIGRP Works. *safaribooksonline.com.* [online]. [cit. 2016-04-05]. Dostupné z: *https://www.safaribooksonline.com/library/view/ip-routing/0596002750/ch04s03.html*

[19] How Does Unequal Cost Path Load Balancing (Variance) Work in IGRP and EIGRP?. *http://www.cisco.com.* [online]. 3.6.2009 [cit. 2016-04-05]. Dostupné z: *http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13677-19.html*

[20] Introduction to EIGRP. *http://www.cisco.com.* [online]. 10.8.2005 [cit. 2016-04-05]. Dostupné z: *http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.html*

[21] IP Multicast Technology Overview. CISCO. Technology White Paper [online]. 2001 [cit. 2015-11-29]. Dostupné z: *http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html*.

[22] JEŘÁBEK, Ing. Jan Ph.D. Pokročilé komunikační techniky [online]. 2014, [cit. 2014-10-13]. Dostupné z : <https://www.vutbr.cz/www_base/priloha.php?dpid=67088>.

[23] Konfigurovanie routra. CISCO NETWORKING ACADEMY. Cisco Academy Aspone [online]. 2008 [cit. 2015-11-29]. Dostupné z: http://cisco-academy.aspone.cz/konfigurovanie-routra.html

[24] MPLS: Configuration Examples and TechNotes. CISCO. CISCO [online]. 2009 [cit. 2015-11-29]. Dostupné z: http://www.cisco.com/c/en/us/tech/multiprotocol-label-switching-mpls/mpls/tech-configuration-examples-list.html

[25] Multiprotocol Label Switching (MPLS). CISCO. CISCO [online]. 2011 [cit. 2015-11-29]. Dostupné z: http://www.cisco.com/c/en/us/products/ios-nx-os-software/multiprotocol-label-switching-mpls/index.html

[26] Multiprotocol Label Switching (MPLS) on Cisco Routers. CISCO. MPLS Basic MPLS Configuration Guide, Cisco IOS XE Release 3S [online]. 2009 [cit. 2015-11-29]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_basic/configuration/xe-3s/mp-basic-xe-3s-book/mp-mpls-cisco-rtrs.html

[27] OSPF commands. CISCO. *CISCO* [online]. 2006 [cit. 2015-11-29]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfospf.html

[28] OSPF Design Guide. CISCO. Cisco IOS IP Configuration Guide, Release 12.2 [online]. 2005 [cit. 2015-11-29]. Dostupné z: http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

[29] Quick Start Guide for Windows Users. GNS3. GNS3 Jungle [online]. 2014 [cit. 2015-11-29]. Dostupné z: https://community.gns3.com/docs/DOC-1751

[30] Smerovanie a smerovacie protokoly. CISCO ACADEMY. Cisco Academy Aspone [online]. 2008 [cit. 2015-11-29]. Dostupné z: http://cisco-academy.aspone.cz/smerovanie-a-smerovacie-protokoly.html.

12 ZOZNAM ZKRATIEK

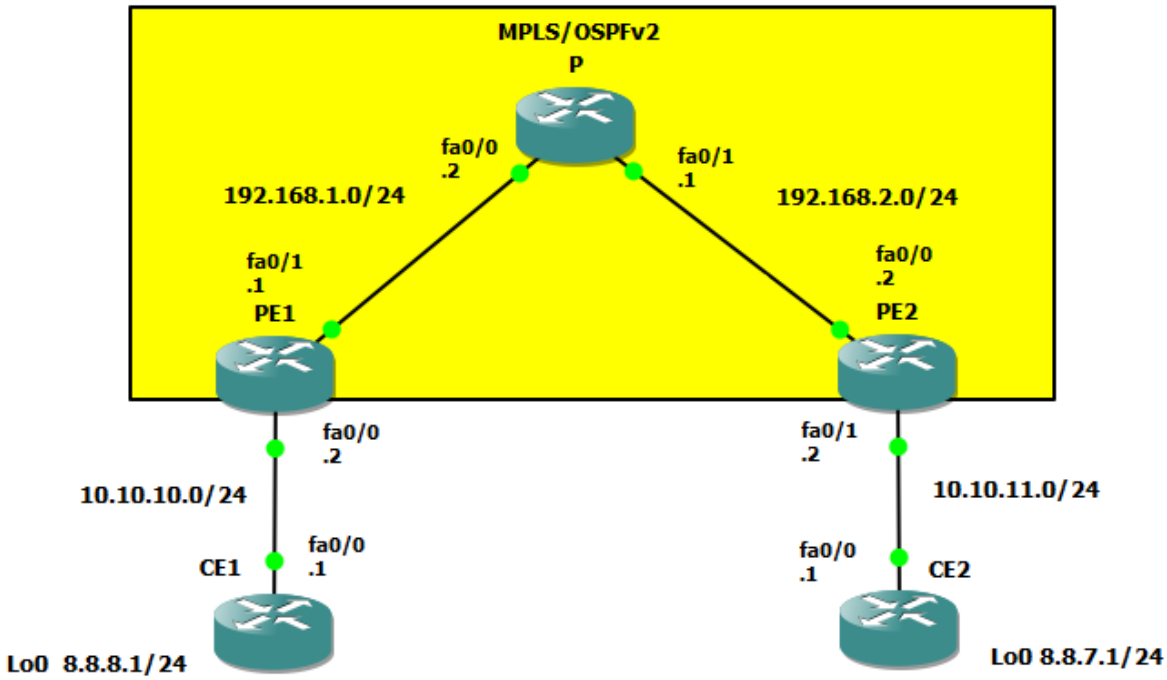
ABR	Area Border Router
ACK	Acknowledgement
AS	Autonomous system
ASBR	Autonomous System Border Router
ASIC	Application Specific Integrated Circuit
ATM	Asynchronous Transfer Mode
AT&T	American Telephone and Telegraph
BDR	Backup Designaed Router
BGP	Border Gateway Protocol
CE	Customer Edge
CIDR	Clasless Inter – Domain Routing
CLI	Command Line Interface
CRC	Cyclic Redundacy Check
DDP	Data Description Packet
DF	Do Not Fragment
DHCP	Domain Host Configuration Protocol
DR	Designated Router
DUAL	Difusing Update ALgorithm
ECN	Explicit Congestion Notification
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
FD	Feasible Distance
FIB	Forwarding Information Base
FSM	Finite State Machine
GNS	Graphical Network Simulator
iBGP	Internal Border Gateway Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IOS	Internetwork Operating System
IP	Internet Protocol
LAN	Local Area Network
LER	Label Edge Router
LFIB	Label Forwarding Information Base
LSA	Link State Advertisment
LSAck	Link State Acknowledgement
LSR	Label Switch Router
LSU	Link State Update
MED	Multi Exit Discriminator
MD5	Message Digest 5
MIPS	Microprocessor Without Interlocked Pipeline Stages
MPLS	Multi Protocol Label Switching
MF	More Fragments
NASA	National Aeronautics and Space Administration
NBMA	Non Broadcast Multi Access
NLRI	Network Layer Reachability Information
NSSA	Not So Stuby Area
OSPF	Open Shortest Path First

P	Provider
PE	Provider Edge
PIM	Protocol Independent Multicast
QoS	Quality of Service
RD	Reported Distance
RFC	Request For Comments
RIB	Routing Information Base
RIP	Routing Information Protocol
RTP	Real-time Transport Protocol
SPF	Shortest Path First
SONET	Synchronous Optical NETwork
TCP	Transmission Control Protocol
TLV	Type/Lenght/Value
TTL	Time To Live
UDP	User Datagram Protocol
VLSM	Variable Lenght Subnet Mask

1 Príloha

1.1 Laboratorní úloha 1

1.1.1 Topologie sítě



Obrázok 28: Topologie sítě.

1.1.2 Teoretický úvod

MPLS (Multi Protokol Label Switching) je mechanismus směrování síťového provozu mezi uzly sítě na základě návěstí (Label) pevné délky a né IP adres. Tímhle se vynechává prohledávání směrovacích tabulek a proces je tak mnohem rychlejší. Návěstí neidentifikuje koncové body jako IP adresa ale virtuální spoje mezi směrovači. Jak s názvu plyne MPLS může přenášet a zapouzdrovat různé směrovací protokoly. Hlavní výhodou MPLS je odstranení závyslosti na technologii linkové vrstvy jako ATM, Frame Realy, SONET, nebo Ethernet. MPLS pracuje na rozhraní druhé a třetí vrstvě modelu ISO/OSI a proto se často označuje jako vrstva 2,5.

1.1.3 Úkol 1 – konfigurace adres a směrování OSPF

a) Podle obrázku č. 28 nakonfigurujte IP adresy rozhraní jednotlivých směrovačů. A ověřte základní konektivitu mezi sousedními směrovači pomocí příkazu ***ping***.

```
CE1#conf t
CE1(config)#int fa 0/0
CE1(config-if)#ip address 10.10.10.1 255.255.255.0

CE1(config-if)#no sh
CE1#ping 10.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max =
16/31/48 ms
```

Nakonfigurujte také loopback rozhraní a změnte typ jeho sítě.

```
CE1(config)#int lo0
CE1(config-if)#ip address 8.8.8.1 255.255.255.0
CE1(config-if)#ip ospf network point-to-point
```

b) Když máme nakonfigurované všechny IPv4 adresy a ověřili jsme konektivitu mezi sousedními směrovači, nyní přejdeme ke konfiguraci směrovacího protokolu OSPF. V této úloze využijeme pouze OSPF oblast 0, teda jádro a OSPF proces 1. OSPF nakonfigurujeme z konfiguračního módu rozhraní.

```
CE1(config-if)# ip ospf 1 area 0
```

Po konfiguraci OSPF na všech rozhraních se mám vytvořila mezi směrovači sousedství, a směrovače jsi vyměnili směrovací informace. Následně ověříme konektivitu mezi směrovači CE1 a CE2.

1.1.4 Úkol 2 – konfigurace MPLS

c) Po konfiguraci protokolu OSPF a ověření funkčnosti směrování přistoupíme ke konfiguraci samotného MPLS. MPLS spustíme na všech portech, které patří do MPLS domény pomocí příkazu ***mpls ip***. Pro výměnu MPLS zpráv zvolíme protokol LDP (Label Distribution Protokol).

```
PE1(config)#int fa0/1
PE1(config-if)#mpls ip
PE1(config-if)#mpls label protocol ldp
```

Po nakonfigurování MPLS a LDP si zobrazíme informace o sousedech pomocí příkazu ***sh mpls ldp neighbor***.

```
PE1#sh mpls ldp neighbor
    Peer LDP Ident: 192.168.2.1:0; Local LDP Ident
192.168.1.1:0
        TCP connection: 192.168.2.1.64246 - 192.168.1.1.646
        State: Oper; Msgs sent/rcvd: 46/47; Downstream
        Up time: 00:33:26
        LDP discovery sources:
          FastEthernet0/1, Src IP addr: 192.168.1.2
        Addresses bound to peer LDP Ident:
          192.168.1.2     192.168.2.1
```

Ve výpise vidíme informace o sousedovy jako IP adresu, čísla potrů, všimněme si, že pro spojení se využíva spojově orientovaný TCP protokol. Dále vidíme stav spojení Oper, délka spojení a rozhraní přes, které jsou LDP zpávy příjímány v tomto případe Fa 0/1 a zdrojová IP adresa odkud k nám LDP zprávy přichází. Parametry protokolu LDP si zobrazíme pomocí příkazu ***sh mpls ldp parameters***.

```
PE1#sh mpls ldp parameters
Protocol version: 1
Downstream label generic region: min label: 16; max label:
100000
Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery targeted hello: holdtime: 90 sec; interval: 10 sec
Downstream on Demand max hop count: 255
LDP for targeted sessions
LDP initial/maximum backoff: 15/120 sec
LDP loop detection: off
```

Z výpisu vidíme detaily protokolu LDP, verze protokolu je 1. Vidíme, že návěstí se začínají přiřazovat od hodnoty 16 do 100000, to protože hodnoty návěstí 0-15 jsou rezervovány. Dále vidíme nastavení časování pro různé intervaly.

d) Na směrovači P si zobrazíme tabulky přiřazení návěstí jednotlivým sítím pomocí příkazu ***sh mpls ip bindig***.

```
P#sh mpls ip binding
  8.8.7.1/32
        in label:     19
        out label:    19        lsr: 192.168.1.1:0
        out label:    19        lsr: 192.168.2.2:0    inuse
  8.8.8.1/32
        in label:     18
```

```
        out label:     18         lsr: 192.168.1.1:0    inuse
        out label:     18         lsr: 192.168.2.2:0
  10.10.10.0/24
        in label:      16
        out label:     imp-null   lsr: 192.168.1.1:0    inuse
        out label:     16         lsr: 192.168.2.2:0
  10.10.11.0/24
        in label:      17
        out label:     16         lsr: 192.168.1.1:0
        out label:     imp-null   lsr: 192.168.2.2:0    inuse
  192.168.1.0/24
        in label:      imp-null
        out label:     imp-null   lsr: 192.168.1.1:0
        out label:     17         lsr: 192.168.2.2:0
  192.168.2.0/24
        in label:      imp-null
        out label:     17         lsr: 192.168.1.1:0
        out label:     imp-null   lsr: 192.168.2.2:0
```

Z výpisu je vidět, že k přepisování návěstí dochádí na směrovači P na portech 192.168.1.1 a 192.168.2.2, směrovač je označen jako LSR – Label Switch Router. Dále si zobrazíme LFIB tabulky na směrovačích P a PE1.

```
P#sh mpls forwarding-table
Local  Outgoing    Prefix    Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id   switched   interface
16     Pop tag  10.10.10.0/24  570  Fa0/0   192.168.1.1
17     Pop tag  10.10.11.0/24  0    Fa0/1   192.168.2.2
18     18       8.8.8.1/32     0    Fa0/0   192.168.1.1
19     19       8.8.7.1/32    590   Fa0/1   192.168.2.2
```

```
PE1#show mpls forwarding-table
Local  Outgoing    Prefix   Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id  switched   interface
16     17      10.10.11.0/24  0  Fa0/1      192.168.1.2
17     Pop tag 192.168.2.0/24 0  Fa0/1      192.168.1.2
18     Untagged 8.8.8.1/32    0  Fa0/0      10.10.10.1
19     19       8.8.7.1/32    0  Fa0/1      192.168.1.2
```

Ve výpisu je vidět odchozí rozhraní a next hop adresa. Pop tag nám udáva, že dochází k odstranení návěstí a Untagged zase, že nedochází k přidělení štítku.

