

**Univerzita Pardubice**

**Fakulta elektrotechniky a informatiky**

**Měření doby konvergence síťové architektury  
při využití Singl-Area a Multiarea OSPF**

**Martin Jebavý**

**Bakalářská práce  
2016**

Univerzita Pardubice  
Fakulta elektrotechniky a informatiky  
Akademický rok: 2015/2016

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Martin Jebavý**  
Osobní číslo: **I13139**  
Studijní program: **B2646 Informační technologie**  
Studijní obor: **Informační technologie**  
Název tématu: **Měření doby konvergence síťové architektury při využití  
Single-Area a Multiarea OSPF**  
Zadávající katedra: **Katedra informačních technologií**

### Z á s a d y p r o v y p r a c o v á n í :

Cílem práce je podrobně představit principy fungování směrovacího protokolu OSPF se zdůrazněním rozdílů při nasazení protokolu v prostředí v rámci jedné a více oblastí. Autor dále navrhne možnosti měření konvergence fyzické topologie v režimech jedné a více oblastí, provede sadu měření konvergence sítě na různých topologiích a získané výsledky porovná s teoretickými předpoklady a výpočty doby konvergence protokolu OSPF.

Rozsah grafických prací:

Rozsah pracovní zprávy: 50

Forma zpracování bakalářské práce: tištěná

Seznam odborné literatury:

**RANSOME, James F a John W RITTINGHOUSE. Ospf 140 success secrets - 140 most asked questions on ospf - what you need: internet telephony and the future voice network. 1st edition. S.l.: Emereo Publishing, 2014, xxvii, 402 p. ISBN 978-148-8528-743.**

**MOY, John T a John W RITTINGHOUSE. OSPF complete implementation: internet telephony and the future voice network. 1st edition. Boston: Addison-Wesley, 2001, xxi, 372 s. ISBN 07-686-8216-9.**

Vedoucí bakalářské práce: **Mgr. Josef Horálek, Ph.D.**  
Katedra informačních technologií

Datum zadání bakalářské práce: **31. října 2015**  
Termín odevzdání bakalářské práce: **13. května 2016**



prof. Ing. Simeon Karamazov, Dr.  
děkan



L.S.



Mgr. Josef Horálek, Ph.D.  
vedoucí katedry

V Pardubicích dne 31. března 2016

## **PROHLÁŠENÍ**

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 9. 5. 2016

Martin Jebavý

## **PODĚKOVÁNÍ**

Rád bych poděkoval Mgr. Josefu Horálkovi Ph.D. za poskytnutí užitečných rad, připomínek a možností ke zpracování závěrečné práce. Dále bych chtěl poděkovat mé rodině za podporu, kterou mi věnovali během celého studia.

## **ANOTACE**

Závěrečná práce se zabývá měřením rychlosti konvergence při využití dynamického protokolu OSPF. V teoretické části jsou popsány metody směrování s důkladem na jejich rozdílnosti, výhody a nevýhody. Samostatná část práce se zabývá samotným protokolem OSPF, kde se vysvětlují vlastnosti, pakety a operační stavy protokolu. Praktická část zahrnuje měření v rámci jedné a více oblastí. Porovnávají se jejich vlastnosti, pozitiva a negativa v závislosti na zvolené konfiguraci. Je přiblížen postup pro měření konvergence a zjištění komunikačních cest v topologii. V závěru práce se vyhodnotí naměřené hodnoty a na základě výsledků se rozhodne, který ze dvou způsobů konfigurace bude výhodnější pro použití a kdy v budoucnu aplikovat jednotlivé druhy konfigurace.

## **KLÍČOVÁ SLOVA**

směrování, OSPF, měření konvergence, pakety, algoritmus, Single-Area, Multiarea, konfigurace

## **TITLE**

Measurement of the convergence time of network architecture with Single-Area and Multiarea OSPF

## **ANNOTATION**

The thesis covers measurement of the convergence time when using the dynamic OSPF protocol. In the theoretical part, different routing methods are described, along with differences, advantages and disadvantages of each method. Next part of the thesis is dedicated to the OSPF protocol, describing its characteristics, packets and operating states of the protocol. The practical part covers the measurement in the frame of a single-area and multiarea environment. Their characteristics, advantages and disadvantages are compared, in relation to the chosen configuration. The convergence measurement methodology is described, as well as the topology analysis for communication ways. The conclusion analyses the measured values, and decides which of the two configurations is more viable for use, and when to apply the individual configuration types in the future.

## **KEYWORDS**

routing, OSPF, measuring convergence, packets, algorithm, Single-Area, Multiarea, configuration

# OBSAH

|   |           |
|---|-----------|
| ÚVOD .....                                  | 12        |
| <b>1 LITERÁRNÍ REŠERŠE.....</b>             | <b>13</b> |
| <b>2 SMĚROVÁNÍ .....</b>                    | <b>15</b> |
| 2.1 STATICKÉ SMĚROVÁNÍ .....                | 15        |
| 2.2 DYNAMICKÉ SMĚROVÁNÍ .....               | 15        |
| 2.2.1 SMĚROVACÍ PROTOKOLY.....              | 16        |
| 2.2.2 VLASTNOSTI DYNAMICKÝCH PROTOKOLŮ..... | 17        |
| 2.2.3 PROTOKOLY VEKTORU VZDÁLENOSTI.....    | 18        |
| 2.2.4 PROTOKOLY STAVU LINKY.....            | 18        |
| 2.2.5 DIJKSTRŮV ALGORITMUS .....            | 19        |
| <b>3 OSPF .....</b>                         | <b>22</b> |
| 3.1 VLASTNOSTI OSPF .....                   | 22        |
| 3.1.1 ZÁKLADNÍ KOMPONENTY OSPF.....         | 23        |
| 3.1.2 DATOVÉ STRUKTURY .....                | 23        |
| 3.1.3 ZPRÁVY SMĚROVACÍHO PROTOKOLU .....    | 24        |
| 3.1.4 ALGORITMUS .....                      | 24        |
| 3.2 DRUHY PAKETŮ OSPF .....                 | 25        |
| 3.3 OPERAČNÍ STAVY OSPF.....                | 28        |
| 3.4 PAKETY LSA .....                        | 30        |
| <b>4 KONVERGENCE V SINGLE-AREA .....</b>    | <b>32</b> |
| 4.1 NEVÝHODY SINGLE-AREA .....              | 32        |
| 4.2 PAKETY LSA V SINGLE-AREA .....          | 33        |
| 4.3 MĚŘENÍ RYCHLOSTI KONVERGENCE.....       | 34        |
| 4.3.1 ZJIŠTĚNÍ KOMUNIKAČNÍCH CEST .....     | 35        |
| 4.3.2 MĚŘENÍ V SIMULAČNÍM PROGRAMU .....    | 36        |
| 4.3.3 MĚŘENÍ NA FYZICKÉM ZAŘÍZENÍ.....      | 38        |

|          |   |           |
|----------|---|-----------|
| <b>5</b> | <b>KONVERGENCE V MULTIAREA OSPF .....</b> | <b>39</b> |
| 5.1      | PAKETY LSA V MULTIAREA .....              | 41        |
| 5.2      | MĚŘENÍ RYCHLOSTI KONVERGENCE.....         | 42        |
| 5.2.1    | <i>MĚŘENÍ V SIMULAČNÍM PROGRAMU .....</i> | <i>43</i> |
| 5.2.2    | <i>MĚŘENÍ NA FYZICKÉM ZAŘÍZENÍ.....</i>   | <i>44</i> |
|          | <b>ZÁVĚR.....</b>                         | <b>45</b> |
|          | <b>POUŽITÁ LITERATURA.....</b>            | <b>46</b> |



## SEZNAM TABULEK A ILUSTRACÍ

|  |           |
|--|-----------|
| <b>Tabulka 1 – Administrativní vzdálenosti směrovacích protokolů .....</b> | <b>17</b> |
| <b>Tabulka 2 – Datová struktura OSPF .....</b>                             | <b>24</b> |
| <b>Tabulka 3 – Druhy paketů OSPF .....</b>                                 | <b>25</b> |
| <b>Tabulka 4 – OSPF Packet Header a OSPF Hello Packet.....</b>             | <b>26</b> |
| <b>Tabulka 5 – Pakety LSA .....</b>  | <b>30</b> |
|  |           |
| <b>Obrázek 1 – Stromová hierarchie dynamických protokolů.....</b>          | <b>16</b> |
| <b>Obrázek 2 – Dijkstrův algoritmus - část 1.....</b>                      | <b>19</b> |
| <b>Obrázek 3 – Dijkstrův algoritmus - část 2.....</b>                      | <b>20</b> |
| <b>Obrázek 4 – Dijkstrův algoritmus - část 3.....</b>                      | <b>20</b> |
| <b>Obrázek 5 – Dijkstrův algoritmus - část 4.....</b>                      | <b>21</b> |
| <b>Obrázek 6 – Dijkstrův algoritmus - část 5.....</b>                      | <b>21</b> |
| <b>Obrázek 7 – Základní vlastnosti OSPF protokolu.....</b>                 | <b>23</b> |
| <b>Obrázek 8 – OSPF paket.....</b>   | <b>26</b> |
| <b>Obrázek 9 – Postup stavů OSPF .....</b>                                 | <b>28</b> |
| <b>Obrázek 10 – Pakety LSA v Single-Area Top. 1.....</b>                   | <b>33</b> |
| <b>Obrázek 11 – Pakety LSA v Single-Area Top. 2.....</b>                   | <b>34</b> |
| <b>Obrázek 12 – Měřená topologie Single-Area .....</b>                     | <b>35</b> |
| <b>Obrázek 13 – Pakety LSA v Multiarea.....</b>                            | <b>41</b> |
| <b>Obrázek 14 – Měřená topologie Multiarea.....</b>                        | <b>43</b> |

## SEZNAM ZKRATEK A ZNAČEK

|       |  |
|-------|--|
| ABR   | Area Border Router                         |
| ASBR  | Autonomous System Boundary Router          |
| DR    | Designated Router                          |
| BDR   | Backup Designated Router                   |
| BGP   | Border Gateway Protocol                    |
| CIDR  | Classless Interdomain Routing              |
| CPU   | Central Processing Unit                    |
| DBD   | Database description                       |
| EGP   | Exterior Gateway Protocols                 |
| EIGRP | Enhanced Interior Gateway Routing Protocol |
| IGP   | Interior Gateway Protocols                 |
| IGRP  | Interior Gateway Routing Protocol          |
| IPv4  | Internet Protocol version 4                |
| IPv6  | Internet Protocol version 6                |
| IS-IS | Intermediate System to Intermediate System |
| LSA   | Link-state advertisement                   |
| LSAck | Link-state acknowledgment                  |
| LSDB  | Link-state database                        |
| LSR   | Link-state request                         |
| LSU   | Link-state update                          |
| MD5   | Message Digest 5                           |
| NBMA  | Non-broadcast multiaccess                  |
| OPNET | Optimized Network Engineering Tools        |
| OSI   | Open Systems Interconnection               |
| OSPF  | Open Shortest Path First                   |

|      |                              |
|------|------------------------------|
| SPF  | Shortest Path First          |
| RAM  | Random Access Memory         |
| RID  | Router ID                    |
| RIP  | Routing Information Protocol |
| VLSM | Variable-Length Subnet Mask  |

## ÚVOD

Začátkem bude představeno fungování směrování a jeho rozdělení. Práce představí dynamické, kam patří OSPF protokol, ale i statické směrování. Bude přiblíženo hlavně dynamické směrování, kde se protokoly rozdělí do větví podle jejich vlastností s přiblížením, v jaké části rozčleněné hierarchie se OSPF protokol nachází. V následujících částí se v krátkosti rozebere hierarchie dělení dynamických protokolů. Umožní získat správný pohled na zařazení a fungování OSPF, které zahrnuje charakteristiku a odlišnosti od jiných větví v hierarchickém dělení. OSPF protokol využívá pro směrování Dijkstrův algoritmus, proto je nutné se seznámit podrobně s jeho fungováním, na jehož základě se určují nejkratší cesty k cíli v síti.

Následující kapitola bude věnována protokolu OSPF se zaměřením zejména na jeho základní vlastnosti, které určují charakter protokolu. OSPF obsahuje několik komponentů a různé druhy paketů. Budou rozebrány jednotlivé stavy, do kterých se směrovače dostávají, než dojde ke konvergenci. Důležitým bodem bude vysvětlení jednotlivých typů paketů LSA, se kterými se pracuje v další části práce.

