ŽILINSKÁ UNIVERZITA V ŽILINE
FAKULTA RIADENIA A INFORMATIKY

RÝCHLE ZOTAVENIE SIETE – IP FAST REROUTE

Dizertačná práca

28360020153003

Študijný program:	Aplikovaná informatika
Študijný odbor:	9.2.9
Pracovisko:	Fakulta riadenia a informatiky Katedra informačných sieti Žilinská univerzita
Školiteľ:	Doc. Ing. Pavel Segeč, PhD.
Školiteľ špecialista:	Ing. Peter Palúch, PhD.

Žilina, 2015 **Ing. Jozef Papán**

Annotation

Type of the work :	Dissertation work
Academic year :	2014/2015
Title of the work :	IP FAST REROUTE
Author :	Ing. Jozef Papán
Supervisor :	Doc. Ing. Pavel Segeč, PhD.
Co-Supervisor:	Ing. Peter Palúch, PhD.
Language :	Slovak
Number of pages :	114
Number of figures :	40
Number of tables :	8
Number of references:	75
Keywords :	IP Fast Reroute; IPFRR; multicast; RPF; PIM-DM;

Čestné prehlásenie

Prehlasujem, že som zadanú prácu vypracoval samostatne, pod odborným vedením vedúceho práce doc. Ing. Pavla Segeča, PhD. a školiteľa špecialistu Ing. Petra Palúcha, PhD. V práci som použil literatúru uvedenú v zozname.

.....

Ing. Jozef Papán

Poďakovanie

Chcel by som hlavne poďakovať vedúcemu práce doc. Ing. Pavlovi Segečovi, PhD. a školiteľovi špecialistovi Ing. Petrovi Palúchovi, PhD. za pomoc a rady počas celej práce na projekte. Zároveň chcem poďakovať mojej rodine za podporu.

Abstract

PAPÁN, Jozef: IP Fast Reroute. [Dissertation Thesis]. - University of Žilina; Faculty of Management Science and Informatics; Department of Infocomms network. - Doc. Ing. Pavel Segeč, PhD., Ing. Peter Palúch, PhD. Qualification level: Doctor of Philosophy. City: Žilina, 2014/2015. Number of pages 114.

After a link or node failure, a process of network convergence starts in a network, during which routers must update their routing tables. The overall time of network convergence might take from a few milliseconds up to tens of seconds. During this process, several destinations in the network might become unavailable, packet loss might increase or even routing loops might occur. Several solutions have been introduced and developed for solving these negative impacts - these mechanisms are called by a common term Fast Reroute (FRR) mechanisms.

The first FRR mechanism was Multiprotocol Label Switching (MPLS) FRR, which uses an explicit backup routes. However, since the MPLS mechanisms are not used in every network and MPLS is not scalable enough, the next development lead towards the IPFRR mechanisms.

The main goal of all IPFRR mechanisms is to minimize network recovery time after node or link failure. The key feature of these mechanisms is calculation of alternative route before the failure occurs. The computation of alternative route requires network topology information and therefore most of the existing IPFRR mechanisms strongly depend on the usage of link-state routing protocols.

In this thesis a new innovative Multicast Repair (M-REP) IPFRR mechanism, which uses an IP multicast technology, is presented. The proposed M-RER mechanism uses Protocol Independent Multicast - Dense Mode (PIM-DM) with modified algorithm of the Reverse Path Forwarding (RPF). The key contribution of this thesis is the fact that the proposed M-REP IPFRR mechanism is independent of the link-state routing protocols and the internal algorithm does not explicitly calculate the alternative path.

Keywords: IP Fast Reroute; IPFRR; multicast; RPF; PIM-DM;

Abstrakt

PAPÁN, Jozef: Rýchle zotavenie siete. [Dizertačná práca]. - Žilinská univerzita; Fakulta riadenia a informatiky; Katedra informačných sietí. - Doc. Ing. Pavel Segeč, PhD., Ing. Peter Palúch, PhD., Stupeň odbornej kvalifikácie: Doktor filozofie. Mesto: Žilina, 2014/2015. Počet strán 114.

Po zlyhaní linky alebo smerovača v sieti nastáva proces konvergencie siete, počas ktorého smerovače musia aktualizovať svoje smerovacie tabuľky. Celková doba procesu konvergencie siete môže trvať od niekoľkých milisekúnd až do desiatok sekúnd. Počas tohto procesu môže dôjsť k nedostupnosti cieľových sietí, prerušeniu komunikácie, stratám paketov, vzniku smerovacích slučiek či iným negatívnym dopadom na sieťové služby. Na riešenie týchto problémov boli rozpracované a vyvinuté nové mechanizmy tzv. rýchleho zotavenia siete – Fast Reroute (FRR).

Prvý FRR mechanizmus bol Multiprotocol Label Switching (MPLS) FRR, ktorý využíval explicitné záložné trasy. Keďže však nie každá sieť používa MPLS a povaha MPLS FRR bola v zásade málo škálovateľná, ďalší vývoj sa uberal smerom k IPFRR.

Hlavným cieľom všetkých IPFRR mechanizmov je minimalizovať pri zlyhaní linky alebo smerovača dobu potrebnú pre obnovenie sieťovej komunikácie. Kľúčovou vlastnosťou týchto mechanizmov je vypočítanie alternatívnej trasy skôr, ako dôjde k samotnej chybe v sieti. Výpočet alternatívnej cesty vyžaduje informácie o topológii siete, a preto väčšina existujúcich IPFRR mechanizmov je závislá na link-state smerovacích protokoloch.

V tejto práci je prezentovaný inovatívny Multicast Repair (M-REP) IPFRR mechanizmus, ktorý využíva technológiu IP multicast. V práci navrhnutý M-REP mechanizmus využíva multicastový protokol Protocol Independent Multicast – Dense Mode (PIM-DM) s modifikáciou pravidla Reverse Path Forwarding Check (RPF). Medzi hlavné prínosy M-REP IPFRR mechanizmu patrí nezávislosť od link-state smerovacích protokolov a fakt, že alternatívna cesta nie je explicitne vypočítaná vnútorným algoritmom.

Kľúčové slová: IP Fast Reroute; IPFRR; rýchle zotavenie siete, multicast; RPF; PIM-DM;

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM SKRATIEK

ANSA	–	Automated Network Simulation and Analysis
BFD	–	Bidirectional Forwarding Detection
BGP	–	Border Gateway Protocol
Cisco IOS	–	Cisco Internetwork Operating System
CSPF	–	Constrained Shortest Path First
DLCI	–	Data Link Connection Identifier
DSCP	–	Differentiated Services Code Point
ECMP	–	Equal Cost Multiple Paths
FIR	–	Failure Insensitive Routing
GPL	–	General Public License
IDE	–	Integrated Development Environment
IGMP	–	Internet Group Management Protocol
IP	–	Internet Protocol
IPFRR	–	IP Fast Reroute
ISF	–	Interface-Specific Forwarding
IS-IS	–	Intermediate System to Intermediate System
LAN	–	Local Area Network
LDP	–	Label Distribution Protocol
LFA	–	Loop - Free Alternates
LSP	–	Label Switched Path
MPLS	–	Multiprotocol Label Switching
MPLS-TE FRR	–	MPLS - Traffic Engineering Fast Reroute
MRC	–	Multiple Routing Configurations
MRT	–	Maximally Redundant Trees
MTU	–	Maximum Transmission Unit
OS	–	Operating system
OSPF	–	Open Shortest Path First
PIM-DM	–	Protocol Independent Multicast - Dense Mode
PIM-SM	–	Protocol Independent Multicast - Sparse Mode
PIM-SSM	–	Protocol Independent Multicast - Source-Specific Multicast
QoS	–	Quality of Service
RFC	–	Request for Comments

RIP	–	Routing Information Protocol
RIPE	–	Réseaux IP Européens
RIPE NCC	–	RIPE Network Coordination Centre
RIPng	–	RIP Next Generation
RP	–	Rendezvous Point
RSVP-TE	–	Resource Reservation Protocol - Traffic Engineering
SCTP	–	Stream Control Transmission Protocol
SPF	–	Shortest Path First
SPT	–	Shortest Path Tree
SRLG	–	Shared Risk Link Groups
TCP	–	Transmission Control Protocol
ToS	–	Type of Service
UDP	–	User Datagram Protocol
VLAN	–	Virtual LAN
VoIP	–	Voice over Internet Protocol
VTY	–	Virtual Terminal

ÚVOD

V minulosti sa komunikácia v IP sieťach sústreďovala najmä na služby elektronickej pošty, prenosu súborov a sprístupňovania webového obsahu, avšak v priebehu posledných pár rokov IP siete významne pokročili v poskytovaní hlasových služieb (VoIP) a video služieb. Tieto služby kladú omnoho vyššie požiadavky na prenosové zdroje siete. Na poskytovanie požadovanej služby vyžadujú určité požiadavky na garanciu niektorých kvalitatívnych parametrov, ako je dostupnosť a rýchle zotavenie samotnej siete. Zotavenie siete chápeme ako obnovenie komunikácie v prípade výpadku linky alebo smerovača. Všeobecnou požiadavkou je, aby sa sieť po výpadku linky alebo smerovača zotavila v čo najkratšom čase.

Ak v sieti nastane výpadok konektivity alebo zmena v topológii, smerovacie protokoly, ako sú napríklad Open Shortest Path Free (OSPF) alebo Intermediate System to Intermediate System (IS-IS), reagujú na túto zmenu opätovným procesom konvergencie v sieti. Počas tohto procesu smerovacie protokoly musia aktualizovať svoje smerovacie informácie a smerovače, ktoré sú ovplyvnené chybou, rozposielajú správy o zmene v topológii siete. Doba procesu konvergencie siete je závislá najmä od komplexnosti siete a od použitého smerovacieho protokolu.

Veľkosť a komplexnosť sietí poskytovateľov ako aj nevyhnutnosť poskytovať požadované služby pre zákazníkov nepretržito zvýšili dopyt po efektívnych a rýchlych mechanizmoch ochrany voči výpadkom v sieti. Tieto mechanizmy by mali poskytovať vhodné prostriedky ochrany a reakcie voči spomínaným, z pohľadu výskytu a doby trvania ťažko predpovedateľným výpadkom v sieťach s IP protokolom. Odpoveďou na tieto požiadavky sú mechanizmy IP Fast Reroute (IPFRR), ktorých základnou úlohou je obnoviť pri výpadku linky alebo smerovača prerušenú komunikáciu v čo najkratšom čase na dobu, kým neprebehne v sieti proces konvergencie smerovacieho protokolu.

Primárnym účelom mechanizmov IPFRR je proaktívny výpočet alternatívnych záložných ciest do známych cieľov v sieti. Tie sú v predstihu pripravené a okamžite využiteľné v momente, keď na primárnej ceste zlyhá linka alebo celý smerovač. Tieto cesty sú vypočítavané v predstihu ako alternatívne záložné smerovacie cesty pre prípady špecifického zlyhania liniek daného smerovača alebo zlyhania samotného susedného smerovača. Mechanizmy IPFRR zvyčajne môžu ako podporný mechanizmus urýchľujúci

reakciu na výpadok využívať rýchlu detekciu dostupnosti liniek alebo susedov. Tieto špecializované mechanizmy ponúkajú podstatne rýchlejšiu detekciu lokálneho výpadku ako mechanizmy vstavané v súčasných smerovacích protokoloch (napr. OSPF, EIGRP Hello mechanizmy).

Po detekcii výpadku linky so susedným smerovačom mechanizmy IPFRR použijú vopred vypočítanú alternatívnu cestu a realizujú tak obchádzku komunikácie okolo chybného spojenia. Alternatívna cesta je aktívna minimálne takú dobu, kým sa proces konvergencie v sieti nedokončí. Obnovenie komunikácie mechanizmami IPFRR je rýchlejšie ako samotná konvergencia smerovacích protokolov na smerovačoch v sieti.

Predkladaná práca sa skladá z šiestich kapitol. Prvá kapitola sa venuje základnému opisu procesu konvergencie siete, elementárnemu princípu IPFRR a základnej terminológii v oblasti IPFRR. Ďalej je v kapitole popísaný mechanizmus výpočtu alternatívnej cesty, rýchla detekcia chýb linky, základné spôsoby ochrany pomocou IPFRR mechanizmov a problematika efektivity mechanizmov IPFRR.

Druhá kapitola rozoberá problematiku IPFRR. V kapitole sú definované základné požiadavky na mechanizmy IPFRR. Následne je vykonaná analýza existujúcich mechanizmov v oblasti IPFRR . Analyzované existujúce mechanizmy IPFRR sú hodnotené na základe porovnávania s definovanými všeobecnými požiadavkami na mechanizmy IPFRR. Na konci kapitoly sa nachádza vyhodnotenie analýzy súčasného stavu a určenie problémových oblastí.

V tretej kapitole je definovaný hlavný cieľ práce ako aj nasledovné parciálne ciele práce. Hlavným cieľom tejto dizertačnej práce je návrh nového IPFRR mechanizmu.

Štvrtá kapitola ponúka podrobný popis navrhnutého IPFRR mechanizmu. Mechanizmus využíva multicastový protokol Protocol Independent Multicast - Dense Mode (PIM-DM) s modifikovaným RPF pravidlom. Mechanizmus je pre potreby práce nazvaný Multicast Repair, alebo skrátene M-REP. Ďalej je v kapitole analyzovaná a zvolená metodika pre overenie navrhnutého M-REP IPFRR mechanizmu.

Piata kapitola ponúka matematické overenie a simulačné otestovanie funkčnosti návrhu M-REP IPFRR mechanizmu. Táto kapitola obsahuje matematicky dôkaz, ktorý dokáže korektnosť v práci navrhnutej modifikácie originálneho PIM RPF mechanizmu.

Ďalej sa v kapitole sústredíme na výber vhodného simulačného nástroja, v ktorom budeme testovať navrhnutý mechanizmus v rôznych scenároch s výpadkami v sieti.

V šiestej kapitole sú identifikované a rozobraté dosiahnuté prínosy M-REP IPFRR mechanizmu, ako aj je ponúknuté porovnanie s existujúcimi riešeniami, identifikované problémové oblasti a načrtnuté ďalšie oblasti výskumu.

1 SÚČASNÝ STAV RIEŠENIA PROBLEMATIKY

Jeden z hlavných dôvodov, prečo sa mechanizmy IPFFR dostávajú do popredia výskumu je, že proces konvergencie po výpadku linky alebo smerovača trvá v mnohých prípadoch dlhší čas ako je očakávané od prevádzkovateľa siete. V nasledujúcich podkapitolách bude bližšie rozobratá problematika samotného procesu konvergencie siete spolu so základnými princípmi v oblasti IPFRR.

1.1 Proces konvergencie siete

Doba potrebná pre dokončenie procesu konvergencie siete sa pohybuje v rozmedzí od niekoľkých stoviek milisekúnd až po desiatky sekúnd vo väčších sieťach [**1**]. Doba konvergencie siete je závislá od rôznych faktorov, ako sú napr. počet smerovačov v danej sieti, komplexnosť topológie, typ smerovacieho protokolu a nastavenie jeho jednotlivých časovačov. Podľa zdroja [**2**] doba procesu konvergencie siete (smerovacieho procesu) pozostáva z nasledujúcich čiastkových dôb:

- **Doba potrebná pre detekciu výpadku.** Na fyzickej vrstve môže detekcia výpadku trvať niekoľko ms. Na úrovni smerovacieho protokolu môže trvať až niekoľko desiatok sekúnd. Počas tejto doby sú pakety stratené.
- **Doba potrebná pre reakciu lokálneho smerovača na výpadok linky.** Počas tejto doby smerovač zvyčajne generuje a rozposiela smerovacie aktualizácie.
- **Doba potrebná pre informovanie ostatných smerovačov o výpadku.** Táto doba zvyčajne trvá od 10 ms až po 100 ms pre každý next-hop smerovač [**2**].
- **Doba potrebná pre prepočítanie smerovacích tabuliek.** Prepočítanie smerovacích tabuliek trvá približne niekoľko ms pre link-state smerovací protokol, ktoré používajú Dijkstrov algoritmus [**3**]. Táto doba je závislá najmä od veľkosti siete a množstva topologických informácií.
- **Doba potrebná pre inštaláciu nových smerovacích tabuliek do hardvéru.** Táto doba je závislá od samotného typu smerovača a od počtu prefixov, ktoré boli ovplyvnené chybou.

Prerušenie komunikácie v sieti trvá dovtedy, kým smerovače ovplyvnené chybou dokončia celý proces konvergencie siete. Počas procesu konvergencie siete môže dôjsť

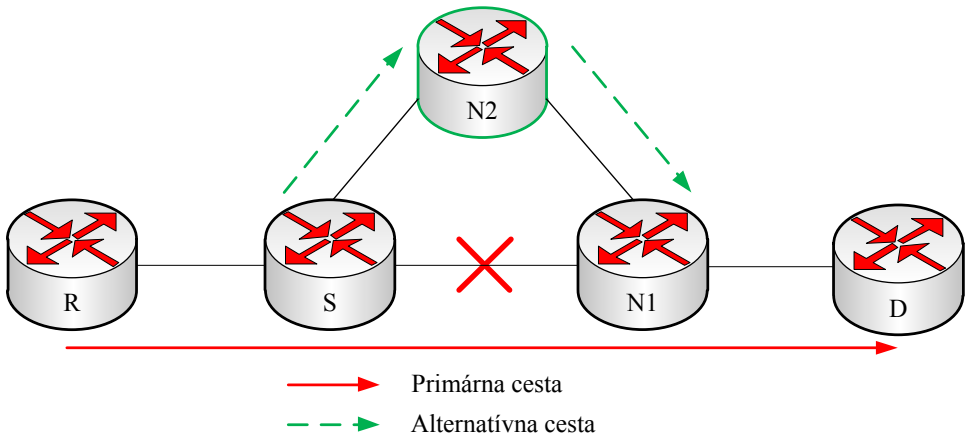
medzi smerovačmi k tzv. mikro-slučkám**.** Tento jav je zvyčajne spôsobený neaktuálnymi informáciami v smerovacích tabuľkách smerovačov. Bližšie informácie sú uvedené v [**4**].

Počas procesu konvergencie siete môžu vznikať rôzne problémy ako napr. prerušenie spojenia, zahodenie paketov a mnoho iných. Na základe týchto problémov sa výskum zameral na vyvinutie nového IPFRR mechanizmu.

1.2 Princíp IPFRR

Činnosť IPFRR mechanizmu sa začína rýchlou detekciou zlyhania linky a končí sa po úspešnej konvergencii siete. Je veľmi dôležité, aby sa aktivita IPFRR mechanizmu neskončila ešte predtým, ako dôjde k potrebným aktualizáciám na úrovni smerovacích protokolov.

Ak nastane výpadok linky v sieti, IPFRR mechanizmus smeruje pakety vopred vypočítanou alternatívnou cestou po dobu konvergencie siete (obrázok 1). Počas tejto doby smerovací protokol aktualizuje informácie o zmene v sieti. Táto aktualizácia smerovacích protokolov prebieha na pozadí. Následne po jej skončení preberá kontrolu nad smerovaním paketov opäť smerovací protokol.



Obrázok 1: Elementárny princíp IPFRR

V terminológii IPFRR sa používajú špecifické označenia pre smerovače, ktoré majú špeciálny význam:

- **Smerovač S** (označuje sa aj **source router**) je taký smerovač, ktorý zistil výpadok pripojenej linky alebo susedného smerovača a následne spúšťa lokálnu IPFRR opravu.

- **Smerovač D** (označuje sa aj **destination router**), je cieľovým smerovačom pôvodného toku dát.

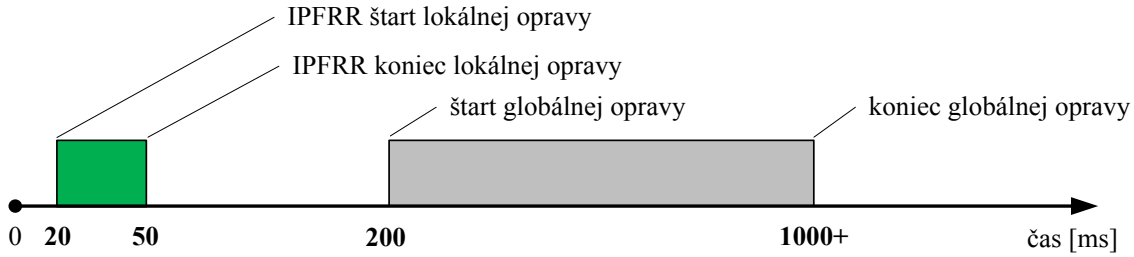
V rôznych zdrojoch sa stretneme s ďalšími označeniami smerovačov ako napr. N, N_1, N_2... Tieto označenia zvyčajne patria smerovačom, ktoré sú použité ako alternatívny nasledujúci smerovač (ďalej označovaný ako next-hop) pre záložnú cestu v prípade zlyhania linky resp. smerovača.

Elementárny popis priebehu rýchleho zotavenia v sieti na smerovači S vyzerá potom nasledovne:

- Rýchla detekcia výpadku linky špecializovanou IPFRR technológiou (aktivácia IPFRR mechanizmu)
- Dočasné pozmenenie smerovacích informácií IPFRR mechanizmom. **Inštalácia vopred vypočítanej alternatívnej cesty** (IPFRR aktívny)
- Aktualizácia smerovacieho protokolu na pozadí. IPFRR mechanizmus zabezpečuje dočasné smerovanie paketov (IPFRR aktívny)
- Smerovací protokol dokončí aktualizáciu smerovacích informácií. IPFRR mechanizmus sa deaktivuje a kontrolu nad smerovaním preberá smerovací protokol (deaktivácia IPFRR mechanizmu)

Jedným z používaných spôsobov, ktorý určuje dobu aktivácie IPFRR mechanizmu a tým zabezpečuje dostatočne dlhý čas na dokončenie procesu konvergencie v sieti je použitie časovača (tzv. **hold down timer**). Tento časovač je nastavený na minimálne taký čas, aby bol proces konvergencie dokončený. Po uplynutí tohto časovača sa dočasné smerovacie informácie odstránia, resp. nahradia, a IPFRR mechanizmus sa deaktivuje [**5**].

Oprava mechanizmom IPFRR (nazýva sa aj lokálna oprava, z angl. Local Repair) je niekoľkonásobne rýchlejšia, ak ju porovnáme s globálnou opravou na úrovni smerovacích protokolov (obrázok 2).



Obrázok 2: Porovnanie IPFRR lokálnej a globálnej opravy

Dôležitým faktorom pri IPFRR je doba zotavenia siete po výpadku linky alebo smerovača. Preto táto hodnota by mala predstavovať jeden z kľúčových faktorov pri posudzovaní IPFRR mechanizmov. Priemerná reakčná doba súčasných IPFRR mechanizmov pre rýchle zotavenie siete je **50ms** [**6**] , [**7**], [**8**].

1.3 Prípravné výpočty

Ak smerovač zistí, že spojenie so susedným smerovačom zlyhalo, použije vopred **vypočítanú záložnú cestu** pre opätovné obnovenie komunikácie. Táto vopred vypočítaná záložná cesta sa označuje aj ako **pre-computed backup path**. Smerovač teda použije vopred pripravenú cestu na obchádzku chybnej linky alebo smerovača. Princíp vopred vypočítanej alternatívnej cesty sa označuje **pre-computing**. Táto alternatívna cesta **nesmie** prechádzať cez zlyhanú linku alebo zlyhaný smerovač. Smerovač môže obsahovať aj viac vopred vypočítaných záložných ciest. Pri ich použití sa každý smerovač rozhoduje nezávisle od ostatných smerovačov. To znamená, že sa rozhoduje na základe vlastných vnútorných pravidiel. V súčasnosti existujú viaceré mechanizmy IPFRR, ktoré sa vzájomne odlišujú spôsobom výpočtu záložných alternatívnych ciest. Jednotlivé IPFRR mechanizmy sú bližšie opísané v kapitole 2.

Princíp vopred vypočítanej záložnej cesty v súčasnosti používajú **všetky** IPFRR mechanizmy. Tento spôsob je kľúčovým faktorom k dosiahnutiu minimálneho času vyžadovaného pre zotavenie siete po zlyhaní linky alebo smerovača.

1.4 Detekcia chýb v IPFRR

Dosiahnutie rýchleho zotavenia siete po zlyhaní linky alebo smerovača sa začína rýchlou detekciou tohto zlyhania. IPFRR mechanizmy používajú pre detekciu výpadku linky

technológie, ktoré sa snažia **minimalizovať** detekčný čas. Je nutné poznamenať, že detekcia výpadku linky trvá **najdlhšiu** dobu z celkovej doby pre rýchle zotavenie siete. Medzi najznámejšie detekčné technológie pre IPFRR podľa zdroja [**2**] patria:

- **Detekcia na fyzickej úrovni**, napr. strata bitovej, rámcovej alebo super rámcovej synchronizácie, nosnej frekvencie, riadiacich signálov (ako napr. Data Set Ready/Data Terminal Ready), svetla (loss of light), nárast bitovej chybovosti apod.
- **Detekcia špecializovaným protokolom, ktorý je nezávislý od smerovacieho protokolu**. Jeden z najpoužívanejších je Bidirectional Forwarding Detection (BFD) [**9**]. Tento protokol používa princíp overovania stavu linky za pomoci posielania rýchlych "Hello" správ.
- **Detekcia smerovacím protokolom**. Rýchlu detekciu v rámci smerovacieho protokolu je možné získať použitím rýchlejších "Hello" správ s intervalom pod 1s, napr. OSPF Fast Hello Packets [**10**].

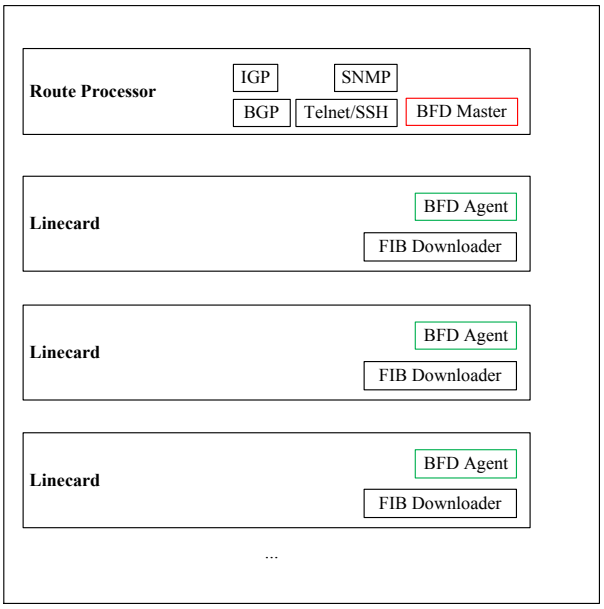
V oblasti IPFRR je dôležité rozlišovať, či ide o zlyhanie linky alebo smerovača. Ak zlyhá linka k susednému smerovaču, je nutné sa jej vyhnúť, ale smerovač za ňou je možné v mechanizme IPFRR použiť. V prípade zlyhania smerovača je nutné sa vyhnúť všetkým pripojeným linkám k nemu.