1.1.5 Úkol 3 – nastavení autentizace MPLS pomocí algoritmu md5

Pro zabezpečení MPLS sítě se v praxi využíva autentizace LDP zpráv pomocí algoritmu MD5. V této části úlohy si vyzkoušíme konfiguraci autentizace medzi směrovači PE1, PE2 a P. Autentizace se konfiguruje pomocí parametru router ID souseda, v našem případe je router ID představováno jako nejvyšší IP adresa nakonfigurovaná na daném směrovači. Toto nastavení leze však změnit pomocí příkazu ***mpls ldp router-id*** *<ID>* ***force***. Příkaz force nám zabezpečí že změna se vykoná ihned. Samotná konfigurace se provádí pomocí příkazu ***mpls ldp neighbor*** *< IP addressa >* ***password*** *< heslo >*. Nastavení se provádí v konfiguračním režimu směrovače.

a) Na směrovačích nastavte a ověřte router ID.

```
PE1(config)#mpls ldp router-id fastEthernet 0/1 force
```

Nastavení router ID si můžeme ověřit příkazem ***sh mpls ldp discovery***.

```
PE1#sh mpls ldp discovery
Local LDP Identifier:
192.168.1.1:0
```

b) Nastavte autentizaci mezi směrovači PE1, P a PE2 jako heslo použijte slovo ***student***.

```
PE1(config)#mpls ldp neighbor 192.168.2.1 password student
PE1(config)#
*Mar  1 00:13:55.723: %LDP-5-NBRCHG: LDP Neighbor 192.168.2.1:0
(1) is DOWN (Session's MD5 password changed)
PE1(config)#
*Mar    1   00:14:02.819:   %TCP-6-BADAUTH:   No   MD5   digest   from
192.168.2.1(34344) to 192.168.1.1(646)
PE1(config)#
```

Po nakonfigurování autentizace na směrovači PE1 vidíme, že došlo ke ztrátě sousedství mezi směrovači PE1 a P. To proto, že i protějšek musí mít nakonfigurovanou autentizaci a sousedovy odesílat společné heslo. Ztrátu sousedstvý si můžeme ověřit.

```
PE1#sh mpls ldp neighbor
Peer LDP Ident: 192.168.2.1:0
No TCP connection; Downstream
Up time: 00:05:17
 Addresses bound to peer LDP
Ident:
 192.168.1.2     192.168.2.1
```

Z výpisu vidíme, že není sestaveno TCP spojení. Po nakonfigurování autantizace i na směrovači P se spojení opět obnoví.

```
P(config)#mpls ldp neighbor 192.168.1.1 password student
P(config)#
*Mar  1 00:23:59.591: %LDP-5-NBRCHG: LDP Neighbor 192.168.1.1:0
(2) is UP
```

```
PE1#sh mpls ldp neighbor
    Peer LDP Ident: 192.168.2.1:0; Local LDP Ident
192.168.1.1:0
        TCP connection: 192.168.2.1.29308 - 192.168.1.1.646
        State: Oper; Msgs sent/rcvd: 9/9; Downstream
        Up time: 00:00:16
        LDP discovery sources:
          FastEthernet0/1, Src IP addr: 192.168.1.2
        Addresses bound to peer LDP Ident:
          192.168.1.2     192.168.2.1
```

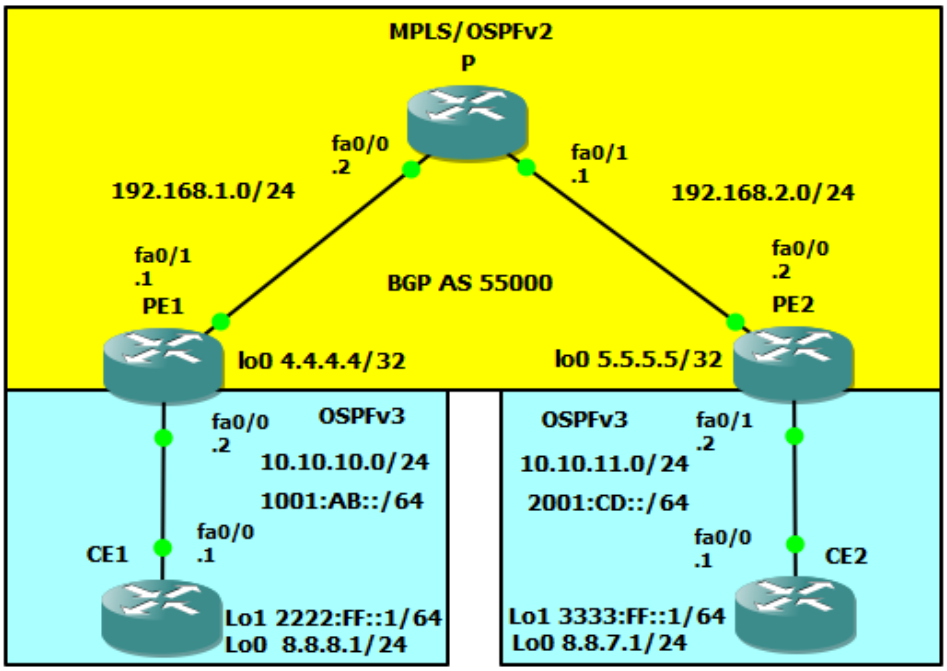
Nastavení autentizace pomocí MD5 si můžeme ověřit pomocí příkazu ***show mpls ldp neighbor detail***. Na výpise vidíme, že autantizace MD5 je ON.

```
PE1#show mpls ldp neighbor detail
    Peer LDP Ident: 192.168.2.1:0; Local LDP Ident
192.168.1.1:0
        TCP connection: 192.168.2.1.57341 -
192.168.1.1.646; MD5 on
        State: Oper; Msgs sent/rcvd: 11/10; Downstream;
Last TIB rev sent 12
```

```
        Up time: 00:01:43; UID: 5; Peer Id 0;
        LDP discovery sources:
          FastEthernet0/1; Src IP addr: 192.168.1.2
            holdtime: 15000 ms, hello interval: 5000 ms
        Addresses bound to peer LDP Ident:
          192.168.1.2     192.168.2.1
        Peer holdtime: 180000 ms; KA interval: 60000 ms;
Peer state: estab
```

1.1.6 Úkol 4 – Propojení IPv6 PE oblastí přes MPLS IPv4 jádro pomocí metody 6PE – samostatní úkol.

Proveďte změny konfigurace podle obrázku č.29, samostatně si nastudujte techniku 6PE a pokuste se docílit toho aby bylo možné komunikovat pomocí IPv6 protokolu přes IPv4 MPLS jádro.



Obrázok 29: Úloha 1 – úkol 4

Řešení samostatného úkolu

a) Proveďte změny konfigurace podle obrázku.

```
CE1(config)#int lo1
CE1(config-if)#ipv6 address 2222:FF::1/64
CE1(config-if)#exit
CE1(config)#int fa0/0
CE1(config-if)#ipv6 address 1001:AB::1/64

PE1(config)#int fa0/0
PE1(config-if)#ipv6 address 1001:AB::2/64
```

Obdobně nakonfigurujte i dvojici směrovačů PE2 a CE2.

b) Spustě směrování IPv6 na směrovačích CE1, PE1, PE2 a CE2 pomocí příkazu ***ipv6 unicast routing.***

```
CE1(config)#ipv6 unicast-routing
```

c) Nakonfigurujte směrovací protokol OSPFv3 na směrovačích CE1, PE1, PE2 a CE2. Do měrovacího precesu zahrnte i loopback rozhraní.

```
CE1(config)#int fa0/0
CE1(config-if)#ipv6 ospf 1 area 0
CE1(config-if)#int lo1
CE1(config-if)#ipv6 ospf 1 area 0
```

d) Nyní na PE směrovačích nakonfigurujeme BGP protokol a mezi těmito směrovači navážeme BGP sousedstvý. Autonomní číslo zvolíme libovolně, v našem případe 55000. Jako BGP router ID nám poslouží IPv4 loopback rozhraní, které zaneseme do směrovacího protokolu OSPFv2.

```
PE1(config)#int lo0
PE1(config-if)#ip address 4.4.4.4 255.255.255.255
PE1(config-if)#ip ospf 1 area 0

PE2(config)#int lo0
PE2(config-if)#ip address 5.5.5.5 255.255.255.255
PE2(config-if)#ip ospf 1 area 0

PE1(config)#router bgp 55000
PE1(config-router)#bgp router-id 4.4.4.4
PE1(config-router)#neighbor 5.5.5.5 remote-as 55000
PE1(config-router)#neighbor 5.5.5.5 update-source loopback 0
```

```
PE2(config)#router bgp 55000
PE2(config-router)#bgp router-id 5.5.5.5
PE2(config-router)#neighbor 4.4.4.4 remote-as 55000
PE2(config-router)#neighbor 4.4.4.4 update-source loopback 0
```

e) Ověříme, že došlo k navázání sousedstvý mezi směrovači PE1 a PE2.

```
PE1#sh ip bgp summary
BGP router identifier 4.4.4.4, local AS number 55000
BGP table version is 1, main routing table version 1

Neighbor V  AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down
State/PfxRcd
5.5.5.5      4 55000    7  7    1    0    0 00:04:26    0
```

f) Niní nakonfigurujeme funkci IPv6 BGP protokolu, rozesílání MPLS návěstí sousedovy a redistribuci OSPFv3 cest na směrovačích PE1 a PE2.

```
PE1(config)#router bgp 55000
PE1(config-router)#address-family ipv6
PE1(config-router-af)#neighbor 5.5.5.5 activate
PE1(config-router-af)#neighbor 5.5.5.5 send-label
PE1(config-router-af)#redistribute ospf 1

PE2(config)#router bgp 55000
PE2(config-router)#address-family ipv6
PE2(config-router-af)#neighbor 4.4.4.4 activate
PE2(config-router-af)#neighbor 4.4.4.4 send-label
PE2(config-router-af)#redistribute ospf 1
```

g) Na směrovačích PE1 a PE2 nastavíme redistribuci cest z BGP do OSPFv3, metriku redistribuovaných cest nastavíme na 2.

```
PE1(config)#ipv6 router ospf 1
PE1(config-rtr)#redistribute bgp 55000 metric 2

PE2(config)#ipv6 router ospf 1
PE2(config-rtr)#redistribute bgp 55000 metric 2
```

h) Samostatně si zobrazte směrovací tabulky IPv6 (***show ipv6 route***) na PE1 a PE2 a prostudujte je. Ověřte konektivitu mezi loopback rozhraními CE1 a CE (***ping 3333:FF::1 source loopback 1***)

1.1.7 Kontrolní otázky.

1. Jak lze nakonfigurovat router ID a kdy je toto nastavení důležité?
2. Jaký protokol a jaký port se používá pro přenos LDP Hello zpráv ?
3. Na jakém pricipu pracuje MPLS ?
4. Jaký protokol je využíván pro distribuci návěstí ?
5. Jaké typy směrovačů v rámci MPLS znáte a jaká je jejich úloha ?
6. Jaký hešovací algoritmus se používa k autentizaci v MPLS ?
7. Když ste provedli kontrolu konektivity po základní konfiguraci sítě pomocí příkazu ping tak první paket neprošel:

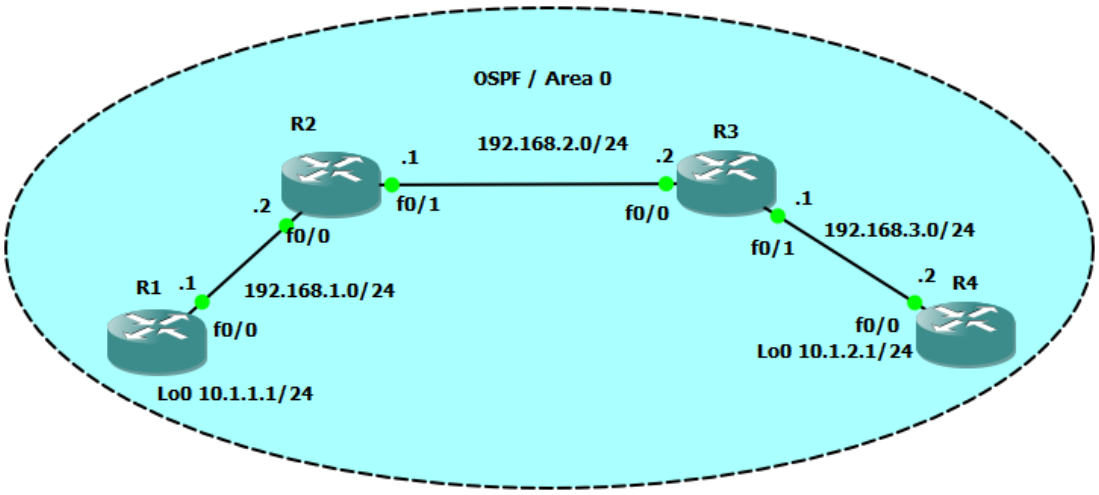
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:

.!!!!