Praktická část se bude věnovat měření na vlastní vytvořené topologii nakonfigurované jako Single-Area. Představí se konfigurace a použití v praxi. Budou ukázány základní nevýhody konfigurace v Single-Area. Na demonstrativních topologiích se přiblíží výskyt paketů LSA v rámci jedné oblasti. Na začátku měření se vysvětlí postup zjištění komunikačních cest mezi zdrojovým a cílovým směrovačem ve vytvořené topologii. Další body kapitoly se budou věnovat samotnému měření konvergence v simulačním programu a na fyzickém zařízení. Podrobněji se vysvětlí postup měření konvergence, který se bude využívat ve všech následujících měřeních.

Následně se upraví vytvořená topologie z předchozí kapitoly a překonfiguruje z původního nastavení Single-Area na Multiarea. Budou vysvětleny základní vlastnosti Multiarea, odlišnosti oproti Single-Area, výhody použití, typy oblastí a jednotlivé typy skupin směrovačů. Důkladně se rozeberou typy paketů LSA, které se vyskytují v topologii rozdělené na více oblastí. Následuje měření v simulačním programu a na fyzickém zařízení, kde se využijí poznatky a postupy z předešlého měření.

V závěru práce se zhodnotí výsledky jednotlivých měření a porovnájí se s teoretickými předpoklady. Rozhodne se, který ze dvou způsobů konfigurace bude výhodnější pro použití na testované topologii a kdy v budoucnu aplikovat jednotlivé druhy konfigurace.

## 1 LITERÁRNÍ REŠERŠE

Účelem závěrečné práce je představit fungování směrovacího protokolu OSPF. V dané kapitole budou ukázány jednotlivé práce, které pomohou rozšířit obzor a přiblížit řešenou problematiku.

Článek „*Zlepšení rychlosti konvergence a škálovatelnosti OSPF*“ byl publikován v práci „*Communications Surveys & Tutorials*“ v roce 2012, který byl napsán Goyal M., Soperi M. a dalšími, je rozdělen do několika sekcí, která budou ve zkratce shrnuta. Úvod popisuje základní vlastnosti dynamického protokolu. Zahrnuje historii od samotné existence, jeho vývoj v průběhu času a poukazuje na další rivalitní protokoly. Zdůrazňuje důležité vlastnosti, charakteristické znaky a uplatnění v praxi. Další část zahrnuje řešení rozložení sítě do oblastí podle velikosti sítě. Přibližuje základní komunikaci mezi prvky v topologii při prvním připojení do sítě. Na tuto sekci navazuje kapitola o detekování nesprávné konfigurace popřípadě selhání prvků v topologii. Věnuje se zde komplexnímu řešení postupu při vyskytnutí chyby v síti od hardwarové až po softwarovou konfiguraci. V neposlední řadě se práce věnuje detailnějšímu pohledu na komunikaci mezi dvěma směrovači. Poukazuje nejen na základní vlastnosti průběhu informací mezi prvky, ale navrhuje nám různá vylepšení pro komunikaci, která může zefektivnit a ulehčit výměnu informací. Další část popisuje, jak směrovače získávají informace o topologii sítě. Řeší se, jestli se prvky nacházejí v jedné oblasti nebo ve více oblastech. V následující části je podrobně popsán specifický algoritmus pro určení nejlepší komunikace mezi směrovači. Tyto důležité sekce práce pomohou při řešení a objasnění problematiky závěrečné práce.

Publikace článku „*Area Configuration and Link Failure Effect in IP Networks using OSPF Protocol*“, který je obsažen v práci „*International Journal of Scientific and Research Publications*“, byl vydaný v dubnu 2013, umožní větší přehled o problematice OSPF a dalších dynamických protokolů. Z větší části je řešeno fungování OSPF v Single-Area nebo Multiarea. Pro podrobnější znázornění obsahuje článek vyobrazené různé topologie, na kterých je vysvětleno především fungování Multiarea OSPF. Navazuje na to představení paketů OSPF a jejich popis a fungování. Praktická část článku se věnuje několika scénářům, kde je OSPF nakonfigurována podle různých parametrů. Výsledkem měření jsou různé scénáře. Na základě porovnání nejkratších cest, provozů v síti a přenosů dat je vybrán nejlepší scénář k pozdější implementaci. V neposlední řadě závisí výběr na počtu vyskytnutých chyb nebo výpadků v síti.

Práce „*A comparative study on RIP and OSPF protocols*“, kde nás Jayakumar a další spoluautoři informují o důležitosti procesu směrování datových paketů v internetu. Směrovací protokol specifikuje způsob komunikace mezi směrovači propojených mimo jednu síť. Je představena řada směrovacích protokolů, jako je OSPF, RIP, EIGRP, OPNET, IGRP, atd., kde každá z nich má své určité vlastnosti. Dokument představuje jednoduché srovnávací studie RIP a dynamického směrovacího protokolu OSPF.

„*Implementing OSPF Protocol in CISCO 2800 Series Router*“ sepsána Ramya a Vishnu Vinod, představuje řešení implementace dynamického protokolu RIP a poukázání na nevhodnost jeho použití ve větších sítích. Neúčelnost se pokusí nahradit protokolem OSPF. Na začátku je představen pojem směrovací protokol, definice protokolu a popsání modelu OSI. Fungování a specifické vlastnosti protokolu RIP jsou popsány v další části práce. Tato část se věnuje charakteristice protokolu OSPF, při níž je patrné, v čem a jak se protokoly liší. Následuje simulace, která objasňuje nevýhody použití RIP ve větších topologiích. Ukazuje na nedostatky protokolu RIP a jeho omezené vlastnosti. Cílem projektu je porozumět, že všechny hlavní nevýhody RIP mohou být překonány prostřednictvím OSPF, které zahrnuje i další různá vylepšení.

V článku „*Autonomous System Network Topology Discovery Algorithm Based On OSPF Protocol*“ se prezentuje algoritmus na objevení topologie sítě založený na protokolu OSPF a jeho představení. Autoři poukazují na důležitost správného sestavení topologie sítě. Vysvětluje plno pojmů, které souvisí nebo částečně zahrnuje OSPF. Důležitou část tvoří podrobné popsání fungování algoritmu OSPF. Experiment s OSPF v práci ukazuje postupné analyzování sítě. Závěr hodnotí experiment a možnosti OSPF protokolu.

## 2 SMĚROVÁNÍ

Datové sítě se využívají v každodenním životě k různým věcem. Pracovní rozsah závisí na nasazení v malých lokálních nebo velkých globálních sítích. Doma může mít uživatel jeden směrovač a více počítačů. V pracovní odvětví závisí počet směrovačů a přepínačů dle velikosti organizace, kde se počty diametrálně liší na charakteru firmy.

Směrování je jádrem pro veškerou komunikaci od zdroje k cíli. Směrovače jsou zařízení zodpovědné za přenos paketů z jedné sítě do druhé. Dozví se o vzdálených sítích buď dynamicky, pomocí směrovacích protokolů, nebo ručně, pomocí statických cest. Ve větších sítích se mnohdy objevuje kombinace obou způsobů. Rozlišují se dvě možnosti směrování:

- statické
- a dynamické směrování.

V práci bude důležitou složkou zejména dynamické směrování se zaměřením na protokol OSPF.

### 2.1 STATICKÉ SMĚROVÁNÍ

Patří k nejjednodušší formě směrování v rámci malých sítí. V porovnání s dynamickým směrováním, statické nabízí větší bezpečnost, menší náročnost na paměť a na procesorový čas směrovače. Administrátor sítě musí znát celou topologii sítě, kde se jednotlivé prvky nacházejí a s jakým nastavením. Každý prvek v síti je na pevně nastaven a v případě připojení nového zařízení, musí administrátor pevně stanovit cestu k připojenému prvku. Je-li v síti více a více prvků zvyšuje se čas i náklady na údržbu sítě. Více prvků znamená více výpadků, a proto se musí administrátor účastnit řešení každého výpadku, který nastane, z důvodu staticky nastavených cest mezi směrovači.

### 2.2 DYNAMICKÉ SMĚROVÁNÍ

Pokud je velká síť a mnoho podsítí, konfigurace a údržba statické trasy vyžaduje velkou administrativní a provozní režie. Obzvláště náročná bude provozní režie, jestli dojde ke změnám v síti, zejména při výpadku nebo při implementaci nového prvku do sítě. Implementace dynamického směrování umožní zmírnit tíhu úkolů na konfiguraci a údržbu administrátorem, tím nám umožní škálovatelnost<sup>1</sup> sítě.

---

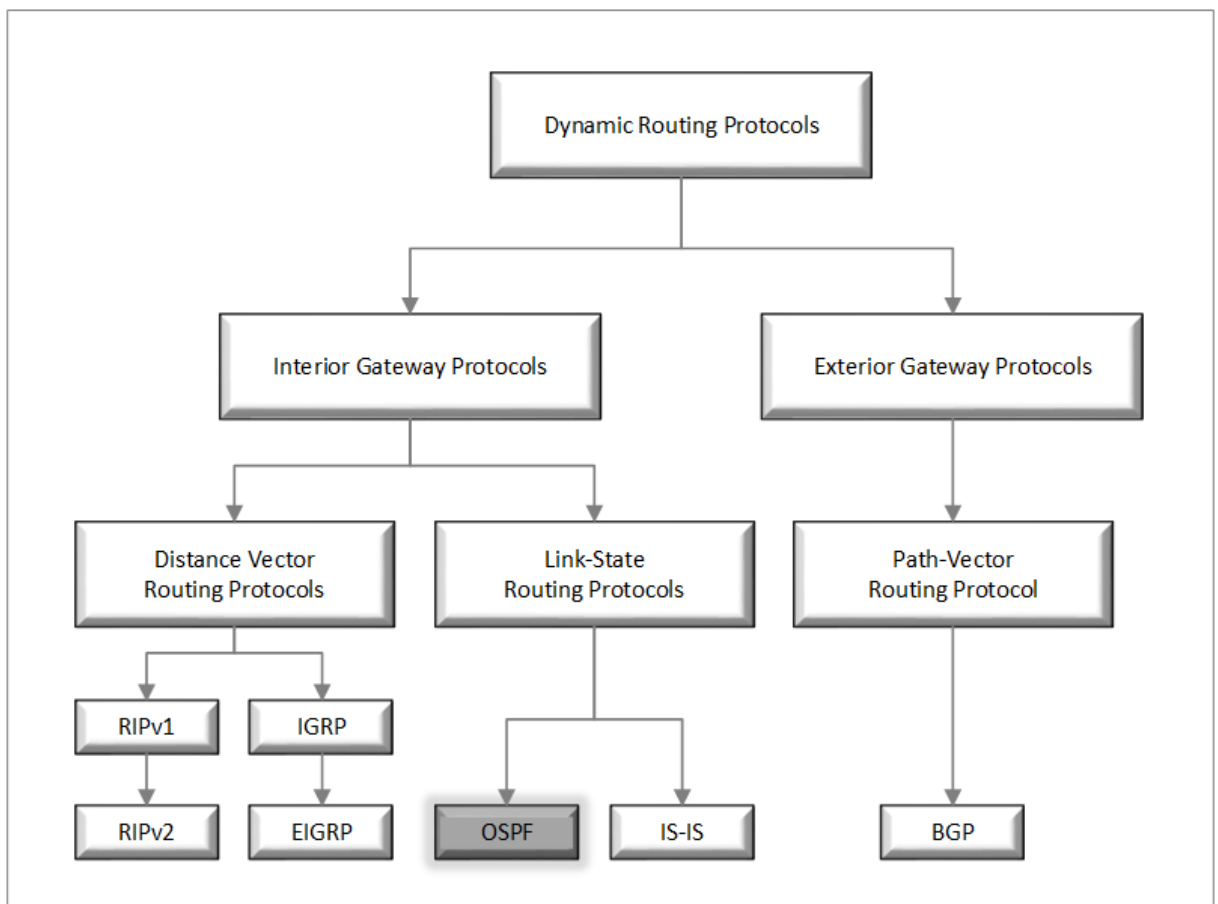
<sup>1</sup> Schopnost rozšíření velikosti sítě

## 2.2.1 SMĚROVACÍ PROTOKOLY

Směrovací protokoly se používají za účelem usnadnění výměny informací mezi směrovači. Účelem protokolů je možnost dynamicky sdílet informace o vzdálených sítích a automaticky přidat zjištěné informace do směrovací tabulky. S ohledem na zvolený protokol se používají odlišné množiny procesů, algoritmů a zpráv k výměně informací o směrování. Cílem dynamických směrovacích protokolů je:

- objevení vzdálených sítí,
- udržování aktuální směrovacích informací (aktuální směrovací tabulka),
- výběr nejlepší cesty k cíli
- a schopnost najít alternativu v případě výpadku jedné z cest v síti.