V zdroji [**2**] je uvádzaný pojem Shared Risk Link Groups (SRLG). Ide o skupinu liniek, ktoré sú realizované nad tou istou podkladovou konektivitou (napr. viaceré virtuálne LAN na trunku, viaceré DLCI identifikátory na jednom Frame Relay porte), kde rozpad podkladovej konektivity má za dôsledok rozpad všetkých liniek realizovaných nad ňou.

1.5 Bidirectional Forwarding Detection (BFD)

BFD je najpoužívanejší mechanizmus, ktorý sa používa na rýchlu detekciu chýb linky v oblasti IPFRR. BFD môže poskytovať detekciu chýb na spojení medzi rôznymi systémami vrátane fyzických liniek, virtuálnych okruhov, tunelov, MPLS LSPs a ciest medzi nesusednými smerovačmi. BFD používa mechanizmus "Hello" správ, avšak pakety BFD sa posielajú po sieti **nezávisle** od použitého smerovacieho protokolu. Tieto BFD správy sú odosielané po sieti ako unicastová komunikácia [**9**].

BFD kopíruje mechanizmus "Hello" klasických smerovacích protokolov, avšak s nižšou réžiou a vyššou rýchlosťou. Mechanizmus BFD môže pracovať na linkových kartách smerovača (line cards), čo v takom prípade znamená, že nezaťažuje primárne RP CPU (route processor) smerovača (obrázok 3) [**11**].



Obrázok 3: Príklad architektúry BFD na smerovači

BFD používa pre nadviazanie a ukončenie BFD relácie trojcestný mechanizmus. Dvojica systémov si posiela periodicky BFD pakety a ak jedna zo strán prestane od suseda prijímať BFD pakety určitý čas, mechanizmus BFD deklaruje toto spojenie ako nedostupné (down). Mechanizmus BFD môže pracovať v dvoch primárnych režimoch:

- **Asynchrónny režim** (Asynchronous mode): systémy periodicky a nepretržite odosielajú riadiace BFD pakety svojim susedom
- **Režim na vyžiadanie** (Demand mode): po nadviazaní BFD relácie sa riadiace BFD správy odosielajú len vtedy, ak je potrebné explicitne overiť dostupnosť suseda

Doplnkový mód k primárnym dvom režimom je funkcia Echo. Ak je funkcia echo aktívna, systém, ktorý príjme BFD echo paket, posiela tento paket späť. Ak nie je prijatý určitý počet paketov, BFD relácia sa prehlási za nedostupnú. Množstvo BFD paketov na spojení je možné obmedziť nastavením asynchrónneho režimu alebo eliminovať kompletne nastavením režimu na vyžiadanie.

Mechanizmus BFD môže pracovať s IGP (Interrior Gateway Protocols) smerovacími protokolmi ako sú napr. OSPF, IS-IS, s EGP protokolmi (BGP) ako aj s MPLS (LDP) [**11**]. V [**12**] autor uvádza, že mechanizmus BFD dokáže spoľahlivo zistiť výpadok linky už od 9ms (3 x 3 ms Hello interval).

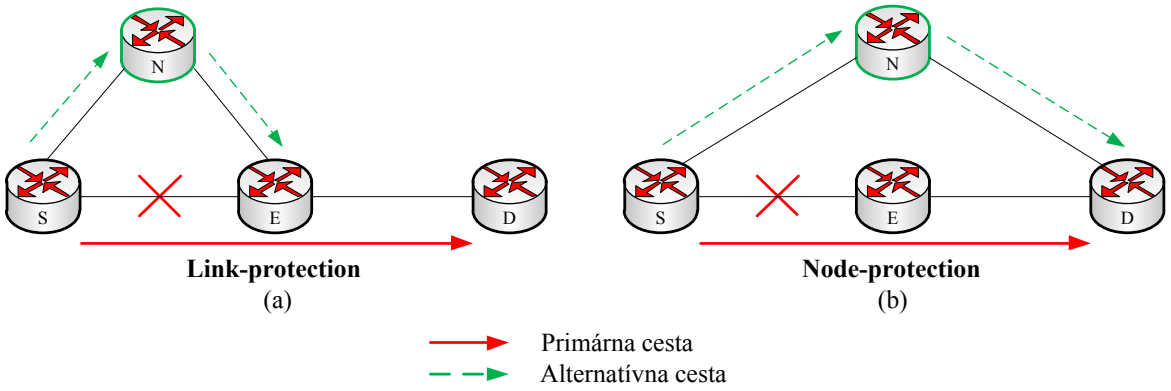
1.6 Ochrana linky vs ochrana uzla

Vo všeobecnosti smerovač S, ktorý má implementovaný IPFRR mechanizmus, môže poskytovať dva elementárne princípy ochrany (obrázok 4) [**13**]:

- **Ochranu linky**, označuje sa aj **link-protection.**
- **Ochranu smerovača**, označuje sa aj **node-protection.**

Linka, ktorú smerovač S chráni pred jej výpadkom, sa nazýva **protected link**. Znamená to, že ak táto linka zlyhá, smerovač S vie poskytnúť alternatívnu cestu a zlyhanú **linku** obíde. Smerovač S v tomto prípade poskytuje **link-protection** (obrázok 4a).

Smerovač E, ktorý je chránený pred výpadkom, sa nazýva **protected node**. Znamená to, že ak tento smerovač E zlyhá, susedný smerovač použije alternatívny smerovač a chybný **smerovač** obíde. Smerovač S v tomto prípade poskytuje **node-protection** (Obrázok 4b).



Obrázok 4: Link-protection vs Node-protection

Ak IPFRR mechanizmus dokáže okrem link-protection poskytnúť aj node-protection, jeho efektivita pri vypočítaní alternatívnej cesty je vyššia. Jednotlivé typy ochrán môžu byť samozrejme poskytnuté len ak to fyzické zapojenie danej topológie umožňuje.

1.7 Repair coverage

IP FRR mechanizmy sa odlišujú najmä v tom, do akej miery dokážu ochrániť sieť pred špecifickými chybami liniek alebo smerovačov. V terminológii IPFRR sa označuje efektivita IPFRR mechanizmov termínom **repair coverage**.

Ak IPFRR mechanizmus dokáže opraviť všetky potenciálne chyby v danej sieti, označujeme tento jav ako 100% repair coverage. Vo všeobecnosti môžeme povedať, že čím väčší repair coverage IPFRR mechanizmus má, tým je jeho koncepcia komplexnejšia. V nasledujúcej kapitole bude vykonaná analýza existujúcich mechanizmov IPFRR.

2 ANALÝZA EXISTUJÚCICH RIEŠENÍ

Aj keď ešte nedávno boli niektoré mechanizmy IPFRR len víziou budúcnosti, už dnes existujú funkčné a spoľahlivé spôsoby, ako tieto mechanizmy začleniť do procesu ochrany siete pred výpadkami. Jednotlivé IPFRR mechanizmy sa rozlišujú spôsobmi, ako pristupujú k hľadaniu alternatívnej cesty.

2.1 Požiadavky na IPFRR

K vyriešeniu problémov, ktoré súvisia s problematikou IPFRR, nám môže značne pomôcť základný prehľad požiadaviek pre rýchle zotavenie siete. Základnými problémovými oblasťami IP Fast Reroute je splnenie požiadaviek, ktoré môžeme na základe zdrojov [**14**] [**15**] [**16**] [**17**] [**18**] zhrnúť nasledovne:

- Výpočtová náročnosť algoritmu, pre-computing
- Repair coverage približujúca sa k 100%
- Jednoduchá integrácia do existujúcej topológie
- Ochrana pred výpadkom linky a smerovača
- Efektívna a rýchla obnova komunikácie do 50 ms
- Úspešnosť približujúca sa k 100% zachránených paketov
- Podpora pre technológiu multicast
- Rýchla detekcia chýb v sieti

Nasledujúce kapitoly budú venované popisu stavu problematiky a **analýze existujúcich riešení** z pohľadu plnenia daných požiadaviek.

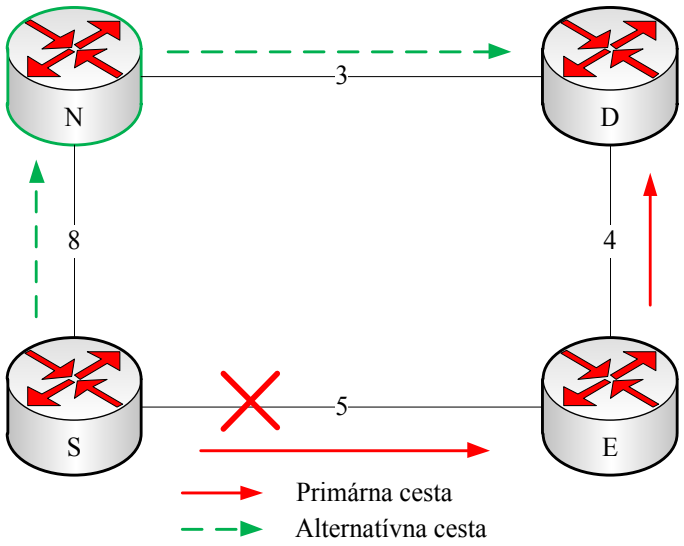
2.2 Loop-Free Alternates (LFA)

Jeden z prvých vyvinutých mechanizmov v oblasti rýchleho zotavenia siete je Loop-Free Alternates (v skratke LFA). Mechanizmus LFA využíva alternatívneho next-hop suseda, ktorý poskytuje náhradnú cestu okolo zlyhanej linky resp. smerovača.

Keď smerovač S vypočíta najkratšiu cestu a vzdialenosť k cieľovému smerovaču D (obrázok 5), smerovač S použije ako primárny next-hop smerovač E. S mechanizmom LFA smerovač S vypočíta aj alternatívny next-hop k cieľovému smerovaču D. V tomto prípade

smerovač S vypočíta, že môže použiť smerovač N ako alternatívny next-hop. Alternatívny next-hop smerovač, musí byť **priamo pripojený** k smerovaču S [**19**] [**20**].

Ak linka s primárnym next-hop smerovačom E zlyhá, smerovač S po detekcii výpadku linky prestane posielať pakety cez primárny next-hop. Smerovač S použije vopred vypočítaný alternatívny next-hop smerovač N. Alternatívny next-hop bude platný, kým smerovací protokol neurčí nové primárne cesty v zmenenej topológii.



Obrázok 5: Loop-Free Alternates

Ak by sa zmenila cena linky zo smerovača N do D z 3 na 30 (obrázok 5), smerovač N by už nebol bezslučkovou alternatívou a nestal by sa alternatívnym next-hop smerovačom, pretože cena cesty zo smerovača N do smerovača D cez smerovač S by bola 17, kým cena zo smerovača N do smerovača D by bola 30. Z toho vyplýva, že mechanizmus LFA je primárne závislý na topológii siete a cenách jednotlivých liniek.

Terminológia LFA mechanizmu je uvádzaná v [**2**] a [**13**], kde S je označenie smerovača, ktorý vyberá LFA (označuje sa aj ako calculating router); N je potenciálny LFA susedný smerovač smerovača S. Označenie smerovačov N_1, N_2 sa používa, ak smerovač S má viacero potenciálnych LFA susedných smerovačov.

Vo všeobecnosti, aby smerovač S vedel vypočítať LFA pre špecifickú destináciu D, potrebuje minimálne vedieť nasledovné informácie [**13**]:

- Cena najkratšej cesty od smerovača S do destinácie D: **Cost(S, D)**
- Cena najkratšej cesty od susedného smerovača N do destinácie D: **Cost(N, D)**
- Cena najkratšej cesty od susedného smerovača N k smerovaču S: **Cost(N, S)**

Všetky uvedené vzdialenosti je možné získať zo smerovacieho protokolu bežiaceho na smerovačoch v sieti. V prípade protokolov s vektorom vzdialeností (RIPv2, EIGRP) sú vzdialenosti smerovačov od jednotlivých destinácií bezprostredným obsahom ich smerovacích správ. V prípade protokolov so stavom linky (OSPF, IS-IS) musí smerovač na základe znalosti topológie tieto vzdialenosti cielene vypočítať, potrebné informácie pre ich výpočet však má k dispozícii.

Aby smerovač bol vybraný ako LFA, musí splniť nasledovné podmienky [**19**] [**13**] [**5**]:

Podmienka 1: Loop-Free

$$\mathbf{Cost(N, D) < Cost(N, S) + Cost(S, D)} \quad (1)$$

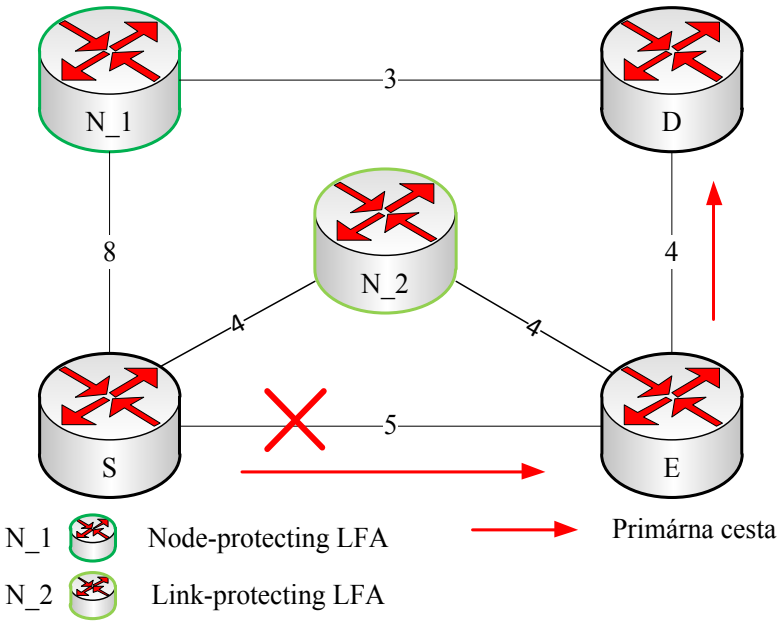
Podmienka 2: Downstream Path

$$\mathbf{Cost(N, D) < Cost(S, D)} \quad (2)$$

Podmienka 3: Node-Protecting Loop-Free Alternate

$$\mathbf{Cost(N, D) < Cost(N, E) + Cost(E, D)} \quad (3)$$

Ak smerovač N splní podmienku č. 1, znamená to, že nespôsobí smerovaciu slučku pri odosielaní paketov k cieľovému smerovaču D. Ak smerovač splní podmienku 2, znamená to (obrázok 6), že smerovač N poskytuje ochranu linky (**Link-Protecting LFA**). Podmienka 3 zaručuje, že smerovač N poskytuje ochranu pred výpadkom smerovača (**Node-Protecting LFA**).



Obrázok 6: Node-protecting LFA vs Link-Protecting LFA

Podľa zdroja [**19**] sa LFA rozdeľuje na per-prefix LFA a per-link LFA. Tieto spôsoby sa odlišujú v princípe, akým je vypočítaný alternatívny next-hop smerovač.

Per-prefix LFA pre destináciu D na smerovači S je vopred vypočítaný záložný IGP next-hop pre danú destináciu D. To znamená, že bude vypočítaný alternatívny LFA smerovač pre **každý** prefix. Pri per-prefix LFA mechanizmus berie do úvahy aj LFA kandidátov, ktorí nie sú priamo pripojení k primárnemu next-hop smerovaču (obrázok 6, smerovač N_1). Per-prefix LFA môže poskytovať ochranu linky alebo ochranu smerovača (link-protecting or node-protecting LFA).

Per-link LFA pre linku S-E je jeden vopred vypočítaný next-hop smerovač pre **všetky** destinácie, ktoré je možné dosiahnuť cez linku SE. Per-link LFA poskytuje iba ochranu linky. Alternatívny next-hop smerovač musí byť priamo pripojený k primárnemu next-hop smerovaču. Ak zoberieme do úvahy uvedenú topológiu (obrázok 6), tak v tomto prípade per-link LFA nájde iba jeden alternatívny next-hop smerovač N_2.

Smerovač S môže odstrániť aj viacero primárnych next-hop smerovačov zo smerovacej tabuľky, ak boli ovplyvnené výpadkom. Pokým proces konvergencie v sieti nie je kompletný, smerovač S musí v smerovacej tabuľke k dotknutým cieľom ponechať alternatívny next-hop smerovač.

Zhrnutie

LFA patrí k jedným z prvých a najpoužívanejších mechanizmov v oblasti IPFRR. Mechanizmu LFA dokáže ochrániť sieť pred výpadkom linky alebo pred výpadkom celého smerovača.

Výber bezslučkového a vhodného alternatívneho next-hop smerovača zabezpečujú striktné podmienky, ktorých splniteľnosť závisí na fyzickej topológii siete a od cien jednotlivých liniek. V reálnych zapojeniach môžu nastať prípady, kedy žiadny smerovač nespĺňa dané podmienky a LFA mechanizmus nedokáže poskytnúť alternatívne riešenie v prípade chyby v sieti.

Po nakonfigurovaní LFA mechanizmu na smerovači sa spustia dodatočné výpočty pre vyhľadanie vhodného LFA next-hop smerovača [**21**]. Tieto výpočty vyžadujú čas, ktorý je závislý od topológie siete a od spôsobu výpočtu LFA (per-prefix alebo per-link).

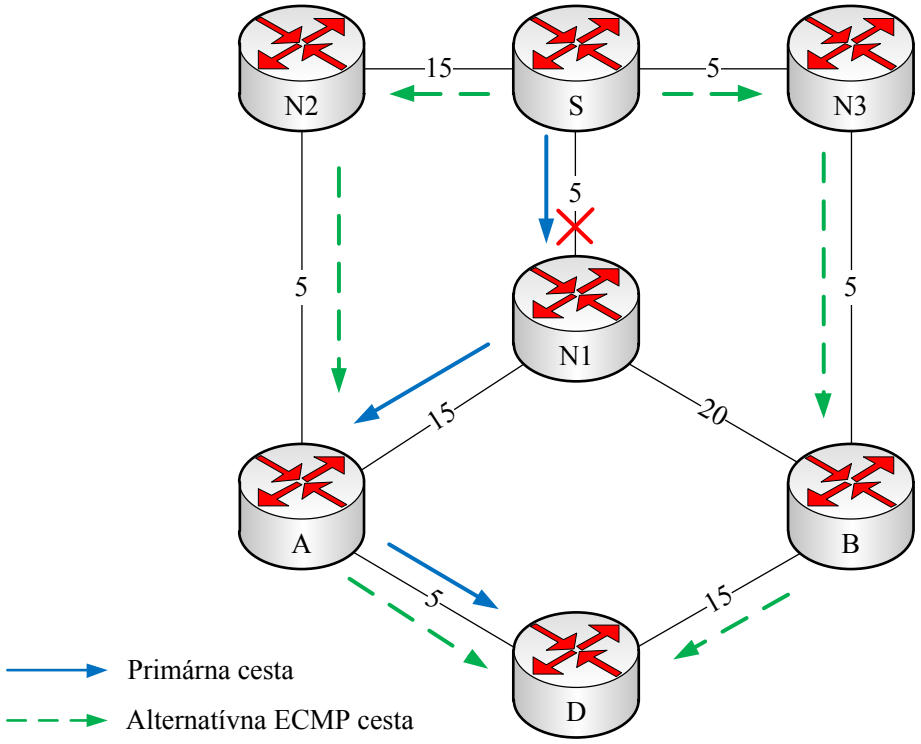
Výpočet alternatívneho next-hop smerovača môže byť per-prefix a per-link. Per-prefix LFA poskytuje vyššiu repair coverage oproti per-link [**22**]. Per-link LFA poskytuje iba ochranu linky, inak povedané, vypočíta alternatívny next-hop, ktorý je priamo pripojený k primárnemu next-hop smerovaču. Ak sa pozrieme na oba spôsoby z hľadiska výpočtovej náročnosti na CPU, per-prefix LFA vyžaduje viac výpočtových prostriedkov smerovača. Vo všeobecnosti LFA poskytuje repair coverage od 60% do 90% [**5**].

Implementácie LFA na smerovačoch od Cisco Systems [**23**] a Juniper Networks [**24**] sú navrhnuté podľa štandardu RFC 5286 [**13**].

2.3 Equal-Cost Multi-Path (ECMP)

ECMP mechanizmus využíva princíp alternatívnych ciest, ktoré majú rovnakú cenu do cieľa ako primárna cesta. V oblasti IPFRR sa mechanizmus ECMP primárne používa pre rýchle presmerovanie prevádzky z originálnej cesty na **jednu** alternatívnu cestu s rovnakou cenou [**13**] [**25**] [**5**].

Zdrojový smerovač S vopred vypočíta alternatívne ECMP next-hop smerovače N_2 a N_3 pre destináciu D (obrázok 7). Ak nastane výpadok linky k primárnemu next-hop smerovaču N, ECMP mechanizmus zmení primárny next-hop smerovač N_1 na alternatívny next-hop smerovač N_2. Ak by došlo aj k výpadku linky k smerovaču N_2, smerovač S by nastavil ako primárny next-hop pre destináciu D smerovač N_3.



Obrázok 7: Equal-Cost Multi-Path

Podľa [**5**] základným kritériom pre výber ECMP cesty smerovačom S, je nasledovná podmienka, ktorú musí splniť alternatívny next-hop smerovač N_j:

Podmienka 4:

$$\mathbf{Cost\ (N_i, D) = Cost\ (N_j, D),\ N_i \neq N_j} \qquad (4)$$

- N_i: aktuálny primárny next-hop smerovač
- N_j: alternatívny next-hop smerovač
- Cost(N_i, D): cena cesty od zdrojového smerovača S cez primárny next-hop smerovač N_i do destinácie D
- Cost(N_j, D): cena cesty od zdrojového smerovača S cez alternatívny next-hop smerovač N_j do destinácie D

Mechanizmus ECMP sa takisto využíva pri distribúcii tokov dát medzi viaceré cesty do tej istej destinácie s cieľom efektívnejšie využívať disponibilnú prenosovú kapacitu siete. Tieto mechanizmy sú takisto známe pod názvom rozkladanie záťaže (load-balancing) [**26**].

Ďalšou možnosťou využitia mechanizmu ECMP a load-balancingu v oblasti IPFRR podľa zdroja [**14**] je distribuovanie komunikácie po výpadku jednej ECMP cesty na zvyšné ECMP cesty.

Nech smerovač S má aktívny load-balancing a distribuuje komunikáciu cez next-hop smerovače N_1, N_2 a N_3. Smerovač S by v takomto prípade po detekcii výpadku linky so smerovačom N_1 distribuoval komunikáciu cez next-hop smerovače N_2 a zároveň cez N_3 (obrázok 7). Podľa typu implementácie môžu pri load-balancingu vznikať rôzne problémy, ako napr. prijatie paketov v rôznom poradí (viac v [**14**]).

Zhrnutie

ECMP cesty vytvárajú orientovaný acyklický graf čiže orientovaný strom, v anglickej literatúre označovaný aj ako Directed Acyclic Graph (DAG). V takejto štruktúre grafu sa nenachádza cyklus, čo znamená, že v sieti použitím ECMP smerovacie slučky nevznikajú.

ECMP mechanizmus je primárne závislý na cenách liniek, z čoho vyplýva, že nájsť alternatívnu ECMP cestu v sieti môže byť problémom. V niektorých prípadoch je výhodné manuálne pozmeniť ceny liniek na vyhovujúce hodnoty a získať tak alternatívnu ECMP cestu.

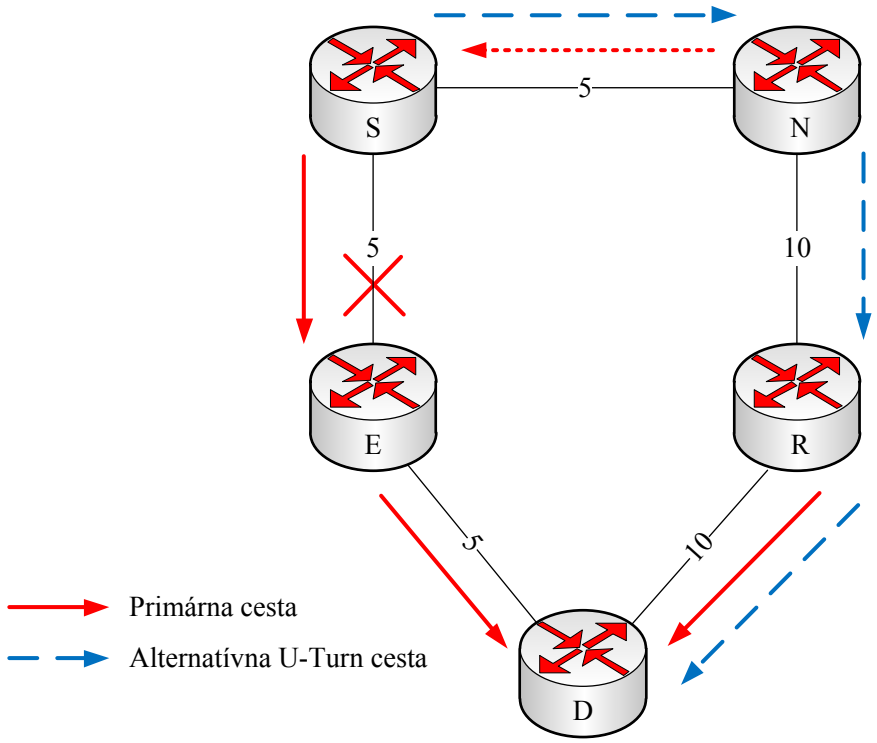
Z hľadiska implementácie ECMP mechanizmus nie je náročný, a preto patrí medzi používané mechanizmy v oblasti IPFRR. V [**14**] sa autor zaoberá implementáciou a testovaním ECMP mechanizmu s využitím technológie load-balancing v smerovacích protokolov IS-IS a OSPF. Priemerná doba obnovenia komunikácie v testoch s použitím BFD bola dosiahnutá 90 ms a najlepšia 31 ms. Ďalej je v práci porovnaná rýchlosť zotavenia siete s použitím technológie IPFRR a bez. Z výsledkov testov vyplýva, že použitím technológie ECMP IPFRR je obnova komunikácie rýchlejšia.