Zamyslete se, proč tomu tak je ? (Otázka z přijímacího pohovoru do AT&T).

1.2 Laboratórní úloha 2

1.2.1 Topologie sítě



Obrázok 30: Topologie sítě

1.2.2 Teoretický úvod

OSPF (Open Shortest Path First) je vnitřní link state ne-proprietární směrovací protokol. Tento protokol si vytváří mapu celé sítě – topologicku databázi. Z této databáze poté pomocí algoritmu SFP vyhledává nejoptimálnější cesty do cílové sítě. Při každé změně sítě se spustí SFP algoritmus znova. Sousedné směrovače vytváří za pomocí hello zpráv sousedstvý a budují si tabulku sousedů. Dále si směrovače vyměňují LSA zprávy prostřednictvím DR směrovače, které obsahují stavy jednotlivých cest a další informace o síti. Existuje několik typů LSA zpráv. Tyto LSA zprávy si směrovače ukládají do své topologické databáze. Všechny směrovače v dané síti mají stejnou topologickou databázi. V broadcastových a NBMA (non-broadcast multiaccess) sítích se volí DR a BDR směrovač, DR sprostředkovává přenos LSA zpráv, BDR je záloha v případě selhání DR. To znamená, že směrovače posílají své LSA zprávy DR směrovači a ten je pak posílá všem ostatním. Má se tím snížit zahlcení sítě. Aby se ještě více ušetřili výpočetní prostředky směrovačů, tak se sítě delí do takzvaných OSPF oblastí. Je to logická část sítě. Mezi těmito oblastmi se nešíří LSA zprávy, také SFP algoritmus běží pro každou oblast zvlášť. Tyto oblasti jsou propojeny pomocí ABR směrovačů. Výchozí oblast je oblast 0, všechny ostatní oblasti musí být propojeny s touto oblastí. Existuje několik typů oblastí, stub area, totally stuby area a not so stubby area . Odlišují

se v tom jaké směrovací informace (LSA zprávy) jsou do dané oblasti zasílány.

1.2.3 Úkol 1 – konfigurace adres

a) Podle obrázku č.30 nakonfigurujte IP adresy rozhraní jednotlivých směrovačů. A ověřte základní konektivitu mezi sousedními směrovači pomocí příkazu ***ping***.

1.2.4 Úkol 2 – konfigurace směrovacího protokolu OSPF

a) Nyní budeme konfigurovat směrovací protokol OSPF. Tady máme dvě možnosti jak provést konfiguraci. A to zaprvé v konfiguračním rozhraní směrovače pomocí příkazu R1(config)#***router ospf 1***, číslo 1 nám udáva číslo směrovacího procesu. Následně by jsme použili příkaz R1(config-router)#***network 192.168.1.0 0.0.0.255 area 0*****,** kterým by jsme síť 192.168.1.0/24 zahrnuli do směrovacího procesu. Všiměte si, že v příkazu se zadávavá inverzní formát masky, tzv. Wildcard mask. Kde "0" jsou nahrazeny "1" a zase naopak. Příkaz ***Area 0*** nám udává číslo oblasti. Další možnost je jednoduhší a to nastavení směrování cez konfiruračí rozhraní portu.

```
R1(config)#int fa0/0
R1(config-if)#ip ospf 1 area 0
R1(config-if)#int lo0
R1(config-if)#ip ospf 1 area 0
```

b) Nastavte OSPF na směrovači R2 a zapněte si debug a sledujte proces sestavení sousedstvý mezi R1 a R2. Po prohlédnutí debug zase vypněte.

```
R2#debug ip ospf adj
OSPF adjacency events debugging is on
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int fa0/0
R2(config-if)#ip os
R2(config-if)#ip ospf 1 are
R2(config-if)#ip ospf 1 area 0
R2(config-if)#
*Mar  1 00:47:57.579: OSPF: Interface FastEthernet0/0 going Up
*Mar  1 00:47:58.079: OSPF: Build router LSA for area 0, router
ID 192.168.2.1, seq 0x80000001
R2(config-if)#
*Mar  1 00:48:03.395: OSPF: 2 Way Communication to 10.1.1.1 on
FastEthernet0/0, state 2WAY
*Mar  1 00:48:03.395: OSPF: Backup seen Event before WAIT timer
on FastEthernet0/0
*Mar  1 00:48:03.399: OSPF: DR/BDR election on FastEthernet0/0
*Mar  1 00:48:03.399: OSPF: Elect BDR 192.168.2.1
*Mar  1 00:48:03.399: OSPF: Elect DR 10.1.1.1
```

```
*Mar  1 00:48:03.399: OSPF: Elect BDR 192.168.2.1
*Mar  1 00:48:03.399: OSPF: Elect DR 10.1.1.1
*Mar  1 00:48:03.399:         DR: 10.1.1.1 (Id)    BDR:
192.168.2.1 (Id)
*Mar  1 00:48:03.403: OSPF: Send DBD to 10.1.1.1 on
FastEthernet0/0 seq 0x10A9 opt 0x52 flag 0x7 len 32
R2(config-if)#
*Mar  1 00:48:07.639: OSPF: Rcv DBD from 10.1.1.1 on
FastEthernet0/0 seq 0xC53 opt 0x52 flag 0x7 len 32  mtu 1500
state EXSTART
*Mar  1 00:48:07.643: OSPF: First DBD and we are not SLAVE
*Mar  1 00:48:08.403: OSPF: Send DBD to 10.1.1.1 on
FastEthernet0/0 seq 0x10A9 opt 0x52 flag 0x7 len 32
*Mar  1 00:48:08.403: OSPF: Retransmitting DBD to 10.1.1.1 on
FastEthernet0/0 [1]
*Mar  1 00:48:08.451: OSPF: Rcv DBD from 10.1.1.1 on
FastEthernet0/0 seq 0x10A9 opt 0x52 flag 0x2 len 52  mtu 1500
state EXSTART
*Mar  1 00:48:08.451: OSPF: NBR Negotiation Done. We are the
MASTER
*Mar  1 00:48:08.455: OSPF: Send DBD to 10.1.1.1 on
FastEthernet0/0 seq 0x10AA opt 0x52 flag 0x3 len 52
*Mar  1 00:48:08.455: OSPF: Database request to 10.1.1.1
*Mar  1 00:48:08.455: OSPF: sent LS REQ packet to 192.168.1.1,
length 12
*Mar  1 00:48:08.515: OSPF: Rcv DBD from 10.1.1.1 on
FastEthernet0/0 seq 0x10AA opt 0x52 flag 0x0 len 32  mtu 1500
state EXCHANGE
*Mar  1 00:48:08.515: OSPF: Send DBD to 10.1.1.1 on
R2(config-if)#FastEthernet0/0 seq 0x10AB opt 0x52 flag 0x1 len
32
*Mar  1 00:48:08.591: OSPF: Rcv DBD from 10.1.1.1 on
FastEthernet0/0 seq 0x10AB opt 0x52 flag 0x0 len 32  mtu 1500
state EXCHANGE
*Mar  1 00:48:08.591: OSPF: Exchange Done with 10.1.1.1 on
FastEthernet0/0
*Mar  1 00:48:08.595: OSPF: Synchronized with 10.1.1.1 on
FastEthernet0/0, state FULL
*Mar  1 00:48:08.595: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.1 on
FastEthernet0/0 from LOADING to FULL, Loading Done
```

Všiměnete si, že po zapnutí směrovacího procesu na R2 nastáva volba DR/BDR směrovače. V tomto případě je zvolen za DR směrovač R1, (DR: 10.1.1.1 (id) a jako BDR je zvolen R2 (BDR: 192.168.2.1 (id)). RD/BRD je volen pro každou jednu IP síť, proto naše topologie neobsahuje pouze jeden DR/BDR. Výběr DR/BDR probíhá defaultně na základě priority, ta je však defaultně nastavena na všech směrovačích na stejnou hodnotu, proto se automaticky projde k výběru na základě router ID. Poslední zpráva ve výpisu nám říká že sousedstvý bylo sestaveno.

c) Nastavte OSPF na všech aktivních rozhraních směrovačů v síti a ověřte konektivitu

mezi směrovači R1 a R4. Zobrazte si směrovací tabulku na R1 a ověřte správnost konfigurace.

```
R1#sh ip route
< skrácený výstup >
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O       10.1.2.1/32 [110/31] via 192.168.1.2, 00:21:56,
FastEthernet0/0
C       10.1.1.0/24 is directly connected, Loopback0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
O    192.168.2.0/24 [110/20] via 192.168.1.2, 00:21:56,
FastEthernet0/0
O    192.168.3.0/24 [110/30] via 192.168.1.2, 00:21:56,
FastEthernet0/0
```

Vidíme, že směrovací tabulka obsahuje záznam o každé síti. Dále si zobrazíme nastavení směrovacího protokolu pomocí přákazu ***sh ip protocols***. Z výpisu vidíme, že směrovací protokol je OSPF s procesem 1. Router ID je nastaveno na hodnotu 10.1.1.1 což je IP adresa loopback rozhraní. Směrovač si vybírá své ID na základě svých IP adres. Přednostně jsou vybírány loopback rozhraní před fyzickými rozhraními. Když je situace taková, že na směrovači je více loopback rozhraní tak je jako ID zvolena ta nejvyšší IP adresa. Například 192.168.1.1 je vyšší jako 10.1.1.1. Router ID jde samozřejme měnit ručně. Dále je patrné, že defaultní administrativní vzdálenost protokolu OSPF je 110. Všiměte si také, že směrovač R1 má informaci o síti 10.1.2.1/32 ale ze špatnou maskou. Je to dáno defaultním nastavením typu sítě u loopback rozhraní, které je typu stub host.

```
R1#sh ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
  Routing on Interfaces Configured Explicitly (Area 0):
    Loopback0
    FastEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.2.1             110      00:03:04
    192.168.3.1          110      00:03:04
    192.168.2.1          110      01:02:05
  Distance: (default is 110)
```

d) Na směrovači R1 si zobrazíme tabulku sousedů. R1 má jenom jednoho souseda, to protže sousedstvý je navazováno jenom v rámci sítě. R2 bude mít 2 sousedy a to R1 a R3 .

```
R1#sh ip ospf neighbor
Neighbor ID  Pri   State      Dead Time   Address  Interface
192.168.2.1  1     FULL/BDR   00:00:32    192.168.1.2  fa0/0
```

Z výpisu na R1 vidíme neighbor ID nejvyšší IP adresu na R2.

```
R2#sh ip ospf neighbor

Neighbor ID Pri  State    Dead Time  Address     Interface
192.168.3.1  1   FULL/DR  00:00:37   192.168.2.2     fa0/1
10.1.1.1     1   FULL/BDR 00:00:36   192.168.1.1     fa0/0
```

Stav FULL/BDR, FULL/DR nám značí, že sousedstvý s DR a BDR je plně navázáno (FULL).