Na obrázku 1 jsou rozděleny dynamické protokoly do stromové struktury dle jejich vlastností, principu fungování a využití. Pro přehlednost zařazení je OSPF protokol v hierarchii zvýrazněn s důrazem na jeho umístění a odlišnost oproti ostatním protokolům.



Obrázek 1 – Stromová hierarchie dynamických protokolů

Zdroj: Přepracováno podle (*Routing and Switching Essentials Companion Guide, 2014*)



## 2.2.2 VLASTNOSTI DYNAMICKÝCH PROTOKOLŮ

Mezi hlavní složky dynamických protokolů patří datové struktury, které jsou obvykle ve formě tabulky nebo databáze. Informace se ukládají do paměti RAM. Protokoly využívají různé typy zpráv pro objevení sousedních směrovačů a výměnu informací o směrování. Pro usnadnění směrování informací a stanovení nejlepší cesty se používají algoritmy.

K určení nejlepší cesty mezi různými směrovači v síti se používá metrika<sup>2</sup>. Mezi základní druhy metrik patří:

- šířka pásma (bandwidth),
- cena (cost),
- zpoždění (delay),
- počet přeskoků (hop count),
- výkon (load)
- a spolehlivost (reliability).

O kvalitě a spolehlivosti cesty pojednává administrativní vzdálenost, která se nachází ve směrovací tabulce. Mezi nejspolehlivější cesty řadíme přímá připojení, kde je hodnota nula. Pokud existuje několik cest k cílovému směrovači, vždy se vybere cesta s nejnižší administrativní vzdáleností. Přehled vzdáleností pro jednotlivé směrovací protokoly zobrazuje Tabulka 1.

**Tabulka 1 – Administrativní vzdálenosti směrovacích protokolů**

| <b>Route Source</b> | <b>Administrative Distance</b> |
|---------------------|--------------------------------|
| Connected           | 0                              |
| Static              | 1                              |
| EIGRP summary route | 5                              |
| External BGP        | 20                             |
| Internal EIGRP      | 90                             |
| IGRP                | 100                            |
| OSPF                | 110                            |
| IS-IS               | 115                            |
| RIP                 | 120                            |
| External EIGRP      | 170                            |
| Internal BGP        | 200                            |

*Zdroj: Přepřacováno podle (Routing and Switching Essentials Companion Guide, 2014)*

<sup>2</sup> Hodnota, podle níž se určuje nejlepší cesta mezi směrovači.

### 2.2.3 PROTOKOLY VEKTORU VZDÁLENOSTI

Dynamické protokoly jsou rozděleny do dvou skupin. První se zabývá vektorem vzdálenosti. Směrovač začíná vyměňovat informace s přímo připojenými sousedy. Aktualizace se pravidelně zasílají po určité periodě (RIP – každých 30 sekund, IGRP – každých 90 sekund).

Všechny protokoly vektoru vzdálenosti sdílejí několik klíčových vlastností jako:

- pravidelné aktualizace směrovací tabulky,
- pomalejší konvergence<sup>3</sup>,
- citlivost na výskyt smyček<sup>4</sup> v síti,
- využití metriky
- a k určení nejkratší cesty použití Bellman-Fordova algoritmu.

### 2.2.4 PROTOKOLY STAVU LINKY

Směrovací protokoly stavu linky byly vyvinuty, aby zlepšily rychlost konvergence, kterou trpí protokoly vektoru vzdálenosti, a vyřešily problémy se smyčkami. Protokoly udržují tři samostatné tabulky:

- tabulku sousedů, která obsahuje seznam všech sousedů směrovače,
- topologickou tabulku zaznamenávající mapu všech vazeb v rámci jedné oblasti
- a tabulku uchovávající nejlepší cesty od směrovače k cíli.

Všechny směrovače v rámci oblasti znají každou vazbu v topologii, kterou následně uchovávají v topologické tabulce. Protokoly stavu linky mohou rychle konvergovat a jsou imunní vůči smyčkám. Aktualizace o změnách v topologii se neděje pravidelně. Informace o změnách se posílá, pokud daná změna nastane. Zasílají se jen podrobnosti o změně a ne celá tabulka. Tím jsou protokoly stavu linky méně náročné na šířku pásma než protokoly vektoru vzdálenosti. Avšak využívají více paměti RAM a CPU na směrovači. Protokoly stavu linky užívají určitou formu nákladů, založenou obvykle na šířce pásma.

K určení nejkratší cesty se používá Dijkstrův algoritmus.

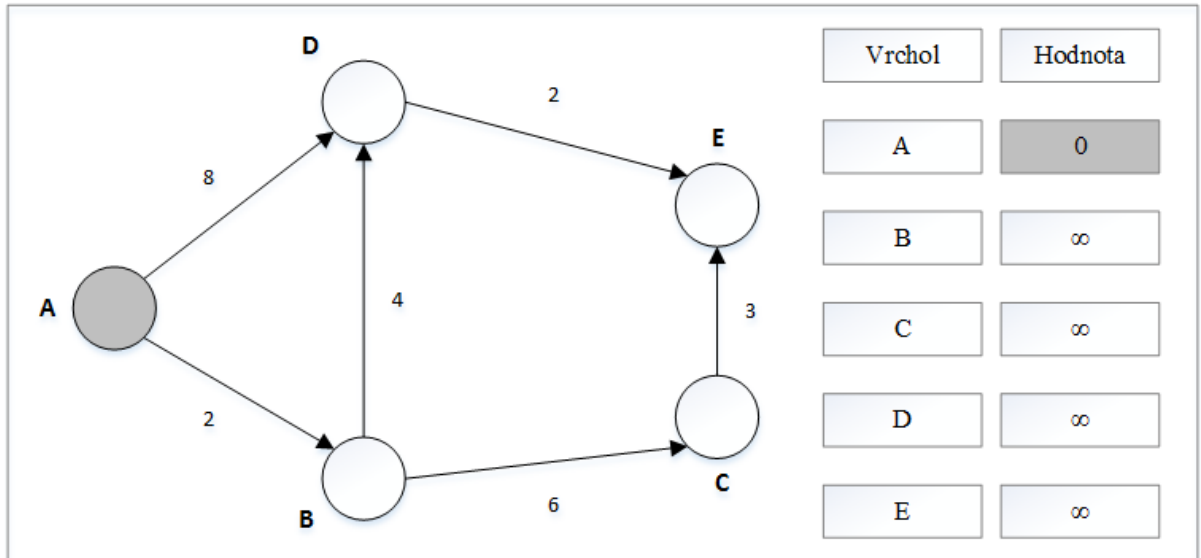
---

<sup>3</sup> Stav, kdy směrovače mají veškeré dostupné informace o topologii sítě

<sup>4</sup> Zatlacení sítě množstvím paketů, což má za následek přetížení nebo ztráty konektivity

### 2.2.5 DIJKSTRŮV ALGORITMUS

Algoritmus se používá pro nalezení nejkratší cesty od počátečního vrcholu ke všem ostatním v grafu. Počáteční vrchol (A) je ohodnocen hodnotou nula a všechny další hodnotou nekonečno. Základní nastavení vyobrazuje Obrázek 2.

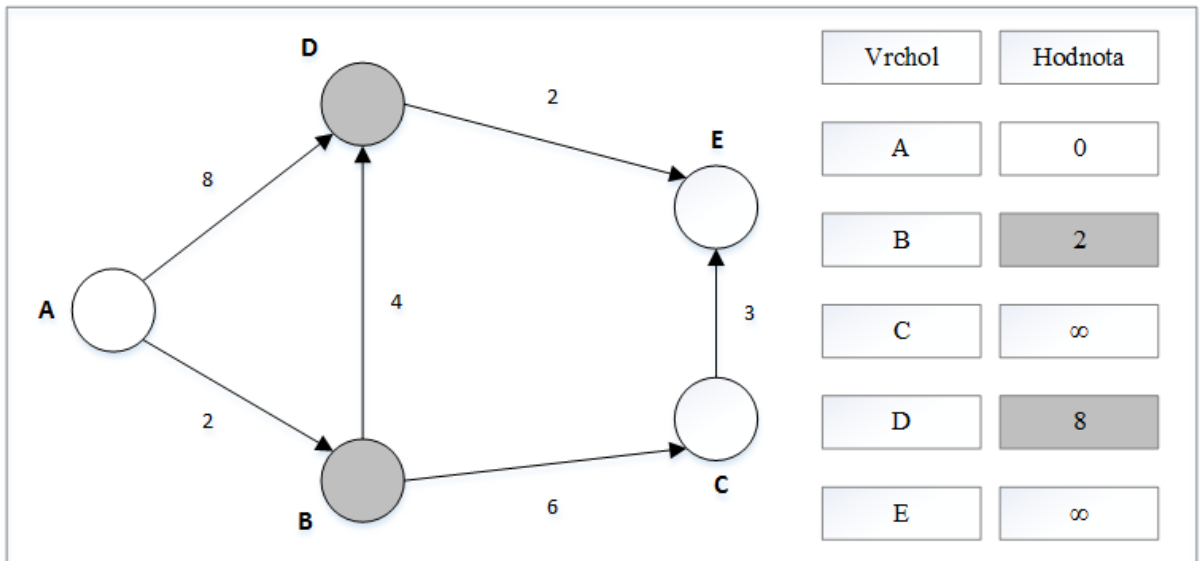


Obrázek 2 – Dijkstrův algoritmus - část 1

*Zdroj: Vlastní*

Nyní nastává testování všech potomků aktuálního vrcholu, jestli se nenachází blíže oproti původní hodnotě v tabulce. Porovnání má na starosti následující podmínky:  $VZ(z) + DH(z, p) < VZ(p)$ , kde  $VZ(z)$  znázorňuje vzdálenost právě kontrolovaného vrcholu,  $DH(z, p)$  ukazuje délku hrany mezi kontrolovaným vrcholem a jeho potomkem a  $VZ(p)$  představuje původní vzdálenost před testováním. Nastane-li výsledek podmínky kladný, nová vzdálenost je kratší než předchozí nastavená a potomku se nastaví nové ohodnocení vrcholu.

První potomci počátečního vrcholu (A) mohou být ihned ohodnoceny hodnotami příležitých hran. Stav změn v hodnocení zobrazují barevné změny na Obrázku 3.



Obrázek 3 – Dijkstrův algoritmus - část 2

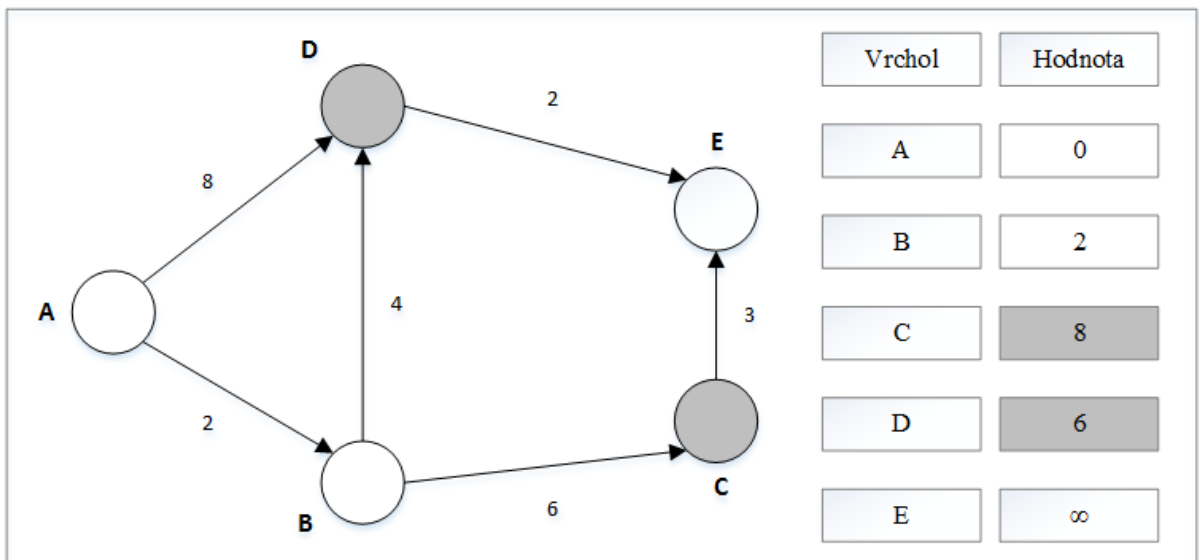
Zdroj: Vlastní

Následně vybereme vrchol, jehož ohodnocení je nejmenší (vrchol B). Potomky určeného vrcholu podrobíme podmínce, která již byla zmíněna v textu výše.

$2 + 6 < \infty$  ? Podmínka vyhovuje, proto ohodnotíme vrchol C hodnotou 8.