2.4 U-Turn Alternates

V určitých situáciách môžu nastať prípady (obrázok 8), kde v danej topológii pre smerovač S neexistuje LFA ani ECMP alternatíva, ale je možné použiť alternatívny U-Turn smerovač.

Pri U-Turn mechanizme využíva zdrojový smerovač S taký susedný smerovač N, ktorého primárny next-hop smerovač pre destináciu D je **sám** smerovač S (podmienka 5). To znamená, že smerovač N nie je bezslučkovou alternatívou. Ďalej, smerovač N má pre destináciu D vlastný LFA next-hop smerovač R (podmienka 1), ktorého primárna

cesta ale už neprechádza cez zdrojový smerovač S. Takýto smerovač N nazývame **U-Turn smerovač** [**27**].



Obrázok 8: U-Turn Alternates

Aby bol smerovač N zvolený ako potenciálny alternatívny U-Turn smerovač smerovača S, musí podľa [**5**] splniť nasledovnú podmienku:

Podmienka 5: Node Selection Criteria

$$\mathbf{Cost(N, D) \geq Cost(N, S) + Cost(S, D)} \quad (5)$$

- S: zdrojový smerovač
- N: potenciálny U-Turn smerovač
- D: cieľový smerovač
- Cost(N, D): cena najkratšej cesty z U-Turn smerovača N do cieľového smerovača D
- Cost(N, S): cena najkratšej cesty z U-Turn smerovača N do zdrojového smerovača S
- Cost(S, D): cena najkratšej cesty zo smerovača S do cieľového smerovača D

Po detekcii výpadku linky začne smerovač S posielať komunikáciu vopred vypočítanému smerovaču U-Turn (N). Tento smerovač ju nesmie zahodiť alebo poslať späť, pretože by spôsobil smerovaciu slučku. Z týchto dôvodov musí U-Turn smerovač obsahovať mechanizmus, ktorý určí komunikáciu od smerovača S za korektnú a pošle ju svojmu alternatívnemu LFA smerovaču R pre destináciu D. Detekčný mechanizmus môže rozpoznať komunikáciu od smerovača S **implicitne** alebo **explicitne**.

Implicitná identifikácia komunikácie U-Turn **nevyžaduje** modifikáciu paketov, ktoré sú smerované pre U-Turn smerovač. Keď U-Turn smerovač príjme IPFRR paket pre destináciu D od jeho primárneho next-hop smerovača S, identifikuje ho ako U-Turn paket a odošle ho svojmu LFA pre destináciu D. Ide teda o identifikáciu U-Turn paketu na základe rozhrania, ktorým paket prišiel.

Explicitná identifikácia U-Turn komunikácie **vyžaduje** modifikáciu paketov použitím MPLS návestia alebo nastavením špecifických bitov paketu v L2 hlavičke. Bližšie informácie sú uvedené v [**5**] [**28**].

Zhrnutie

U-Turn smerovač používa implicitnú alebo explicitnú detekciu pre U-Turn komunikáciu, ktorá slúži aj ako ochrana pred nechceným zahodením paketov alebo pred vytvorením smerovacej slučky. Implicitná detekcia nevyžaduje modifikáciu paketov, ale smerovač sleduje, od ktorého susedného smerovača komunikácia prišla. Explicitná detekcia vyžaduje modifikáciu paketov, ktorá môže spôsobiť rôzne problémy s kompatibilitou [**5**] [**29**].

Mechanizmus LFA nie vždy dokáže nájsť alternatívny smerovač, ktorý spĺňa bezslučkové kritérium. Spojením LFA a U-Turn mechanizmu je možné dosiahnuť vyššiu repair coverage. Podľa zdroja [**29**] U-Turn mechanizmus zvyšuje repair coverage LFA mechanizmu od 79,5% do 98,4%. Okrem zvýšenia repair coverage sa zvyšuje aj komplexnosť a implementačná náročnosť algoritmu.

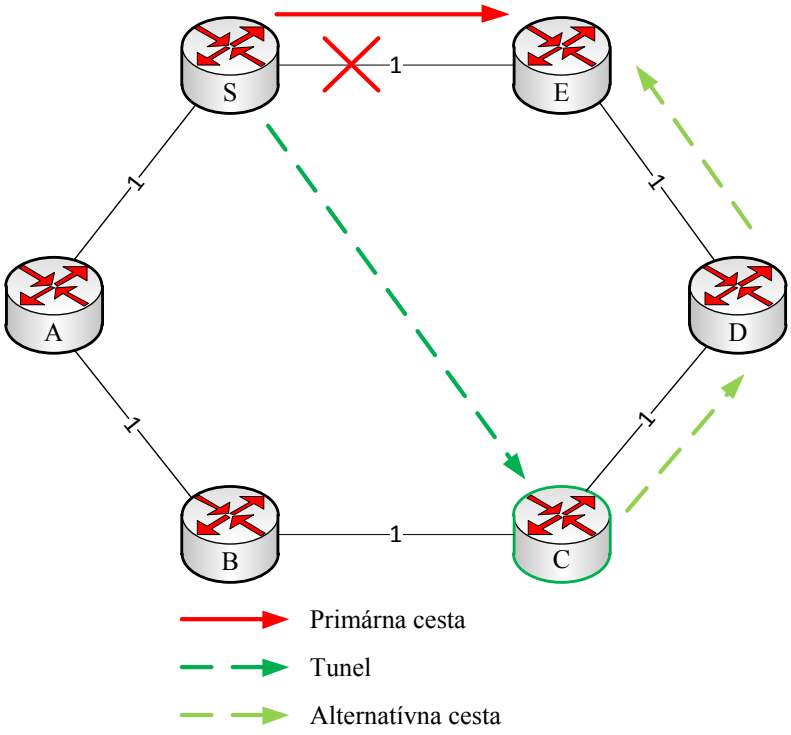
2.5 Remote LFA (RLFA)

Základný mechanizmus LFA, ktorý je popísaný v [**13**] a [**19**], poskytuje dobrú repair coverage v topológiách, ktoré sú "highly meshed", teda s vysokou hustotou vzájomných prepojov medzi rôznymi smerovačmi. Avšak v topológiách, ako je napr. kruh, je ochrana

prostredníctvom mechanizmu LFA nedostačujúca. Ak zoberieme do úvahy topológiu na obrázku 9 a mechanizmus LFA, smerovač S nedokáže nájsť vhodné LFA pre cieľové smerovače E a D. Z týchto dôvodov bolo navrhnuté rozšírenie klasického LFA, ktoré sa nazýva Remote LFA (RLFA) [**30**]. Tento mechanizmus používa technológiu **tunelovania** pre vytvorenie ďalších logických liniek, ktoré sú použité pre dosiahnutie vzdialeného LFA smerovača.

Základná terminológia k mechanizmu Remote LFA, ktorá je uvádzaná v [**30**] [**31**]:

- **P-space alebo P-priestor:** Pod P-priestorom daného smerovača S vzhľadom na danú chránenú linku sa rozumie množina všetkých tých smerovačov, ktoré sú zo smerovača S dosiahnuteľné po súčasných najkratších cestách bez prechodu chránenou linkou.
- **Q-space alebo Q-priestor:** Pod Q-priestorom daného smerovača E vzhľadom na danú chránenú linku sa rozumie množina všetkých tých smerovačov, z ktorých je smerovač E dosiahnuteľný po súčasných najkratších cestách bez prechodu chránenou linkou.
- **PQ node alebo PQ uzol:** Pod PQ uzlom vzhľadom na smerovač S a chránenú linku S-E sa rozumie taký smerovač, ktorý je súčasne prvkom P-priestoru smerovača S vzhľadom na chránenú linku S-E a prvkom Q-priestoru smerovača E vzhľadom na chránenú linku S-E.
- **Remote LFA:** Použitie vhodného PQ uzla ako LFA smerovača namiesto bezprostredného suseda smerovača S.



Obrázok 9: Remote LFA

Na obrázku 9 smerovač S chce odoslať dáta smerovaču E, linka S-E je považovaná za chránenú linku. Najkratšie cesty zo smerovača S do iných smerovačov v tejto topológii, ktoré neprechádzajú linkou S-E, sú S-A, S-A-B a S-A-B-C. Smerovače A, B a C sú preto **P-space** smerovača S.

Najkratšie cesty iných smerovačov do smerovača E, ktoré neprechádzajú chránenou linkou S-E, sú D-E a C-D-E. Tieto smerovače D a C sú preto Q-space smerovača E. Smerovač B nie je prvkom Q-space smerovača E, pretože preňho existujú dve rovnocenné cesty do E, B-A-S-E a B-C-D-E. Ak by smerovač S pomocou vhodne vytvoreného tunela poslal paket adresovaný na E smerovaču B, smerovač B by sa mohol právoplatne rozhodnúť, že paket pošle cestou B-A-S-E, čím by vznikla smerovacia slučka.

Jediný smerovač, ktorý sa nachádza v P-space smerovača S a Q-space smerovača E s ohľadom na chránenú linku S-E, je smerovač C. Z tohto dôvodu bude smerovač C zvolený ako koniec opravného tunela (repair tunnel's end-point). Inak povedané, smerovač C sa stane **Remote LFA** smerovača S pre cieľové smerovače E a D.

Technika Remote LFA nie je viazaná striktne na kruhovú topológiu, ale je ju možné použiť všade tam, kde nie je možné nájsť priamo pripojený LFA pre smerovač S a destináciu D.

Zhrnutie

Dokument popisujúci Remote LFA [**27**] predpokladá, že chránená linka je typu bod-bod a v sieti nastane výpadok iba jednej linky. Ak nastane výpadok celého smerovača, vzniká risk, že oprava pomocou RLFA spôsobí smerovacie slučky. V topológii podľa obrázku 9 by mohli nastať smerovacie slučky v prípade, ak by došlo k zlyhaniu celého smerovača E. Smerovač D by smeroval komunikáciu na smerovač S a smerovač S na smerovač D. Tento problém a možnosti ochrany pred smerovacími slučkami je podrobnejšie popísaný v dokumente [**30**] a [**32**].

Rovnako ako pri klasickom LFA, RLFA je závisle na cenách jednotlivých liniek. Môžu nastať situácie, kedy žiadny smerovač sa nenachádza súčasne v P-space a Q-space, čo znamená, že oprava prostredníctvom RLFA nie je možná.

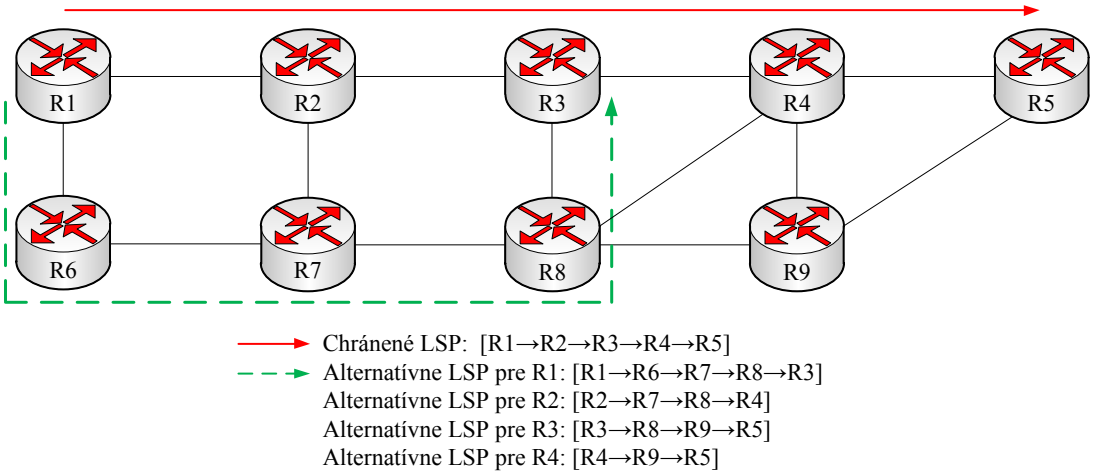
Remote LFA ma značne väčšiu repair coverage oproti klasickému LFA. Porovnanie repair coverage LFA a RLFA je v [**30**] (sekcia 8.4). Najväčší zaznamenaný nárast repair coverage použitím mechanizmu RLFA bol v rámci daného zdroja z 78.5% na 99.7%. Mechanizmus RLFA má komerčné uplatnenie v spoločnosti Cisco [**21**] a v Juniper Networks [**33**]. Ide o jeden z najrozšírenejších IPFRR mechanizmov v súčasnosti.

2.6 MPLS-TE FRR

Funkcionalita rýchleho zotavenia siete pre protokol MPLS je popísaná v dokumente RFC 4090 “Fast Reroute Extensions to RSVP-TE for LSP Tunnels” [**34**]. Tento dokument definuje rozšírenie protokolu Resource Reservation Protocol - Traffic Engineering (RSVP-TE) pre vytvorenie záložného Label-Switched Path (LSP) tunela v prípade lokálneho zlyhania LSP.

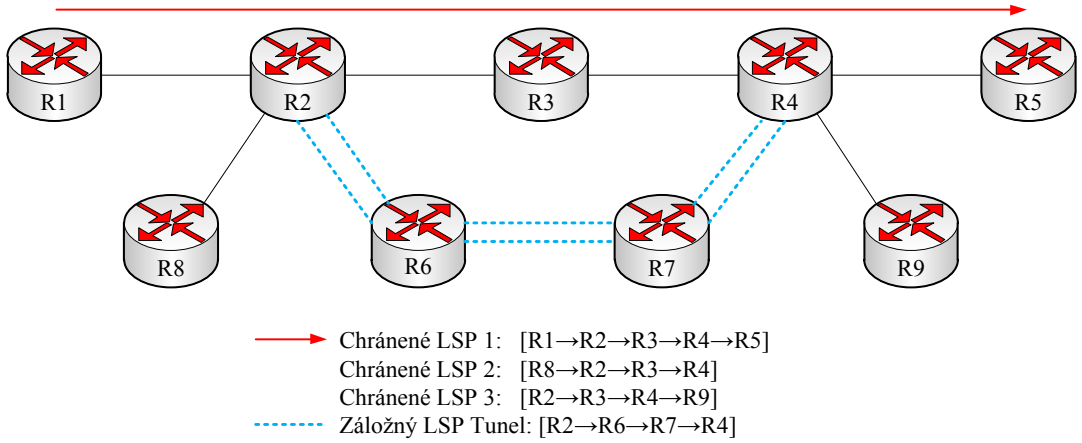
V dokumente [**34**] sú definované dve základné metódy pre vytvorenie záložných LSP. Prvá metóda sa nazýva **One-to-One Backup** a druhá **Facility Backup** (označuje sa aj **Many-to-one Backup).**

Metóda **One-to-One** Backup vytvára jeden záložný LSP tunel pre každé chránené LSP, resp. **protected LSP**. V danej topológii na obrázku 10, každý smerovač chráni LSP k primárnemu susednému smerovaču. Smerovač R_1 vytvorí v tejto topológii metódou one-to-one backup záložné LSP s trasou [$R_1 \rightarrow R_6 \rightarrow R_7 \rightarrow R_8 \rightarrow R_3$]. Ostatné smerovače vytvoria vlastné záložné LSP tunely.



Obrázok 10: MPLS One-to-One Backup

Metóda **Facility Backup** resp. **Many-to-one Backup** vytvára jeden záložný LSP tunel pre všetky chránené LSP. Namiesto vytvárania záložného tunela pre každé chránené LSP, ako je to u metódy One-to-One, metóda Many-to-one Backup vytvára len jeden LSP tunel pre všetky chránené LSP.



Obrázok 11: MPLS Many-to-One Backup

Ak berieme do úvahy topológiu na obrázku 11, smerovač R_2 vytvorí záložný tunel pre prípad zlyhania linky $R_2 \rightarrow R_3$ alebo smerovača R_3. Tento záložný tunel $[R_2 \rightarrow R_6 \rightarrow R_7 \rightarrow R_4]$ je možné použiť aj pre ochranu LSP smerovačov R_1, R_2 alebo R_8 do cieľových smerovačov R_4, R_5 alebo R_9.

Smerovač, ktorý presmeruje komunikáciu na záložný LSP tunel, sa označuje Point of Local Repair (PLR). Smerovač, na ktorom sa komunikácia vracia na originálnu cestu, sa označuje ako Merge Point (MP). Pre viac informácií ohľadom rozsiahlej terminológie k MPLS-TE FFR viď zdroj RFC 4090 [**34**].

Zhrnutie

Pre výpočet záložného LSP tunela používa RSVP protokol algoritmus Constrained Shortest Path First (CSPF). Tento algoritmus zohľadňuje oproti SPF algoritmu aj LSP atribúty (ako napr. požiadavky na šírku pásma) a atribúty liniek (ako napr. farby jednotlivých liniek) [**35**].

Mechanizmus MPLS-TE FRR je určený len pre siete s technológiou MPLS. Ochrana MPLS many-to-one backup umožňuje použitie jedného záložného MPLS LSP tunela pre ochranu viacero LSP.

Ak porovnáme komplexnosť ochrany many-to-one a one-to-one, ochrana many-to-one vyžaduje menšiu výpočtovú náročnosť a je efektívnejšia. Ochrana one-to-one vyžaduje pre kompletnú ochranu všetkých LSP ciest N-1 záložných tunelov, kde N je počet chránených LSP. To znamená, že ochrana one-to-one vyžaduje podstatne viac záložných LSP tunelov.

Autori v práci [**36**] prezentujú nový algoritmus s lineárnou výpočtovou náročnosťou pre optimalizáciu výberu alternatívnej cesty LSP tunela. Práca sa zameriava aj na optimalizáciu výberu viacerých alternatívnych LSP tunelov pre účel load-balancingu. Výhodou týchto optimalizácií záložných ciest je zohľadnenie aj iných výkonnostných faktorov, ktoré môžu dopomôcť k vyhľadaniu výhodnejšej alternatívnej cesty. Avšak napriek spomínaným výhodám sa komplexnosť prípravných výpočtov (pre-computing) podstatne zvyšuje.

Pridanie podpory FRR do protokolu MPLS prinieslo so sebou aj niekoľko problémových oblastí. Medzi najdôležitejšie problémy patrí dodatočná signalizácia záložných LSP tunelov, zvýšenie komplexnosti a riziko zmeny poradia doručovaných paketov [**37**].

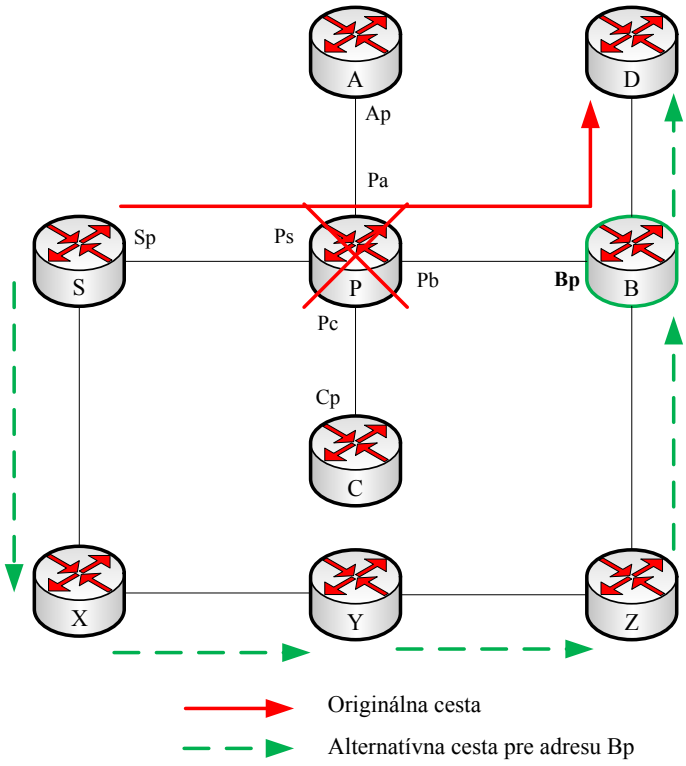
V oblasti merania účinnosti FRR mechanizmov v súčasnosti existuje vypracovaná metodika pre benchmarking MPLS-TE FRR mechanizmov, ktorá je dostupná na [**38**].

Mechanizmus MPLS-TE FRR je v súčasnosti implementovaný v IOS (Internetwork Operating System) na smerovačoch od spoločnosti Cisco Systems [**39**] a zároveň v Junos OS na smerovačoch od spoločnosti Juniper Networks [**40**].

2.7 Not-Via Addresses

Mechanizmus Not-Via Addresses využíva zapuzdrenie paketu na špecifickú adresu (Not-Via) pre obchádzku zlyhaného smerovača [**41**]. Majme danú topológiu podľa obrázku 12, kde smerovač S chce poslať paket určený pre cieľový smerovač D primárnou cestou cez smerovače P a B.

Smerovač S zistí výpadok linky so smerovačom P. V mechanizme Not-Via smerovač S zapuzdrí paket na adresu Bp. Táto adresa nesie v sebe informáciu, že cieľový smerovač je B a na smerovači P nastala chyba. Ostatné smerovače budú zohľadňovať tieto informácie a smerovač P bude pri smerovaní paketov obídený. Keď smerovač B príjme paket s cieľovou adresou Bp, paket rozbalí a smeruje ho do cieľovej destinácie D.



Obrázok 12: Not-Via Addresses

Not-Via mechanizmus vyžaduje, aby všetky smerovače na trase zo smerovača S do smerovača B mali vypočítanú cestu na adresu Bp. Túto cestu je možné vypočítať SPF algoritmom odstránením smerovača P a nájsť tak najkratšiu cestu k smerovaču B.

Pre kompletnú ochranu v sieti voči nefunkčnému smerovaču P je nutné, aby aj ostatné susedné smerovače vlastnili Not-Via adresu svojho rozhrania (Cp, Ap), ktorá zabezpečí aby sa ku ním dostala komunikácia od iných smerovačov.

Zhrnutie

Mechanizmus Not-Via poskytuje plnú repair coverage, ktorá sa približuje k 100%. Problém Not-Via mechanizmu je počet Not-Via adries, ktorý rapídne narastá s veľkosťou siete. Pre zredukovanie adries potrebných pre Not-Via mechanizmus je možné použiť Not-Via spolu s LFA mechanizmom [**13**], pretože LFA nepotrebuje prídavné adresy pre signalizáciu alternatívnej trasy. Veľký počet Not-Via adries vyžaduje aj veľkú výpočtovú náročnosť.

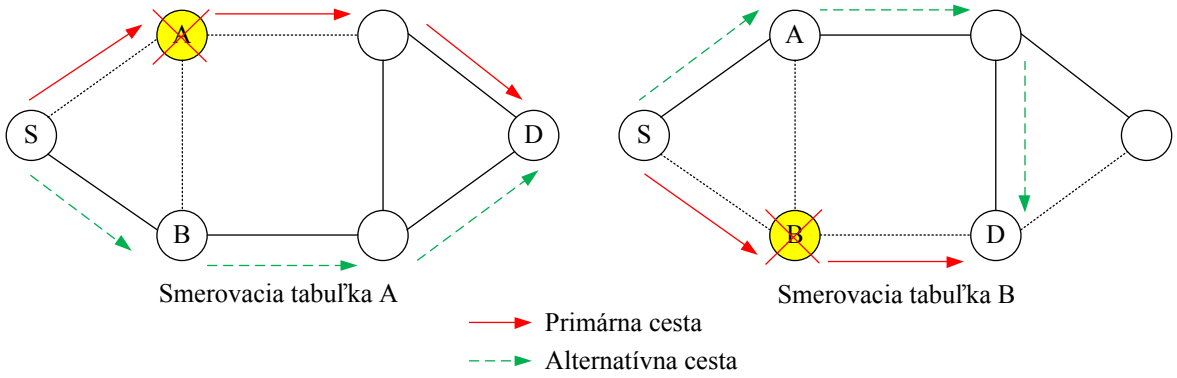
Redukovaním Not-Via adries sa zoberajú v práci [**42**]. Autori v nej prezentujú modifikovaný mechanizmus Lightweight Not-Via, ktorý bol vylepšený aplikovaním redundantných stromov. Vylepšený Not-Via mechanizmus má podstatnú výhodu aj v zníženej výpočtovej náročnosti.

Z všeobecného hľadiska má mechanizmus Not-Via relatívne vysokú výpočtovú a implementačnú náročnosť, ktorá zabraňuje implementácii tohto mechanizmu do existujúcich systémov spoločnosti Cisco Systems a Juniper Networks.

2.8 Multiple Routing Configurations (MRC)

Mechanizmus Multiple Routing Configurations (v skratke MRC) využíva princíp viacerých smerovacích tabuliek v smerovači. Každý smerovač v sieti vopred vypočíta SPF algoritmom niekoľko alternatívnych smerovacích tabuliek pre rôzne prípady zlyhania smerovačov v sieti [**43**] [**44**].

Na obrázku 13 máme dva rôzne prípady zlyhania smerovačov. V prvom prípade došlo k chybe na smerovači A, v druhom prípade nastala chyba na smerovači B. V prvom prípade smerovač S použije takú smerovaciu tabuľku, v ktorej bude smerovač A vylúčený zo smerovania. V druhom prípade použije smerovač S takú smerovaciu tabuľku, v ktorej bude vynechaný smerovač B zo smerovania.



Obrázok 13: Multiple Routing Configurations

Aby aj ostatné smerovače vedeli o tejto chybe, smerovač S uloží informáciu o použitej smerovacej tabuľke priamo do paketu. Na základe tejto modifikácie paketu ostatné smerovače zvolia príslušnú smerovaciu tabuľku. Pre uloženie potrebných informácii sa používa v hlavičke IPv4 pole Differentiated Services Code Point (DSCP) a v IPv6 rozširujúca hlavička [**45**].