1.2.5 Úkol 3 – Olvivnění výběru DR/BDR, změna odesílané masky, časovače a nastavení autentizace MD5

a) Změnte nastavení tak aby jste ovlivnily výběr DR/BRD na síti 192.168.1.0/24. R1 byl na začátku zvolen jako DR, nyní pomocí nastavení OSPF priority na R2 a restartu OSPF procesu na R1 a R2 příkazem ***clear ip ospf proces*** dosáhneme, že jako DR bude zvolen R2.

```
R2(config)#int fa0/0
R2(config-if)#ip ospf pri
R2(config-if)#ip ospf priority 33


R1#clear ip ospf proces
Reset ALL OSPF processes? [no]: yes

R2#clear ip ospf proces
Reset ALL OSPF processes? [no]: yes
```

Ve výpise informací o sousedu si ověříme zda nyní je R2 DR.

```
R1#sh ip ospf neighbor detail
 Neighbor 172.16.3.97, interface address 192.168.1.2
    In the area 0 via interface FastEthernet0/0
    Neighbor priority is 33, State is FULL, 6 state changes
    DR is 192.168.1.2 BDR is 192.168.1.1
```

b) Proveďte změnu nastavení tak aby byli sítě z loopback rozhraní oznamovány se správnou maskou.

```
R1(config)#int lo0
R1(config-if)#ip ospf network point-to-point
```

c) OSPF podporuje zabezpečení rozesílaných směrovacích informací pomocí hešovacího algoritmu md5. Nyní nastavíme autentizaci na lince mezi směrovači R1 a R2, jako heslo použijeme slovo ***student***. Na obou směrovačích si zapneme debug OSPF sousedství.

```
R1(config)#int fa0/0
R1(config-if)#ip ospf authentication message-digest
R1(config-if)#ip ospf message-digest-key 1 md5 student
R1(config-if)#
*Mar  1 01:16:59.927: OSPF: Rcv pkt from 192.168.1.2,
FastEthernet0/0 : Mismatch Authentication type. Input packet
specified type 0, we use type 2
R1(config-if)#
*Mar  1 01:17:02.259: OSPF: Send with youngest Key 1

*Mar  1 01:17:19.903: OSPF: 11.11.1.97 address 192.168.1.2 on
FastEthernet0/0 is dead
*Mar  1 01:17:19.903: OSPF: 11.11.1.97 address 192.168.1.2 on
FastEthernet0/0 is dead, state DOWN
*Mar  1 01:17:19.903: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.1.97
on FastEthernet0/0 from FULL to DOWN, Neighbor Down: Dead timer
expired
```

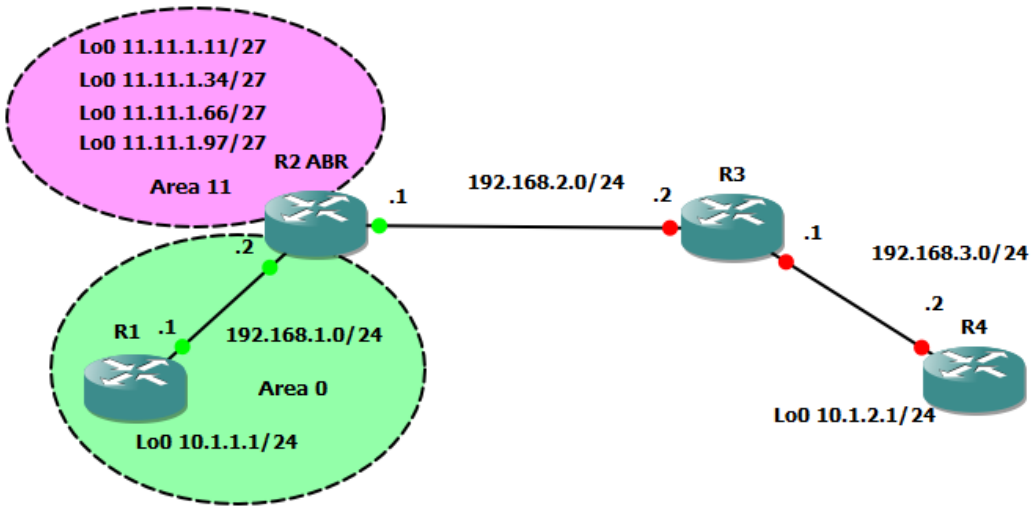
Z debug výstupu vidíme, že po nastavení autentizace na portu fa 0/0 na R1 je sousedstvý s R2 straceno. Sousedství bylo přerušeno po vypršení Dead intervalu, což je doba po kterou musí být přijat hello paket od souseda, jinak je soused ozančen jako down. Po nastavení autentizace na portu Fa 0/0 na R2 bude sousedství znova obnoveno.

```
< skrácený výstup >
*Mar  1 01:28:50.243: OSPF: Exchange Done with 10.1.1.1 on
FastEthernet0/0
*Mar  1 01:28:50.243: OSPF: Synchronized with 10.1.1.1 on
FastEthernet0/0, state FULL
*Mar  1 01:28:50.243: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.1 on
FastEthernet0/0 from LOADING to FULL, Loading Done
< skrácený výstup >
```

d) Nastavení autentizace si můžeme prohlédnout v nastavení portu pomocí příkazu ***show ip ospf interface fa 0/0***. Výstup toho příkazu nám také ukáže nastavení OSPF časovačů.

```
R1#sh ip ospf interface fa0/0
< skrácený výstup >

  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 11.11.1.97  (Designated Router)
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

1.2.6 Úkol 4 – Sumarizace adres a default route



Obrázok 31: Úloha 2 - úkol 4

a) Nyní provedeme změnu konfigurace sítě podle obrázku č.31. Na směrovači R2 nastavíme loopback rozhraní lo0 až lo3 a přiřadíme IP adresy, loopback rozhraní nastavte tak aby byla odesílána správna maska. Pak tyto rozhraní zaneseme do směrovacího procesu OSFP s oblastí 11. R2 nyní figuruje jako ABR směrovač.

```
R2(config)#int lo0
R2(config-if)#ip address 11.11.1.11 255.255.255.224
R2(config-if)#ip ospf network point-to-point
R2(config-if)#ip ospf 1 area 11
```

b) Nyní si zobrazte směrovací tabulku na směrovači R1.

```
R1#sh ip route
< skrácený výstup >

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback0
     11.0.0.0/27 is subnetted, 4 subnets
O IA    11.11.1.0 [110/11] via 192.168.1.2, 00:01:03, fa0/0
O IA    11.11.1.32 [110/11] via 192.168.1.2, 00:00:53, fa0/0
O IA    11.11.1.64 [110/11] via 192.168.1.2, 00:00:53, fa0/0
O IA    11.11.1.96 [110/11] via 192.168.1.2, 00:00:12, fa0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
O    192.168.2.0/24 [110/20] via 192.168.1.2, 00:17:48, fa0/0
```

Vidíme, že pro každou síť z loopback rozhraní na R2 je v tabulce samostatný záznam. Dále si všimněme, že tyto sítě jsou sousední sítě a mohou být zastoupeny jediným záznamem (11.11.1.0 255.255.255.128) v směrovací tabulce, tuto techniku označujeme sumarizace IP adres. Sumarizace může být prováděna pouze na ABR nebo ASBR směrovačích. Tím zrychlíme proces vyhledávaní správne cesty při směrování.

c) Proveďte změnu konfigurae na R2 tak aby sítě z loopback rozhraní byla do oblasti 0 rozesílána jako jediný záznam. To provedeme v konfiguračním rozhraní OSPF procesu, pomocí příkazu ***area 11 range 11.11.1.0 255.255.255.128***.

```
R2(config)#router ospf 1
R2(config-router)#area 11 range 11.11.1.0 255.255.255.128
```

d) Nyní si zobrazte směrovací tabulku na R1.

```
R1#sh ip route
< skrácený výstup >

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback0
     11.0.0.0/25 is subnetted, 1 subnets
O IA    11.11.1.0 [110/11] via 192.168.1.2, 00:01:05, fa0/0
C    192.168.1.0/24 is directly connected, fa0/0
O    192.168.2.0/24 [110/20] via 192.168.1.2, 00:38:37, fa0/0
```

Vidíme, že v tabulce je místo 4 záznamů jeden. Všiměnte si, že cesta je označena jako IA co zanamená Inter-Area route. To značí že cesta byla obdržena z jiné oblasti.

e) R1 nastavíme tak aby rozesílal default route. Tady jsou dvě možnosti jak provést nastavení a to pomocí příkazu ***default-information originate*** anebo pomocí ***default-information originate always***. Rozdíl je v tom, že v prvím případe musí být default route nakonfigurována předem. My tedy zvolíme druhou možnost. Příkaz je spušten v

konfiguračním módu OSPF proccesu.

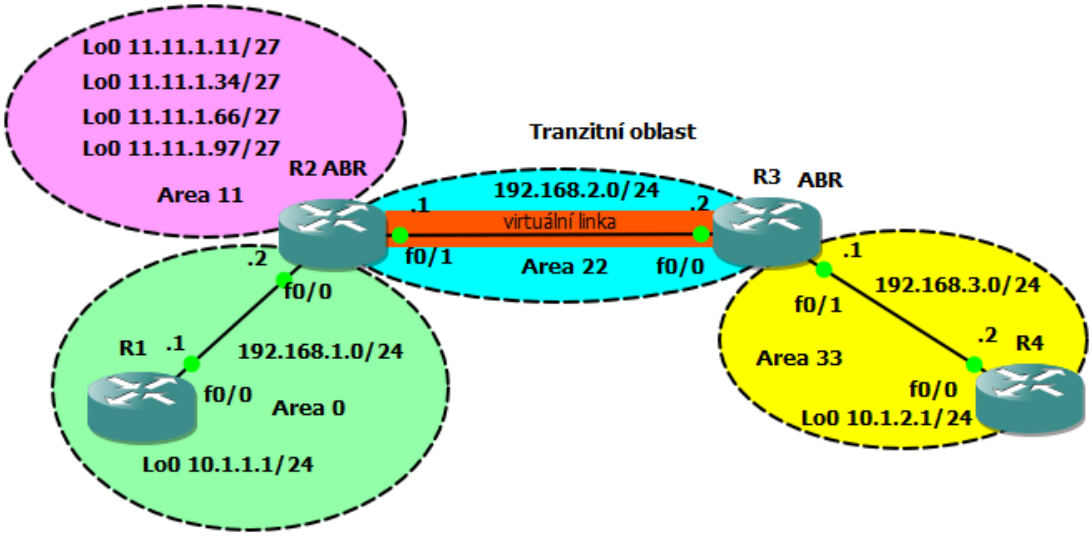
```
R1(config)#router ospf 1
R1(config-router)#default-information originate always
```

e) Zobrazíme si směrovací tabulku na R2

```
R2#sh ip route
< skrácený výstup >
Gateway of last resort is 192.168.1.1 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
O       10.1.1.0 [110/11] via 192.168.1.1, 00:11:38,
FastEthernet0/0
     11.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       11.11.1.0/27 is directly connected, Loopback0
O       11.11.1.0/25 is a summary, 01:36:07, Null0
C       11.11.1.32/27 is directly connected, Loopback1
C       11.11.1.64/27 is directly connected, Loopback2
C       11.11.1.96/27 is directly connected, Loopback3
C    192.168.1.0/24 is directly connected, fa0/0
C    192.168.2.0/24 is directly connected, fat0/1
O*E2 0.0.0.0/0 [110/1] via 192.168.1.1, 00:11:40, fa0/0
```

Z výpisu vidíme, že R2 nyní obsahuje defaultní cestu, defaultní cesta je označena *. Cesta je typu E2. To je označení pro cesty, které byly naučeny prostřednictvým redistribuce. V OSPF existují ješte E1 cesty. Avšak této problematice se podrobně venuje kurz CCIE což je vysoko nad rámcem náročnosti této úlohy a proto lze zjednodušene říct, že rozdíl je v tom jak se počítá metrika pro tyto cesty.

1.2.7 Úkol 5 – konfigurace virtuální linky a více oblastí, OSPF databáze



Obrázok 32: Úloha 2 - úkol 5

a) Jak víte z teorie, tak každá oblast v OSPF doméně musí být fyzicky propojená s oblastí 0. V některých případech však toto propojení z různých důvodů není možné a proto se použie virtuální spoj. Oblast, která spojuje backbone oblast (oblast 0) a non-backbone oblast se nazývá tranzitní oblast. Virtuální linku nakonfigurujeme pomocí příkazu ***area*** *<area-id>* ***virtual-link*** *<router-id>* kde ***area-id*** je id přidelené tranzitní oblasti, v našem případe ***area 22***. Router-id je id sousedního směrovače. Příkaz se spouští v konfiguračním rozhraní směrovacího procesu. Nakonfigurujte síť podle obrázku č.32.

```
R2(config)#int fa 0/1
R2(config-if)#no ip ospf 1 area 0
R2(config-if)#ip ospf 1 area 22

R3(config)#int fa0/0
R3(config-if)#no ip ospf 1 area 0
R3(config-if)#ip ospf 1 area 22
R3(config)#int fa0/1
R3(config-if)#no ip ospf 1 area 0
R3(config-if)#ip ospf 1 area 33

R4(config)#int fa0/0
R4(config-if)#no ip ospf 1 area 0
R4(config-if)#ip ospf 1 area 33
R4(config-if)#int lo0
R4(config-if)#no ip ospf 1 area 0
R4(config-if)#ip ospf 1 area 33
```

b) Konfiguraci si můžeme ověřit nasledovně. Ve výpisu z příkazu ***show ip protocols*** vidíme, které rozhraní je zahrnuto v OSPF směrovacím rocesu a do které oblasti patří.