$2 + 4 < 8$  ? Podmínka splněna, proto přehodnotíme nastavení vrcholu D na hodnotu 6.

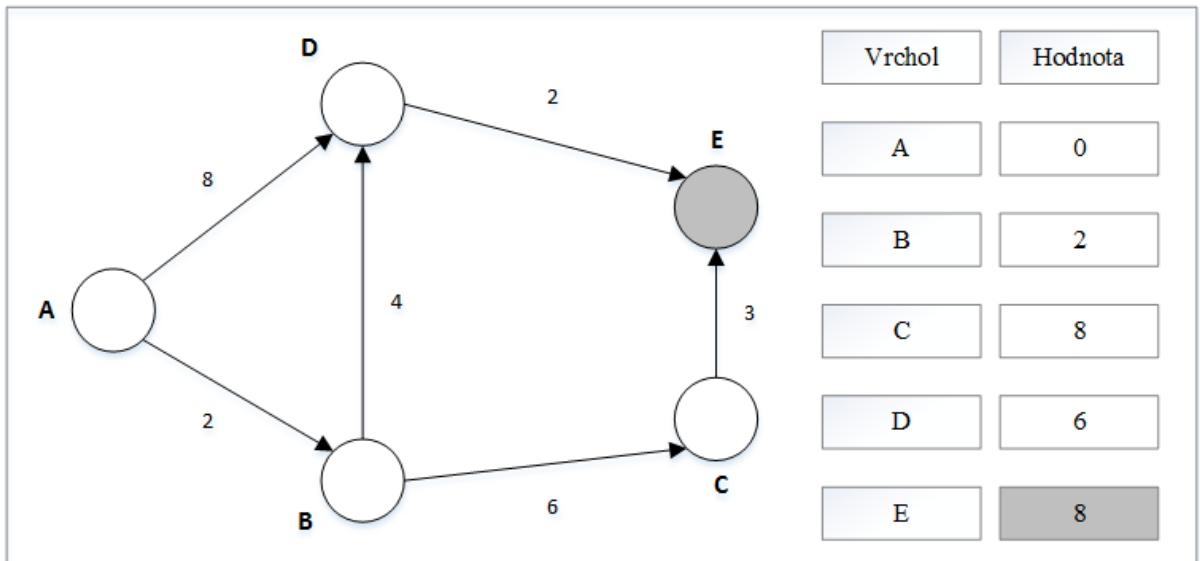
Následné vyobrazení Obrázku 4 demonstruje veškeré provedené změny.



Obrázek 4 – Dijkstrův algoritmus - část 3

Zdroj: Vlastní

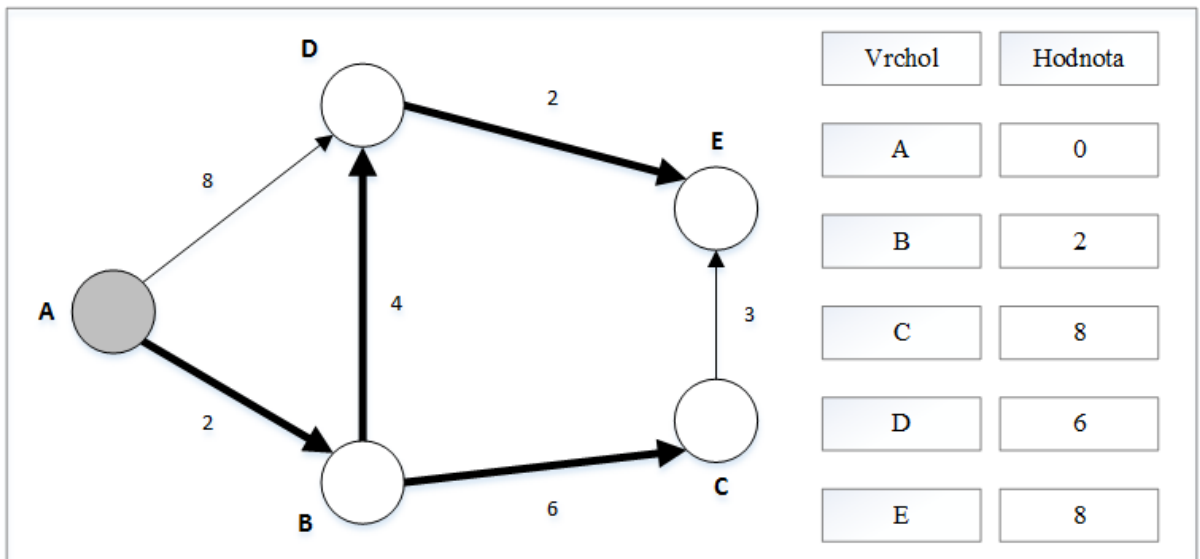
Obrázek 5 zobrazuje změny po opakování podmínky. Tentokrát je testování uplatněno na vrcholu D.



Obrázek 5 – Dijkstrův algoritmus - část 4

*Zdroj: Vlastní*

Nyní podle zhotovené tabulky lze sestavit nejkratší možné cesty vzhledem počátečnímu vrcholu A. Obrázek 6 ukazuje strom nejkratších cest v grafu.



Obrázek 6 – Dijkstrův algoritmus - část 5

*Zdroj: Vlastní*

## 3 OSPF

OSPF nepatří do kategorie proprietárních protokolů, proto jeho využití a nasazení se nekonkretizuje na zařízení jednoho výrobce. Patří mezi IGP protokoly, konkrétněji mezi protokoly stavu linky, kde si jednotlivé směrovače utvoří vlastní vizi na topologii sítě pomocí seskupení informací z ostatních směrovačů. Charakteristika protokolů IGP a stavu linky byly představeny v předchozí kapitole.

### 3.1 VLASTNOSTI OSPF

Mezi typické vlastnosti OSPF patří beztrždní směrování (CIDR), kde je při zasílání směrovacích aktualizací posílána maska podsítě. Následkem je využívání většího množství adres a efektivnější využívání adresového prostoru. K beztrždnímu směrování se zavádí VLSM, kde lze umožnit definovat délku masky, aby rozsah byl rozdělen na specifický počet podsítí a hostů.

Efektivnost OSPF protokolu zaručují vlastnosti protokolů stavu linky. Jeho nasazení může být rozmanité. Snadné pro použití IPv4 a IPv6 protokolu.

Mezi typickou vlastnost se řadí i rychlá konvergence. OSPF protokol velmi rychle reaguje na změny v síti.

Škálovatelnost umožňuje nasadit protokol do malých i velkých sítí. Ve větších topologiích lze směrovače seskupit do oblastí pro zlepšení rychlosti a efektivnosti směrování.

Bezpečnost OSPF protokolu má na starosti autentizace<sup>5</sup> MD5.

---

<sup>5</sup> Ověření identity

Na Obrázku 7 jsou zobrazeny základní důležité vlastnosti protokolu.



**Obrázek 7 – Základní vlastnosti OSPF protokolu**

*Zdroj: Přepracováno podle (Routing and Switching Essentials Companion Guide, 2014)*

### 3.1.1 ZÁKLADNÍ KOMPONENTY OSPF

Veškeré směrovací protokoly sdílejí podobné komponenty. Protokoly využívají pro výměnu informací na trase určitý typ zpráv, které pomáhají k vybudování datových struktur, a posléze jsou zpracovány pomocí směrovacího algoritmu. Směrovací protokol OSPF zahrnuje tři základní komponenty.

### 3.1.2 DATOVÉ STRUKTURY

OSPF protokol vytváří a udržuje následující databáze, která jsou udržovány v paměti RAM:

- databáze sousedů,
- link-state databázi a
- směrovací databázi.

Tabulka 2 popisuje vlastnosti zmíněných datových struktur.

**Tabulka 2 – Datová struktura OSPF**

| Databáze                   | Tabulka             | Popis   |
|----------------------------|---------------------|---|
| Databáze sousedů           | Tabulka sousedů     | <ul style="list-style-type: none"><li>• Databáze sousedů vytváří tabulku sousedů.</li><li>• V tabulce se uchovává seznam všech sousedících směrovačů.</li><li>• Tabulka je unikátní pro každý směrovač.</li></ul>   |
| Link-state databáze (LSDB) | Topologická tabulka | <ul style="list-style-type: none"><li>• LSDB sestavuje topologickou tabulku.</li><li>• V tabulce se udržuje seznam informací o každém směrovači nacházejícím se v síti.</li><li>• Databáze reprezentuje síťovou topologii.</li><li>• Všechny směrovače v rámci jedné oblasti mají totožnou LSDB.</li></ul>  |
| Směrovací databáze         | Směrovací tabulka   | <ul style="list-style-type: none"><li>• Směrovací databáze vytváří směrovací tabulku.</li><li>• Seznam se generuje, když algoritmus běží na LSDB.</li><li>• Každý směrovač má jedinečnou směrovací tabulku, která obsahuje záznamy o tom, jak a hlavně kam posílat pakety do ostatních směrovačů.</li></ul> |

*Zdroj: Přepřacováno podle (Routing and Switching Essentials Companion Guide, 2014)*

### 3.1.3 ZPRÁVY SMĚROVACÍHO PROTOKOLU

OSPF vyměňuje informace mezi směrovači pomocí pěti různých typů paketů:

- Hello,
- Database description (DBD),
- Link-state request (LSR),
- Link-state update (LSU) a
- Link-state acknowledgment (LSAck).

Pakety se používají k objevování sousedních směrovačů a vyměňování informací, které je nutné pro zachování přesného stavu sítě. Jednotlivým paketům bude věnována samostatná podkapitola.

### 3.1.4 ALGORITMUS

Procesor směrovače vytvoří topologickou tabulku a tabulku sousedů využitím algoritmu SPF, který je založen na kumulování ceny k dosažení k cíli. Metrika OSPF je cena založena na šířce pásma. Směrovače vše hodnotí z vlastního pohledu. Pro výpočet nejlepší trasy se používá Dijkstrův algoritmus.



SPF vytvoří strom, kde kořenem je daný směrovač, a vypočítává nejkratší cestu ke každému uzlu. Sestavený strom se používá pro výpočet nejlepší trasy. Následně OSPF umístí nejlepší cesty do směrovací databáze.

### 3.2 DRUHY PAKETŮ OSPF

OSPF protokol používá pakety pro navazování, udržení sousedů a k výměně aktualizací mezi směrovači.

Následující Tabulka 3 poskytne přehled druhů paketů OSPF.

**Tabulka 3 – Druhy paketů OSPF**

| Typ | Název paketu                      | Popis  |
|-----|-----------------------------------|--|
| 1   | Hello                             | Objevuje sousedy a vytváří mezi nimi vztah sousedství        |
| 2   | Database description (DBD)        | Kontroluje databázovou synchronizaci mezi směrovači          |
| 3   | Link-state request (LSR)          | Požádá o konkrétní položku ze sousedovy topologické databáze |
| 4   | Link-state update (LSU)           | Nese samotnou topologickou informaci                         |
| 5   | Link-state acknowledgment (LSAck) | Slouží k potvrzení úspěšného přijetí LSA                     |

*Zdroj: Přepřacováno podle (Routing and Switching Essentials Companion Guide, 2014)*

Link-state advertisement (LSA) je datová struktura zasílaná v paketech OSPF, která přenáší topologické informace. Nejedná o samostatný paket. V jednom paketu LSAck může být potvrzeno několik různých LSA. LSA typům bude věnována samostatná část.

#### Hello paket

Prvním z typů paketů OSPF je paket Hello. Využívá se zejména:

- k objevování sousedů a navázání sousedství,
- propagované parametry v paketu musí mezi směrovači souhlasit, aby se mohli směrovače stát sousedy,
- a k volbě DR/BDR.

DR představuje centrální bod pro výměnu informací. Ostatní směrovače se dotazují na tento směrovač. BDR zálohuje činnost DR. Při výpadku je záložní směrovač (BDR) nastaven jako DR a plní jeho funkci.

|                        |                  |                    |  |
|------------------------|------------------|--------------------|--|
| Data Link Frame Header | IP Packet Header | OSPF Packet Header | OSPF Packet Type-Specific Data<br><b>Hello Paket</b> |
|------------------------|------------------|--------------------|--|

**Obrázek 8 – OSPF paket**

*Zdroj: Přepřacováno podle (Routing and Switching Essentials Companion Guide, 2014)*

Paket je rozdělen do několika polí (Obrázek 8), kde budou nejvíce důležitá zejména pole:

- OSPF Packet Header
- a OSPF Hello Packet.

Charakteristika zmíněných polí shrnuje Tabulka 4.