Smerovač S pri počítaní novej smerovacej konfigurácie pre prípad zlyhania smerovača A, tento smerovač ignoruje. Následne SPF algoritmus pri výpočte najkrajších ciest k špecifickým destináciám vylúči smerovač A zo smerovania.

Zhrnutie

Mechanizmus MRC poskytuje repair coverage približujúcu sa k 100%. Smerovacie konfigurácie umožňujú veľmi dobrú kontrolu nad alternatívnou trasou, ktorá je použitá v kritických situáciách. Ak sa v sieti nachádza skupina liniek SRLG (viac v kapitole 1.4), mechanizmus MRC dokáže zohľadniť tieto skutočnosti a vypočítať príslušnú smerovaciu konfiguráciu [**17**].

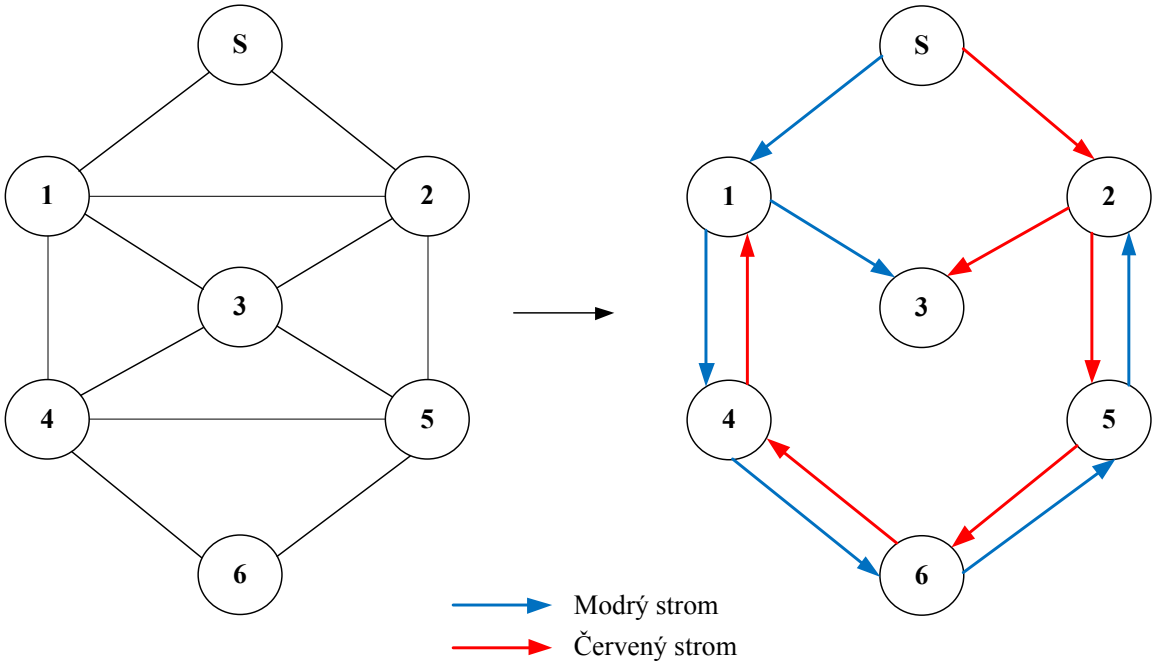
MRC mechanizmus využíva viacero smerovacích tabuliek pre obchádzku zlyhaného smerovača. Problematickou oblasťou je práve **počet** týchto smerovacích tabuliek. Ak budeme brať do úvahy každú smerovaciu tabuľku pre každé možné zlyhanie jedného smerovača, počet môže byť naozaj vysoký. Z týchto dôvodov sa existujúce implementácie sústreďujú aj na minimalizáciu počtu smerovacích tabuliek [**43**].

Na záver zhodnotenia mechanizmu MRC je nutne podotknúť, že aj napriek vysokej repair coverage (takmer 100%), mechanizmus vyžaduje vysokú implementačnú a výpočtovú náročnosť. V čase písania tejto práce mechanizmus MRC nebol doteraz implementovaný v operačných systémoch Juniper Networks alebo Cisco Systems.

2.9 Maximally Redundant Trees (MRT)

Mechanizmus Maximally Redundant Trees (v skratke MRT) využíva pre smerovanie v sieti princíp dvoch maximálne disjunktných stromov pre obchádzku zlyhanej linky alebo smerovača [**46**].

Ak v sieti nenastala žiadna porucha, prevádzka sa smeruje na základe modrého stromu. Ak však v sieti dôjde k výpadku linky alebo smerovača, použije sa pre smerovanie prevádzky červený strom (obrázok 14). Maximálne redundantné stromy majú tú vlastnosť, že cesta zo špecifického smerovača ku koreňu stromu cez modrý strom a cesta z toho istého smerovača ku koreňu stromu cez červený strom majú minimálny počet spoločných hrán.



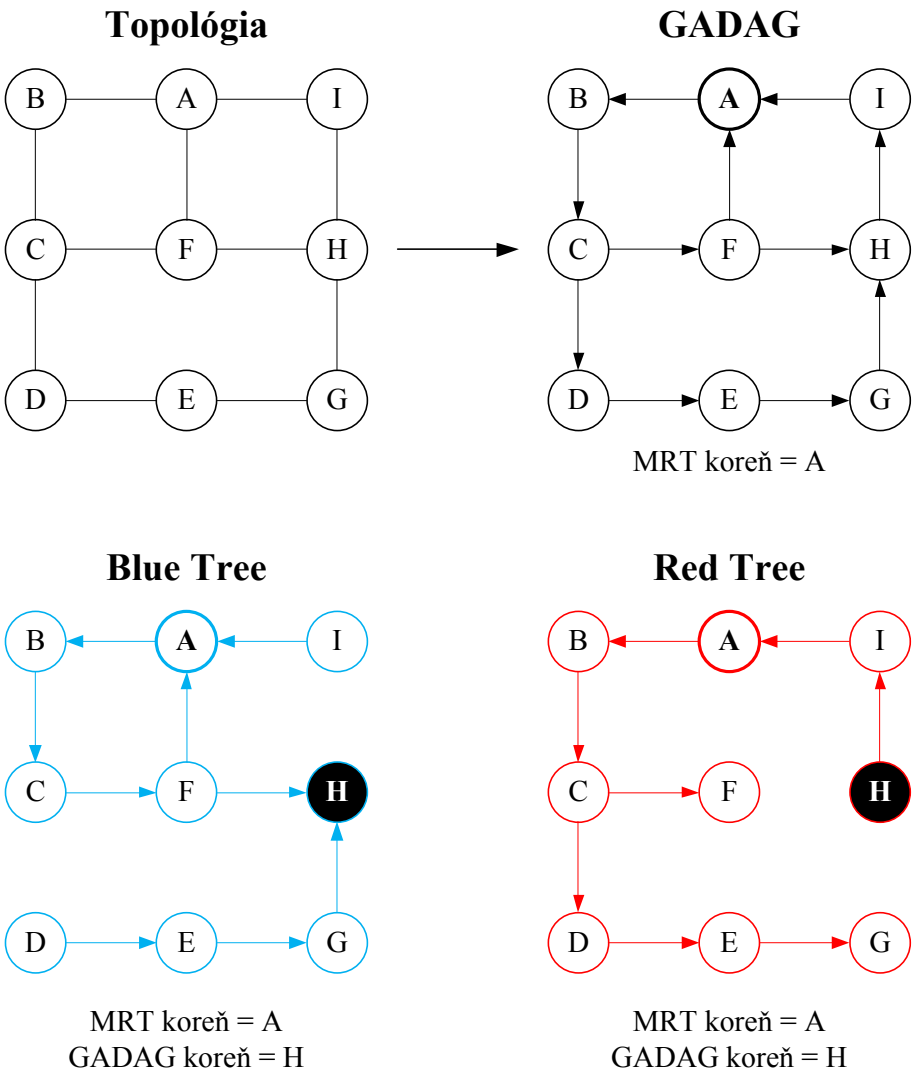
Obrázok 14: Všeobecný princíp MRT

Pre vysvetlenie mechanizmu MRT stručne popíšeme algoritmus, ktorý je uvedený v [**47**]. Ak zoberieme do úvahy topológiu siete na obrázku 15, mechanizmus MRT vyberie v rámci danej sieti jeden tzv. MRT koreň (MRT Root) a vypočíta pre daný MRT koreň Generalized Almost Directed Acyclic Graph (GADAG).

MRT koreň je smerovač s najnižším označením a je spoločný pre všetky smerovače, čo znamená, že GADAG bude rovnaký na všetkých smerovačoch. GADAG má tú vlastnosť, že ak odstránime z grafu vstupujúce hrany MRT koreňa, dostaneme orientovaný acyklický graf (DAG). Po vypočítaní GADAG, každý smerovač vypočíta modrý a červený strom.

Uvedený algoritmus vypočíta maximálne redundantné stromy aj v takých sieťach, v ktorých ak odstránime špecifickú linku, vzniknú dve oddelené topológie. Takáto linka bude zdieľaná v oboch stromoch.

Modrý strom smerovač vypočíta tak, že odstráni z GADAG vystupujúce hrany z vrcholu, ktorý ho reprezentuje. Červený strom vypočíta smerovač podobne, avšak odstráni vstupujúce hrany z vrcholu, ktorý ho reprezentuje.



Obrázok 15: Maximally Redundant Trees

Aby aj ostatné smerovače na ceste k cieli vedeli, aký strom použiť, smerovač S uloží informáciu o použitom strome do paketu. Bližšie informácie ako uložiť informáciu o použitom strome sú uvedené v [**48**].

Prvý MRT algoritmus bol predstavený v práci [**49**], ktorý poskytoval len ochranu proti zlyhaniu linky (link-protection). Prvý MRT algoritmus, ktorý zahŕňal aj ochranu

smerovača (node protection) a bol riešiteľný v polynomiálnom čase, je prezentovaný v [**50**]. Zložitosť MRT algoritmu bola neskôr znížená na lineárnu v práci [**51**]. Prehľad súčasných algoritmov, ktoré súvisia s problematikou MRT, sa nachádza v [**50**].

Zhrnutie

MRT mechanizmus poskytuje repair coverage približujúcu sa k 100%. Pre smerovanie komunikácie využíva dva nezávislé distribučné stromy – modrý a červený. Výhodou je použitie druhého alternatívneho distribučného stromu v prípade zlyhania linky alebo smerovača. Vytvorenie týchto stromov prináša so sebou vysokú implementačnú a výpočtovú náročnosť. Komplexnosť algoritmu MRT sa postupom času o niečo zjednodušila.

Princíp fungovania MRT je podobný s tým, ktorý používa mechanizmus MRC. Rozdiel je v tom, že MRT používa dve smerovacie konfigurácie, kým MRC môže použiť podstatne viac smerovacích konfigurácií.

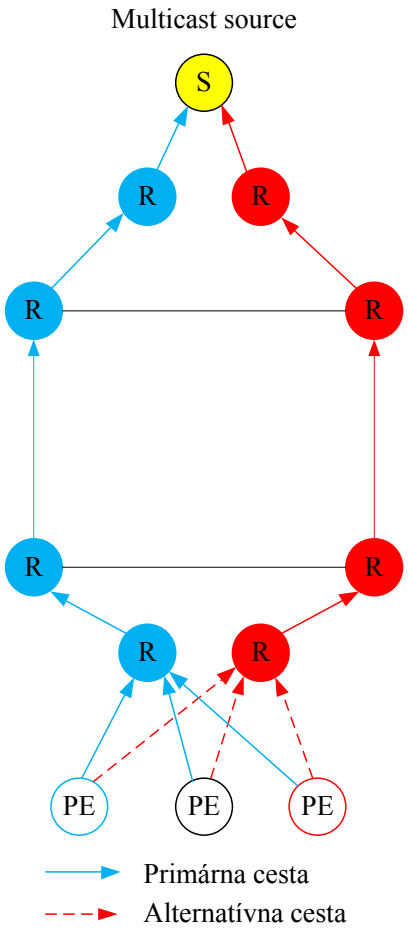
Autori v práci [**48**] porovnávajú mechanizmus MRT s mechanizmom Not-Via Addresses. Potvrdzujú, že s mechanizmom MRT je počet potrebných dodatočných adries menší. Na základe vykonaných testov autori uvádzajú, že mechanizmus MRT vyžaduje menšiu implementačnú a výpočtovú náročnosť oproti mechanizmu Not-Via Addresses.

2.10 Multicast only Fast Re-Route (MoFRR)

Mechanizmus Multicast only Fast Re-Route (MoFRR) slúži len na ochranu multicastovej komunikácie. Základný princíp MoFRR je využitie dvoch disjunktných distribučných stromov (opäť nazvaných ako modrý a červený), ktoré sú vytvorené od zdroja multicastového vysielania po okrajový smerovač poskytovateľa, tzv. Provider Edge (PE) smerovač [**52**] [**53**].

Alternatívny distribučný strom je vytvorený tak, že smerovač PE odošle alternatívnu PIM Join správu na susedný smerovač smerom k zdroju multicastového vysielania (obrázok 16). Výsledkom duplicitnej PIM Join správy je vytvorenie ďalšieho alternatívneho multicastového distribučného stromu, čo znamená, že PE smerovač bude prijímať rovnaký multicastový tok dvakrát.

Originálny multicastový tok sa bude vysielať cez modrý strom a duplicitný tok cez červený strom. Smerovač PE akceptuje iba ten multicastový tok, ktorý je prijatý na RPF rozhraní modrého stromu. Duplicitný multicastový tok, ktorý je prijatý na rozhraní červeného stromu, je RPF kontrolou neakceptovaný.



Obrázok 16: Multicast only Fast Re-Route

Smerovač PE s mechanizmom MoFRR po detekcii výpadku linky s primárnym modrým distribučným stromom zmení svoje RPF rozhranie tak, aby začal prijímať multicastový tok z červeného stromu. Prepnutie z modrého multicastového distribučného stromu na červený a obnovenie multicastovej komunikácie je realizované podľa [**52**] do 200 ms.

Zhrnutie

Mechanizmus MoFRR je určený iba pre ochranu multicastového toku. Nie je určený pre unicastový typ komunikácie. Kladie veľké požiadavky na fyzické zapojenie siete. Ďalšou problémovou oblasťou je trvalé zaťaženie siete duplicitnou multicastovou komunikáciou.

Implementácia mechanizmu MoFRR od Cisco Systems vyžaduje cesty s rovnakou cenou (ECMP cesty) [**52**]. MoFRR vyžaduje v sieti aktívny protokol PIM-SM alebo PIM-SSM.

V súčasnosti existuje draft Multicast only Fast Re-Route [**53**], kde autori uvádzajú, že je možné využiť mechanizmus MoFRR spoločne s mechanizmom LFA. Ak smerovač PE nemá susedný next-hop smerovač, ktorý poskytuje ECMP k zdroju multicastového vysielania, je možné použiť LFA smerovač pre odoslanie duplicitnej správy Join smerom k zdroju multicastu.

Mechanizmus MoFRR je v súčasnosti implementovaný na smerovačoch od spoločnosti Cisco Systems (od IOS XE Release 3.2S) [**52**] a Juniper Networks (od Junos OS 14.1) [**54**].

2.11 Zhrnutie problematiky

Predchádzajúce podkapitoly sa zaoberali jednotlivými mechanizmami pre IP Fast Reroute. Nedá sa jednoznačne prehlásiť, ktorý mechanizmus je najlepší. Každý z jednotlivých mechanizmov má svoje výhody a nevýhody.

Veľké komerčné spoločnosti, ako sú Cisco Systems a Juniper Networks, sa aktívne venujú implementácii IPFRR mechanizmov do ich existujúcich operačných systémov v smerovačoch. Komerčné uplatnenie v oboch spoločnostiach našli najmä mechanizmy LFA a Remote LFA.

Niektoré mechanizmy poskytujú vysokú mieru repair coverage približujúcu sa k 100%, avšak za cenu vysokej miery komplexnosti (Not-Via Addresses, MRC, MRT). Len máloktoré mechanizmy sa dajú jednoducho implementovať do už existujúcej architektúry.

Väčšina z nich je testovaná v experimentálnych podmienkach, resp. v simulačných nástrojoch, ale len málo z nich je reálne nasadených. Medzi najznámejšie experimentálne prostredia v oblasti IPFRR patria: OMNeT++, NS-2, NS-3 a Quagga.

Na základe vykonanej analýzy existujúcich IPFRR mechanizmov sme zhrnuli všetky dôležité fakty v tabuľke 1. Tento súhrn informácií nám pomôže v hľadaní problémových oblastí v IPFRR.

	100% repair coverage	Prípravné výpočty (Pre-computing)	Modifikácia paketov	Závislosť na link-state smerovacích protokoloch
LFA	Nie	**Áno**	Nie	Nie
ECMP FRR	Nie	**Áno**	Nie	Nie
U-Turn	Nie	**Áno**	Áno/Nie	**Áno**
Remote LFA	Nie	**Áno**	Áno	**Áno**
MPLS-TE FRR	Nie	**Áno**	Áno	Nie
MoFRR	Nie	**Áno**	Nie	Nie
Not-Via Addresses	Áno	**Áno**	Áno	**Áno**
MRC	Áno	**Áno**	Áno	**Áno**
MRT	Áno	**Áno**	Áno	**Áno**

Tabuľka 1: Prehľad základných vlastností IPFRR mechanizmov

V nasledujúcich podkapitolách sa budeme venovať jednotlivým problémovým oblastiam existujúcich IPFRR mechanizmov.

2.11.1 Prípravné výpočty

Základný princíp analyzovaných IPFRR mechanizmov je založený na rýchlej detekcii výpadku linky a vopred vypočítaných alternatívnych cestách, resp. pre-computingu. Práve komplexnosť týchto vopred vykonaných výpočtov je problém.

S rastúcim počtom smerovačov v sieti narastá aj výpočtová náročnosť jednotlivých mechanizmov. Výpočty je nutné opäť vykonať po zmene v topológii siete pre aktualizáciu alternatívnej cesty. Tieto výpočty sú zvyčajne realizované na smerovačoch ako procesy s nízkou prioritou a sú vykonávané v čase nečinnosti CPU smerovača.

Dodatočné výpočty alternatívnej cesty tak zaberajú dôležitý čas a systémové prostriedky smerovača. **Môžeme konštatovať, že jednou z problémových oblastí existujúcich IPFRR mechanizmov sú preto práve prípravné výpočty**.

Na základe informácií z tabuľky 1 je nutné poznamenať, že **všetky analyzované IPFRR mechanizmy sú závislé na prípravných výpočtoch alternatívnej cesty.**

Táto problematika otvára novú výskumnú otázku: Je možné navrhnúť IP Fast Reroute mechanizmus, ktorý poskytne alternatívnu cestu bez prípravných výpočtov?

2.11.2 Závislosť na link-state smerovacích protokoloch

Ďalším dôležitým faktom je, že mnohé analyzované algoritmy IPFRR vyžadujú pre výpočet alternatívnej cesty topologické informácie o sieti z link-state smerovacích protokolov. Táto skutočnosť obmedzuje uplatnenie IPFRR mechanizmov iba na siete, kde je primárne nasadený link-state smerovací protokol. **Väčšina existujúcich IPFRR mechanizmov je závislých na link-state smerovacích protokoloch**.

2.11.3 Repair coverage

Vedecké články uvádzajú **rôzne** výsledky meraní repair coverage jednotlivých testovaných mechanizmov (napr. [**6**], [**55**]). Tento fakt je spôsobený tým, že všeobecná metóda pre zistenie repair coverage jednotlivých mechanizmov **nie je zatiaľ presne definovaná**. Navyše podmienky, pri ktorých boli jednotlivé IPFRR mechanizmy testované neboli rovnaké. Preto špecifický IPFRR mechanizmus má rôzne výsledky repair coverage.

V súčasnosti existuje dokument RFC 6894 Methodology for Benchmarking MPLS Traffic Engineered (MPLS-TE) Fast Reroute Protection [**38**], ktorý definuje metodiku pre testovanie MPLS Fast Reroute mechanizmov. RFC 6894 ďalej poskytuje testovacie metódy a referenčnú topológiu pre meranie času, ktorý je potrebný pre rýchle zotavenie siete (recovery time). V dokumente sa však nenachádza samotná metodika pre meranie repair coverage.

Ďalším dôležitým dokumentom v oblasti testovania IPFRR mechanizmov je RFC 6414 - Benchmarking Terminology for Protection Performance [**56**]. Tento dokument definuje všeobecnú terminológiu pre testovanie MPLS-FRR mechanizmov.

Táto problematika otvára novú výskumnú otázku: Akým korektným spôsobom merať repair coverage u mechanizmov IP Fast Reroute?

2.11.4 IPFRR v IPv6

Ak sa zameriame na podporu mechanizmov pre protokol IPv6, môžeme konštatovať, že táto oblasť si vyžaduje väčšiu mieru pozornosti. V uvádzanej literatúre sme sa stretli len s malou podporou pre protokol IPv6.

Prechod na IPv6 je síce v súčasnej dobe problematický, avšak voľné IPv4 adresy sa vyčerpali (podľa zdroja Ripe Network Coordination Centre – RIPE NCC, [**57**]) a prechod na IPv6 je neodkladný. Kedy k tomu dôjde nie je jasné, ale problematiku IP Fast Reroute v IPv6 je nutné riešiť už v súčasnej dobe.

Hlavička paketu v IPv6 je vo veľkej miere odlišná a ponúka nové možnosti využitia ako napr. **extension headers** [**58**]. Protokol IPv6 teda ponúka nové možnosti a s tým súvisí aj jeho nové využitie pre oblasť IPFRR.

2.11.5 Modifikácia paketov

Dôležitou súčasťou pri IPFRR je detekcia chyby a spôsob jej oznámenia ostatným smerovačom, ktorým výpadok narušil smerovanie. V niektorých z popísaných IPFRR mechanizmov sa informácia o výpadku linky šíri modifikovaním špeciálnych bitov v IPv4 hlavičke, zapuzdrením paketu ďalšou hlavičkou alebo na základe rozhrania, ktorým bol paket prijatý.

Modifikovanie paketov prináša so sebou rôzne problémy s kompatibilitou a problémy s presiahnutím Maximum Transmission Unit (MTU) na linkách siete [**41**].

3 CIELE PRÁCE

Význam rýchleho zotavenia siete posilnil najmä trend zväčšujúcich sa sietí a požiadavky zákazníkov. S rozrastajúcimi sa sieťami sa zvyšoval aj dopyt po technológiách, ktoré by dokázali zotaviť sieť v minimálnom čase.

Rýchle zotavenie siete je predmetom mnohých výskumných prác, avšak stále zostávajú niektoré problémové oblasti nevyriešené. Medzi tieto problémové oblasti patria najmä:

- Prípravné výpočty v IPFRR mechanizmoch (pre-computing)
- Závislosť na link-state smerovacích protokoloch
- Komplexnosť algoritmov
- Meranie repair coverage
- Modifikácia paketov

Z analýzy existujúcich riešení sme zistili, že existujúce mechanizmy síce spĺňajú základné požiadavky IPFRR, avšak sú komplikované. Preto sme sa zamerali na vývoj nového mechanizmu, ktorý by splnil základné požiadavky IPFRR a bol by jednoduchší ako existujúce mechanizmy. Jednou z možností, ktorá nebola využitá v súčasných IPFRR mechanizmoch, bola technológia multicast. Tu začala naša cesta hľadania nového mechanizmu, ktorý by bol odlišný od súčasných mechanizmov a priniesol by nový princíp v oblasti IPFRR. Keď sme sa rozhodli využiť technológiu multicast, nastala ďalšia otázka: aký multicastový protokol použiť? Náš výskum sa zameral najmä na protokol PIM. Na základe týchto faktov sme určili hlavný cieľ práce:

Hlavným cieľom tejto dizertačnej práce je vytvorenie nového mechanizmu v oblasti rýchleho zotavenia siete, ktorý využíva princíp viacnásobného doručovania (multicastingu).

Parciálne ciele práce sú:

- Preskúmať možnosť viacnásobného doručovania datagramov v mechanizmoch rýchleho zotavenia
- Preskúmať využitie technológie multicast v oblasti rýchleho zotavenia siete

- Na základe získaných výsledkov z predchádzajúcich cieľov navrhnúť nový mechanizmus v oblasti rýchleho zotavenia v siete
- Implementovať a overiť navrhnutý mechanizmus rýchleho zotavenia siete v laboratórnych podmienkach

3.1 Využitie PIM-DM v oblasti IPFRR

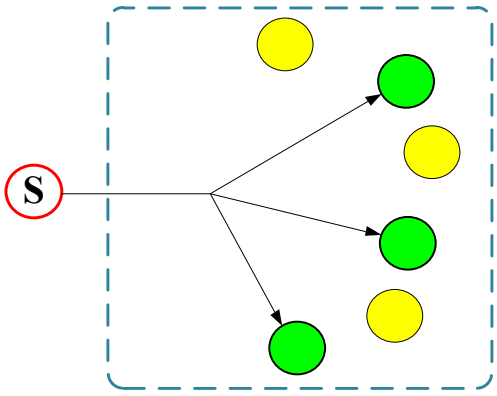
V novom IPFRR mechanizme sme sa rozhodli využiť existujúci multicastový protokol Protocol Independent Multicast - Dense Mode (PIM-DM) [**59**]. Protokol PIM-DM je v súčasnosti podporovaný takmer na všetkých komerčných produktoch od spoločnosti Cisco Systems a Juniper Networks.

V oblasti IPFRR existuje mechanizmus Multicast only Fast Re-Route (MoFRR) [**52**], ktorý sa sústreďuje **len** na ochranu čisto multicastovej komunikácie. Ak ho porovnáme s ostatnými analyzovanými riešeniami, nejedná sa teda plnohodnotný IPFRR mechanizmus. Mechanizmus MoFRR je popísaný v kapitole 2.10. Naším hlavným zameraním bude vytvorenie nového IPFRR mechanizmu, ktorý bude využívať technológiu multicast, konkrétne protokol PIM-DM, na ochranu špecifického unicastového toku.

3.2 Technológia IP Multicast

IP Multicast je efektívna technológia, ktorá slúži na posielanie IP komunikácie z jedného zdroja do viacerých destinácii (obrázok 17). Zdrojová stanica odošle iba jeden paket, ktorý je adresovaný špecifickej multicastovej skupine [**60**].

Technológia multicast sa vo všeobecnosti primárne používa pre posielanie multimediálneho obsahu cez IP sieť. Pre real-time služby používa multicast väčšinou nespoľahlivý User Datagram Protocol (UDP protokol).