```
R2#sh ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 11.11.1.97
  It is an area border router
  Number of areas in this router is 3. 3 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing on Interfaces Configured Explicitly (Area 0):
    FastEthernet0/0
  Routing on Interfaces Configured Explicitly (Area 11):
    Loopback3
    Loopback2
    Loopback1
    Loopback0
  Routing on Interfaces Configured Explicitly (Area 22):
    FastEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         110      00:23:01
    10.1.2.1              110      00:32:32
    10.1.1.1              110      00:20:22
    192.168.3.1           110      00:32:32
  Distance: (default is 110)
```

c) Zobrazte si směrovací tabulku na R1 a R4 a ověřte, že sítě z oblasti 33 nejsou dostupné.

```
R1#sh ip route
< skrácený výstup >
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback0
     11.0.0.0/25 is subnetted, 1 subnets
O IA    11.11.1.0 [110/11] via 192.168.1.2, 00:11:03, fa0/0
C    192.168.1.0/24 is directly connected, fa0/0
O IA 192.168.2.0/24 [110/20] via 192.168.1.2, 00:09:13, fa0/0
```

```
R4#sh ip route
< skrácený výstup >
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.2.0 is directly connected, Loopback0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

Vidíme, že R4 nedostává nijaké směrovací informace.

c) Nakonfigurujte virtuální linku mezi R2 a R3 a zobrazte si její nastavení.

```
R2(config)#router ospf 1
R2(config-router)#area 22 virtual-link 192.168.3.1

R3(config)#router ospf 1
R3(config-router)#area 22 virtual-link 11.11.1.97
```

```
R2#sh ip ospf virtual-links
Virtual Link OSPF_VL0 to router 192.168.3.1 is up
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 22, via interface FastEthernet0/1, Cost of using
10
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:01
    Adjacency State FULL (Hello suppressed)
    Index 2/3, retransmission queue length 1, number of
retransmission 1
    First 0x6707E614(28)/0x0(0) Next 0x6707E614(28)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
    Link State retransmission due in 2861 msec
```

d) Zobrazte si směrovací tabulku na R4 a ověřte konektivitu z R1. Po nakonfigurování virtuálního spoje má R4 informace o všech sítích v naší OSPF doméně.

```
R4#sh ip route
< skrácený výstup >

Gateway of last resort is 192.168.3.1 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.2.0 is directly connected, Loopback0
O IA    10.1.1.0 [110/31] via 192.168.3.1, 00:07:33, fa0/0
     11.0.0.0/25 is subnetted, 1 subnets
O IA    11.11.1.0 [110/21] via 192.168.3.1, 00:07:33, fa0/0
O IA 192.168.1.0/24 [110/30] via 192.168.3.1, 00:07:33, fa0/0
O IA 192.168.2.0/24 [110/20] via 192.168.3.1, 00:07:53, fa0/0
C    192.168.3.0/24 is directly connected, fa0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.3.1, 00:07:32, fa0/0
```

e) Na R2 si prohlédněte OSPF databázi a zobrazte si informace o OSPF. Rozebereme si co jednotlivé záznamy v OSPF topologické databázi znamenají. Všechny záznamy pod ***Router Link States*** jsou zprávy typu LSA1. Pomocí těchto zpráv směrovače ozanmují stav svých linek. Každá LSA1 zpráva je identifikovaná podle router ID. Vidíme, že v oblasti 0 jsou 3 směrovače, dále vidíme stáří LSA zprávy, sequence number a checksum.

Poslední sloupec Link count nám udáva počet linek, který zpráva LSA obsahuje. Náhled do LSA zprávy získame pomocí příkazu ***sh ip ospf database router*** *<router id>*. V našem případe se podíváme na LSA1 zprávu, kterou zaslal R1. Záznamy pod řádkem ***Net Link States*** jsou zprávy typu LSA2. LSA2 zprávy jsou přítomny vždy když je přítomna multi-access síť. Tyto zprávy zasílá pouze DR směrovač a obsahuje informace o multi-access síti. Vidíme, že zpráva je odesílána DR směrovačem na dané síti. LSA2 zprávu si můžeme zobrazit pomocí příkazu ***sh ip ospf database network*** *<IP adresa linky>*. Zobrazíme si síť 192.168.1.2.

```
R2#sh ip ospf database

            OSPF Router with ID (11.11.1.97) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
Link count
10.1.1.1        10.1.1.1        980         0x80000007 0x00DD35
2
11.11.1.97      11.11.1.97      1207        0x80000008 0x005E05
2
192.168.3.1     192.168.3.1     1   (DNA)   0x80000006 0x0084DC 1
                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
192.168.1.2     11.11.1.97      1209        0x80000001 0x00D5F9

                Summary Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.2.0        192.168.3.1     11    (DNA) 0x80000001 0x002C8B
11.11.1.0       11.11.1.97      868         0x80000003 0x0068C1
192.168.2.0     11.11.1.97      98          0x80000005 0x001338
192.168.2.0     192.168.3.1     11    (DNA) 0x80000001 0x00FE5B
192.168.3.0     192.168.3.1     11    (DNA) 0x80000001 0x00F365
                < skrácený výstup >
                Summary ASB Link States (Area 22)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.1.1        11.11.1.97      1204        0x80000001 0x00317B
10.1.1.1        192.168.3.1     312         0x80000002 0x007735

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum
Tag
0.0.0.0         10.1.1.1        987       0x80000003 0x00C7DB 1
```

Záznamy pod řádkem ***Summary Net Link States*** jsou LSA3 zprávy. Vidíme, že R2 má ve své databázi pět LSA3 zpráv. Tyto zprávy jsou zasílány pouze ABR směrovači, v

našem případě teda směrovači R2 a R3, které jsou ABR pro oblast 0. ABR směrovače provádí sumarizaci adres z jedné oblasti a rozesílají do další oblasti. LSA3 zprávu si zobrazíme pomocí příkazu ***show ip ospf database summary*** *<IP adresa>*. ***Summary ASB Link States*** obsahuje zprávy tupu LSA4, které jsou také rozesílány pouze ABR směrovači. Zprávu typu LSA4 si zobrazíme pomocí příkazu ***sh ip ospf database asbr-summary***. Jsou rozesílány do jiných oblastí. Pod řádkem Type-5 ***AS External Link States*** jsou LSA zprávy tupu 5. Jsou to zprávy, které jsou rozesílány směrovači, které redistribuií cesty do OSPF, v našem případe R1 redistribuuje default route do všech ostatních oblastí. Zobrazíme si ji pomocí příkazu ***sh ip ospf database external***.

```
R2#sh ip ospf database router 10.1.1.1

            OSPF Router with ID (11.11.1.97) (Process ID 1)

                Router Link States (Area 0)

  Routing Bit Set on this LSA
  LS age: 565
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 10.1.1.1
  Advertising Router: 10.1.1.1
  LS Seq Number: 80000003
  Checksum: 0xE531
  Length: 48
  AS Boundary Router
  Number of Links: 2

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 192.168.1.2
     (Link Data) Router Interface address: 192.168.1.1
      Number of TOS metrics: 0
       TOS 0 Metrics: 10

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 10.1.1.0
     (Link Data) Network Mask: 255.255.255.0
      Number of TOS metrics: 0
       TOS 0 Metrics: 1
```

Jak vidíme LSA zpráva z R1 nese informaci o dvou linkách. Jedna je připojená do ***Tranzit network*** a druhá do ***Stub network***. Pro OSPF je Transit network broadcastová síť (multi access síť), v našem případe je to ethernet síť 192.168.1.0. Za stub network OSPF ozančí buďto loobback rozhraní anebo point-to-point síť. V našem případe je to loopback rozhraní na R1. Dále z výpisu vyčteme, že je na síti DR směrovač a jeho adresu a že R1 je k němu připojený přes rozhraní s IP adresou 192.168.1.1, R1 tuto

cestu ohlašuje s metrikou 10.

```
R2#show ip ospf database network 192.168.1.2

            OSPF Router with ID (11.11.1.97) (Process ID 1)

                Net Link States (Area 0)

  Routing Bit Set on this LSA
  LS age: 572
  Options: (No TOS-capability, DC)
  LS Type: Network Links
  Link State ID: 192.168.1.2 (address of Designated Router)
  Advertising Router: 11.11.1.97
  LS Seq Number: 80000002
  Checksum: 0xD3FA
  Length: 32
  Network Mask: /24
        Attached Router: 11.11.1.97
        Attached Router: 10.1.1.1
```

Ve výpise vidíme ID směrovače, který tuto LSA2 zprávu odeslal je to směrovač R2, R2 je DR. Dále vidíme připojené směrovače (loop back rozhnarní na R2, které tvoří samostatnou oblast jsou chápany jako připojený další směrovač).

```
 R2# show ip ospf database summary 10.1.2.0

            OSPF Router with ID (11.11.1.97) (Process ID 1)

                Summary Net Link States (Area 0)

  Routing Bit Set on this LSA
  LS age: 1 (DoNotAge)
  Options: (No TOS-capability, DC, Upward)
  LS Type: Summary Links(Network)
  Link State ID: 10.1.2.0 (summary Network Number)
  Advertising Router: 192.168.3.1
  LS Seq Number: 80000001
  Checksum: 0x2C8B
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 11
< skrácený výstup >
```

Routing Bit nastaven na LSA nám udáva, že táto LSA byla přidána do RIB databáze. IP adresa linky je 10.1.2.0 a maska /24. Aby sme se dostaly k 10.1.2.0 musíme jít přes ABR směrovač 192.168.3.1 (R3). Metrika pro R3 k dosažení této linky 10.1.2.0 je 11.

```
R2#sh ip ospf database asbr-summary

            OSPF Router with ID (11.11.1.97) (Process ID 1)

                Summary ASB Link States (Area 11)

  LS age: 391
  Options: (No TOS-capability, DC, Upward)
  LS Type: Summary Links(AS Boundary Router)
  Link State ID: 10.1.1.1 (AS Boundary Router address)
  Advertising Router: 11.11.1.97
  LS Seq Number: 80000001
  Checksum: 0x317B
  Length: 28
  Network Mask: /0
        TOS: 0  Metric: 10

< skrácený výstup >
```

LSA4 zprávy jsou zasílaný ABR směorvači do jiných oblastí pro dosažení ASBR směrovače. Jak je ale možné že se nám tu objevil ASBR směrovač ? Z výpisu vidíme, že jako ASBR je označen R1, je to proto že na tomto směrovači jsme nastavily redistribuci default route a směrovač se tak nastavil do role ASBR.

```
R2#sh ip ospf database external

            OSPF Router with ID (11.11.1.97) (Process ID 1)

                Type-5 AS External Link States

  Routing Bit Set on this LSA
  LS age: 142
  Options: (No TOS-capability, DC)
  LS Type: AS External Link
  Link State ID: 0.0.0.0 (External Network Number )
  Advertising Router: 10.1.1.1
  LS Seq Number: 80000001
  Checksum: 0xCBD9
  Length: 36
  Network Mask: /0
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 1
        Forward Address: 0.0.0.0
        External Route Tag: 1
```

Zvýpisu vidíme detail LSA zprávy typu 5. Tuto zprávu rozesílá R1, metrika je typu 2.

f) na R2 si zobrazte informace o OSFP a prostudujte je.

```
R2#sh ip ospf
 Routing Process "ospf 1" with ID 11.11.1.97
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 It is an area border router

 < skrácený výstup >

 Number of areas in this router is 3. 3 normal 0 stub 0 nssa
 Number of areas transit capable is 1
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm last executed 00:22:30.336 ago
        SPF algorithm executed 13 times

     < skrácený výstup >

    Area 11
        Number of interfaces in this area is 4
        Area has no authentication
        SPF algorithm last executed 01:11:34.900 ago
        SPF algorithm executed 4 times
        Area ranges are
           11.11.1.0/25 Active(1) Advertise

        < skrácený výstup >

    Area 22
        Number of interfaces in this area is 1
        This area has transit capability: Virtual Link Endpoint
        Area has no authentication
        SPF algorithm last executed 00:37:58.868 ago
        SPF algorithm executed 5 times
   < skrácený výstup >
```

1.2.8 Úkol 6 – Změna typu oblasti – samostaní úkol

Proveďte změnu konfigurace tak aby do oblasti 33 nebyli zasílány LSA3, LSA4 a LSA5 zprávy a směrovač R4 obsahoval ve své směrovací tabulce pouze výchozí cestu, která je oznamována směrovačem R1. Správnost konfigurace ověřte vypsáním směrovací a topologické tabulky na R4.