**Tabulka 4 – OSPF Packet Header a OSPF Hello Packet**

| Část paketu        | Pole              | Popis  |
|--------------------|-------------------|--|
| OSPF Packet Header | Type              | Identifikuje typy paketů: Hello (1), DBD (2), LSR (3), LSU (4) a LSAck (5)   |
|                    | Router ID         | 32-bitová hodnota, vyjádřena ve formátu IPv4 adresy, slouží k jednoznačné identifikaci směrovače   |
|                    | Area ID           | Oblast, odkud paket pochází  |
| OSPF Hello Paket   | Network Mask      | Maska podsítě spojená s vysílajícím rozhraním  |
|                    | Hello Interval    | Interval v sekundách, při kterém směrovač odesílá Hello pakety (musí být stejné na sousedních směrovačích)   |
|                    | Router Priority   | Používá se k výběru DR/BDR, hodnoty priority v rozsahu 0 až 255 (výchozí je 1), větší hodnota priority zvyšuje pravděpodobnost ke zvolení  |
|                    | Dead Interval     | Interval v sekundách, během níž směrovač čeká na odezvu od sousedního směrovače, po překročení je stanoven jako mimo provoz (výchozí nastavení čtyřikrát větší než Hello Interval a hodnota musí být stejná na sousedních směrovačích) |
|                    | DR                | ID směrovače DR  |
|                    | BDR               | ID směrovače BDR   |
|                    | List of Neighbors | Seznam ID sousedních směrovačů   |

*Zdroj: Vlastní*

Hello pakety jsou přenášeny pomocí multicastové adresy 224.0.0.5 v IPv4 and FF02::5 v IPv6 každých:

- 10 sekund (výchozí na multiaccess a point-to-point sítích)
- a 30 sekund (výchozí na nonbroadcast multiaccess sítích, například Frame Relay)

### **DBD paket**

Obsahuje zjednodušený seznam LSDB k synchronizaci topologických databází mezi dvojicemi směrovačů. Daný seznam přenáší pouze Link State ID spolu s pomocnými informacemi o jejich verzi a stáří. Pomocí DBD paketu komunikují směrovače ve fázi, kdy zjišťují, co je nového u souseda. K sestavení SPF stromu musí být LSDB stejné na všech směrovačích v oblasti.

### **LSR paket**

Po výměně paketů DBD může směrovač v topologické databázi nalézt, která konkrétní položka mu chybí. Konkrétní informaci si směrovač vyžádá od příslušného souseda. Přenáší požadovaný databázový klíč.

### **LSU paket**

LSU paket je reakcí na LSR a obsahuje vyžádanou topologickou informaci. Tyto pakety jsou realizovány zaplavením LSA. Každý LSA zahrnuje směrování, metrické a topologické informace, které popisují danou část sítě OSPF. Lokální směrovač propaguje LSA v rámci LSU paketu do sousedních směrovačů.

### **LSAck paket**

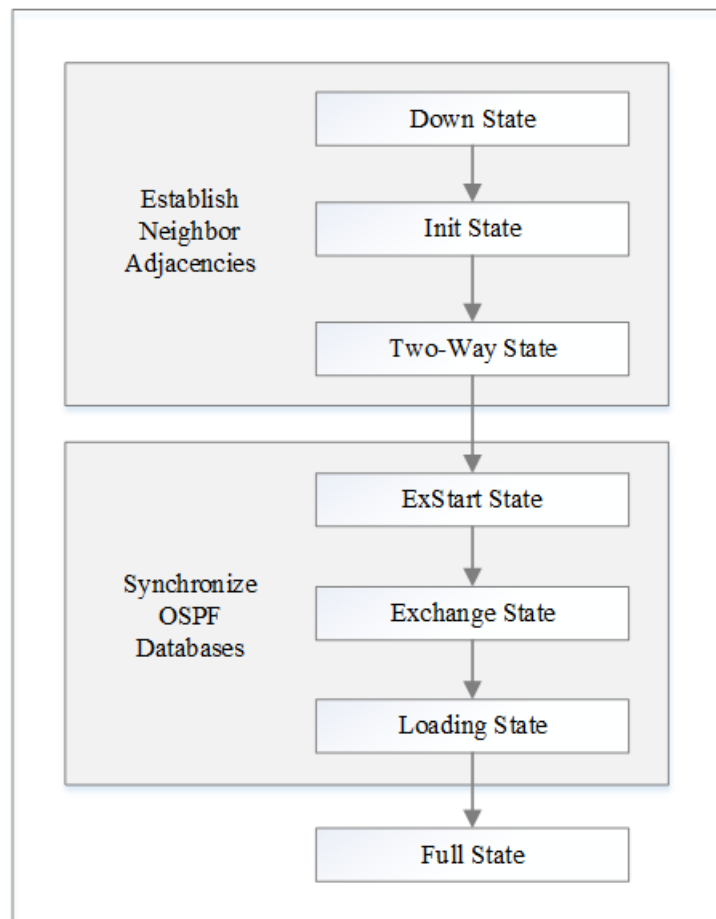
Paket slouží k potvrzování úspěšných přijetí LSA paketů. Jeden LSAck paket umožňuje potvrdit jednotlivé LSA.

### 3.3 OPERAČNÍ STAVY OSPF

Pokud je povoleno OSPF na rozhraní, musí směrovač zjistit, zda neexistuje jiný sousedící směrovač v topologii, využívající též OSPF. Po nastavení OSPF se směrovače pokusí:

- vytvořit adjacencies se sousedy,
- vyměnit si směrovací informace,
- vypočítat nejlepší cestu
- a dosáhnout konvergence.

Než se směrovače stanou sousedy, projdou několika stavy, které jsou ilustrovány na Obrázku 9. Jednotlivé stavy budou rozebrány v následujících podkapitolách.



Obrázek 9 – Postup stavů OSPF

Zdroj: Přepřacováno podle (*Routing and Switching Essentials Companion Guide, 2014*)

### **Down State**

Jedná se o první stav OSPF, kdy doposud nebyly přijaty žádné Hello pakety, ale mohou být v tomto stavu stále zaslány. Pokud je mezi dvěma směrovači stav Full State, jsou zasílány v určitém intervalu Hello pakety. Když není Hello paket obdrženo během Dead intervalu, dojde k přechodu z Full State na Down State.

### **Init State**

V daném stavu již byl obdrženo Hello paket od souseda, ale svoje RID nebylo doposud zahrnuto do paketu. Když směrovač přijme Hello paket od souseda, měl by ve svém Hello paketu vypsat odesílatelovo RID jako potvrzení, že obdržel platný Hello paket.

### **Two-Way State**

Tento stavu označuje, že byla založena obousměrná komunikace mezi dvěma směrovači. Daného stavu je dosaženo, když směrovač přijme Hello paket od souseda a vidí v něm své vlastní RID. Zde se rozhodne, zda směrovače se stanou sousedy a dojde k volbě DR a BDR.

### **ExStart State**

Jakmile je DR a BDR zvolena, může začít vyměňování aktuálních informací mezi směrovači a jejich DR a BDR. Probíhá určování autority pro jednotlivé sítě, kdo se stane master a slave. Směrovač s vyšším RID se stává masterem.

### **Exchange State**

V Exchange state, si směrovače vyměňují pakety DBD. Pakety obsahují pouze hlavičky LSA a zahrnují popis topologické databáze. Na základě zjištěných informací v paketech DBD si jednotlivé směrovače utvoří seznam LSA, kde porovná sousedovy informace s vlastními a posléze si vyžádá chybějící položky.

## Loading State

Během dané fáze dochází k vyžádání konkrétních informací pomocí LSR paketů na základě utvořeného seznamu, které informace směrovač bude požadovat. Aktualizace jsou zaslány v LSU paketech a potvrzeny pakety LSAck.

## Full State

Do Full State se dva sousední směrovače dostanou, když jsou všechny požadované LSA pakety vyměněny. Jejich topologické databáze musí být stejné a plně synchronizované. Full State indikuje normální stav směrovače, kdy je všechno v pořádku. Pokud směrovač uvízl v jednom z předchozích stavů, znamená to, že došlo k problémům při formování sousedství.

## 3.4 PAKETY LSA

Pakety LSA patří mezi základní kameny OSPF pro tvorbu LSDB. Jednotlivé pakety se chovají jako databázové záznamy, které poskytují specifické detaily sítě. Společně popisují celou topologii sítě OSPF.

V současné době lze nastavit až 11 různých typů LSA. Pro realizaci Single-Area a Multiarea stačí prvních pět typů LSA, které budou podrobněji vysvětleny. Liší se zejména v tom, jak budou generovány a propagovány v rámci oblastí sítě.

Tabulka 5 – Pakety LSA

| LSA Type     | Description                     |
|--------------|---------------------------------|
| 1            | Router LSA                      |
| 2            | Network LSA                     |
| 3 and 4      | Summary LSAs                    |
| 5            | AS External LSA                 |
| 6            | Multicast OSPF LSA              |
| 7            | Defined for NSSAs               |
| 8            | External Attributes LSA for BGP |
| 9, 10, or 11 | Opaque LSAs                     |

*Zdroj: Přepřacováno podle (Scaling Networks Companion Guide, 2014)*

### **Typ 1**

Pakety zahrnují seznam přímo připojených rozhraní, typy vazeb a stavy linky. Jednotlivé směrovače v síti generují daný typ paketu a zaplavuje s ní oblast, ve které se nachází. Tento typ se nikdy nešíří mimo oblast, odkud pochází. Inzerování mimo oblast přejímají pakety typu 3. Paket obsahuje originální ID směrovače v celé síti, aby směrovač byl jednoznačně určen.

### **Typ 2**

Daný druh paketů existuje pouze v multiaccess a NBMA síti, kde se volí DR. Paket obsahuje RID všech směrovačů na daném multiaccess segmentu a IP adresu na DR. Účelem typu 2 je poskytnout ostatním směrovačům informaci o multiaccess sítích ve stejné oblasti. Pouze DR zaplavuje pakety pouze v oblasti, ve které se nachází. Nikdy se nedostanou mimo svojí oblast.

### **Typ 3**

Typ paketu je používán směrovači ABR pro propagování sítě do jiných oblastí. Typ popisuje síťovou adresu naučenou na základě paketu typu 1 z LSDB a je vyžadován pro každou podsít'. ABR zaplavuje paketem jiné přímo připojené oblasti a paket je regenerován jiným ABR. Mezi důležité poznatky patří, že ve výchozím stavu nejsou trasy sumarizovány.

### **Typ 4**

Paket slouží k propagování směrovače ASBR do jiných oblastí a zároveň poskytnout cestu k tomu to směrovači. ABR generují tento typ paketu. Veškerý provoz je určený k externímu autonomnímu systému. Vyžaduje znalost tabulky směrování ASBR, které vznikly na externích směrovačích. Umožňuje výpočty metriky do připojených oblastí.

### **Typ 5**

Paket popisuje cesty k sítím mimo autonomní systém OSPF. ASBR vytváří tento druh paketu a zaplavuje s ním celý autonomní systém. Paket je regenerován do dalších oblastí směrovači ABR. Mezi nevýhody patří nedostatek informací pro výpočet externích cest. Proto jsou odesílány spolu s typem 4. Společně slouží k výpočtu nejvýhodnější cesty.

Názorné propagování jednotlivých typů v síti budou ukázány na topologiích v následujících kapitolách.

## 4 KONVERGENCE V SINGLE-AREA

Pod pojmem Single-Area je rozuměno druh rozdělení sítě do jedné oblasti, kde se nacházejí veškeré směrovače v topologii. Rozdělení je používáno zejména na topologie s větším množstvím zařízení. V porovnání s Multiarea je konfigurace a případně její oprava méně náročná. Směrovače v Single-Area využívají první dva typy LSA (typ 1, typ 2), jejichž vysvětlení bylo představeno předešlé kapitole.

Rychlost konvergence patří mezi základní zkoumané prvky pro rozhodnutí, jakou ideologii ze dvou možností použít. Zároveň je důležité brát ohled na další faktory, které se budou muset uplatňovat. Mezi faktory patří hlavně škálovatelnost sítě, a proto se nelze rozhodovat na základě jednoho aspektu. Jednoduché nastavení a konfigurace nemusí být vždy efektivní pro celou síť.