Obrázok 17: Technológia IP multicast

Zdrojová stanica (S) odosiela multicastovú komunikáciu adresovanú multicastovej skupine (G), ktorá reprezentuje multicastových odoberateľov pre špecifickú multicastovú komunikáciu. Ak príjemca chce odoberať špecifickú multicastovú komunikáciu, odošle Internet Group Management Protocol (IGMP) Join správu k najbližšiemu smerovaču. Ten sa následne pomocou signalizácie pripojí k príslušnému distribučnému stromu. Príslušné smerovače, ktoré sú členom daného stromu následne replikujú multicastovú komunikáciu po sieti k odoberateľom multicastového vysielania.

Pre zapnutie multicastového smerovania v sieti, v ktorej je aktívny smerovací protokol, sa používa pre potrebnú signalizáciu Protocol Independent Multicast (PIM). Tento multicastový protokol sa používa najmä v **sparse** [**61**] alebo **dense** [**59**] móde.

3.3 Protocol Independent Multicast - Dense Mode (PIM-DM)

Protokol PIM-DM predpokladá, že pri vysielaní multicastovej komunikácie všetky stanice chcú odoberať multicastovú komunikáciu. Na začiatku vysielania smerovače s aktívnym protokolom PIM-DM rozposielajú multicastové datagramy všetkým ostatným susedným smerovačom v sieti. Tento prvotný proces zaplavovania multicastovými dátami medzi smerovačmi sa nazýva **flooding** [**59**].

Protokol PIM-DM používa pri konštrukcii multicastového distribučného stromu a zároveň na ochranu pred vznikom smerovacích slučiek princíp s názvom **Reverse Path Forwarding** (**RPF**). Multicastový distribučný strom má zabezpečiť doručenie multicastového vysielania po najkratších cestách od zdroja vysielania ku všetkým príjemcom. Predpokladá sa pritom, že sieť je tvorená neorientovaným grafom, v ktorom pre ľubovoľnú dvojicu vrcholov $u, v, u \neq v$ sú najkratšie (u,v) a (v,u) cesty až na vzájomne

obrátené poradie vrcholov a hrán totožné a majú rovnakú cenu. Multicastový distribučný strom v takomto grafe vzniká ako zjednotenie (strom) najkratších ciest od príjemcov k zdroju vysielania. V tomto strome je charakteristické, že na každý smerovač, ktorý je jeho prvkom (vrcholom), prichádza multicastové vysielanie práve tým rozhraním (hranou), ktoré leží na najkratšej ceste späť k zdroju vysielania. Ak multicastové vysielanie vchádza akýmkoľvek iným rozhraním, ktoré neleží na najkratšej ceste k zdroju vysielania, znamená to, že sa vysielanie nešíri po želanom multicastovom strome, lebo ten je tvorený práve najkratšími cestami medzi zdrojom a príjemcami. Práve táto idea tvorí jadro princípu Reverse Path Forwarding, ktorý stanovuje: *Smerovač sa bude zaoberať multicastovým tokom len vtedy, ak ho prijal rozhraním, ktoré leží na najkratšej ceste smerom k zdroju multicastového toku*. Tým je zabezpečené, že sa multicastový tok dát bude šíriť len po strome najkratších ciest, a zároveň, keďže každý strom je acyklický graf, sú vylúčené smerovacie slučky. Rozhranie, ktoré pre daný zdroj multicastového vysielania do danej skupiny leží na najkratšej ceste k zdroju S, sa nazýva RPF rozhranie. Každý smerovač bude mať pre daný multicastový strom (používa sa notácia (S, G), kde S je zdroj vysielania a G je adresa multicastovej skupiny) práve jedno RPF rozhranie. Ak pre daný smerovač existuje niekoľko najkratších ciest k zdroju S a tým niekoľko potenciálnych RPF rozhraní, vyberie si práve jedno podľa pravidiel v [**59**].

Každé rozhranie smerovača v protokole PIM-DM môže v zásade nadobúdať dva stavy: **forward** a **pruned**. Stav **forward** je počiatočným stavom rozhraní v protokole PIM-DM a predstavuje povolenie odosielať daným rozhraním multicastový tok dát. Stav **pruned** je opakom tohto stavu a predstavuje zákaz odosielať daným rozhraním multicastový tok dát. Keďže stav **forward** je východzí stav, do stavu **pruned** sa rozhranie môže dostať len explicitnou signalizáciou medzi smerovačmi.

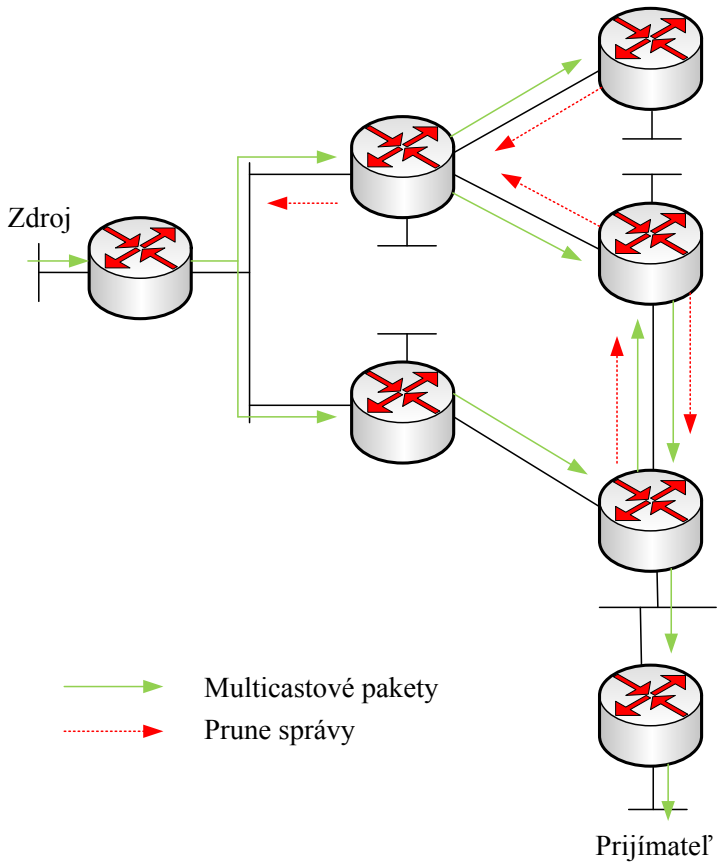
Východzie správanie sa protokolu PIM-DM teda je, že každý smerovač po prijatí multicastového paketu príslušným RPF rozhraním rozošle tento paket všetkými zostávajúcimi rozhraniami, na ktorých je povolený protokol PIM-DM a detegované susedné PIM-DM smerovače. Bezprostredným dôsledkom tohto správania sa je lavínovité rozšírenie sa multicastového paketu do celej siete medzi všetky PIM smerovače – proces, ktorý bol v prechádzajúcom texte označený ako **flooding**.

Každý smerovač má v protokole PIM-DM možnosť požiadať susedný smerovač o zastavenie preposielania daného multicastového toku dát. Táto žiadosť o zastavenie

preposielania sa nazýva **Prune** (obrázok 18). Správu Prune môže smerovač odoslať svojmu susednému smerovaču v dvoch principiálnych prípadoch:

- Keď smerovač prijíma multicastový tok dát iným ako RPF rozhraním, čiže prijíma ho na tomto rozhraní zbytočne. V takomto prípade smerovač odosiela správu Prune práve týmto rozhraním.
- Keď žiadne z rozhraní iných ako RPF rozhranie nemá povolenie odosielať multicastový tok – buď smerovač sám na ňom prijal správu Prune od svojho PIM suseda, alebo je to rozhranie do koncovej siete, v ktorej sa nenachádza príjemca daného toku. V takom prípade smerovač odosiela správu Prune svojím vlastným RPF rozhraním, čím sa vlastne od multicastového distribučného stromu efektívne odhlasuje.

Prijatie i odoslanie správy Prune na rozhraní smerovača spôsobí presunutie tohto rozhrania do stavu **pruned** a zastavenie odosielania i prijímania multicastového toku dát na tomto rozhraní.



Obrázok 18: Protokol PIM-DM

Stav rozhrania **pruned** je spojený so špecifickým (S, G) párom. Ak sa objaví nový príjemca multicastovej komunikácie na smerovači, ktorý sa od multicastového distribučného stromu odhlásil, tento smerovač požiada o opätovné začlenenie do multicastového stromu správou typu **Graft** odoslanou RPF rozhraním. Táto správa povolí na tzv. nadradenom (angl. „upstream“ v zmysle späť k zdroju multicastového toku) smerovači opätovné preposielanie multicastového toku. Rozhranie, ktoré prijalo správu Graft, sa uvedie do stavu **forward** a opätovane sa ním umožní odosielanie multicastových paketov. Ak bol nadradený smerovač sám od distribučného stromu odhlásený, postup s odoslaním správy Graft cez jeho vlastné RPF rozhranie sa na ňom opakuje.

Pre každý (S, G) tok si každý smerovač organizuje vo svojej multicastovej smerovacej tabuľke smerovací záznam, ktorý obsahuje prinajmenšom nasledujúce údaje:

- Adresa zdroja S a skupiny G
- RPF rozhranie a jeho stav
- Zoznam výstupných rozhraní a ich stav

Tento záznam vzniká príchodom prvého multicastového paketu v danom (S, G) toku (pred jeho príchodom neexistuje). Ďalšie pakety toho istého toku sú preposielané na základe informácií v už existujúcej položke multicastovej smerovacej tabuľky. Ak zdroj toku S prestane do skupiny G tento tok odosielať, príslušná položka multicastovej smerovacej tabuľky po istom čase jej nepoužívania expiruje a z tabuľky bude odstránená (v protokole PIM-DM sú to 3 minúty).

4 NÁVRH NOVÉHO M-REP IPFRR MECHANIZMU

Na začiatku multicastového vysielania s multicastovým smerovacím protokolom PIM-DM každý smerovač rozosiela multicastové toky prijaté príslušným RPF rozhraním všetkými ostatnými rozhraniami, na ktorých sú detegovaní ďalší PIM susedia alebo na ktorých sú pripojení priami príjemcovia týchto tokov. Dôsledkom je, že na začiatku procesu šírenia multicastového vysielania (flooding) sa toto vysielanie doručí ku každému PIM smerovaču v sieti. Tento fakt znamená, že sa multicastové pakety (nezávisle od výpadku) dostanú aj k smerovaču, za ktorým sa nachádza pôvodný príjemca. Túto špecifickú vlastnosť protokolu PIM-DM chceme využiť pri návrhu nového IPFRR mechanizmu.

4.1 Modifikácia RPF

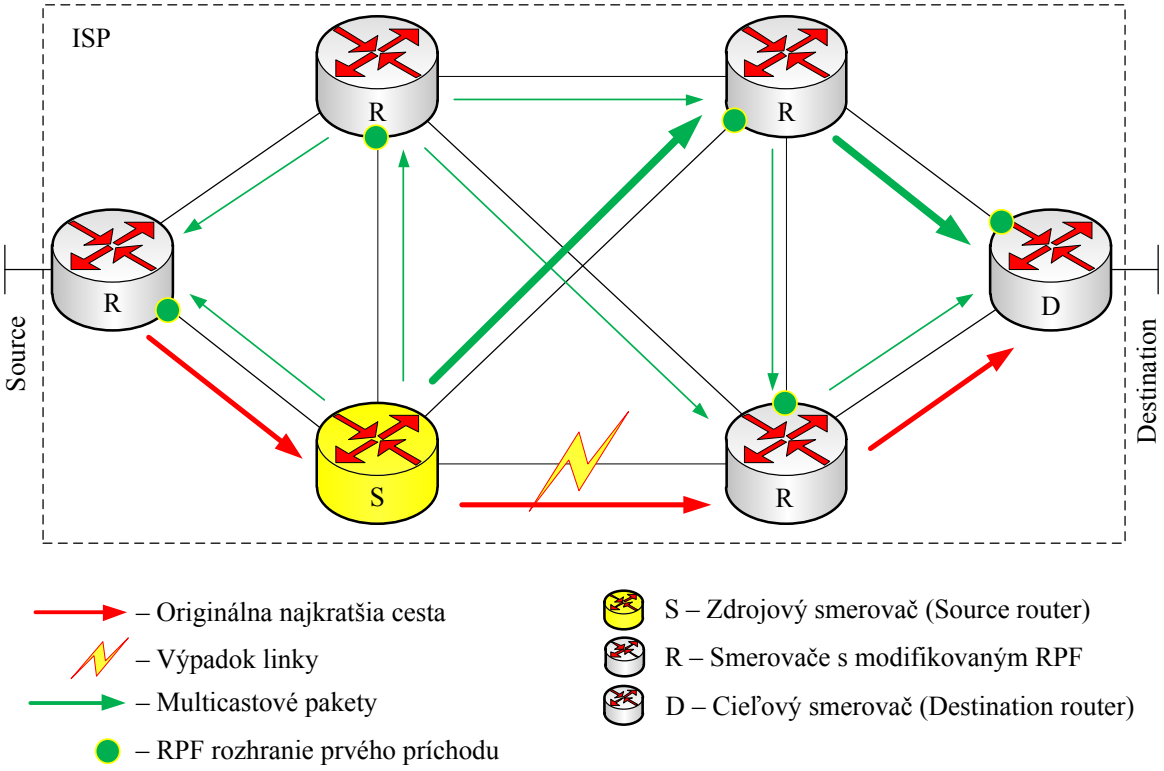
Originálne správanie sa RPF mechanizmu v PIM-DM **nie je vhodné** pre naše využitie v oblasti IPFRR. RPF mechanizmus v pôvodnom PIM-DM využíva informácie z unicastovej smerovacej tabuľky pre výber korektného RPF rozhrania pre špecifický multicastový (S, G) tok. Avšak v sieti, kde nastal výpadok linky alebo uzla, informácie v unicastových smerovacích tabuľkách na smerovačoch nemusia byť aktuálne, kým proces konvergencie unicastového smerovacieho protokolu v sieti nie je kompletný. To znamená, že niektorý zo smerovačov na originálnej ceste do cieľa by multicastovú komunikáciu neakceptoval v dôsledku RPF kontroly, pričom ideou nášho mechanizmu je práve obísť miesto výpadku inou trasou.

4.2 Popis mechanizmu

Nový M-REP (Multicast Repair) IPFRR mechanizmus nie je určený pre ochranu konkrétnej linky alebo uzla (link/node protection), ale pre ochranu **špecifického unicastového toku** (flow protection) v sieti poskytovateľa.

Predpokladajme, že zákazník odosiela dôležitý tok dát do cieľovej destinácie D. Keď niektorý smerovač na ceste k cieľu zistí výpadok spojenia (linky alebo smerovača), stane sa smerovačom **S**, resp. **source router** (obrázok 19).

Zdrojový smerovač S zapuzdrí chránenú unicastovú komunikáciu do multicastového toku na špecifickú cieľovú adresu (špecifický (Source, G) pár), ktorý bude okamžite rozposlaný na všetky rozhrania s aktívnym protokolom PIM v režime Dense Mode. Smerovač S bude vykonávať toto tunelovanie unicastovej komunikácie, kým proces konvergencie v sieti nebude kompletný.



Obrázok 19: Modifikované RPF v PIM-DM

Od momentu, v ktorom nastane v sieti výpadok linky na pôvodnej najkratšej ceste medzi zdrojom a cieľom, smerovacie informácie v smerovacích tabuľkách smerovačov nie sú aktuálne. Dôsledkom je, že smerovače nemajú aktuálne informácie o korektnom RPF rozhraní, kým sa proces konvergencie unicastového smerovacieho protokolu v sieti dokončí. Ak by sme ponechali originálnu logiku výberu RPF rozhrania (t.j. paket musí vojsť rozhraním, ktoré podľa unicastovej smerovacej tabuľky vedie po najkratšej ceste nazad k odosielateľovi tohto paketu), niektorý zo smerovačov by náš multicastový tok zahodil v dôsledku RPF kontroly.

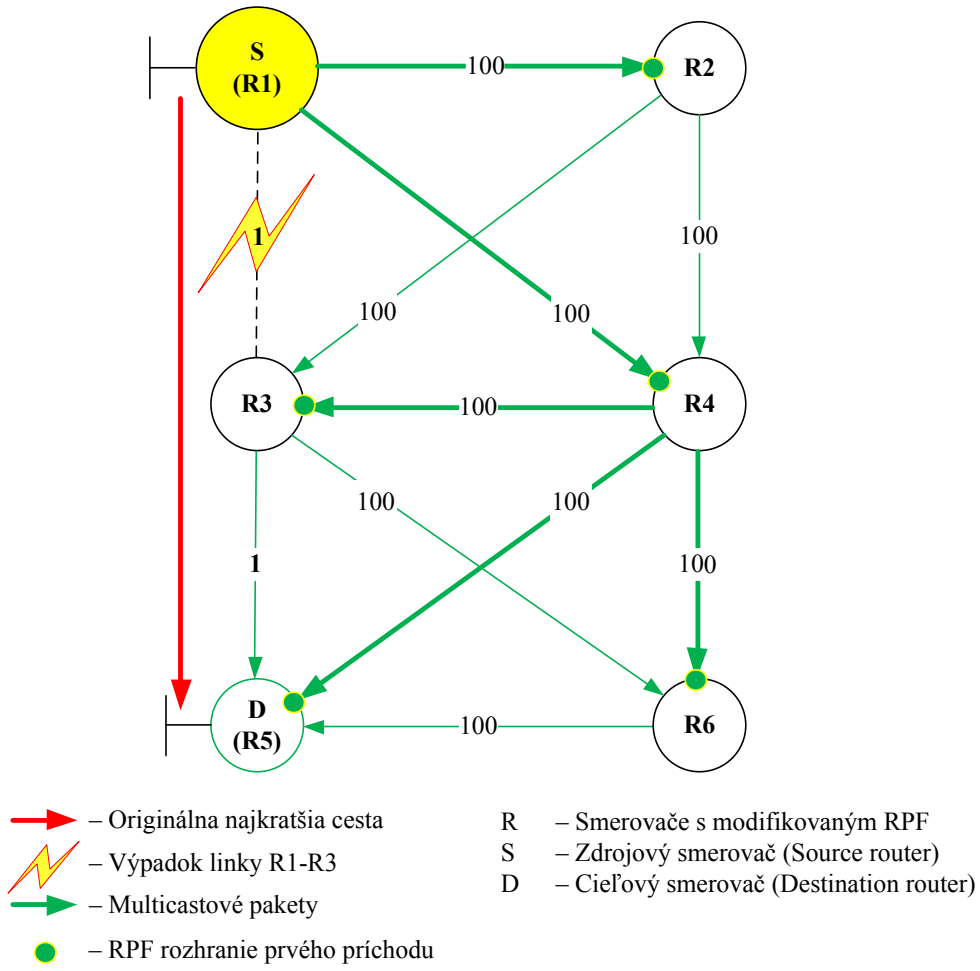
Z tohto dôvodu navrhujeme modifikované pravidlo o výbere RPF rozhrania: *RPF rozhraním sa stane to rozhranie, ktoré príjme prvý multicastový paket pre danú skupinu G.* Označením „prvý paket“ sa rozumie multicastový paket, ktorého spracovanie vedie na vytvorenie nového, doposiaľ neexistujúceho záznamu v multicastovej smerovacej

tabuľke pre pár (Source, G). Inými slovami, RPF rozhranie na všetkých ostatných smerovačoch bude **rozhranie prvého príchodu** (interface of the first arrival) vzhľadom na multicastové pakety špecifického IPFRR (Source, G) páru. Po tomto výbere RPF rozhrania smerovače rozpošlú multicastové pakety ďalej cez všetky ostatné PIM rozhrania.

Pre každý smerovač je povolené iba **jedno RPF** rozhranie. Je možné dokázať, že pre sieť s linkami typu bod-bod takto pozmenený RPF mechanizmus nespôsobí smerovacie slučky. Matematický dôkaz, ktorý potvrdí korektnosť nami vykonanej modifikácie RPF logiky, je uvedený v kapitole 5.1.

Cieľovým smerovačom D sa stane taký smerovač, ktorý má priamo pripojenú pôvodnú cieľovú stanicu (t.j. pôvodná cieľová IP adresa sa nachádza v sieti priamo pripojenej k niektorému rozhraniu tohto smerovača). Tento jediný smerovač nebude svojím RPF rozhraním odosielať správu Prune, pretože sa bude – ako smerovač s priamo pripojeným pôvodným príjemcom – považovať za odoberateľa tohto multicastového toku dát. Má však právo odosielať správy Prune inými rozhraniami v zmysle bežných pravidiel PIM-DM (t.j. ak dostáva multicastový tok dát aj non-RPF rozhraním). Ostatné smerovače majú právo takisto odosielať správy Prune svojimi non-RPF rozhraniami, ak nimi dostávajú multicastový tok, avšak pretože smerovač D sa sám od distribučného stromu neodhlási, v sieti vznikne jednoduchý nerozvetvený distribučný strom – cesta spätne daná smerovačmi a ich RPF rozhraniami počnúc smerovačom D v smere k smerovaču S. Po tejto ceste od smerovača S na smerovač D sa bude šíriť pôvodný chránený tok dát, zapuzdrený ako multicast. Takto vytvorená cesta je náhodne vytvorená cesta. Inak povedané, vytvorená cesta nemusí byť najkratšou možnou cestou.

Ako príklad, máme danú topológiu na obrázku 20, kde nastane výpadok linky medzi smerovačmi R_1 a R_3. Náš IPFRR multicastový tok by s originálnou RPF kontrolou bol odmietnutý smerovačom R_5, pretože tento smerovač R_5 by považoval za korektného a jediného RPF suseda smerovač R_3. S modifikáciou RPF kontroly smerovač R_5 akceptuje multicastový tok aj od smerovača R_4 a doručí dáta do cieľa.



Obrázok 20: Pravidlo prvého príchodu

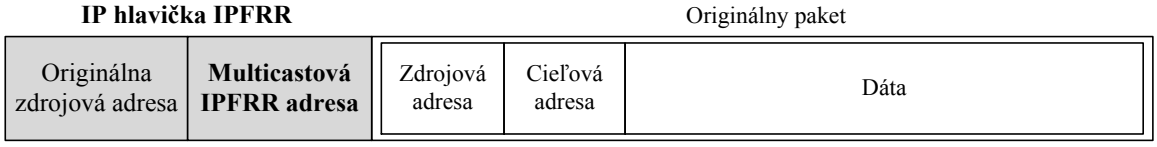
Zapuzdrené IPFRR pakety musia byť pri odchode z chránenej sieťovej domény opäť obnovené do originálneho stavu. Proces obnovenia komunikácie zaisťuje smerovač D, ktorý vykonáva potrebnú dekapsuláciu. To znamená, že koniec IPFRR multicastového toku je na tomto smerovači. Následne po tomto procese dekapsulácie môže byť paket doručený do originálnej cieľovej destinácie.

Modifikované správanie sa výberu RPF rozhrania poskytuje ochranu voči multicastovým smerovacím slučkám pre špecifický multicastový tok medzi smerovačmi v administratívnej doméne. Táto ochrana je účinná iba v sieti s linkami typu bod-bod (**point-to-point**). Požiadavky nášho IPFRR mechanizmu na fyzickú topológiu siete teda sú:

- Predpokladáme medzi smerovačmi linky typu bod-bod.
- Smerovač D: cieľová destinácia originálnej unicastovej komunikácie musí byť priamo pripojená k smerovaču D.

Je nutné poznamenať, že originálny proces pre odosielanie a spracovanie správ Prune v PIM-DM nie je modifikovaný. Ak chránený zapuzdrený multicastový tok príjme smerovač, ktorý ho nemá záujem odoberať alebo nemá priamo pripojeného originálneho príjemcu, tento smerovač sa môže odhlásiť z multicastového distribučného stromu. Finálny výsledok počiatočného procesu šírenia (flooding) je taký, že je vytvorená iba jedna cesta od smerovača S (vykonáva lokálnu opravu tunelovaním komunikácie) k smerovaču D (vykonávaná proces dekapsulácie).

Mechanizmus tunelovania IPv4 unicastovej komunikácie je iba jednou z mnohých možností, ako uchovať informáciu o originálnom odosielateľovi a príjemcovi unicastového paketu (obrázok 21). Zapuzdrenie unicastovej komunikácie s originálnou zdrojovou a novou multicastovou adresou zabezpečí, že takto upravená komunikácia je pripravená pre multicastový proces šírenia.



Obrázok 21: Zapuzdrenie unicastovej komunikácie

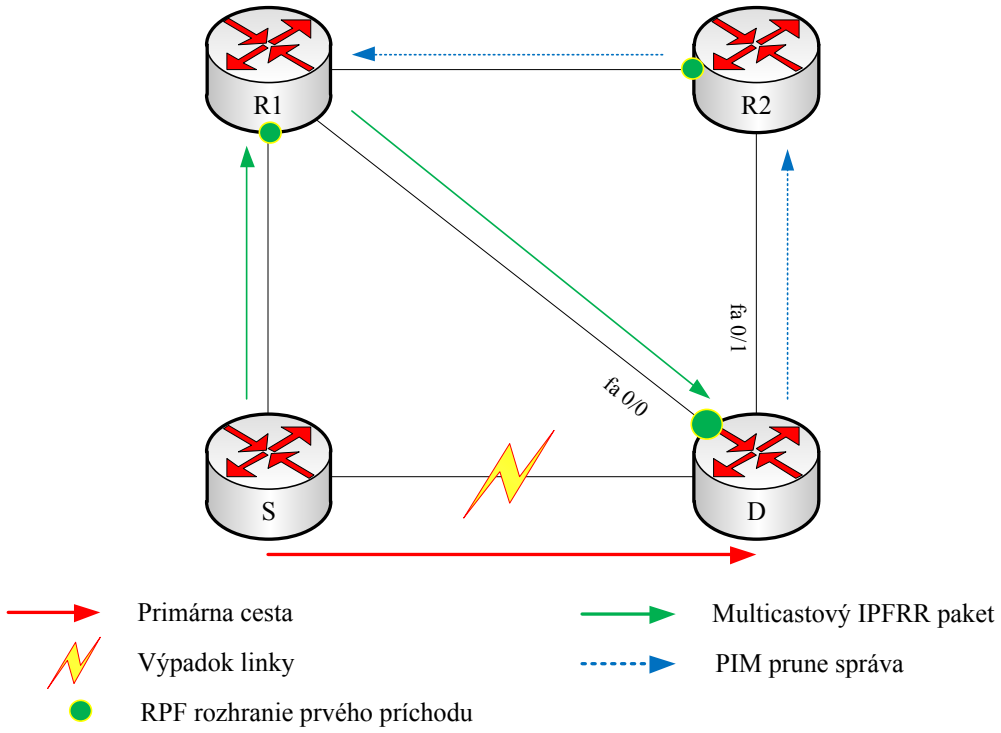
Ďalšou možnosťou je využitie **rozširujúcich hlavičiek v protokole IPv6**, ktoré umožňujú odložiť originálnu zdrojovú a cieľovú IP adresu paketu ako prídavnú hlavičku. Tieto dôležité informácie môžu byť z prídavnej hlavičky neskôr obnovené smerovačom D a použité pre rekonštrukciu originálnej hlavičky unicastového paketu chráneného toku.