Řešení samostatného úkolu.

a) Řešením je nakonfigurovat oblast 33 jako totally stub oblast. To provedeme nasledovným příkazem na směrovači R3.

```
R3(config)#router ospf 1
R3(config-router)#area 33 stub no-summary
```

b) Zobrazíme si směrovací a topologickou tabulku na R4.

```
R4#sh ip route
< skrácený výstup >
Gateway of last resort is 192.168.3.1 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.2.0 is directly connected, Loopback0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1]via 192.168.3.1,00:21:36, FastEthernet0/0
R4#
```

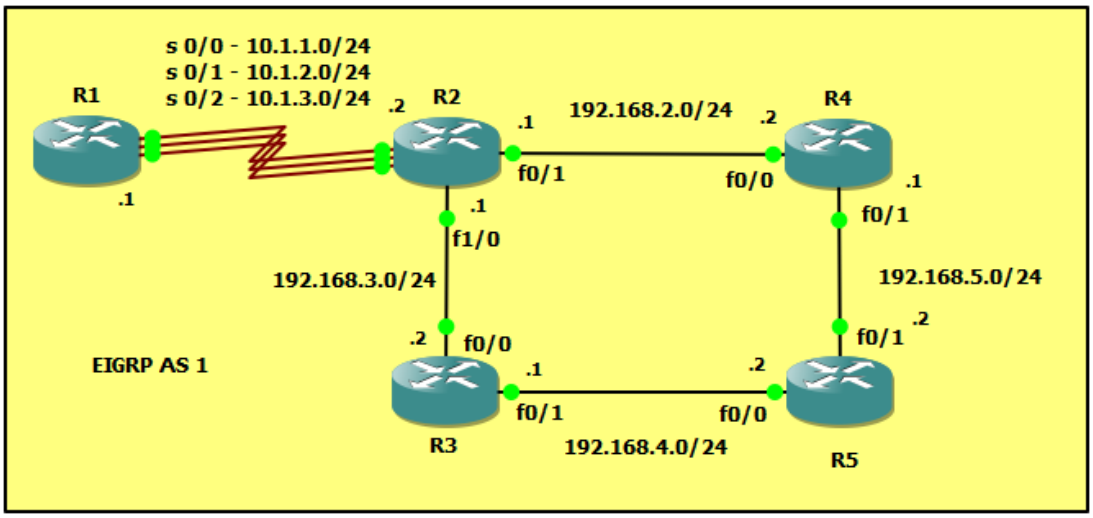
```
R4#sh ip ospf database

            OSPF Router with ID (10.1.2.1) (Process ID 1)

                Router Link States (Area 33)

Link ID         ADV Router      Age         Seq#       Checksum
Link count
10.1.2.1        10.1.2.1        308         0x80000003 0x00A4DB
2
192.168.3.1     192.168.3.1     1647        0x80000003 0x009ED2
1

                Net Link States (Area 33)

Link ID         ADV Router      Age         Seq#       Checksum
192.168.3.1     192.168.3.1     1648        0x80000001 0x00EDF5

                Summary ASB Link States (Area 33)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.1.1        192.168.3.1     1678        0x80000001 0x007934

                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum
Tag
0.0.0.0         10.1.1.1        1861      0x80000001 0x00CBD9 1
```

1.2.9 Kontrolní otázky

1. Proč není uvedena metrika u zprávy typu LSA2 ?
2. Na jakém typu směrovače jde provádět sumarizaci ?
3. Může směrovač typu DROTHER rozesílat zprávy typu LSA2 ?
4. Jaké všechny OSPF parametry musí být stejné na obou portech aby bylo sousedstvý navázáno ?
5. Jakou úlohu sehrává DR směrovač ?

1.3 Laboratorní úloha 3

1.3.1 Topologie sítě



Obrázok 33: Topologie sítě

1.3.2 Teoretický úvod

Protokol EIGRP (Enhanced Interior Gateway Routing Protocol) je CISCO proprietární vnitřní protokol. Je vylepšením protokolu IGRP, oproti svému předchůdci je například rychlejší při konvergenci a zasílá jen tzv. Triggered updates. Je označován za distance – vector protokol, ale dá se říct, že je to hybridní protokol, který pro výpočet metriky dané cesty využívá prvků specifické pro link – state protokoly. Pro výpočet nejlepší cesty do cílové sítě a zabezpečení beze slučkového prostředí využívá algoritmus DUAL (Difusing Update Algorithm). Metriku počítá na základě K hodnot, šířky pásma a opoždění na dané lince. Je to class less protokol, který využívá CIDR a VLMS. EIGRP tak jako OSPF sestavuje sousedstvý mezi směrovači pomocí hello paketů. Aby byly dva směrovače schopny sestavit sousesdstvý tak z pohledu EIGRP musí být ve stejném EIGRP autonomním systému a musí mít stejné K hodnoty. EIGRP podporuje různé protokoly jako IP, IPX a AppleTalk. EIGRP je schopný rovnoměrného i nerovnoměrného loadbalancingu. Protokol si sestavuje dvě tabulky, tabulku sousedů a topologickou tabulku. Protokol má dafaultně nastavenou automatickou sumarizaci sítí, toto je však v případe použití nekontinuálního adresního prostoru nežádoucí, protože v sumarizované adrese sa budou nacházet i sítě, které nejsou použity, nebo, které

nechceme aby byli odesílány. Proto se automatická sumarizace vypne hned na začátku konfigurace.

1.3.3 Úkol 1 – konfigurace adres

a) Nakonfigurujte adresy podle obrázku č.33 a ověřte funkčnost propojení mezi sousedními směrovači. Mezi směrovači R1 a R2 nakonfigurujte sériové linky, clock rate nastavte na 64000.

1.3.4 Úkol 2 – konfigurace EIGRP, EIGRP databáze

a) Na všech směrovačích nakonfigurujte směrovací protokol EIGRP s číslem autonomního systému 1 a vypněte automatickou sumarizaci cest. Následně si zobrazte směrovací tabulky a pomocí příkazu ***ping*** ověřte správnost konfigurace. Na rozdíl od OSPF máme pro konfiguraci EIGRP jen jeden způsob a to v konfiguračním režimu EIGRP. Zapněte si také debug pomocí příkazu ***debug eigrp packets*** a zachyťte sestavení sousedstvý, prohlédněte si výpis a poté debug vypněte.

```
R1(config)#router eigrp 1
R1(config-router)#network 192.168.1.0
R1(config-router)#no auto-summary
```

```
R1#debug eigrp packets
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK,
STUB, SIAQUERY, SIAREPLY)
R1#
R1#
*Mar  1 01:02:05.451: EIGRP: Sending HELLO on FastEthernet0/0
*Mar  1 01:02:05.451:   AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ
un/rely 0/0
*Mar  1 01:02:05.547: EIGRP: Received HELLO on FastEthernet0/0
nbr 192.168.1.2
*Mar  1 01:02:05.551:   AS 1, Flags 0x0, Seq 0/0 idbQ 0/0
*Mar  1 01:02:05.551: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1:
Neighbor 192.168.1.2 (FastEthernet0/0) is up: new adjacency
R1#
*Mar  1 01:02:05.551: EIGRP: Enqueueing UPDATE on
FastEthernet0/0 nbr 192.168.1.2 iidbQ un/rely 0/1 peerQ un/rely
0/0
*Mar  1 01:02:05.555: EIGRP: Requeued unicast on
FastEthernet0/0
*Mar  1 01:02:05.559: EIGRP: Sending HELLO on FastEthernet0/0
*Mar  1 01:02:05.559:   AS 1, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ
un/rely 0/0
*Mar  1 01:02:05.563: EIGRP: Sending UPDATE on FastEthernet0/0
nbr 192.168.1.2
```

```
*Mar  1 01:02:05.563:   AS 1, Flags 0x1, Seq 15/0 idbQ 0/0
iidbQ un/rely 0/0 peerQ un/rely 0/1
*Mar  1 01:02:05.579: EIGRP: Received UPDATE on FastEthernet0/0
nbr 192.168.1.2
```

```
R1#sh ip route
< skrácený výstup >
Gateway of last resort is not set

D 192.168.4.0/24 [90/2198016] via 10.1.3.2, 00:51:50, Serial0/2
                 [90/2198016] via 10.1.2.2, 00:51:50,Serial0/1
                 [90/2198016] via 10.1.1.2, 00:51:50,Serial0/0
D 192.168.5.0/24 [90/2221056] via 10.1.3.2, 00:51:50, Serial0/2
                 [90/2221056] via 10.1.2.2, 00:51:50, Serial0/1
                 [90/2221056] via 10.1.1.2, 00:51:50, Serial0/0
     10.0.0.0/24 is subnetted, 3 subnets
C       10.1.3.0 is directly connected, Serial0/2
C       10.1.2.0 is directly connected, Serial0/1
C       10.1.1.0 is directly connected, Serial0/0
D 192.168.2.0/24 [90/2195456] via 10.1.3.2, 00:51:53, Serial0/2
                 [90/2195456] via 10.1.2.2, 00:51:53, Serial0/1
                 [90/2195456] via 10.1.1.2, 00:51:53, Serial0/0
D 192.168.3.0/24 [90/2172416] via 10.1.3.2, 00:52:01, Serial0/2
                 [90/2172416] via 10.1.2.2, 00:52:01, Serial0/1
                 [90/2172416] via 10.1.1.2, 00:52:01, Serial0/0
```

b) Z výpisu vidíme, že R2 má navázáno sousedstvý na pěti linkách.

```
R2#sh ip eigrp accounting
IP-EIGRP accounting for AS(1)/ID(192.168.3.1)
Total Prefix Count: 7  States: A-Adjacency, P-Pending, D-Down
State Address/Source   Interface  Prefix   Restart  Restart/
                                  Count     Count   Reset(s)
 A    10.1.3.1         Se0/2        2        0        0
 A    10.1.2.1         Se0/1        2        0        0
 A    10.1.1.1         Se0/0        2        0        0
 A    192.168.2.2      Fa0/1        2        0        0
 A    192.168.3.2      Fa1/0        2        0        0
```

```
R2#sh ip eigrp interfaces
IP-EIGRP interfaces for process 1

                     Xmit Queue Mean   Pacing Time   Multicast
  Interface    Peers  Un/Reliable SRTT   Un/Reliable   Flow
Time
Se0/0            1        0/0       28       0/15          903
Se0/1            1        0/0       21       0/15          895
Se0/2            1        0/0       16       0/15          175
Fa0/1            1        0/0      110       0/10          596
Fa1/0            1        0/0       66       0/10          320
```

c) Zobrazte si informace o sousedech. Ve výpise vidíme sloupec ozančen H. Hodnoty podním nám udávají v jakém pořadí bylo navázáno sousedstvý. Takže ze sousedem 10.1.3.1 bylo soousedstvý navázáno jako s druhým v pořradí. Dále je zobrazena adresa souseda, rozhraní přes, které dostáva od něj hello pakety, ***hold time*** – doba po kterou čeká IOS kým označí souseda za nedostupného když neobdrží od něj žádnou zprávu. Při defaultním nastavení je tato doba méně než 15s. Dále tam máme ***uptime*** což je doba po kterou je sousedstvý navázáno. ***SRTT*** je doba v milisekundách a udává nám kolik milisekund uplyne od odeslání paketu sousedovy a obdržení potvrzení daného paket, (Smooted round-trip time). **RTO** nám značí čas po, který IOS čeká kým odešle paket sousedovy z vysílací fronty. ***Q Cnt*** udává počet EIGRP paketů, které čekají na odeslání. **Seq num** nám značí sekvenční číslo posledního paketu přijatého od daného souseda.

```
R2#sh ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address     Interface   Hold Uptime    SRTT   RTO  Q  Seq
                            (sec)          (ms)       Cnt Num
2   10.1.3.1    Se0/2       13 00:14:36    16    200  0  47
1   10.1.2.1    Se0/1       14 00:14:36    21    200  0  49
0   10.1.1.1    Se0/0       13 00:14:36    28    200  0  48
4   192.168.2.2 Fa0/1       12 00:24:48   110    660  0  11
3   192.168.3.2 Fa1/0       11 00:24:56    66    396  0  12
```

d) Podrobnější výpis si můžeme zobrazit pomocí příkazu ***sh ip eigrp neighbors detail***. Kde máme výpis doplněn o další informace. ***Version*** udává verzi, kterou daný soused používá. Sloupec ***retrans*** a ***retries*** nám udává počet vyslání a počet pokusů o vyslání paketu. Počet prefixů nám zančí poslední sloupec.

```
R2#sh ip eigrp neighbors  detail
IP-EIGRP neighbors for process 1
H   Address     Interface Hold Uptime   SRTT   RTO  Q  Seq
                          (sec)         (ms)       Cnt Num
2   10.1.3.1      Se0/2            11 00:28:22   16   200  0  47
   Version 12.4/1.2, Retrans: 0, Retries: 0, Prefixes: 2
1   10.1.2.1    Se0/1             10 00:28:23   21   200  0  49
   Version 12.4/1.2, Retrans: 0, Retries: 0, Prefixes: 2
0   10.1.1.1    Se0/0             13 00:28:23   28   200  0  48
   Version 12.4/1.2, Retrans: 0, Retries: 0, Prefixes: 2
4   192.168.2.2  Fa0/1            12 00:38:34  110   660  0  11
   Version 12.4/1.2, Retrans: 1, Retries: 0, Prefixes: 2
3   192.168.3.2  Fa1/0             13 00:38:43   66   396  0  12
   Version 12.4/1.2, Retrans: 4, Retries: 0, Prefixes: 2
```