### 4.1 NEVÝHODY SINGLE-AREA

Velké množství směrovačů v jedné oblasti zvýší zatížení CPU a nároky na paměť, jelikož se uchovává velká LSDB. Single-Area OSPF je užitečná hlavně v menších sítích, kde propojení jednotlivých směrovačů a cesty k jednotlivým destinacím lze poměrně snadno odvodit. Mezi hlavní nevýhody patří:

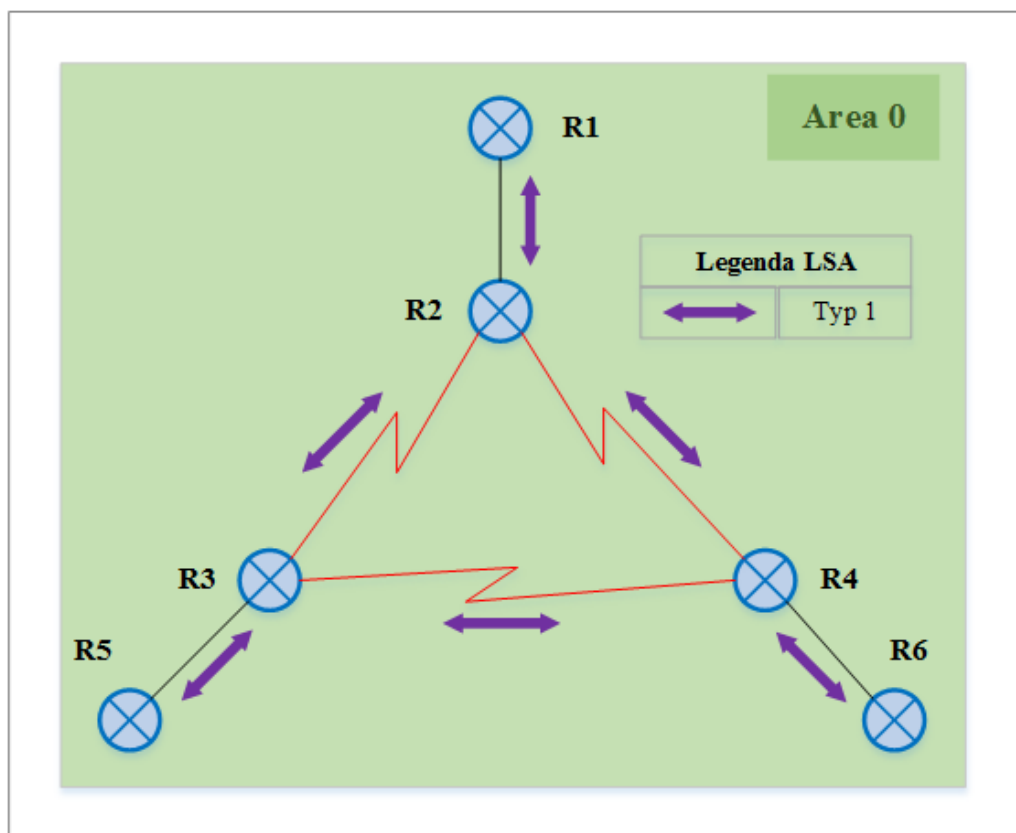
- **Velká směrovací tabulka** – OSPF neprovádí sumarizace ve výchozím nastavení. V případě, že trasy nejsou sumarizovány, směrovací tabulky mohou být rozsáhlé v závislosti na velikosti sítě.
- **Velká LSDB** – Jelikož LSDB zahrnuje topologii celé sítě, musí každý směrovač udržovat záznamy pro každou síť v dané oblasti a to i v případě, že daná cesta není vybrána do směrovací tabulky.
- **Časté výpočty SPF algoritmu** – V rozsáhlé síti dochází k většímu množství změn, a proto je nevyhnutelné, že směrovače stráví plno času cyklickým opakováním SPF algoritmu a aktualizováním svých směrovacích tabulek.



## 4.2 PAKETY LSA V SINGLE-AREA

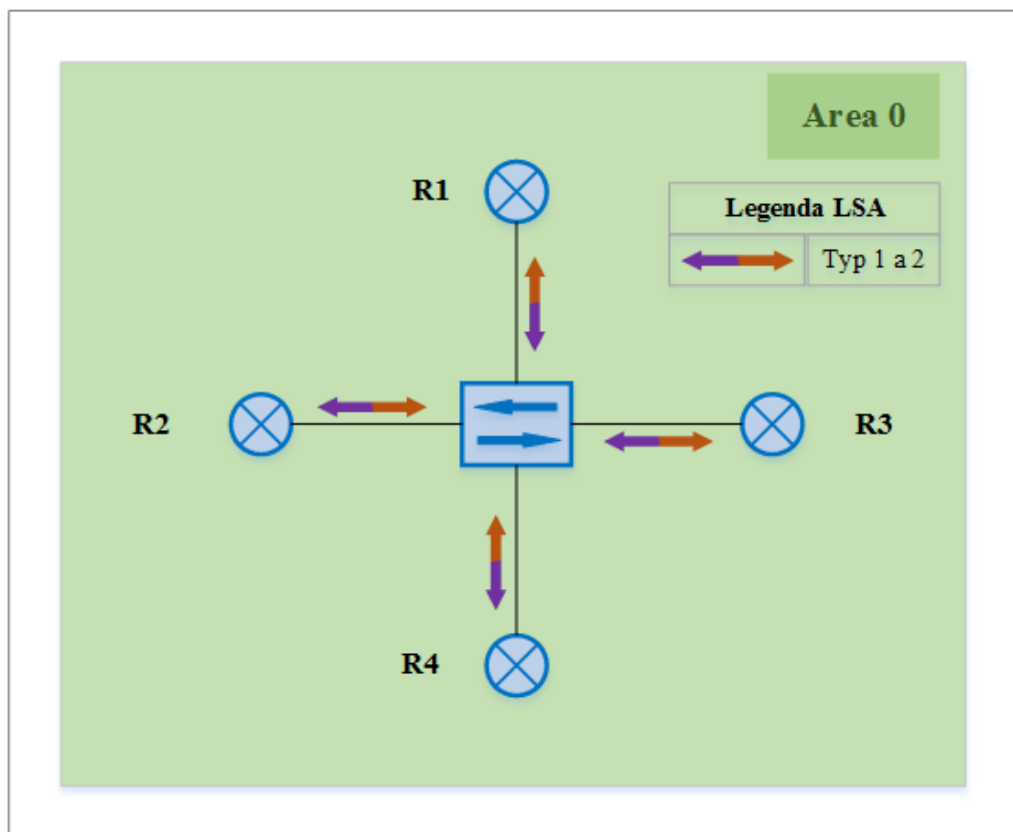
Obrázek 10 vyobrazuje topologii šesti směrovačů, které jsou mezi sebou jednotlivě propojeny. Směrovače rozesílají pakety typu 1 LSA v rámci oblasti 0 (Area 0). Směrovače neodesílají typ 2 LSA, jelikož se nejedná o multiaccess síť.

Obrázek 11 ukazuje topologii, kde jsou jednotlivé směrovače propojené pomocí přepínače. Tento druh sítě nazýváme multiaccess sítí. Na rozdíl od předchozí topologie jsou zde, kromě paketu typu 1 LSA, posílány i pakety typu 2 LSA.



Obrázek 10 – Pakety LSA v Single-Area Top. 1

*Zdroj: Vlastní*



Obrázek 11 – Pakety LSA v Single-Area Top. 2

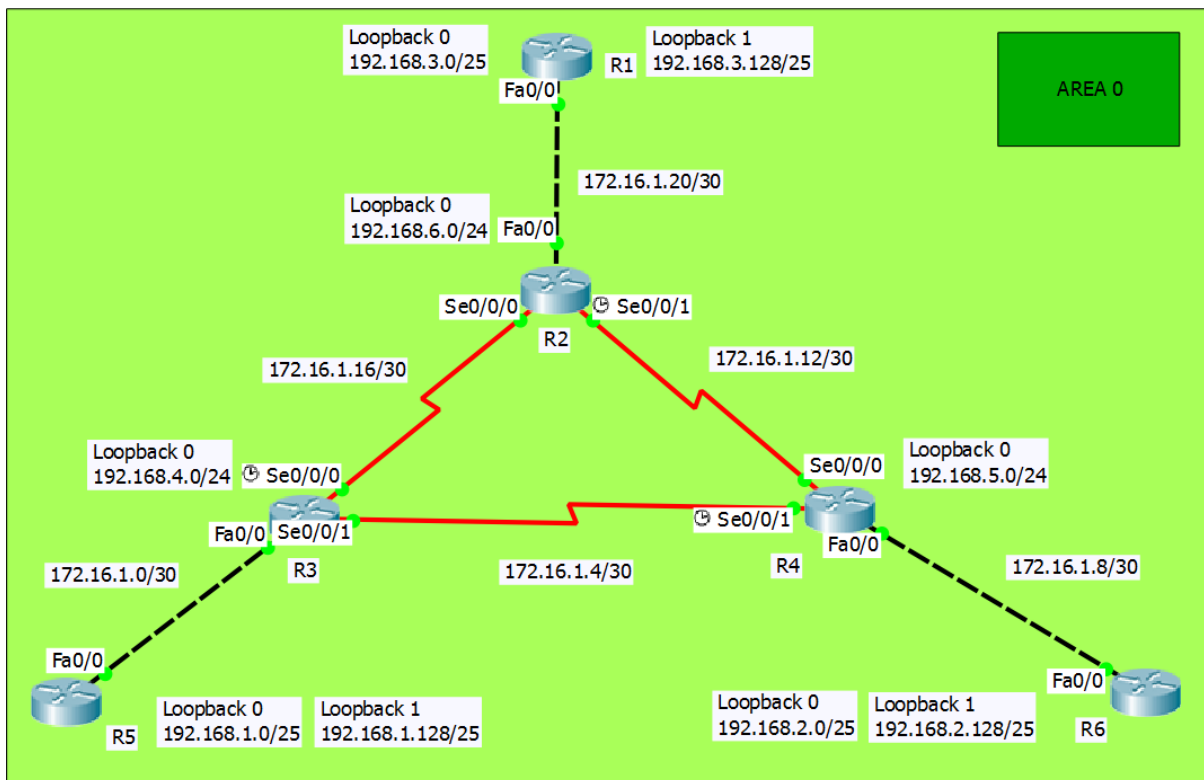
Zdroj: Vlastní

### 4.3 MĚŘENÍ RYCHLOSTI KONVERGENCE

Na základě Obrázku 10 bude vytvořena topologie vhodná pro měření konvergence v simulačním nástroji (Packet Tracer), tak i na fyzickém zařízení. Upravená topologie je zobrazena na Obrázku 12. Jako simulace hostů zde poslouží loopback. Na směrovačích s označením R1, R5 a R6 je přidělena adresa rozdělena na dvě podsítě, přičemž jedna podsít' má 126 hostů. Ostatní směrovače nejsou rozděleny na podsítě, tudíž mohou mít až 254 hostů. Jednotlivá rozhraní loopbacku jsou nastavena na první použitelnou adresu.

Jednotlivé směrovače mezi sebou komunikují pomocí jedné adresy, která je rozdělena na podsítě tak, že maximální počet hostů v jedné podsíti jsou 2. Dva směrovače propojené mezi sebou využívají vždy jednu ze dvou použitelných adres.

Všechny směrovače se nacházejí v jedné oblasti. Jelikož se nejedná o multiaccess síť, směrovače si vyměňují mezi sebou pouze pakety LSA typu 1.



Obrázek 12 – Měřená topologie Single-Area

Zdroj: Vlastní

#### 4.3.1 ZJIŠTĚNÍ KOMUNIKAČNÍCH CEST

Zvolí si dva body, mezi kterými bude probíhat komunikace, R6 a R1. Cesta od zdroje k cíli bude:

R6 → R4 → R2 → R1

Pro ověření cesty se zadá na směrovači R6 v příkazovém řádku příkaz „traceroute”, kde jako cílovou adresu bude uvedena adresa loopbacku 0 na směrovači R1.

```
R6#traceroute 192.168.3.1          ← Adresa loopbacku 0 na R1
Type escape sequence to abort.
Tracing the route to 192.168.3.1

 1  172.16.1.10  0 msec 0 msec 0 msec      ← R4
 2  172.16.1.13  1 msec 6 msec 1 msec      ← R2
 3  172.16.1.21  1 msec 0 msec 0 msec      ← R1
```

Po zadání příkazu se zjistí korektnost cesty a podrobnější informace o cestě. K dosažení cíle jsou potřeba 3 přeskoky. Přičemž první skokem od zdroje je uvedena adresa rozhraní připojeného směrovače R4. Adresa rozhraní na R4 (Fa0/0) je 172.16.1.10. Mezi každým přeskokem jsou zasílány tři traceroute pakety, jejichž časy jsou zaznamenány v každém

přeskoku. Například pro řádek se směrovačem R2 jsou časy (1 msec 6 msec 1 msec) naměřeny od prvního přeskoku R4 (172.16.1.10) do druhého přeskoku R2 (172.16.1.13). Pokud jeden ze tří paketů nedorazí na další přeskok, tak se místo času vyobrazí „\*“.