4.3 Viacnásobné zlyhanie liniek v rôznych časoch

M-REP IPFRR mechanizmus dokáže nájsť alternatívnu cestu aj v prípade, keď dôjde k postupným výpadkom viacerých liniek v sieti a v rôznych časoch.

Máme danú topológiu na obrázku 22, kde dôjde k výpadku linky medzi smerovačmi S a D. Smerovač S začne zapuzdrovať chránenú unicastovú komunikáciu na špecifickú multicastovú (Source, G) komunikáciu. Alternatívna cesta, ktorá vznikne na základe pravidla prvého príchodu špecifického multicastového paketu, bude $S \rightarrow R_1 \rightarrow D$. Avšak smerovač D dostáva rozhraním fa 0/1 nadbytočnú multicastovú komunikáciu, odošle preto týmto rozhraním správu Prune smerovaču R_2 pre odhlásenie z multicastového

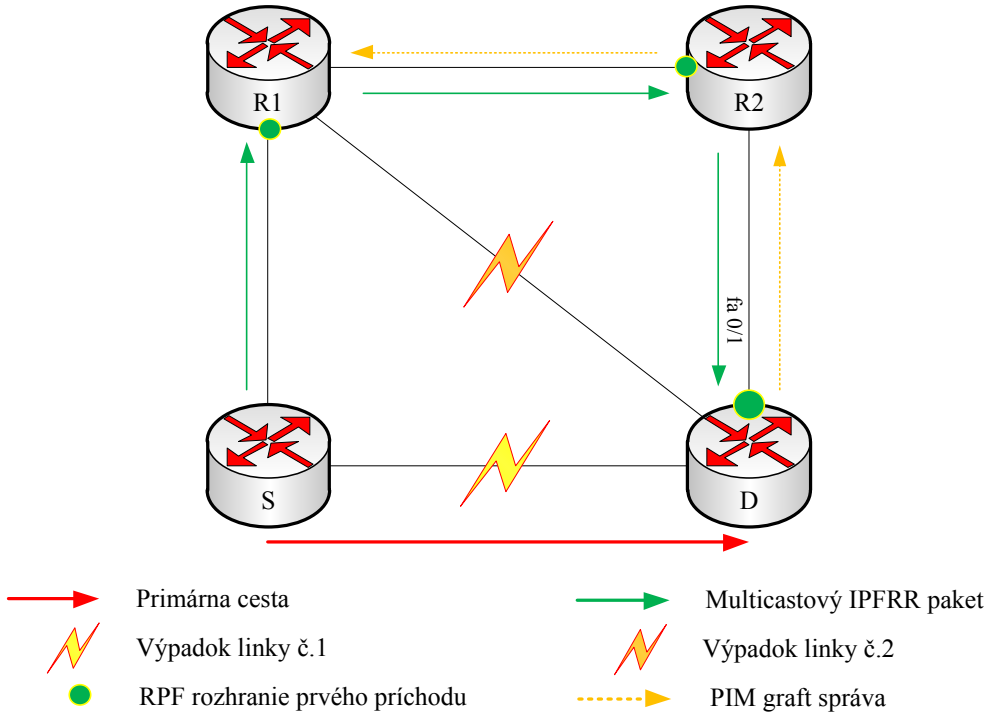
vysielania (Source, G). Výsledkom bude vytvorená len jediná cesta S→R_1→D pre špecifický multicast od smerovača S k smerovaču D.



Obrázok 22: Viacnásobné zlyhanie liniek v rôznych časoch

Problém nastane vtedy, keď dôjde k ďalšiemu výpadku linky na alternatívnej trase už po vytvorení špecifického (Source, G) multicastového distribučného stromu prvým IPFRR paketom. Ak by došlo k ďalšiemu výpadku linky ešte pred vytvorením tohto špecifického IPFRR multicastového distribučného stromu, nenastal by žiadny problém.

Smerovač D akceptuje špecifické IPFRR multicastové pakety len z RPF rozhrania fa 0/0, ktoré bolo nastavené na základe nami zavedeného pravidla prvého príchodu. Predpokladajme, že smerovač D zistí výpadok linky na rozhraní fa 0/0 smerom na R1. Keďže došlo k výpadku linky na jeho RPF rozhraní, je nutná re-inicializácia RPF rozhrania na smerovači D a opätovné pripojenie na špecifický (Source, G) multicastový distribučný strom (obrázok 23).



Obrázok 23: Odoslanie PIM graft správy

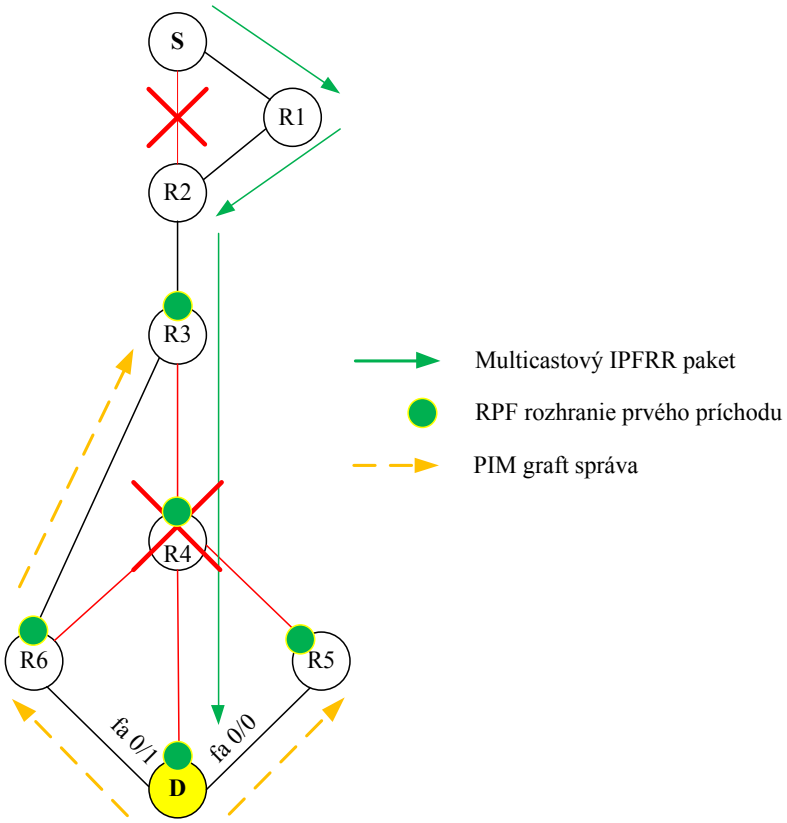
Protokol PIM-DM na re-inicializáciu distribučného stromu a pre zrušenie stavu odhlásenia používa správu Graft. V klasickom PIM-DM sa správa Graft posiela RPF rozhraním. V prípade nášho mechanizmu však musíme riešiť práve stratu RPF rozhrania, preto pravidlá pre použitie správy Graft budú v našom mechanizme modifikované.

V pôvodnom protokole PIM-DM platia o správe Graft nasledujúce pravidlá: Ak smerovač príjme Graft správu na rozhraní, ktoré je v stave pruned, nastaví toto rozhranie na stav forward, čím umožní opätovné preposielanie multicastového toku týmto rozhraním. Ak smerovač, ktorý prijal Graft správu, mal všetky výstupné rozhrania v stave pruned a odhlásil sa už od nadradeného smerovača z multicastového vysielania správou Prune, musí odoslať správu Graft jeho nadradenému smerovaču pre obnovenie multicastového vysielania. Tento proces sa opakuje dovtedy, kým sa opätovne nevytvorí multicastový distribučný strom k prvému smerovaču, ktorý chce opäť prijímať multicast a odoslal správu Graft.

Graft správa sa podľa štandardu RFC 3973 [**59**] odosiela RPF rozhraním pre špecifický (S, G) strom. V našom prípade (obrázok 23) musí smerovač D ešte pred pokusom o odoslanie Graft správy vybrať korektné RPF rozhranie. Tu vzniká problém, ktoré rozhranie vhodne zvoliť za nové RPF rozhranie – je pritom potrebné

zdôrazniť, že v našom modifikovanom RPF pravidle je RPF rozhranie principiálne náhodné – je totiž určené paketom prvého príchodu. Pri výpadku RPF a odosielaní správy Graft však práve na príchod takéhoto paketu nemožno čakať. Cieľom Graft správy je znovu vytvorenie multicastového distribučného stromu, čo v našom prípade znamená obnovenie alternatívnej cesty. V danej topológii (obrázok 23), by preto smerovač D odoslal správu Graft rozhraním fa 0/1 nadradenému smerovaču R_2. Ten by nastavil rozhranie, ktorým prijal správu Graft do stavu forward a opäť by odoslal správu Graft nadradenému smerovaču R_1. Týmto procesom sa alternatívna cesta obnoví a bude $S \rightarrow R_1 \rightarrow R_2 \rightarrow D$.

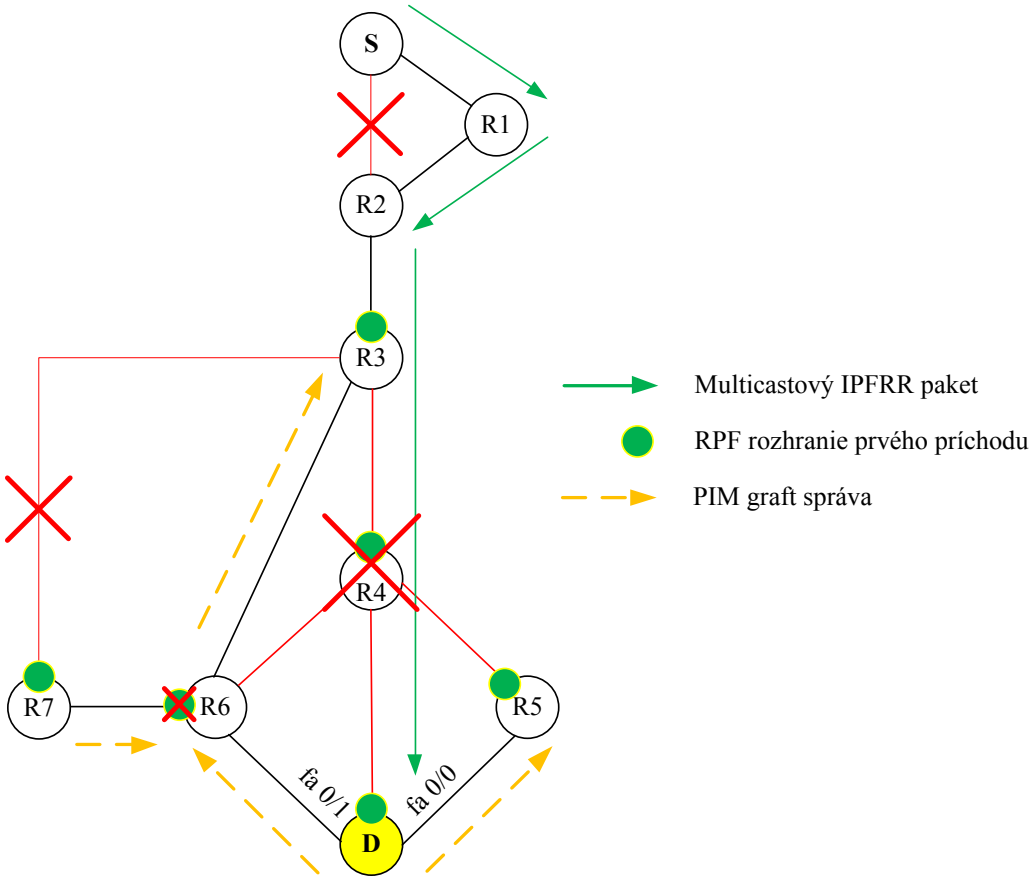
Ukážme si aplikáciu modifikovanej procedúry RPF a Graft mechanizmu M-REP na nasledujúcom zložitejšom príklade. Majme danú topológiu podľa obrázku 24, kde nastane prvý výpadok linky na smerovači R_2. Smerovač, ktorý zistí tento výpadok, sa stane smerovačom S a začne zapuzdrovať unicastovú komunikáciu na špecifický multicast špecifikovaný párom (Source, G). Nech alternatívna cesta vytvorená pravidlom prvého príchodu bude $S \rightarrow R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_4 \rightarrow D$. Smerovače, ktoré prijali neželanú multicastovú komunikáciu, sa odhlásia správou Prune. V sieti následne nastane ďalší výpadok, avšak tentokrát výpadok smerovača R_4. Smerovač D musí obnoviť alternatívnu cestu. Nastáva otázka, ktoré rozhranie zvoliť na smerovači D za RPF rozhranie a odoslať ním správu Graft nadradenému smerovaču.



Obrázok 24: Riešenie postupných výpadkov 1/2

Ak by smerovač D zvolil za RPF rozhranie fa 0/0 a odoslal ním Graft správu, smerovač R_5 by nedokázal obnoviť alternatívnu cestu, pretože sám stratil konektivitu s nadradeným smerovačom R_4. Z toho vyplýva, že smerovač D nevie určiť v danej situácii správne RPF rozhranie. Preto smerovač D pre špecifický (Source, G) multicastový tok nenastaví žiadne rozhranie za RPF rozhranie, ale odošle Graft správu všetkými zostávajúcimi rozhraniami a z vlastnej multicastovej smerovacej tabuľky úplne odstráni záznam pre (Source, G). Smerovač R_6 po prijatí Graft správy nastaví dané rozhranie na forward a odošle svojím RPF rozhraním prvého príchodu ďalšiu správu Graft nadradenému smerovaču. Keď smerovač D opäť príjme špecifický (Source, G) multicastový tok (evidentne od smerovača R_6), nastaví svoje nové RPF rozhranie. Alternatívna cesta sa obnoví a bude $S \rightarrow R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_6 \rightarrow D$. Pakety budú doručené do cieľa až po obnovení distribučného stromu. Kým nebude obnovený špecifický (Source, G) multicastový distribučný strom, budú pakety zahodené smerovačom R_3 alebo niektorým z jeho nadradených smerovačov. Treba zdôrazniť, že ochrana voči postupným výpadkom v sieti je dodatočná vlastnosť základného mechanizmu M-REP.

Ak upravíme predošlú topológiu z obrázku 24 na topológiu v obrázku 25, môže vzniknúť pri predchádzajúcom scenári problém. Predpokladajme, že v čase výpadku smerovača R_4 dôjde k výpadku aj na linke medzi smerovačom R_3 a R_7.



Obrázok 25: Riešenie postupných výpadkov 2/2

Keď smerovač R_7 stratí konektivitu na RPF rozhraní prvého príchodu, odošle Graft správu na všetky zostávajúce rozhrania, čo znamená v rámci danej topológie odoslanie Graft správy smerovaču R_6. V klasickom PIM-DM by smerovač R_6 Graft správu prijatú vlastným RPF rozhraním neakceptoval. Preto je nutná modifikácia správania sa smerovača, keď príjme Graft správu na RPF rozhraní prvého príchodu.

Ak smerovač príjme Graft správu na svojom vlastnom RPF rozhraní prvého príchodu, odstráni z multicastovej smerovacej tabuľky záznam (Source, G), zruší výber aktuálneho RPF rozhrania a odošle Graft správu zostávajúcimi rozhraniami. Po príchode multicastového toku opätovne nastaví nové RPF rozhranie na základe pravidla prvého príchodu špecifického (Source, G) multicastového paketu. Výsledná alternatívna cesta bude $S \rightarrow R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_6 \rightarrow D$.

4.4 Metodika overenia riešenia práce

Predmetom nášho výskumu je využitie technológie multicast v oblasti IPFRR. Súčasné IPFRR mechanizmy sú závislé na prípravných výpočtoch alternatívnej cesty (pre-computing), čo prináša rôzne problémové oblasti. Pre danú problematiku sme navrhli riešenie, ktoré nie je závisle na prípravných výpočtoch a smerovacích protokoloch. Navrhli sme nový IPFRR mechanizmus, ktorý využíva multicastový protokol PIM-DM. Originálny RPF mechanizmus nebol kompatibilný pre naše účely, preto sme logiku RPF mechanizmu modifikovali.

Originálny RPF mechanizmus je určený na ochranu voči smerovacím slučkám, ktoré môžu vzniknúť najmä pri prvotnom procese šírenia multicastových paketov v PIM-DM. Náš IPFRR využíva modifikovaný výber RPF rozhrania, preto je dôležité vykonať overenie nami navrhnutého riešenia. Medzi možnosti umožňujúce overenie v práci prezentovaného riešenia sú nasledujúce:

- **Overenie v simulačnom prostredí** (NS-2, NS-3, OMNeT++)
- **Overenie v experimentálnom prostredí s reálnymi smerovačmi** (napr. Quagga/Linux, Cisco IOS)
- **Overenie matematickým dôkazom**

V prvom kroku sme sa zamerali na overenie, či nami vykonaná modifikácia RPF mechanizmu v PIM-DM nevedie k vzniku multicastových slučiek. Toto je vykonané matematickým dôkazom, kde sme vybrali dôkaz sporom.

Druhým krokom je overenie implementovatelnosti a funkčnosti v práci navrhnutého M-REP IPFRR mechanizmu. Z dôvodu časovej a implementačnej náročnosti sme sa rozhodli overiť funkčnosť nového IPFRR mechanizmu vo vhodnom simulačnom prostredí. Na základe tohto rozhodnutia je nutné vybrať vhodné simulačné prostredie.

5 OVERENIE NOVÉHO PIM-DM IPFRR MECHANIZMU

Multicastový protokol PIM-DM používa mechanizmus RPF, ktorý je primárne určený ako ochrana voči smerovacím slučkám. Nový M-REP IPFRR mechanizmus využíva modifikovaný RPF mechanizmus. Preto je nutné matematickým dôkazom dokázať, že nami vykonaná modifikácia RPF logiky mechanizmu **nespôsobí smerovacie slučky**. Následne simuláciou overíme **implementovatelnosť a funkčnosť** nového M-REP IPFRR mechanizmu.

5.1 Matematický dôkaz korektnosti modifikácie RPF algoritmu

Dohoda o značení: Zápisom $\mathbb{I}_e^k \rightarrow i^l$ budeme rozumieť stav medzi smerovačmi *k* a *l*, kde multicastová smerovacia tabuľka smerovača *k* obsahuje v množine výstupných rozhraní $\mathbb{I}_e^k$ aspoň jedno také rozhranie, ktoré leží s ľubovoľným rozhraním i^l smerovača *l* na totožnej linke (t.j. so špecifickým ohľadom na dvojicu smerovačov *k* a *l*, smerovač *k* preposiela multicastový tok dát na rozhranie smerovača *l*).

Definícia: Nech $r_1, r_2, ..., r_k$ je postupnosť smerovačov, ktoré sú po dvojiciach susedné. Smerovacia slučka je stav multicastových smerovacích tabuliek na týchto smerovačoch, pri ktorom platí:

1. $\mathbb{I}_e^j \rightarrow i^{j+1}$ pre $j=1, 2, ..., k-1$
2. $r_k = r_1$

a multicastové pakety smerované podľa obsahu smerovacích tabuliek na týchto smerovačoch sú preposielané v nekonečnej postupnosti r_1-r_2-...-r_k=r_1-r_2...

Pravidlá:

1. V sieti budú len linky typu bod-bod medzi smerovačmi.
2. Celá nasledujúca procedúra je stanovená pre konkrétnu dvojicu (S, G).
3. Zdrojový smerovač S nebude preposielať multicastový tok.
4. Zdrojový smerovač S bude mať iba výstupné rozhrania.
5. Každý smerovač, ktorý nie je S, bude mať práve jedno vstupné rozhranie a ostatné výstupné rozhrania.
6. Vstupné rozhranie je dané pravidlom prvého príchodu.

7. Množina všetkých rozhraní $\mathbb{I}$, vstupné rozhranie $I_i \in \mathbb{I}$, množina výstupných rozhraní $\mathbb{I}_e$, pre ktoré platí:
   7.1. $\mathbb{I}_e \subset \mathbb{I}$
   7.2. $I_i \notin \mathbb{I}_e$
   7.3. $\{I_i\} \cup \mathbb{I}_e = \mathbb{I}$
8. Pravidlo prvého príchodu: Rozhranie, na ktorom prijatie multicastového paketu si vynúti vytvorenie novej smerovacej položky v multicastovej smerovacej tabuľke.
9. V prípade, že pre konkrétnu dvojicu (S, G) pravidlo prvého príchodu neurčuje vstupné rozhranie jednoznačne (pri paralelných architektúrach), za vstupné rozhranie sa považuje rozhranie, ktoré vyhovuje pravidlu prvého príchodu a má najvyššie SNMP ifindex.
10. Multicastový tok vchádzajúci rozhraním I_i je replikovaný všetkým rozhraniami množiny $\mathbb{I}_e$.
11. Multicastový tok dát vchádzajúci rozhraním rôznym od I_i je v tichosti zahodený.

Veta: Distribúcia multicastových tokov v sieti riadená uvedeným pravidlami nespôsobí smerovaciu slučku.

Dôkaz sporom: Predpokladajme, že do istého času *t* je multicast preposielaný v postupnosti po dvojiciach susedných smerovačov $r_1, r_2, ..., r_{k-1}$. Predpokladajme, že pri zachovaní pravidiel vznikne v čase *t* smerovacia slučka tým, že sa smerovač r_1 rozhodne akceptovať a replikovať multicastový tok dát prijatý od smerovača r_{k-1}. To znamená, že rozhodnutím smerovača r_1 v čase *t* vznikne postupnosť po dvojiciach susedných smerovačov $r_1, r_2, ... r_k$, pre ktoré platí:

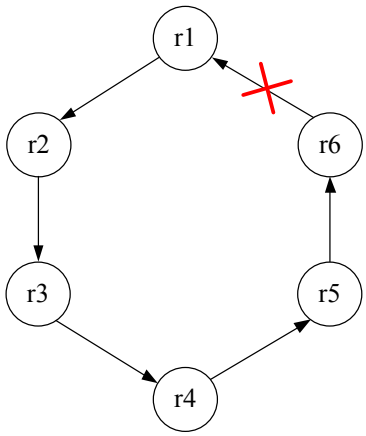
1. $\mathbb{I}_e^j \rightarrow i^{j+1}$ pre $j=1, 2, ..., k-1$
2. $r_k = r_1$

a multicastové pakety preposielané týmito smerovačmi sa pohybujú v postupnosti smerovačov r_1-r_2-...-r_k=r_1-r_2...

Ak do času *t* smerovač r_1 replikoval multicastový tok dát v smere k r_2, buď bol zdrojom toku (v takom prípade nemá vstupné rozhranie I_i), alebo mal svoje vstupné

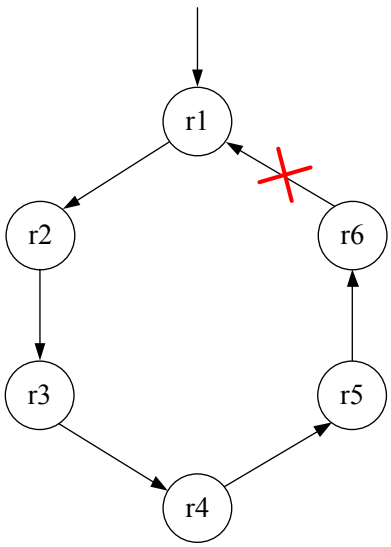
rozhranie už identifikované. V takom prípade je však **nemožné**, aby v čase *t* vznikla smerovacia slučka akceptovaním toku od smerovača r_{k-1}:

1. Ak r_1 je zdrojom, musel by preposielať multicastový tok dát, čo je v **spore s pravidlom 3** (obrázok 26)**.**



Obrázok 26: Dôkaz sporom, spor č.1

2. Ak r_1 nie je zdrojom, muselo by dôjsť buď k akceptovaniu dát niektorým z rozhraní z množiny $\mathbb{I}_e$, čo je v **spore s pravidlom 11**, alebo by muselo dôjsť k zmene rozhrania I_i, čo je v spore s vlastnosťou rozhrania I_i ako rozhrania prvého príchodu, t.j. toho rozhrania, na ktorom si prijatie multicastového paketu vynúti vytvorenie novej smerovacej položky v multicastovej smerovacej tabuľke (obrázok 27).



Obrázok 27: Dôkaz sporom, spor č.2

Matematický dôkaz sporom potvrdil, že nami vykonaná modifikácia RPF logiky v PIM-DM **nespôsobí smerovacie slučky**.

5.2 Overenie realizovateľnosti a implementovateľnosti simuláciou

Ďalším spôsobom, ktorým preveríme realizovateľnosť a implementovateľnosť nového M-REP IPFRR mechanizmu, bude realizovanie simulácií. Naším primárnym zámerom je testovanie mechanizmu na rôznych kritických situáciách, ktoré môžu nastať aj v reálnych podmienkach. Mechanizmus bude preto testovaný na nasledujúcich situáciách:

- Scenár č.1: simulácia výpadku linky.
- Scenár č.2: simulácia výpadku celého smerovača.
- Scenár č.3: simulácia postupných výpadkov rôznych liniek a smerovača.