e) Informace o provozu v autonomním systému si můžeme zobrazi pomocí příkazu ***sh ip eigrp traffic***. Výpis nám dává informace o počtu EIGRP paketů.

```
R2#sh ip eigrp traffic
IP-EIGRP Traffic Statistics for AS 1
  Hellos sent/received: 4698/4489
  Updates sent/received: 34/51
  Queries sent/received: 5/8
  Replies sent/received: 8/5
  Acks sent/received: 41/30
  Input queue high water mark 6, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 229
  PDM Process ID: 228
```

f) Pomocí příkazu ***sh ip protocols*** si zobrazte další informace o EIGRP. Všiměnete si nastavení K hodnot pro výpočet metriky. Dále vidíme, že automatická sumarizace je vypnutá, což jsme provedli při konfiguraci směrování. Dále vidíme pro, které sítě máme nastaveno směrování, zdroje směrovacích informací a defaultní administrativní vzdálenost, která je pro protokol EIGRP 90.

```
R2#sh ip protocols
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
    192.168.2.0
    192.168.3.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.2.1              90      01:02:17
    10.1.3.1              90      01:02:17
    10.1.1.1              90      01:02:17
    192.168.2.2           90      01:02:17
    192.168.3.2           90      01:02:17
  Distance: internal 90 external 170
```

g) Příkazem ***sh ip eigrp topology*** si zobrazte topologickou databázi.

```
R2#sh ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(192.168.3.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R -
Reply,
       r - reply Status, s - sia Status

P 10.1.3.0/24, 1 successors, FD is 2169856
        via Connected, Serial0/2
P 10.1.2.0/24, 1 successors, FD is 2169856
        via Connected, Serial0/1
P 10.1.1.0/24, 1 successors, FD is 2169856
        via Connected, Serial0/0
P 192.168.2.0/24, 1 successors, FD is 281600
        via Connected, FastEthernet0/1
P 192.168.3.0/24, 1 successors, FD is 28160
        via Connected, FastEthernet1/0
P 192.168.4.0/24, 1 successors, FD is 284160
        via 192.168.3.2 (284160/281600), FastEthernet1/0
P 192.168.5.0/24, 1 successors, FD is 307200
        via 192.168.2.2 (307200/281600), FastEthernet0/1
```

Z výpisu vidíme, že všechny cesty jsou označeny písmenkem P což značí ***passive***, to znamená, že směrovač nevyhledává nové cesty do dané destinace, síť je stabilní. Pro síť 192.168.5.0 máme jednoho ***successora***, ***feasible distance*** FD má hodnotu 307200, která udáva celkovou metriku z R2 do cílové sítě. Tato síť je dosažitelná přes rozhraní fa0/1 a next hop adresa je 192.168.2.2. Hodnota 307200/281600, 307200 je FD, kterou jsme si popsali výše. Hodnota 281600 je AD (***advvertised distancce***) je to metrika našeho souseda teda R4 do cílové sítě 192.168.5.0. To si můžeme ověřit výpisem topologické tabulky na R4.

```
R4#sh ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(192.168.5.1)
< skrácený výstup >
P 192.168.5.0/24, 1 successors, FD is 281600
        via Connected, FastEthernet0/1
```

1.3.5 Úkol 3 – Autentizace v EIGRP, nedisruptivní změna hesla, změna časovačů

a) Na lince mezi R2 a R4 nastavte autentizaci pomocí hešovacího algoritmu ***md5***. Pro ***key chain*** použijte název ***R2R4*** a jako heslo použijte slovo ***student***. Princip nastavení je takový, že se nejdříve v konfiguračním rozhraní směrovače nastavý key chain a pak heslo. Toto se pak aplikuje na konkrétní rozhraní.

```
R2(config)#key chain R2R4
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string student

R2(config)#int fa0/1
R2(config-if)#ip authentication mode eigrp 1 md5
R2(config-if)#ip authentication key-chain eigrp 1 R2R4

R4(config)#key chain R2R4
R4(config-keychain)#key 1
R4(config-keychain-key)#key-string student

R4(config)#int fa0/0
R4(config-if)#ip authentication mode eigrp 1 md5
R4(config-if)#ip authentication key-chain eigrp 1 R2R4
```

b) Informace o nastavní autentizace si zobrazíme pomocí příkazu ***show key chain.***

```
R2#sh key chain
Key-chain R2R4:
     key 1 -- text "student"
      accept lifetime (always valid) -(always valid) [valid now]
      send lifetime (always valid) - (always valid) [valid now]
```

c) Jak ste si všimly při konfiguraci autantizace v bodě b, tak změna klíče je disruptivní. Niní si úkážeme příklad konfigurace kdy změna klíče proběhne beze stráty sousedstvý a tak nebude ovlivněno směrování. U této úlohy je nutné podotknout, že je si zapotřebý skontrolovat aktuální čas na směrovači pomocí příkazu ***sh clock***, a případně upravit daný čas.

```
R2(config)#key chain R2R4
R2(config-keychain)#key 1
R2(config-keychain-key)# accept-lifetime 00:00:00 Jan 1 2016
00:20:00 April 1 2016
R2(config-keychain-key)# send-lifetime 00:00:00 Jan 1 2016
00:20:00 April 1 2016

R2(config-keychain-key)#exit
R2(config-keychain)#key 2
R2(config-keychain-key)#key
R2(config-keychain-key)#key-string student1
R2(config-keychain-key)#accept-lifetime 23:00:00 March 31 2016
infinite
R2(config-keychain-key)#send-lifetime 00:00:00 April 1 2016
infinite
```

```
R2#sh key chain
Key-chain R2R4:
    key 1 -- text "student"
        accept lifetime (00:00:00 UTC Jan 1 2016) - (00:20:00
UTC Apr 1 2016) [valid now]
        send lifetime (00:00:00 UTC Jan 1 2016) - (00:20:00 UTC
Apr 1 2016) [valid now]
    key 2 -- text "student1"
        accept lifetime (23:00:00 UTC Mar 31 2016) - (infinite)
        send lifetime (00:00:00 UTC Apr 1 2016) - (infinite)
```

Obdobně nakonfigurujte i R4. Nyní jsme nakonfigurovali autentizaci tak, že heslo ***student*** bude přijímáno do 1. Apríla 20 minut po půlnoci 2016, a také bude toto heslo do stejné doby odesílat. A začne přijímat nové heslo ***student1*** od 31. Marca jedenásté hodiny večer, 2016. Takže máme 1 hodinu a 20 minut na odstaranění starého hesla ***student***, bez toho abychom ovlivnily směrování.

d) Na směřovači R2 si zobrazte Hello a Hold intervaly.

```
 R2#sh ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address    Interface Hold Uptime   SRTT   RTO  Q  Seq
                         (sec)         (ms)       Cnt Num
4   192.168.2.2 Fa0/1  10 00:16:51   47   282  0  22
< skrácený výstup >
```

```
R2#sh ip eigrp interfaces detail fastEthernet 0/1
IP-EIGRP interfaces for process 1

< skrácený výstup >
  Hello interval is 5 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/3  Un/reliable ucasts: 4/9
  Mcast exceptions: 2  CR packets: 2  ACKs suppressed: 4
  Retransmissions sent: 1  Out-of-sequence rcvd: 2
  Authentication mode is md5,  key-chain is "R2R4"
```

Z výpisů vidíme, že Hello interval je 5s a Hold interval je vždy méně než 15s. Nyní upravíme hodnoty těchto časovačů na Hello=3s a Hold=8s, na lince mezi R2 a R4. Nastavení ověřte.

```
R2(config)#int fa0/1
R2(config-if)#ip hello-interval eigrp 1 3
R2(config-if)#ip hold-time eigrp 1 8

R4(config)#int fa 0/0
R4(config-if)#ip hello-interval eigrp 1 3
```

```
R4(config-if)#ip hold-time eigrp 1 8
```

```
R2#sh ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address      Interface       Hold Uptime   SRTT   RTO  Q
Seq
                                (sec)         (ms)       Cnt Num
4   192.168.2.2  Fa0/1             6 00:30:21   47   282  0   22
```

```
R2#sh ip eigrp interfaces detail fastEthernet 0/1
IP-EIGRP interfaces for process 1
< skrácený výstup >
  Hello interval is 3 sec
  Next xmit serial <none>
  Un/reliable mcasts: 0/3  Un/reliable ucasts: 4/9
  Mcast exceptions: 2  CR packets: 2  ACKs suppressed: 4
  Retransmissions sent: 1  Out-of-sequence rcvd: 2
  Authentication mode is md5,  key-chain is "R2R4"
```

1.3.6 Úkol 4 – Failover linek, úprava metriky, rovnoměrný a nerovnoměrný load balancing

a) Vaším úkolem je provést změny konfigurace tak aby pouze linky s0/0 a 0/1 mezi R1 a R2 byli použity pro přenos s rovnoměrným load balancingem a linka s0/2 bude jako záložná a bude použita v případe, že obě linky s0/0 i 0/1 selžou.

```
R1#sh ip route
< skrácený výstup >

D 192.168.4.0/24 [90/2198016] via 10.1.3.2, 00:08:30, Serial0/2
                 [90/2198016] via 10.1.2.2, 00:08:30, Serial0/1
                 [90/2198016] via 10.1.1.2, 00:08:30, Serial0/0
< skrácený výstup >
```

Ze směrovací tabulky na R1 vidíme, že se pro přenos využívají všechny tři sériové linky. Také z výstupu topologické tabulky vidíme, že například pro síť 192.168.4.0/24 má R1 tři successory. To proto, že všechny tři liky mají stejnou metriku, a parametr ***maximum path*** je defaultně nastaven na hodnotu 4 což si můžeme skontrolovat ve výpise ***sh ip protocols*** na R1. Takže proto se do směrovací tabulky dostanou všechny tři cesty. EIGRP defaultně provádí rovnoměrný load balancing mezi cestami, je nutné podotknout, že tento load balancing se provádí takzvaně per destination, to zanamená, že skupina paketů určená do stejné destinace je zasílána stejnou cestou. Typ load balancingu můžeme změnit na per paket pomocí příkazu ***ip load - sharing per – paket*** v konfiguračním rozhraní interfejsu. Tvrzení, že pro přenos se používají všechny tři cesty

si můžeme ověřit také pomoci příkazu traceroute.

```
R1#sh ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(10.1.3.1)

< skrácený výstup >

P 192.168.4.0/24, 3 successors, FD is 2198016
        via 10.1.3.2 (2198016/284160), Serial0/2
        via 10.1.2.2 (2198016/284160), Serial0/1
        via 10.1.1.2 (2198016/284160), Serial0/0
```

```
R1#sh ip protocols
Routing Protocol is "eigrp 1"
  < skrácený výstup >

  Maximum path: 4
  < skrácený výstup >
```

```
R1#traceroute 192.168.5.1

Type escape sequence to abort.
Tracing the route to 192.168.5.1

  1 10.1.3.2 4 msec
    10.1.2.2 16 msec
    10.1.1.2 8 msec
```

b) Upravíme metriku sériových linek. EIGRP počíta metriku také ze šířky pásma, parametr BW ve výpise ***sh ip interfaces s0/0***.

```
R1#sh interfaces serial 0/0
Serial0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
< skrácený výstup >
```

Na lince s0/0 necháme parametr BW tak jak je, ale na lince s0/1 nastavíme tuto hodnotu na 772 kb a na lince s0/2 nastavíme na 380 kb.

```
R1(config)#int se0/1
R1(config-if)#bandwidth 772
R1(config-if)#exit
R1(config)#int se0/2
R1(config-if)#bandwidth 380

R2(config)#int se0/1
R2(config-if)#bandwidth 772
R2(config-if)#exit
R2(config)#int se0/2
```

```
R2(config-if)#bandwidth 380
```

c) Zobrazte si směrovací a topologickou tabuku na R1 a porovnejte jí s výstupem v bodě a). Vidíme, že v směrovací tabulce je pouze jedna cesta do sítě 192.168.4.0/24. A to cesta přes s0/0. V topologické tabulce vidíme, že do této sítě má tři cesty ale pouze jednoho successora. A tím je cesta přes s0/0.

```
R1#sh ip route
< skrácený výstup >
D    192.168.4.0/24 [90/2198016] via10.1.1.2,00:00:54, Serial0/0
```

```
R1#sh ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(10.1.3.1)

< skrácený výstup >

P 192.168.4.0/24, 1 successors, FD is 2198016
        via 10.1.1.2 (2198016/284160), Serial0/0
        via 10.1.3.2 (7276800/284160), Serial0/2
        via 10.1.2.2 (3856128/284160), Serial0/1
```

d) Parametr ***maximum path*** změníme na hodnotu 2 aby EIGRP mohl využívat pro load balancing pouze dvě cesty. Změnu provedeme v konfiguračním režimu EIGRP protokolu na R1 a R2.

```
R1(config)#router eigrp 1
R1(config-router)#maximum-paths 2
```

e) Změníme hodnotu parametru ***maximum metric variance*** na 2, defaultní hodnota tohoto parametru je nastavena na 1 a můžeme si to skontrolovat ve výpise příkazu ***sh ip protocols***. Tato změna umožní to aby byl prováděn load balancing mezi linkami s0/0 a s0/1. Nastavení provedeme opět v konfiguračním rozhraní EIGRP protokolu. Nastavení provedeme na R1 i R2.

```
R1#sh ip protocols
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
< skrácený výstup >
```

```
R1(config)#router eigrp 1
```

```
R1(config-router)#variance 2
```

f) Zobrazíme si směrovací a topologickou tabulku na R1 a výstup porovnáme s výstupy v bodě a) a c). Vidíme, že v směrovací tabulce jsou již dva záznamy pro síť 192.168.4.0/24. A v topologické tabulce je pořád jeden successor. Pro přenos se využívají linky s0/0 a s0/1. Všimněte si, že v směrovací tabulce jsou dvě cesty s odlišnou metrikou, to nám umožnila změna parametru variance na 2. A toto je nerovnoměrný load balancing.

```
R1#sh ip route
< skrácený výstup >

D    192.168.4.0/24[90/3856128]via 10.1.2.2,00:00:51, Serial0/1
                   [90/2198016]via 10.1.1.2,00:00:51, Serial0/0
< skrácený výstup >
```

```
R1#sh ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(10.1.3.1)

< skrácený výstup >
P 192.168.4.0/24, 1 successors, FD is 2198016
        via 10.1.1.2 (2198016/284160), Serial0/0
        via 10.1.3.2 (7276800/284160), Serial0/2
        via 10.1.2.2 (3856128/284160), Serial0/1
```