Pokud se vypojí nebo vypne rozhraní na R4 (s0/0/0), přes které je vedena komunikace, dojde k aktivování záložní cesty do R1. Nyní cesta do R1 bude:

R6 → R4 → R3 → R2 → R1

Výsledná trasa se opět ověří pomocí příkazu „traceroute“.

```
R6#traceroute 192.168.3.1          ← Adresa loopbacku 0 na R1
Type escape sequence to abort.
Tracing the route to 192.168.3.1

 0  172.16.1.1  0 msec 0 msec 0 msec  ← R6
 1  172.16.1.10 0 msec 0 msec 1 msec   ← R4
 2  172.16.1.5  4 msec 1 msec 2 msec   ← R3
 3  172.16.1.17 1 msec 1 msec 1 msec   ← R2
 4  172.16.1.21 0 msec 4 msec 2 msec   ← R1
```

#### 4.3.2 MĚŘENÍ V SIMULAČNÍM PROGRAMU

Pro změření rychlosti konvergence je posláno 100 paketů ping, přičemž každý má časový limit jednu sekundu. Na základě zjištěných informací z předešlé podkapitoly budou pakety odesílány ze směrovače R6 na loopback 0 (192.168.3.1) směrovače R1 pomocí příkazu „ping“. Další hodnoty příkazu zůstanou ve výchozím nastavení. Během průběhu přenosu se odpojí nebo vypne rozhraní na R4 (s0/0/0) a ve výsledku příkazu bude zjištěna doba konvergence potřebnou pro aktualizaci cesty k cíli.

```
R6#ping
Protocol [ip]:
Target IP address: 192.168.3.1      ← Adresa loopbacku 0 na R1
Repeat count [5]: 100               ← Počet odesílaných paketů
Datagram size [100]:
Timeout in seconds [2]: 1           ← Časový limit
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.3.1, timeout is 1 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 95 percent (95/100), round-trip min/avg/max = 1/5/19 ms
```

Na ukázce je znázorněn každý úspěšně doručený paket „ ! “ a selhání reprezentováno znakem „ . “. Úspěšnost doručených paketů do cíle činí 95%. Minimální, průměrná a maximální doba ping-packet-round-trip je 1ms, 5ms a 19ms.

První 42 paketů bylo posláno původní cestou z R6 do R1, která byla zjištěna při trasování v předchozí podkapitole. Následně došlo k přerušení komunikace po této cestě tím, že se vypnulo rozhraní na R4 (s0/0/0). Během přechodné doby, kdy směrovací protokol konverguje, dochází ke ztrátě pěti paketů. Po dokončení konvergence OSPF je zbývajících 53 paketů doručeno záložní cestou.

Měření je vyzkoušeno na několika různých trasách s několika opakováními, aby se zjistili další hodnoty konvergence a případně získali průměrnou dobu konvergence. Průměrnou dobu konvergence nebylo potřeba měřit z důvodu totožných výsledků měření.

Jelikož v průběhu přechodové doby je pět paketů ztraceno s časovým limitem jedna sekunda znamená to, že OSPF potřebuje pět sekund ke konvergenci v dané topologii.

**Celkem bylo posláno 100 paketů. Bylo doručeno celkem 95 paketů a 5 jich bylo ztraceno. Čas konvergence je 5 sekund.**

### 4.3.3 MĚŘENÍ NA FYZICKÉM ZAŘÍZENÍ

Měření konvergence bude probíhat obdobně jako při měření v simulačním programu (Packet Tracer). Fyzicky se sestaví totožná topologie, jako byla navrhována v simulačním programu. Opět se stanoví počet odesílaných paketů na 100 s časovým limitem jedna sekunda. Postup měření konvergence bude stejný jako v předchozím případě.

```
R6#ping
Protocol [ip]:
Target IP address: 192.168.3.1          ← Adresa loopbacku 0 na R1
Repeat count [5]: 100                  ← Počet odesílaných paketů
Datagram size [100]:
Timeout in seconds [2]: 1              ← Časový limit
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.3.1, timeout is 1 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 94 percent (94/100), round-trip min/avg/max = 12/20/36 ms
```

Měření se zkoušelo na několika různých cestách a s několika opakováními. Výsledky vyšly po každý stejné, a proto nebylo potřeba určovat průměrnou hodnotu rychlosti konvergence.

**Celkem bylo posláno 100 paketů. Bylo doručeno celkem 94 paketů a 6 jich bylo ztraceno. Čas konvergence je 6 sekund.**

## 5 KONVERGENCE V MULTIAREA OSPF

Multiarea se používá zejména k rozdělení velké sítě, kde se nachází větší počet směrovačů. Aby bylo OSPF efektivnější a škálovatelné, podporuje hierarchické směrování pomocí oblastí. Oblast OSPF představuje skupinu směrovačů, které sdílejí stejné informace ze svých LSDB. Multiarea OSPF je zejména užitečná ve větších topologiích ke snížení zpracování požadavků a zatížení paměti.

Například, když směrovač přijímá nové informace o topologii, musí znovu spustit algoritmus SPF, vytvořit nový strom a aktualizovat směrovací tabulky. Algoritmus SPF je náročný na CPU a čas potřebný pro výpočet závisí na velikosti oblasti. Příliš mnoho směrovačů v jedné oblasti způsobí větší LSDB a zatížení CPU. Z tohoto důvodu se směrovače rozdělují do oblastí, tím lze potencionálně rozdělit velké databáze na menší, které jsou potom lépe zvládnutelné.

Multiarea OSPF vyžaduje hierarchický návrh sítě. Hlavní oblast se nazývá páteřní oblast (Area 0) a další oblasti musí k ní být připojeny. Směrovače se zabírají pouze oblastí, ve které se nacházejí. Mezi výhody patří:

- menší směrovací tabulky,
- minimalizace požadavků na paměť a zpracování
- a snížená četnost výpočtů.

Multiarea je implementována v dvouvrstvou oblastní hierarchii:

- **Páteřní oblast** – Oblast OSPF, jejichž primární funkcí je rychlost a efektivita pohybu paketů IP. Páteřní oblast musí být propojená s ostatními oblastmi. Obecně platí, že koncoví uživatelé se nenacházejí v páteřní oblasti. Páteřní oblast je nazývána též jako oblast 0 (Area0).
- **Nepáteřní oblast** – Zde se nacházejí většinou koncoví uživatelé. Oblasti jsou rozděleny do různých funkčních oblastí, kde každá oblast může zastupovat jinou funkci. Nastavení neumožňuje komunikovat s jinou oblastí, aniž by nebyla propojena s páteřní oblastí.

Optimální počet směrovačů na jednu oblast závisí na různých faktorech (např. stabilita). Cisco doporučuje několik zásad pro rozdělení do oblastí:

- oblast by měla mít více než 50 směrovačů,
- směrovač by se neměl nacházet ve více než 3 oblastech
- a každý směrovač by neměl mít více než 60 sousedů.

Na základě funkcí, kterou směrovače vykonávají, je rozdělujeme do čtyř různých skupin:

- **Interní směrovač** – Jedná se o směrovač, který má všechna jeho rozhraní ve stejné oblasti. Všechny interní směrovače v oblasti mají stejnou LSDB.
- **Páteřní směrovač** – Jedná se o směrovač, který se nachází v páteřní oblasti (Area 0).
- **Hraniční směrovač (ABR)** – Jedná se o směrovač, který má svá rozhraní připojená k více oblastem. Udržuje samostatné LSDB pro každou oblast, ke které je připojen, aby mohl směrovat mezi těmi to oblastmi. ABR je výstupním bodem oblasti, což znamená, že informace o směrování pro jiné oblasti se mohou dostat z aktuální sítě pouze přes ABR. ABR mohou být nakonfigurovány tak, že sumarizují informace o směrování z připojených oblastí. ABR šíří informace o směrování do páteřní oblasti, kde je tato informace předána dalším hraničním směrovačům.
- **Hraniční směrovač autonomního systému (ASBR)** – Jedná se o směrovač, kde alespoň jedno rozhraní je připojené k dalšímu autonomnímu systému.

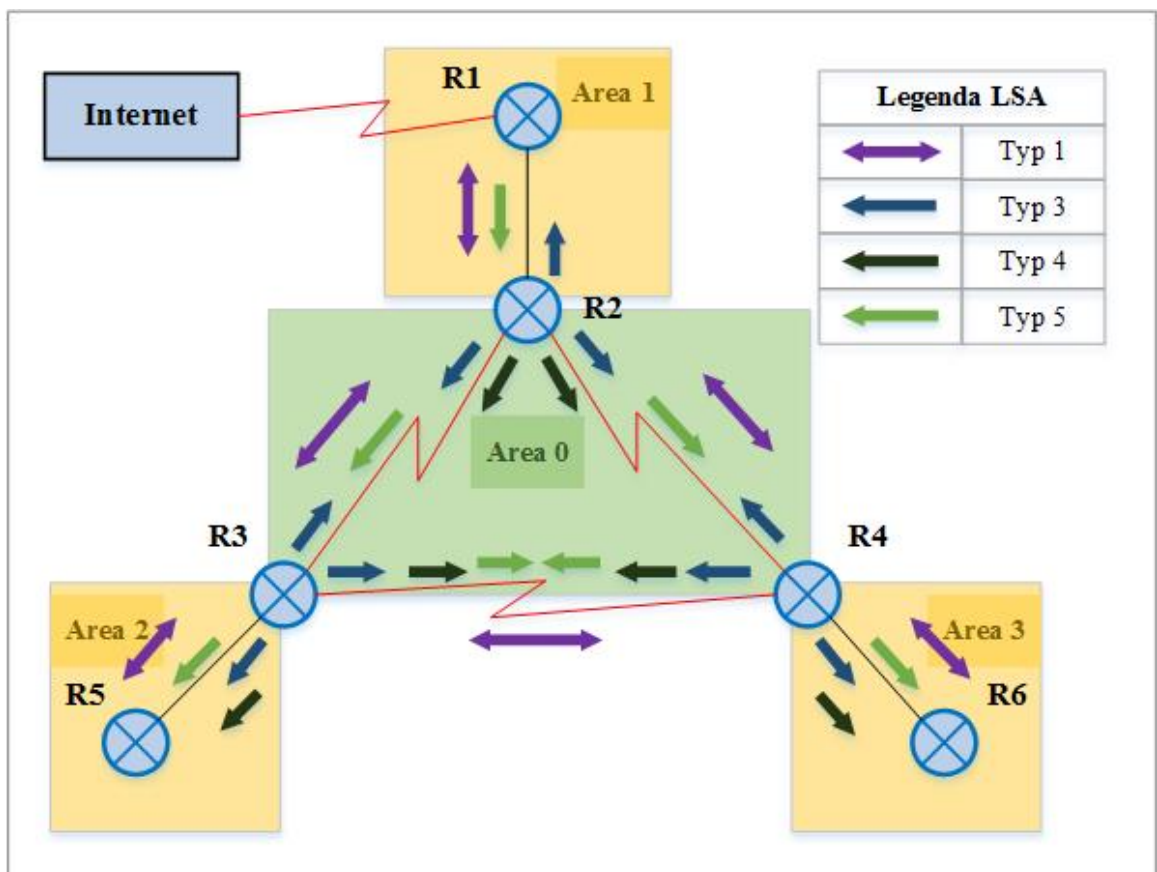
Směrovač může být zařazen do více skupin. Pokud směrovač spojuje dvě oblasti (Area 0 a Area 1) a udržuje informace o směrování do jiného autonomního systému, můžeme směrovač označit jako páteřní směrovač, ABR a ASBR.



## 5.1 PAKETY LSA v MULTIAREA

Na Obrázku 12 se nachází přepracovaná topologie vyobrazená na Obrázku 10. Oproti původní topologii se směrovače nenacházejí pouze v jedné oblasti, ale jsou rozdělena na páteřní oblast (Area 0) a na oblasti, s ní spojenou (Area 1, 2, 3). Topologie je doplněna o externí autonomní systém, aby bylo možno demonstrovat více paketů LSA.

Na topologii jsou vyznačeny základní typy paketů LSA kromě typu 2, jelikož se nejedná o multiaccess síť. Typ 2 byl vysvětlen na ukázkové topologii na Obrázku 11. Jednotlivé pakety LSA byly vysvětleny v kapitole 3.



Obrázek 13 – Pakety LSA v Multiarea

Zdroj: Vlastní

## 5.2 MĚŘENÍ RYCHLOSTI KONVERGENCE

Na základě již se sestavené topologie z Obrázku 12 se překonfiguruje nastavení pro měření konvergence v Multiarea. Směrovače se rozdělí do několika oblastí (Area):

- **Area 0 (páteřní oblast)** – směrovače R2, R3, R4
- **Area 1** – směrovače R1, R2
- **Area 2** – směrovače R3, R5
- **Area 3** – směrovače R4, R6

Jelikož některé směrovače se vyskytují ve dvou oblastech, je nutné si uvědomit, kterou funkci bude jednotlivý směrovač zastávat.