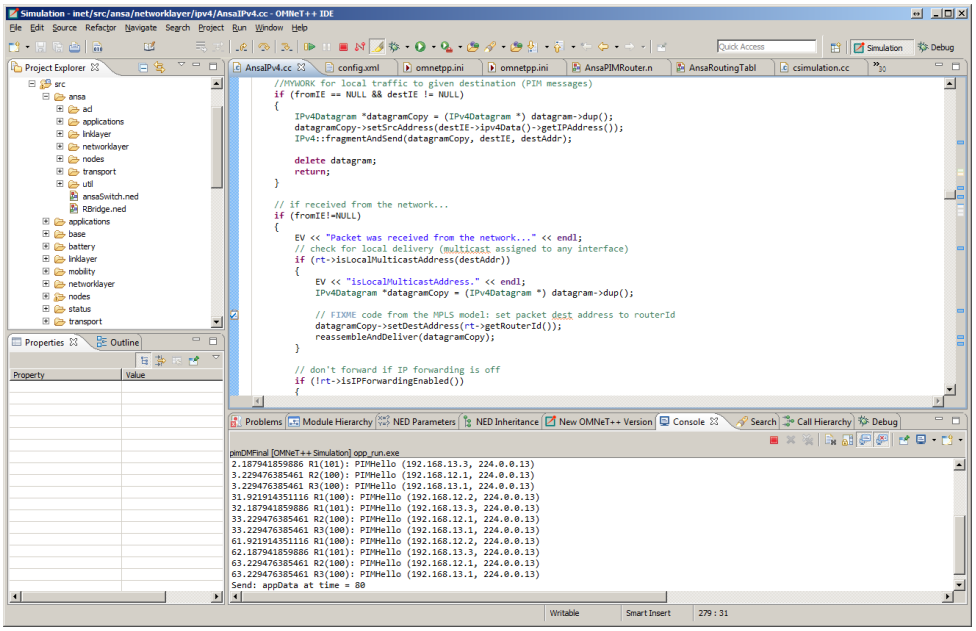
5.2.1 Analýza nástrojov pre overenie simuláciou

Problematika IP Fast Reroute je pomerne nová, avšak už teraz existujú experimentálne prostriedky, ktoré pomáhajú implementovať a overiť nové techniky IPFRR. Medzi použiteľné experimentálne prostriedky v oblasti IPFRR patria OMNeT++, NS-2, NS-3 a Quagga.

Na základe analýzy existujúcich IPFRR riešení a stanovených cieľov práce sme sa rozhodli, že ďalšie smerovanie práce bude mierené na vývoj nového IPFRR mechanizmu, ktorý bude primárne využívať technológiu multicast. Veľkou výhodou by preto bolo nájdenie existujúcej a funkčnej implementácie multicastového protokolu PIM-DM v simulačnom prostredí, čo by následne zjednodušilo tvorbu simulačných scenárov bez potreby kompletnej implementácie samotných mechanizmov PIM-DM.

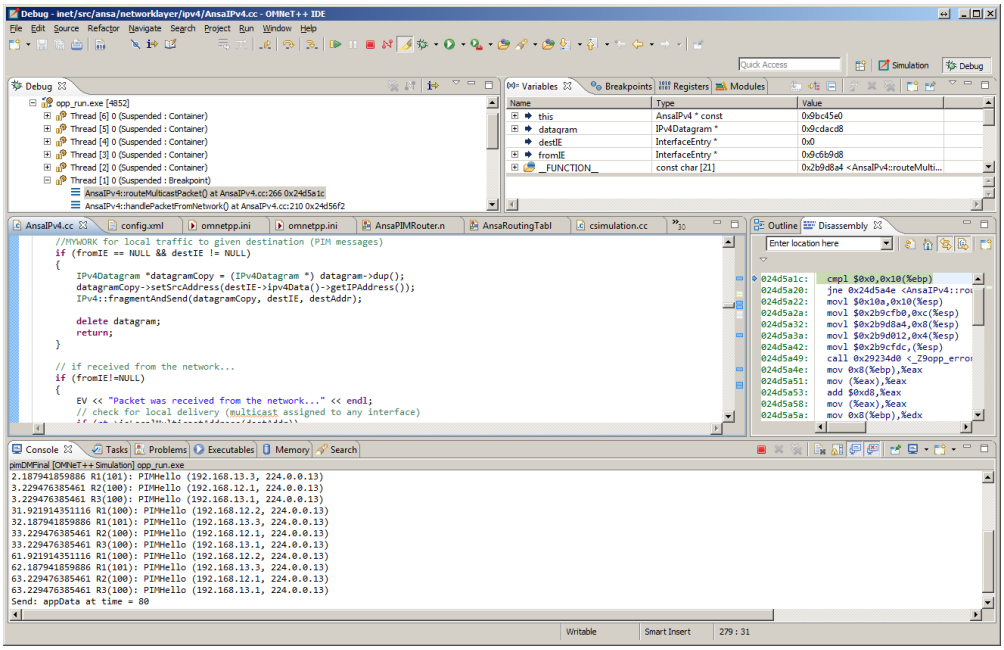
5.2.2 OMNeT++

OMNeT++ je diskrétne simulačné prostredie. Je primárne určené pre vytváranie sieťových simulácií, ale používa sa aj pre simuláciu komplexných IT systémov, systémov hromadnej obsluhy alebo simuláciu hardvérovej architektúry. OMNeT++ je rozšíriteľné, modulárne a komponentovo založené C++ simulačné prostredie [**62**]. OMNeT++ ponúka grafické IDE prostredie založené na Eclipse platforme (obrázok 28).



Obrázok 28: OMNeT++ IDE Simulation

Okrem simulačného prostredia ponúka OMNeT++ aj rozsiahle a pokročilé prostredie pre ladenie (Debug, obrázok 29).



Obrázok 29: OMNeT++ IDE Debug

OMNeT++ poskytuje komponenty pre modelovanie architektúry sietí. Tieto komponenty sú programovateľné v jazyku C++. Pre popis topológie systému používa OMNeT++ jazyk Network Description Language (NED).

Simulačné prostredie OMNeT++ sa skladá z nasledovných primárnych komponentov:

- NED (jazyk pre popis topológie systému)
- OMNeT++ IDE založené na platforme Eclipse
- Simulation kernel library
- GUI pre spustenie simulácii (Tkenv)
- Command-line rozhranie pre spustenie simulácií (Cmdenv)
- Rôzne iné nástroje (ako napr. makefile creation tool)
- Dokumentácia a vzorové simulácie

Simulačné prostredie OMNeT++ IDE podporuje platformy Windows, Linux, Mac OS X a iné unixovo založené systémy. Aktuálna verzia simulačného prostredia OMNeT++ v čase písania práce bola 4.6. Pre nekomerčné a školské účely je simulačné prostredie dostupné zadarmo. OMNeT++ je vyvíjaný pod licenciou Academic Public License [**62**]. Pre komerčné účely je určená verzia Omnest [**63**].

Veľkou výhodou pre simulačné prostredie OMNeT++ je dostupná rozsiahla knižnica INET Framework [**64**]. Knižnica INET Framework obsahuje funkčné implementácie pre niekoľko základných protokolov ako sú UDP, TCP, SCTP, IP, IPv6, Ethernet, 802.11, MPLS, OSPF a mnoho iných. INET Framework je pravidelne aktualizovaná a je vyvíjaná ako open source. Aktuálna stabilná verzia knižnice INET Framework v čase písania práce bola INET-2.5.0. Využitie knižnice INET Framework by mohlo značne zefektívniť ďalšiu prácu na vývoji nového mechanizmu v oblasti IPFRR.

Pre simulačné prostredie OMNeT++ existuje takisto projekt *Automated Network Simulation and Analysis* (ANSA), ktorý je rozšírením existujúcej primárnej knižnice INET Framework. Tento projekt je vyvíjaný na Fakulte informačných technológií VUT v Brne [**65**].

Jedným z hlavných cieľov projektu ANSA bolo využitie simulačného prostredia OMNeT++ na simuláciu prevádzky univerzitnej siete VUT. Knižnicu ANSA je možne stiahnuť z GitHub [**66**]. Knižnica ANSA obsahuje niekoľko vylepšení oproti primárnej knižnici INET Framework. Jednou z hlavných výhod, ktorú prináša OMNeT++ spolu s knižnicou ANSA pre našu prácu, je získanie podpory pre technológiu IP Multicast.

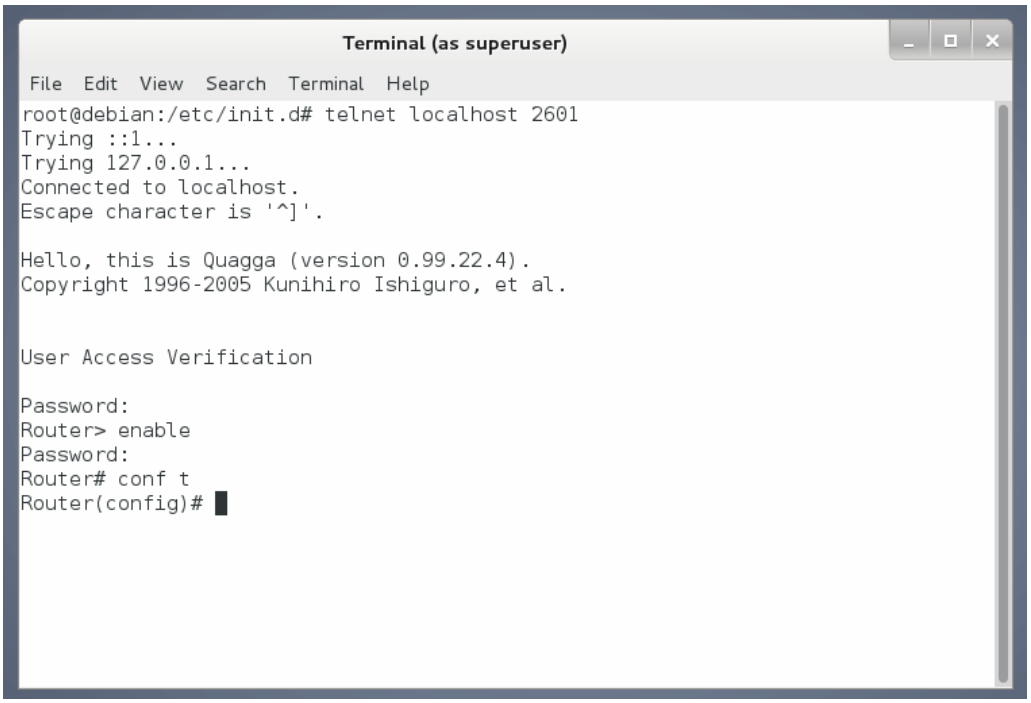
Knižnica ANSA obsahuje v sebe funkčnú implementáciu multicastových protokolov PIM-DM a PIM-SM. Implementácia multicastového protokolu PIM-DM vznikla v rámci diplomovej práce - Modelování multicastového směrování v prostředí OMNeT++ [**67**]. Ďalšou podstatnou výhodou je dobrá komunikácia a podpora od autorov projektu ANSA.

5.2.3 Quagga

Quagga je softvérový balík smerovacích protokolov určený pre prevádzku na operačných systémoch unixového typu (obrázok 30). Quagga poskytuje implementáciu protokolov OSPFv2, OSPFv3, IS-IS, OLSR, MPLS, BFD, RIPv1, RIPv2, RIPng, EIGRP a BGP-4. Quagga je nástupcom predchádzajúceho softvérového projektu Zebra [**68**].

Program Quagga je vhodný nástroj pre experimentálnu implementáciu, hlavne kvôli dostupnosti zdrojových kódov. Quagga je vydaný pod otvorenou licenciou GPL (General Public Licence) a je distribuovaný v podobe zdrojových kódov a binárnych balíčkov pre systémy unixového typu (FreeBSD, Linux, Solaris a NetBSD).

Program sa skladá z niekoľkých tzv. daemonov (služieb bežiacich na pozadí operačného systému). Daemon Zebra zhromažďuje smerovacie informácie od konkrétnych smerovacích protokolov, spolupracuje s jadrom operačného systému a upravuje jeho smerovacie tabuľky. Ostatné daemony ako ripd, ripngd, ospfd, eigrpd, bgpd predstavujú implementácie konkrétnych typov smerovacích protokolov.



Obrázok 30: Quagga

Každý daemon má vlastný konfiguračný súbor s vlastným rozhraním pre komunikáciu. Pre zjednodušenie konfigurácie je použitý VTY (Virtual Terminal) shell - vtysh, cez ktorý sa riadi celá Quagga.

Quagga napodobňuje svojim konfiguračným jazykom príkazový riadok smerovačov s Cisco IOS. V niektorých prípadoch je Quagga odlišná a nereaguje na aktualizácie tak rýchlo, ako IOS na smerovačoch od spoločnosti Cisco [**69**] [**70**].

Implementáciu multicastového protokolu PIM-DM pre softvér Quagga sa nám nepodarilo nájsť. Na základe zistených informácií je dostupný daemon qpimd (PIM Daemon for Quagga), ktorý obsahuje len implementáciu multicastového protokolu Protocol Independent Multicast - Source-Specific Multicast (PIM-SSM). Tento protokol však nie je vhodný pre overenie nášho riešenia M-REP v oblasti IPFRR.

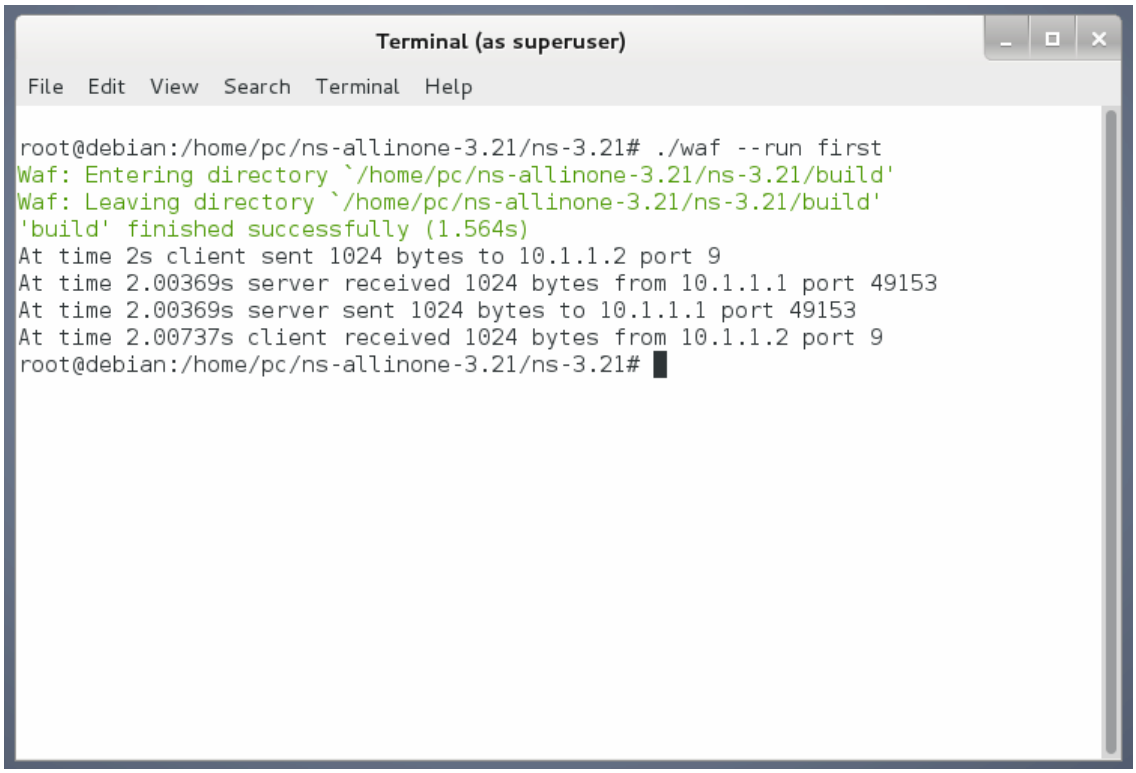
Na základe faktu, že sa nám nepodarilo nájsť vhodnú implementáciu protokolu PIM-DM, softvér Quagga vzhľadom na potrebu implementácie celého PIM-DM mechanizmu a tým celkovej časovej náročnosti riešenia nebude ďalej braný do úvahy a použitý v tejto práci. To ho však nevylučuje ako perspektívny nástroj pre ďalšie experimentálne skúmanie.

5.2.4 NS-3

NS-3 je diskrétny sieťový simulátor, ktorý je primárne určený pre výskumné a vzdelávacie účely. Simulátor ns-3 je voľne dostupný softvér, ktorý je vyvíjaný pod licenciou GNU GPLv2 [**71**]. Predchodcom tohto simulátora bol simulátor ns-2, ktorý už nie je aktívne vyvíjaný [**72**]. Simulátor ns-3 je napísaný v programovacom jazyku C++ a Python s podporou skriptov. Simulátor ns-3 využíva Python bindings (pybindgen) a Waf build system.

Simulátor ns-3 sa sústreďuje na simulácie v IP a non-IP sieťach. Väčšina jeho používateľov sa zameriava na simulácie Wi-Fi, WiMAX, LTE (1 a 2 vrstva), simulácie dynamických protokolov, ako sú Optimized Link State Routing (OLSR) a Ad hoc On-Demand Distance Vector (AODV).

Jednou z hlavných odlišností tohto simulátora od ostatných je orientácia na príkazový riadok. Simulátor ns-3 v základnej inštalácii neobsahuje GUI. Simulácie a modely sú napísané v jazyku C++ a Python. Na obrázku 31 je možné vidieť ukážku výstupu simulácie súboru *first*.



Obrázok 31: Simulátor NS-3

Dôležitou informáciou je, že simulátor ns-3 nie je spätne kompatibilný s jeho predchodcom ns-2. Je to spôsobené faktom, že autori vytvorili simulátor ns-3 od samotných základov a kompatibilita s predošlými verziami nebola možná. Simulátor ns-3 je podporovaný na operačných systémoch Linux, OS X a FreeBSD.

Pre simulátor ns-3 existuje implementácia protokolu PIM-DM od autora Alessandro Russo, ktorá je dostupná na [**73**]. Avšak túto implementáciu sa nám ani po dlhšom čase a experimentovaní nepodarilo spustiť.

Pokúsil som sa autora kontaktovať ohľadom daných problémov a zistil som, že autor už k tejto implementácii PIM-DM neposkytuje žiadnu podporu. Autor v odpovedi napísal, že sa tejto téme už dlhší čas nevenuje a akákoľvek pomoc, resp. spolupráca z jeho strany nie je možná.

Z týchto dôvodov sme sa rozhodli, že simulátor ns-3 nepoužijeme v budúcnosti ako experimentálny nástroj pre overenie M-REP IPFRR mechanizmu.

5.2.5 Vyhodnotenie analýzy simulačných nástrojov

Na základe predošlých faktov a informácií môžeme konštatovať, že simulačné prostredie OMNeT++ spolu s knižnicami INET Framework a ANSA je vhodným simulačným nástrojom pre našu ďalšiu výskumnú činnosť.

Keďže sme sa rozhodli budúce experimenty realizovať v simulačnom prostredí OMNeT++, je nutné vybrať aj príslušný mechanizmus pre rýchlu detekciu chýb. Jedným z najpoužívanejších mechanizmov pre rýchlu detekciu chyby, ktorý je založený na softvérovom princípe, je BFD. Tento mechanizmus je bližšie popísaný v kapitole č. 1.5.

Nami navrhnutý M-REP mechanizmus vyžaduje linky typu bod-bod, čo znamená, že smerovače sú medzi sebou priamo spojené linkami. Preto nie je nutné použiť softvérový princíp detekcie výpadku linky, ktorý využíva overovanie stavu linky prostredníctvom "Hello" správ (BFD), ale budeme zisťovať výpadok linky zmenou stavu rozhrania ovplyvneného chybou. Tento princíp detekcie výpadku je rýchlejší ako mechanizmus BFD a nepredstavuje nadbytočnú záťaž na sieť.

5.3 Simulácie v OMNeT++

V tejto kapitole sa zameriame na testovanie M-REP IPFRR mechanizmu v simulátore OMNeT++ (verzia 4.5). Ako základ pre simuláciu bola použitá existujúca implementácia protokolu PIM-DM z knižnice ANSA (verzia 2.2) [**66**]. Knižnica ANSA je rozsiahla a analýza existujúceho kódu trvala niekoľko týždňov. Po analýze knižnice ANSA sme začali s potrebnými modifikáciami.

Aktivácia mechanizmu M-REP

M-REP mechanizmus sa aktivuje na smerovači v rámci simulácie vtedy, keď smerovač príjme špecifický unicastový paket chráneného toku (metóda *handlePacketFromNetwork* v triede *AnsaIPv4*) a **pri jeho spracovaní zistí výpadok** na originálnom výstupnom rozhraní vzhľadom na chránený unicastový tok. To znamená, že po detekcii výpadku linky na originálnom výstupnom rozhraní sa daný smerovač stane smerovačom S.

Detekcia výpadu linky alebo smerovača

V kapitole č. 1.4 sme uviedli niekoľko spôsobov určených pre rýchlu detekciu výpadku linky. Ak nastane v simulácii výpadok linky, zmení sa jeden z parametrov rozhrania (*datarate*), na ktorom došlo k výpadku. Preto je detekcia výpadku linky v rámci simulácii realizovaná tak, že ak klesne prenosová rýchlosť rozhrania na 0, smerovač vyhlási príslušnú linku za nefunkčnú. Takto navrhnutá detekcia výpadku linky podľa výstupného rozhrania zabezpečí **okamžitú** detekciu výpadku vzhľadom na chránený unicastový tok.

Modifikácia paketov

V reálnej prevádzke by smerovač S zapuzdril ďalšou IP hlavičkou chránenú unicastovú komunikáciu. Avšak v simulácii smerovač S nepridáva ďalšiu IP hlavičku, ale nahradí cieľovú IP adresu originálneho unicastového toku za špecifickú multicastovú adresu a **pôvodnú cieľovú IP adresu zálohuje do premennej** (*IPFRRdestAddrBackUp*) v IPv4 datagrame (ekvivalent paketu v simulátore).

Modifikácia RPF

Originálna metóda *newMulticast*, ktorá sa volá vždy pri vytvorení nového záznamu v multicastovej smerovacej tabuľke, bola upravená tak, že pre špecifický multicastový (Source, G) tok RPF rozhranie nebude zistené z unicastovej smerovacej tabuľky. RPF rozhraním pre chránený unicastový tok v metóde *newMulticast* bude **rozhranie prvého príchodu** paketu tohto toku. Všetky modifikácie RPF sa vykonávajú **len v multicastovej smerovacej tabuľke**. Unicastová smerovacia tabuľka nie je modifikovaná.

Obnova paketov do originálneho stavu

Obnovu paketu zabezpečuje smerovač D. Smerovačom D sa stane taký smerovač, ktorý má priamo pripojenú cieľovú destináciu. Pri obnovení paketu sa pôvodná IP cieľová adresa chráneného toku načíta z premennej (*IPFRRdestAddrBackUp*) a nahradí dočasnú cieľovú multicastovú adresu. Takýto paket môže byť doručený do cieľovej destinácie.

Viacnásobné výpadky v simulácii

Počas testovania IPFRR mechanizmu M-REP sme prišli s myšlienkou ako by sa mechanizmus správal pri viacnásobných výpadkov v sieti. V originálnom návrhu sme s takýmito výpadkami nepočítali. Táto myšlienka naštartovala veľkú diskusiu a otvorila novú veľkú problematiku. Funkcionalita M-REP mechanizmu sa rozšírila a je podrobne

opísaná v kapitole č. 4.3. Ďalšie funkcionality mechanizmu M-REP spojené s viacnásobným výpadkom v sieti boli implementované do knižnice ANSA. Ťažkou úlohou bolo zistenie výpadku RPF rozhrania prvého príchodu.

Výpadok RPF rozhrania prvého príchodu

Simulácie v OMNeT++ prebiehajú tým spôsobom, že aktívnym smerovačom je taký smerovač, ktorý **príjme paket** alebo má **načasovanú udalosť** (použitie periodického časovača).

V simulátore OMNeT++ sme nedokázali vygenerovať správu, ktorá by okamžite informovala o zmene stavu špecifickej linky. Preto bol vytvorený nový časovač (metóda *checkRpfMulticastIPFRR* v triede *PimSplitter*), ktorý v pravidelných intervaloch (0.1 simulačnej sekundy) overuje stav RPF rozhrania prvého príchodu. To predĺžilo v simulácii reakčnú dobu mechanizmu M-REP pri detekcii výpadku RPF rozhrania.

Po zistení výpadku RPF rozhrania prvého príchodu smerovač odošle všetkými výstupnými rozhraniami (okrem pôvodného RPF rozhrania) správu Graft a odstráni špecifický záznam v multicastovej smerovacej tabuľke (metóda *checkRpfMulticastIPFRR* v triede *PimSplitter*). Ak smerovač príjme správu Graft svojím RPF rozhraním prvého príchodu, odošle všetkými ostatnými rozhraniami správu Graft a opäť odstráni špecifický záznam v multicastovej smerovacej tabuľke (metóda *processGraftPacket* v triede *PimDM*).

Odosielanie dát

Nastavenie odosielania dát sa konfiguruje v súbore *omnetpp.ini* v adresári *ANSA-ansainet-2.2\examples\ansa\pimDMFinal*. Príklad konfigurácie odosielania dát z $Source_1$ na adresu $Host_2$ je na obrázku 32. Periódu odosielania dát je možné upraviť (*packetInterval*).

```
**.Source1.ipTrafGen.startTime = 50s
**.Source1.ipTrafGen.packetInterval = 5s
**.Source1.ipTrafGen.numPackets = 1000
**.Source1.ipTrafGen.destAddresses = "192.168.55.100"
```

Obrázok 32: Konfigurácia odosielania dát v OMNeT++

Na nasledujúcom obrázku 33, je výstup odosielania dát zo zdroja $Source_1$ na adresu cieľa $Host_2$ zo simulácie v OMNeT++.

```
#3669    52              Source1 --> R1   appData   id=4064  kind=0 length=146 bytes
#3676    52.00001173     R1 --> R3        appData   id=4073  kind=0 length=146 bytes
#3684    52.00002346     R3 --> R5        appData   id=4082  kind=0 length=146 bytes
#3692    52.00003519     R5 --> Host2     appData   id=4091  kind=0 length=146 bytes
```

Obrázok 33: Odosielanie dát v OMNeT++

5.3.1 Testovacia zostava

Testy v simulátore OMNeT++ boli realizované na stolnom PC s nasledujúcimi hardvérovými parametrami:

- CPU: Intel® Core™ i7-3770 Processor (4 x 3.4 GHz).
- HDD: Hitachi HDS721010CLA630 1TB, 3.5".
- RAM: 16 GB RAM DDR3.
- OS: Microsoft Windows 7 Professional SK SP1 64-bit.