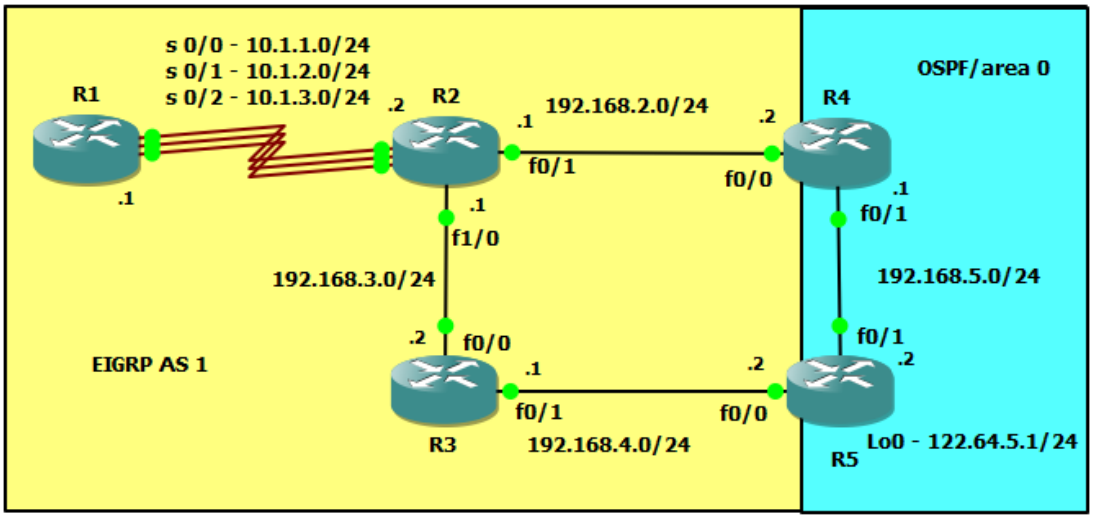
g) Nyní vyzkoušíme jestli nám funguje linka s0/2 jako záložní, pro situaci kdy obě linky s0/0 a s0/1 selžou. Vypněte sériové rozhraní s0/0 a s0/1 na R1. Poté si zobrazte směrovací a topologickou tabulku na R1.

```
R1(config-if)#do sh ip route
< skrácený výstup >

D  192.168.4.0/24 [90/7276800] via 10.1.3.2,00:00:05, Serial0/2
```

```
R1(config)#do sh ip eigrp topo
IP-EIGRP Topology Table for AS(1)/ID(10.1.3.1)

< skrácený výstup >
P 192.168.4.0/24, 1 successors, FD is 2198016
        via 10.1.3.2 (7276800/284160), Serial0/2
```

Z výpisu vidíme, že v směrovací tabulce se objevila cesta přes linku s0/2. Také v topologické tabulce se tato cesta objevila jako successor. Znovu zapněte rozhraní s0/0 a s0/1 a samostatně ověřte, že tyto rozhraní se opět používají pro přesnos.

1.3.7 Úkol 5 – Redistribuce cest mezi EIGRP a OSPF



Obrázok 34: Úloha 3 - úkol 5

a) Provedtě změnu konfigurace sítě podle obrázku č.34. Vypněte rozesílání sitě 192.168.5.0/24 směrovacím protokolem EIGRP. Nakonfigurujte směrovací protokol OSPF aby rozesílal síť 192.168.5.0/24. Dále nakonfigurujte loopback rozhraní na R5, zaneste ho do směrovacího procesu OSPF, změnte typ sítě na tomto rozhraní aby byla odesílána správná maska /24. Samostatně ověřte konfiguraci OSPF.

```
R4(config)#router eigrp 1
R4(config-router)#no network 192.168.5.0
R4(config)#int fa0/1
R4(config-if)#ip ospf 1 area 0
R5(config)#int lo0
R5(config-if)#ip address 122.64.5.1 255.255.255.0
R5(config-if)#ip ospf network point-to-point
R5(config-if)#ip ospf 1 area 0
R5(config)#router eigrp 1
R5(config-router)#no network 192.168.5.0
R5(config)#int fa0/1
R5(config-if)#ip ospf 1 area 0
```

b) Zobrazte si směrovací tabulku na R1 a ověřte, že neobsahuje sítě z OSPF domény.

```
R1#sh ip route
< skrácený výstup >

Gateway of last resort is not set

D    192.168.4.0/24 [90/3856128]via10.1.2.2,01:05:24, Serial0/1
                    [90/2198016]via10.1.1.2,01:05:24, Serial0/0
```

```
     10.0.0.0/24 is subnetted, 3 subnets
C       10.1.3.0 is directly connected, Serial0/2
C       10.1.2.0 is directly connected, Serial0/1
C       10.1.1.0 is directly connected, Serial0/0
D    192.168.2.0/24 [90/3853568]via10.1.2.2,01:05:24, Serial0/1
                    [90/2195456]via10.1.1.2,01:05:24, Serial0/0
D    192.168.3.0/24 [90/3830528]via10.1.2.2,01:05:24, Serial0/1
                    [90/2172416]via10.1.1.2,01:05:27, Serial0/0
```

c) Na směrovači R4 nastavte redistribuci cest z OSPF do EIGRP. Při redistribuci OSPF do EIGRP musíme zadat hodnoty, které slouží pro výpočet metriky v EIGRP pro danou cestu. První hodnota nám udáva sířku pásma v kb, dále pak spoždění v mikrosekundách, spolehlivost, efektivní šířka pásma a velikost MTU.

```
R4(config)#router eigrp 1
R4(config-router)#redistribute ospf 1 metric 1144 50 150 5 1500
```

d) Na R1 si zobrazte směrovací tabulku a prostudujte ji. Vidíme, že se nám v tabulce objevili redistribuované cesty do sítí z OSPF domény.

```
R1#sh ip route
< skrácený výstup >
D    192.168.4.0/24[90/3856128]via 10.1.2.2,00:21:19, Serial0/1
                   [90/2198016]via 10.1.1.2,00:21:19, Serial0/0
D EX 192.168.5.0/24[170/3866368]via10.1.2.2,00:00:56, Serial0/1
                   [170/2788096]via10.1.1.2,00:00:56, Serial0/0
     10.0.0.0/24 is subnetted, 3 subnets
C       10.1.3.0 is directly connected, Serial0/2
C       10.1.2.0 is directly connected, Serial0/1
C       10.1.1.0 is directly connected, Serial0/0
     122.0.0.0/24 is subnetted, 1 subnets
D EX    122.64.5.0[170/3866368]via 10.1.2.2,00:00:59, Serial0/1
                  [170/2788096]via 10.1.1.2,00:00:59, Serial0/0
```

1.3.8 Úkol 6 - řízení toku dat – samostatní úkol

Proveďte změnu konfigurace tak aby opět v celé topologii byl použit protokol EIGRP. Ze směrovače R4 proveďte ***traceroute*** na sériové rozhraní směrovače R1. Všiměte si že je použita vždy pouze jedna cesta a to 192.168.2.1. Vaším úkolem je provést změnu konfigurace tak aby byl traffic posílán i cestou přes R5 a to v poměru 2:3. Teda 2 pakety půjdou přes R2 a další 3 přez R5. Dosáhněte toho změnou parametru ***delay***.

Řešení samostatního úkolu

a) Zrušíme redistribuci a opět v celé topologii zavedeme protokol EIGRP. Ověříme vypsáním směrovacích tabulek.

```
R4(config)#router eigrp 1
R4(config-router)#no redistribute ospf 1 metric 1144 50 150 5
1500
R4(config)#int fa0/1
R4(config-if)#no ip ospf 1 area 0
R4(config)#router eigrp 1
R4(config-router)#network 192.168.5.0


R5(config)#int fa0/1
R5(config-if)#no ip ospf 1 area 0
R5(config-if)#int lo0
R5(config-if)#no ip ospf 1 area 0
R5(config)#router eigrp 1
R5(config-router)#network 192.168.5.0
```

b) Na rozhraních fa 0/0 a fa 0/1 směrovače R4 musíme změnit typ defaultního load – balancingu kterým je per-destination na per-paket.

```
R4(config)#int fa0/0
R4(config-if)#ip load-sharing per-packet

R4(config)#int fa0/1
R4(config-if)#ip load-sharing per-packet
```

c) Zobrazíme si hodnotu delay na rozhraní fa 0/0 na R4. Má hodnotu 1000 μsec. Tuto hodnotu změníme na 3000. A nastavíme parametr variance na 2.

```
R4#sh interfaces fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is c404.1680.0000 (bia
c404.1680.0000)
  Internet address is 192.168.2.2/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
```

```
R4(config)#int fa0/0
R4(config-if)#delay 3000
R4(config)#router  eigrp 1
R4(config-router)#variance 2
```

d) Správnost, že se využívají dvě cesty ověříme vypsáním směrovací a topologické tabulky.

```
R4#sh ip route
< skrácený výstup >

D    10.1.3.0 [90/7325440] via 192.168.5.2, 00:01:51, fa0/1
              [90/8016640] via 192.168.2.1, 00:01:51, fa0/0
D    10.1.2.0 [90/3904768] via 192.168.5.2, 00:01:51, fa0/1
              [90/4595968] via 192.168.2.1, 00:01:51, fa0/0
D    10.1.1.0 [90/2246656] via 192.168.5.2, 00:01:51, fa0/1
              [90/2937856] via 192.168.2.1, 00:01:52, fa0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
D    192.168.3.0/24 [90/332800] via 192.168.5.2, 00:01:52,
fa0/1
```

```
R4#sh ip eigrp topology

< skrácený výstup >
P 10.1.1.0/24, 1 successors, FD is 2246656
        via 192.168.5.2 (2246656/2221056), FastEthernet0/1
        via 192.168.2.1 (2937856/2169856), FastEthernet0/0
```

e) Posílání dat v poměru 2:3, ověříme pomocí příkazu ***sh ip route 10.1.1.0***. Hodnota ***traffic share count*** přes R5 je 30 a přes R2 je 23, což je poměr 2:3.

```
R4#sh ip route 10.1.1.0
Routing entry for 10.1.1.0/24
  Known via "eigrp 1", distance 90, metric 2246656, type
internal
  Redistributing via eigrp 1, ospf 1
  Last update from 192.168.2.1 on FastEthernet0/0, 00:11:23 ago
  Routing Descriptor Blocks:
  * 192.168.5.2, from 192.168.5.2, 00:11:23 ago, via
FastEthernet0/1
    Route metric is 2246656, traffic share count is 30
    Total delay is 23000 microseconds, minimum bandwidth is 1544
Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 3
    192.168.2.1, from 192.168.2.1, 00:11:23 ago, via
FastEthernet0/0
    Route metric is 2937856, traffic share count is 23
    Total delay is 50000 microseconds, minimum bandwidth is 1544
Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

1.3.9 Kontrolní otázky

1. Jaký typ load balancingu se provádi defaultně u EIGRP ?

2. Při konfiguraci OSPF protokolu nemusí být číslo AS stejné aby mohly směrovače sestavit sousedstvý, je tomu tak i u EIGRP protkolu ?

3. Z kterých dvou parametrů se počítá EIGRP metrika ?

4. Pomocí, kterých dvou parametrů můžeme ovlivňovat kolik cest je využito pro směrování ?

5. Co je to feasible successor ?

6 . Vysvětlete význam parametrů maximum path a variance.