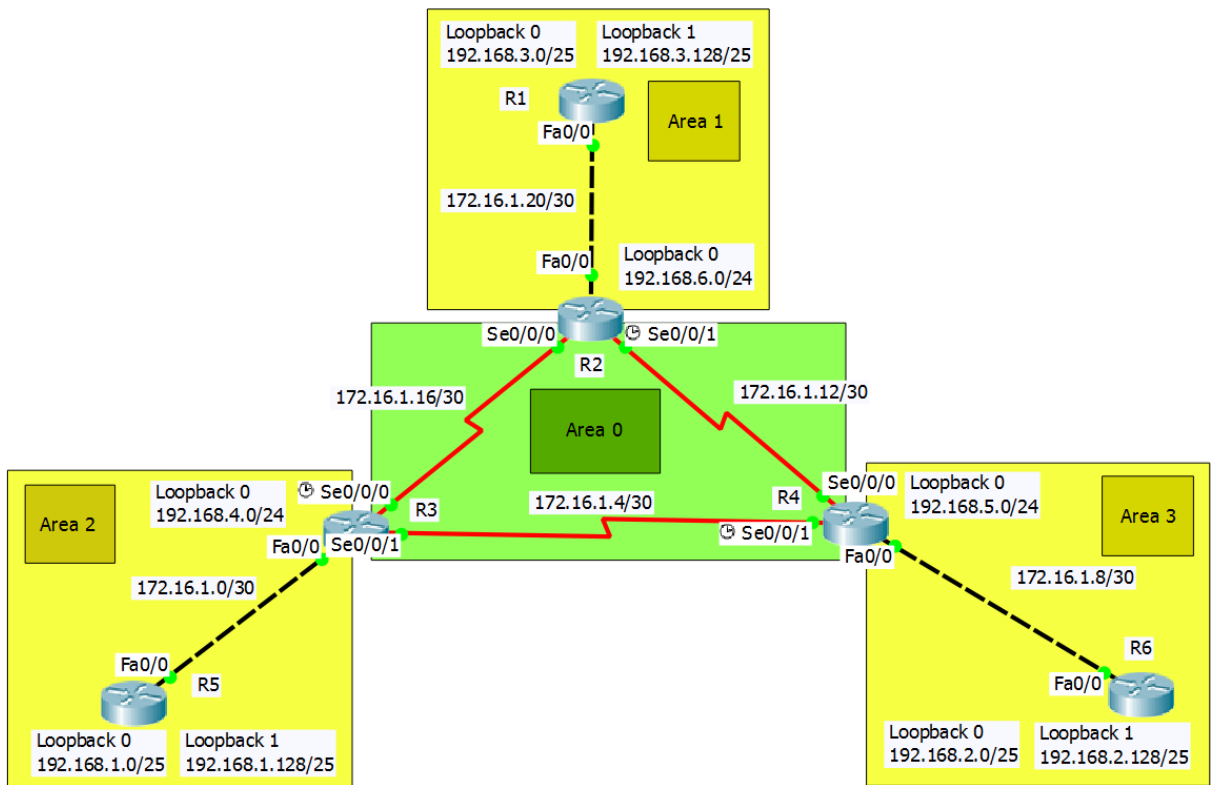
- **Interní směrovač** – R1, R5, R6
- **Páteřní směrovač** – R2, R3, R4
- **Hraniční směrovač (ABR)** – R2, R3, R4

Jak již bylo řečeno v úvodu kapitoly, může směrovač plnit více než jednu funkci. Směrovače R2, R3, R4 plní roli páteřních i hraničních směrovačů.

Přerozdělená topologie je vyobrazena na obrázku 14. Každý loopback, který slouží jako demonstrování koncových uživatelů, je zařazen do nepáteřních oblastí (Area 1, 2, 3). Adresace zůstává totožná jako při konfigurování Single-Area. Mění se zde pouze konfigurace OSPF na směrovačích. Směrovače ABR nabízejí sumarizaci, kterou lze využít k sumarizování podsítí. V topologii jsou reprezentována jako loopbacky na směrovačích R1, R5 a R6.

Všechny cesty, které byly zjištěny v předchozím měření, zůstávají stejné. Pokud bude potřeba zjistit další komunikační cesty od vybraného směrovače určitému cíli, využijeme postup k nalezení cesty uvedený v předchozí kapitole.

Měření konvergence topologie, kde je uplatněna metoda rozdělit topologii do oblastí, bude znovu měřena v simulačním programu (Packet Tracer) a na fyzických zařízeních.



Obrázek 14 – Měřená topologie Multiarea

Zdroj: Vlastní

### 5.2.1 MĚŘENÍ V SIMULAČNÍM PROGRAMU

Postup, který je znám z minulé kapitoly, bude uplatněn i zde. Zašle se 100 paketů ping s časovým limitem jedna sekunda. Pro výpočet rychlosti konvergence bude znovu sloužit cesta ze směrovače R6 na loopback 0 (192.168.3.1) směrovače R1. Pro přesnost výsledku bude toto měření odzkoušeno na různých cestách v topologii s několika opakováními.

```

R6#ping
Protocol [ip]:
Target IP address: 192.168.3.1           ← Adresa loopbacku 0 na R1
Repeat count [5]: 100                   ← Počet odesílaných paketů
Datagram size [100]:
Timeout in seconds [2]: 1               ← Časový limit
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.3.1, timeout is 1 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 95 percent (95/100), round-trip min/avg/max = 7/12/26 ms

```

**Celkem bylo posláno 100 paketů. Bylo doručeno celkem 95 paketů a 5 jich bylo ztraceno. Čas konvergence je 5 sekund.**

### 5.2.2 MĚŘENÍ NA FYZICKÉM ZAŘÍZENÍ

Na fyzických zařízeních se pouze překonfiguruje nastavení OSPF, které již bylo sestaveno při měření Singl-Area. Nastavení příkazu „ping“ bude stejné jako v předešlých případech.

```
R6#ping
Protocol [ip]:
Target IP address: 192.168.3.1          ← Adresa loopbacku 0 na R1
Repeat count [5]: 100                  ← Počet odesílaných paketů
Datagram size [100]:
Timeout in seconds [2]: 1              ← Časový limit
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.3.1, timeout is 1 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 94 percent (94/100), round-trip min/avg/max = 15/23/39 ms
```

**Celkem bylo posláno 100 paketů. Bylo doručeno celkem 94 paketů a 6 jich bylo ztraceno. Čas konvergence je 6 sekund.**

## ZÁVĚR

OSPF je jednoduchý dynamický protokol, který lze snadno implementovat. S podporou beztrždního směrování nabízí možnost nasazení do rozsáhlejších sítí. OSPF patří k velmi rozšířeným, protože umožňuje rychlou konvergenci a efektivitu použití. OSPF nepatří do kategorie proprietárních protokolů, proto ho lze využít na fyzických zařízeních jiných výrobců.

Na základě sestavené topologie bylo naměřeno několik výsledků v závislosti na zvolené konfiguraci a prostředí. Prostředí zahrnovalo měření v simulačním programu (Packet Tracer) a na fyzickém zařízení.

Topologii nakonfigurovanou jako Single-Area bylo dosaženo dvou výsledků. První se zabývá měření v simulačním programu, kde celkový čas konvergence sítě trvá pět sekund. Druhá hodnota byla získána z měření na fyzickém zařízení, kde výsledkem je šest sekund. Pro získání těchto hodnot bylo provedeno několik měření a opakování s využitím různých komunikačních cest.

Po odměření konvergence podle první konfigurace, kde se směrovače v síti nacházely pouze v jedné oblasti, se rozdělila topologie na menší části. Následně došlo znovu k měření rychlosti konvergence s využitím Multiarea. Výsledky měření na fyzickém zařízení poukazují na obdobné výsledky jako v simulačním programu. Stejně jako v předešlém případě vychází rychlost konvergence sítě na pět (simulační program) a šest (fyzické zařízení) sekund.

Porovnání výsledků obou konfigurací lze dojít k závěru, že nasazení Multiarea na menší topologie nemá vliv na rychlost konvergence. Rychlost konvergence je v obou případech stejná. Rozdíl tvoří pouze měření v simulačním programu a na fyzickém zařízení. Výsledky se od sebe odlišují o jednu sekundu. Vliv na rozdílnost souvisí s využitím programu, který nezahrnuje vnější vlivy jako délka kabeláže, opotřebenost směrovačů a další rušivé elementy.

Na základě získaných výsledků se potvrdily teoretické předpoklady. Je vhodné využívat Multiarea zejména ve velmi rozsáhlých sítích, kde lze znatelně zatížit CPU a paměť směrovače. Multiarea nám poskytuje řešení, jak zredukovat velikost databází a náročnost na CPU. V malých sítích není vytížení velké, proto rozdělení do více oblastí nepřináší patřičnou efektivitu. Lze tím poznamenat, že pro malé topologie je vhodné využít Single-Area a pro velké Multiarea.

## POUŽITÁ LITERATURA

1. *Routing and switching essentials*. Indianapolis, IN: Cisco Press, c2014. Cisco Networking Academy Program series. ISBN 1587133180.
2. ACADEMY, Cisco Networking. *Scaling networks companion guide*. 1st Ed. Indianapolis, IN: Cisco Press, 2014. ISBN 9781587133282.
3. GRAZIANI, Rick. a Bob. VACHON. *Routing protocols*. Indianapolis, Indiana, USA: Cisco Press, 2014. Cisco Networking Academy Program series. ISBN 1587133237.
4. KOLÁŘ, Josef. *Teoretická informatika*. 2. vyd. Praha: Česká informatická společnost, 2000. ISBN 80-900853-8-5.
5. GOYAL, M. a SOPERI, M. Improving Convergence Speed and Scalability in OSPF. *Communications Surveys & Tutorials* [online]. 2012 [cit. 2016-05-08]. pp. 443 – 463. ISSN 1553-877X. Dostupné pro zaregistrované na:  
<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5701734&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Ficp.jsp%3Farnumber%3D5701734>
6. Phil, M. Area Configuration and Link Failure Effect in IP Networks using OSPF Protocol. *International Journal of Scientific and Research Publications* [online]. 2013 [cit. 2016-05-08]. pp. 700 – 705. ISSN 2250-315. Dostupné na:  
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.416.2616&rep=rep1&type=pdf#page=701>
7. Jayakumar, Megha, a Bharathi, B. A comparative study on RIP and OSPF protocols. *Innovations in Information, Embedded and Communication Systems* [online]. 2015 [cit. 2016-05-08]. pp. 1 – 5. Dostupné pro zaregistrované na:  
[http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?tp=&arnumber=7193275&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs\\_all.jsp%3Farnumber%3D7193275](http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?tp=&arnumber=7193275&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D7193275)
8. Ramya, P. a Vishnu, V. IMPLEMENTING OSPF PROTOCOL IN CISCO 2800 SERIES ROUTER. *International Journal of Innovations in Engineering and Technology* [online]. 2012 [cit. 2016-05-08]. pp. 77 – 82. ISSN 2319-1058. Dostupné na: <http://ijiet.com/wp-content/uploads/2013/01/13.pdf>
9. Xingchao, M. a Xia, G. Autonomous System Network Topology Discovery Algorithm Based On OSPF Protocol. *3rd International Conference on Material, Mechanical and Manufacturing Engineering* [online]. 2015 [cit. 2016-05-08]. pp. 1099– 1106. Dostupné na: [http://www.atlantis-press.com/php/download\\_paper.php?id=25837823](http://www.atlantis-press.com/php/download_paper.php?id=25837823)

10. Balchunas, A. Static vs. Dynamic Routing. *Router alley* [online]. 2007 [cit. 2016-05-08].  
Dostupné na: [http://www.routeralley.com/guides/static\\_dynamic\\_routing.pdf](http://www.routeralley.com/guides/static_dynamic_routing.pdf)
11. Krzyzanowski, P. Static vs. Understanding Autonomous Systems. *Internet Technology* [online]. 2016 [cit. 2016-05-08]. Dostupné na:  
[https://www.cs.rutgers.edu/~pxk/352/notes/autonomous\\_systems.html](https://www.cs.rutgers.edu/~pxk/352/notes/autonomous_systems.html)
12. OSPF Neighbor States. *Cisco* [online]. 2014 [cit. 2016-05-08]. Dostupné na:  
<http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html>
13. Leahy, E. OSPF Neighbors and Adjacencies. *Eric Leahy* [online]. 2011 [cit. 2016-05-08].  
Dostupné na: <http://ericleahy.com/index.php/ospf-neighbors-and-adjacencies/>