Simulácie v simulátore OMNeT++ je možné spustiť v rýchlostiach normal, fast a express. Na našej testovacej zostave sme dosahovali priemerné rýchlosti v režime fast (130 simsekúnd/sekunda) a v režime express (19000 simsekúnd/sekunda).

Pomer simsekunda/sekunda vyjadruje, koľko simulátor vykoná simulačných sekúnd za jednu reálnu sekundu (v skratke sims) a je závislý na hardvérových parametroch počítača [**74**]. Prvotné kompilovanie nevyhnutných knižníc INET a ANSA trvalo na uvedenej zostave približne 20 minút.

5.3.2 Testovacia topológia

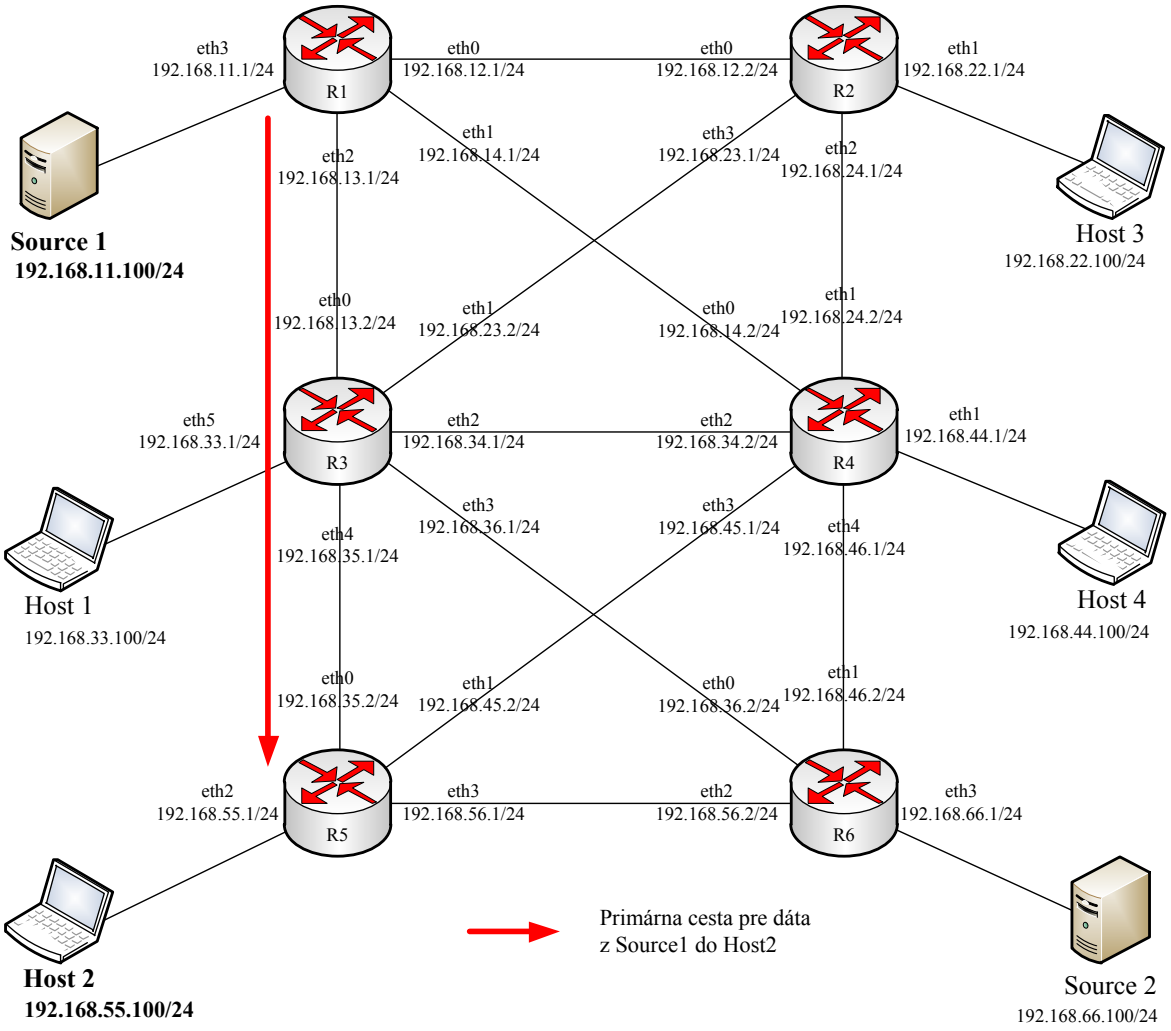
Testovacia topológia by mala byť navrhnutá tak, aby sme dokázali funkčnosť vytvoreného M-REP IPFRR mechanizmu. Preto bola navrhnutá topológia so šiestimi smerovačmi a s dostatočným počtom redundantných liniek (obrázok 34). Takto navrhnutá topológia poskytuje priestor pre overenie M-REP IPFRR mechanizmu proti vzniknutiu smerovacích slučiek a prebehlo na nej testovanie scenára číslo 1, 2 a 3.

V simuláciách používame pre generovanie toku dát zdroj $Source_1$ a príjemca generovaného toku je $Host_2$. **Tok dát zo zdroja $Source_1$ do cieľa $Host_2$ budeme chrániť navrhnutým mechanizmom M-REP**. **Primárna cesta pre tento tok dát je $R_1 \rightarrow R_3 \rightarrow R_5$**. Priebeh komunikácie v sieti je uvedený v príslušných tabuľkách. Z tabuliek boli odstránené nadbytočné položky ako napr. Arp pakety alebo PIM Hello pakety.

Do testovacej topológie boli umiestnené aj ďalšie koncové zariadenia, aby bolo ukázané, že mechanizmus M-REP doručí dáta len do skutočnej cieľovej stanice ($Host_2$).

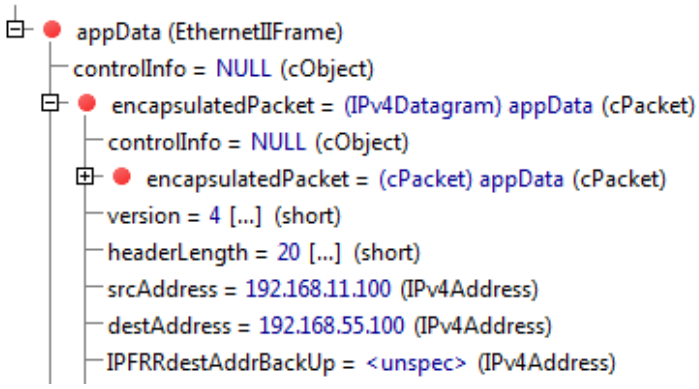
Simulácie sú určené na ukážku procesu šírenia multicastových paketov (flooding), proces odhlásenia (pruning) a vytvorenie IPFRR alternatívnej cesty mechanizmom M-REP. V simulátore OMNeT++ sme vykonali testy s periódou odosielania dát 0.001 sims a 1 sims.

Test s väčšou periódou 1 sims je z dôvodu lepšej prehľadnosti v práci, test s menšou periódou 0.001 sims sa nachádza na priloženom DVD.



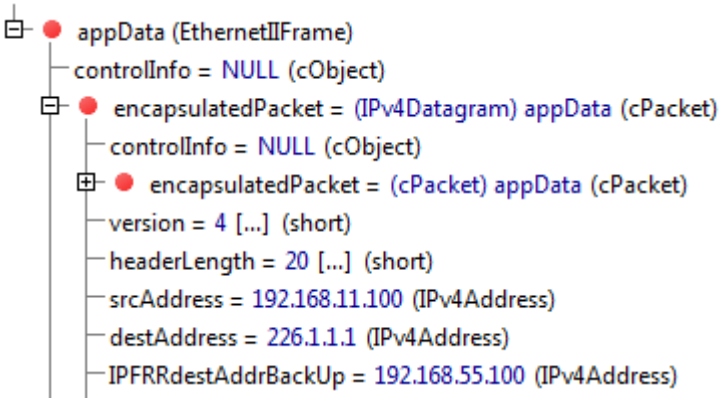
Obrázok 34: Testovacia topológia

Na obrázku 35 je zobrazený originálny paket, ktorý príjme smerovač R_1 od $Source_1$. Tento **paket nie je modifikovaný,** obsahuje originálnu zdrojovú IP adresu (srcAddress) a ešte originálnu cieľovú IP adresu (destAddress).



Obrázok 35: Originálny formát paketu chráneného toku

Na obrázku 36 je zobrazený **modifikovaný paket** smerovačom R_1 po zistení výpadku linky na originálnej ceste do cieľa. Originálna cieľová adresa $Host_2$ je zálohovaná do premennej (*IPFRRdestAddrBackUp*, 192.168.55.100) a dočasnou cieľovou IP adresou sa stane vyhradená multicastová adresa (226.1.1.1). Originálna zdrojová adresa nie je modifikovaná.



Obrázok 36: Modifikovaný formát paketu chráneného toku

Uvedené formáty paketov sú rovnaké vo všetkých realizovaných simuláciách. Modifikovaný paket je obnovený do pôvodného formátu smerovačom, ktorý má priamo pripojenú cieľovú stanicu $Host_2$, čo v danom prípade je smerovač R_5.

Všetky smerovače v testovacej topológii majú na svojich rozhraniach zapnutú podporu multicastového protokolu PIM-DM a nakonfigurované statické smerovanie. Dynamické smerovanie nebolo využívané, pretože implementácia protokolu PIM-DM v knižnici ANSA je kompatibilná len so statickým smerovaním. Po analýze možnosti ďalšieho rozšírenia kompatibility protokolu PIM-DM v knižnici ANSA s dynamickým smerovaní sme zistili, že z časového hľadiska to nie je realizovateľné.

5.3.3 Scenár č.1: výpadok linky

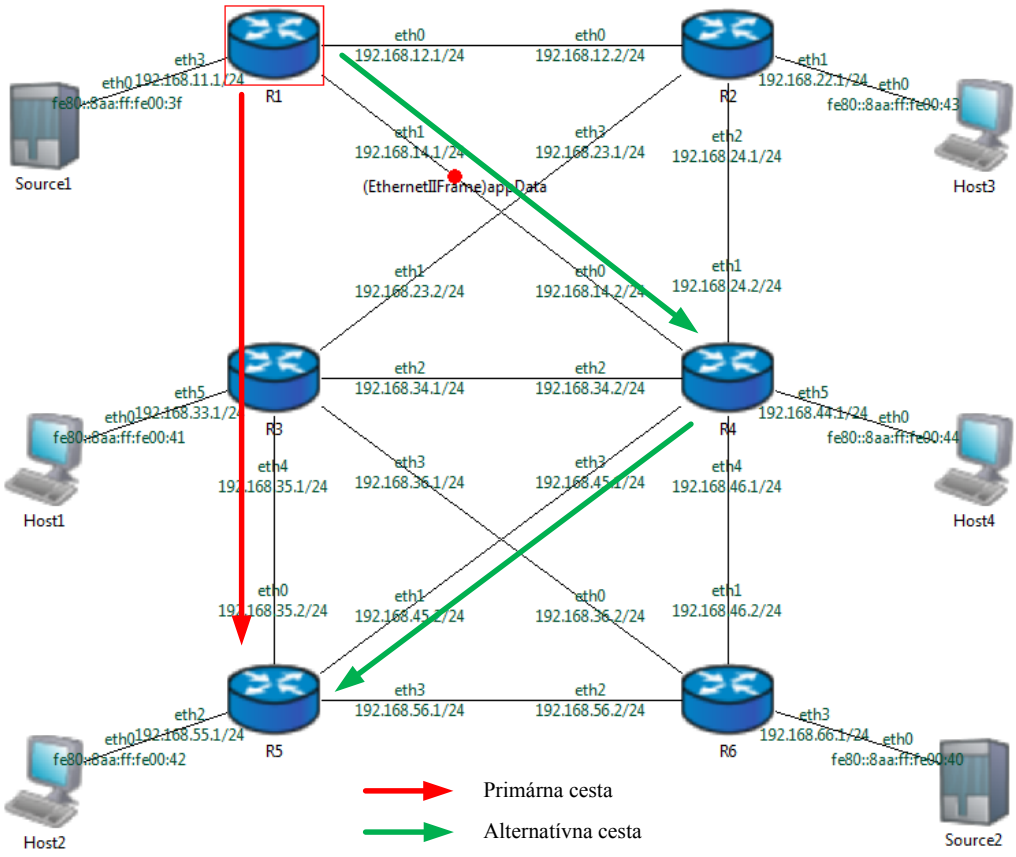
Prvý test sa zameriaval na overenie zostavenia multicatového stromu v mechanizme M-REP ako alternatívnej záložnej cesty pri detekcii výpadku linky na primárnej ceste od zdroja prevádzky do jej cieľa. $Source_1$ (192.168.11.100) bude odosielať dáta na adresu $Host_2$ (192.168.55.100).

Očakávane správanie sa mechanizmu M-REP je také, že mechanizmus dokáže po výpadku linky medzi smerovačmi R_1 a R_3 nájsť alternatívnu cestu k smerovaču, ktorý má priamo pripojený cieľ (smerovač R_5). Následne tento smerovač doručí chránený tok dát v originálnom stave cieľu $Host_2$. V tabuľke 2 je uvedený podrobný časový scenár simulácie.

Č.	Čas (sims)	Sieťový komponent	Akcia
1	50	Source1	Odoslanie dát na adresu Host2, perióda 1sims
2	52	Linka R1-R3	Odpojenie linky
3	54	Linka R1-R3	Pripojenie linky

Tabuľka 2: Popis scenáru 1

$Source_1$ začne odosielať dáta do cieľa $Host_2$. V čase 52 sims nastane výpadok linky medzi smerovačmi R_1 a R_3. Od tohto momentu smerovač R_1 pri spracovaní paketu zistí výpadok linky na originálnej ceste do cieľa a začne modifikovať pakety určené $Host_2$ (obrázok 37). Cieľová adresa týchto paketov bude zmenená na vyhradenú multicastovú adresu (226.1.1.1). Originálna zdrojová adresa zostane nezmenená.



Obrázok 37: Výpadok linky

Smerovač R_1 po modifikácii paketov určených $Host_2$ začne tieto pakety vysielať ako špecifický multicastový tok (192.168.11.100, 226.1.1.1). Protokol PIM-DM na začiatku multicastového vysielania odosiela modifikovaný paket na všetky výstupné rozhrania smerovača R_1 (okrem vstupného rozhrania, ktorým je tok prijatý) s aktívnym PIM-DM.

V tabuľke 3 (zelená farba, riadky 9 až 25) je zachytený počiatočný proces zaplavenia siete modifikovanými multicastovými paketmi protokolu PIM-DM v simulátore OMNeT++ (flooding process).

Každý smerovač, ktorý prvýkrát príjme modifikovaný paket špecifickým rozhraním, nastaví toto rozhranie podľa pravidla prvého príchodu na RPF rozhranie pre špecifický multicastový (Source, G) pár.

Smerovač R_5 sa stane cieľovým smerovačom pre daný multicastový tok, pretože má priamo pripojenú cieľovú stanicu ($Host_2$). Smerovač R_5 zmení v paketoch, ktoré prijal RPF rozhraním prvého príchodu, multicastovú cieľovú adresu (226.1.1.1) na originálnu unicastovú adresu (192.168.55.100). Obnovené pakety budú doručené smerovačom R_5 do cieľa ($Host_2$).

Smerovače, ktoré príjmu neželaný multicastový tok, sa odhlásia od odberu PIMJoinPrune správou (tabuľka 3, modrá farba, riadky 26 až 38). Alternatívna cesta, ktorá vznikne modifikovaným mechanizmom RPF v PIM-DM, je $R_1 \rightarrow R_4 \rightarrow R_5$ (tabuľka 3, riadky 39 až 42).V nasledujúcej tabuľke 3 je zobrazený výstup z simulácie.

Č.	Čas (sims)	Akcia	Typ správy
1	50.00001162	Source1 --> R1	appData
2	50.00003497	R1 --> R3	appData
3	50.00005832	R3 --> R5	appData
4	50.00008167	R5 --> Host2	appData
5	51	Source1 --> R1	appData
6	51.00001173	R1 --> R3	appData
7	51.00002346	R3 --> R5	appData
8	51.00003519	R5 --> Host2	appData
9	52	Source1 --> R1	appData
10	52.00001173	R1 --> R2	appData
11	52.00001173	R1 --> R4	appData
12	52.00002346	R2 --> R4	appData
13	52.00002346	R2 --> R3	appData
14	52.00002346	R4 --> R2	appData
15	52.00002346	R4 --> R3	appData
16	52.00002346	R4 --> R5	appData
17	52.00002346	R4 --> R6	appData
18	52.00003519	R3 --> R4	appData
19	52.00003519	R3 --> R6	appData
20	52.00003519	R3 --> R5	appData
21	52.00003519	R5 --> R3	appData
22	52.00003519	R5 --> Host2	appData
23	52.00003519	R5 --> R6	appData
24	52.00003519	R6 --> R3	appData
25	52.00003519	R6 --> R5	appData
26	52.000036099999	R2 --> R4	PIMJoinPrune
27	52.000036099999	R4 --> R2	PIMJoinPrune
28	52.00004692	R4 --> R3	PIMJoinPrune
29	52.00004692	R6 --> R4	PIMJoinPrune
30	52.000047829999	R3 --> R4	PIMJoinPrune
31	52.000047829999	R3 --> R6	PIMJoinPrune
32	52.000047829999	R3 --> R5	PIMJoinPrune
33	52.000047829999	R5 --> R3	PIMJoinPrune
34	52.000047829999	R5 --> R6	PIMJoinPrune
35	52.000047829999	R6 --> R3	PIMJoinPrune
36	52.000047829999	R6 --> R5	PIMJoinPrune
37	52.00005273	R3 --> R2	PIMJoinPrune
38	52.00005854	R2 --> R1	PIMJoinPrune
39	53	Source1 --> R1	appData
40	53.00001173	R1 --> R4	appData

41	53.00002346	R4 --> R5	appData
42	53.00003519	R5 --> Host2	appData
43	54	Source1 --> R1	appData
44	54.00002335	R1 --> R3	appData
45	54.00003508	R3 --> R5	appData
46	54.00004681	R5 --> Host2	appData

Tabuľka 3: Priebeh komunikácie v sieti po výpadku linky

Výsledok tejto simulácie dopadol podľa očakávaní a dáta boli úspešne doručené od zdroja do cieľa. Test potvrdil, že mechanizmus M-REP dokáže poskytnúť ochranu pred zlyhaním linky.

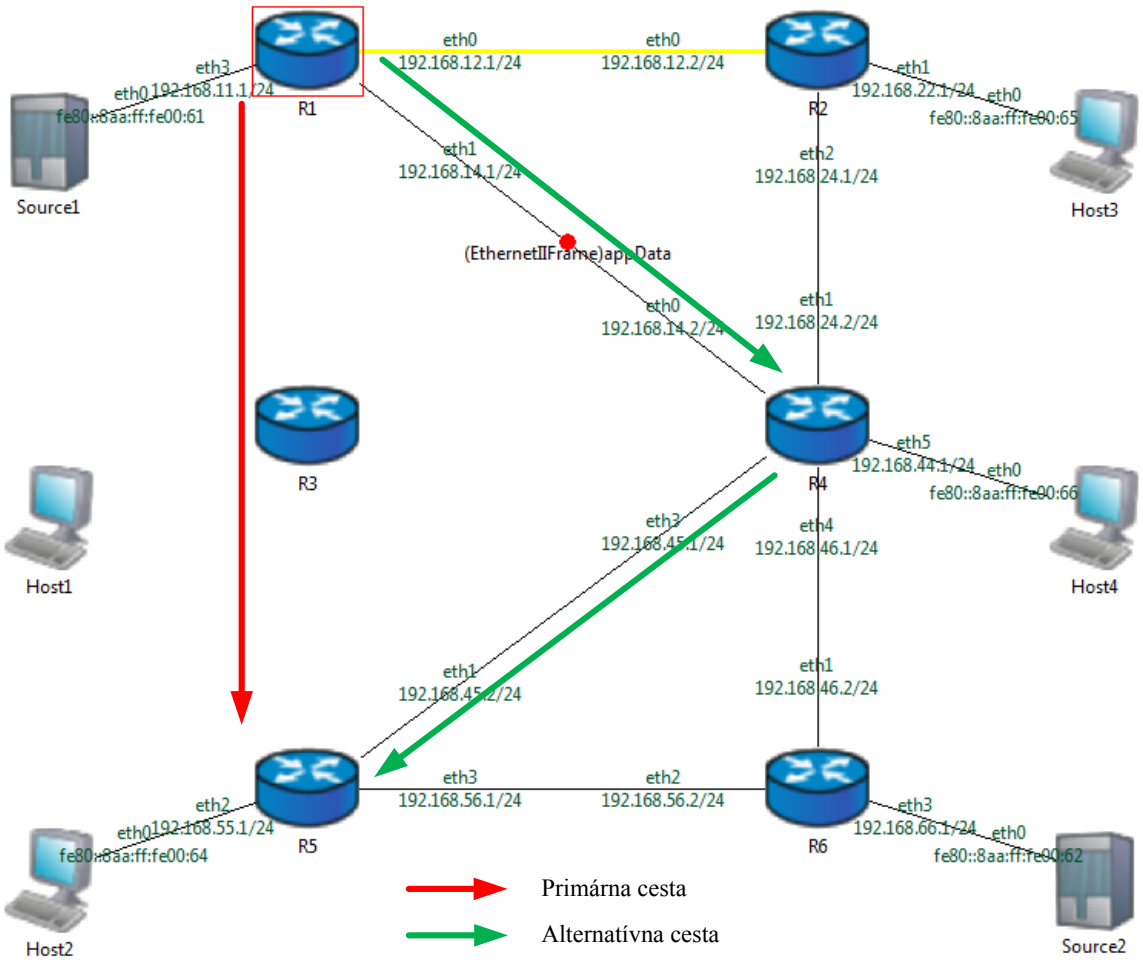
5.3.4 Scenár č.2: výpadok smerovača

Ďalším scenárom je simulácia výpadku celého smerovača, ktorý sa nachádza na primárnej ceste do cieľa. Tento scenár reprezentuje odpojenie všetkých pripojených liniek k smerovaču R_3. V tabuľke 4 je uvedený podrobný časový harmonogram scenára výpadku smerovača R_3.

Č.	Čas (sims)	Sieťový komponent	Akcia
1	50	Source1	Odoslanie dát na adresu Host2, perióda 1sims
2	52	R3	Odpojenie všetkých pripojených liniek
3	54	R3	Pripojenie všetkých liniek

Tabuľka 4: Popis scenáru 2

Očakávané správanie sa mechanizmu M-REP je také, že mechanizmus po výpadku smerovača R_3 nájde alternatívnu cestu okolo zlyhaného smerovača a doručí chránený nezmenený unicastový tok dát do cieľa $Host_2$. Na obrázku 38 je ukážka topológie po výpadku smerovača R_3.



Obrázok 38: Výpadok smerovača

Smerovač R_1 zistí výpadok linky na originálnej ceste do cieľa a začne modifikovať pakety určené $Host_2$. Pakety sú odoslané smerovačom R1 na všetky výstupné rozhrania (okrem vstupného).

Pakety príjme každý smerovač v sieti (tabuľka 5, zelená farba, riadky 9 až 18). Smerovač R_5 zistí, že má priamo pripojenú cieľovú stanicu a pakety obnoví rovnakým spôsobom ako v scenári č.1.

Alternatívna cesta, ktorá sa vytvorí na základe pravidla prvého príchodu špecifických multicastových paketov, je $R_1 \rightarrow R_4 \rightarrow R_5$ (tabuľka 5, riadky 9 až 18, riadky 25 až 28). Táto alternatívna cesta je rovnaká ako v scenári č.1. V tabuľke 5 je uvedený priebeh komunikácie v sieti pred a po výpadku smerovača R_3.

Č.	Čas (sims)	Akcia	Typ správy
1	50.00001162	Source1 --> R1	appData
2	50.00003497	R1 --> R3	appData
3	50.00005832	R3 --> R5	appData
4	50.00008167	R5 --> Host2	appData
5	51	Source1 --> R1	appData
6	51.00001173	R1 --> R3	appData
7	51.00002346	R3 --> R5	appData
8	51.00003519	R5 --> Host2	appData
9	52	Source1 --> R1	appData
10	52.00001173	R1 --> R2	appData
11	52.00001173	R1 --> R4	appData
12	52.00002346	R2 --> R4	appData
13	52.00002346	R4 --> R2	appData
14	52.00002346	R4 --> R5	appData
15	52.00002346	R4 --> R6	appData
16	52.00003519	R5 --> Host2	appData
17	52.00003519	R5 --> R6	appData
18	52.00003519	R6 --> R5	appData
19	52.000036099999	R2 --> R4	PIMJoinPrune
20	52.000036099999	R4 --> R2	PIMJoinPrune
21	52.000041909999	R2 --> R1	PIMJoinPrune
22	52.000047829999	R5 --> R6	PIMJoinPrune
23	52.000047829999	R6 --> R5	PIMJoinPrune
24	52.000053639999	R6 --> R4	PIMJoinPrune
25	53	Source1 --> R1	appData
26	53.00001173	R1 --> R4	appData
27	53.00002346	R4 --> R5	appData
28	53.00003519	R5 --> Host2	appData
29	54	Source1 --> R1	appData
30	54.00002335	R1 --> R3	appData
31	54.0000467	R3 --> R5	appData
32	54.00005843	R5 --> Host2	appData

Tabuľka 5: Priebeh komunikácie v sieti po výpadku smerovača

Tento scenár predstavuje situáciu, ktorá častokrát nastane aj v reálnej prevádzke ISP. Test potvrdil, že M-REP mechanizmus vie ochrániť špecifický unicastový tok pred zlyhaním smerovača.

5.3.5 Scenár č.3: simulácia postupných výpadkov

V tomto scenári sa zameriame na najnáročnejší test, čo znamená simuláciu postupných výpadkov v rôznych častiach siete a v rôznych časoch. Táto problematika viacnásobných výpadkov v sieti je podrobne rozobratá v kapitole 4.3.

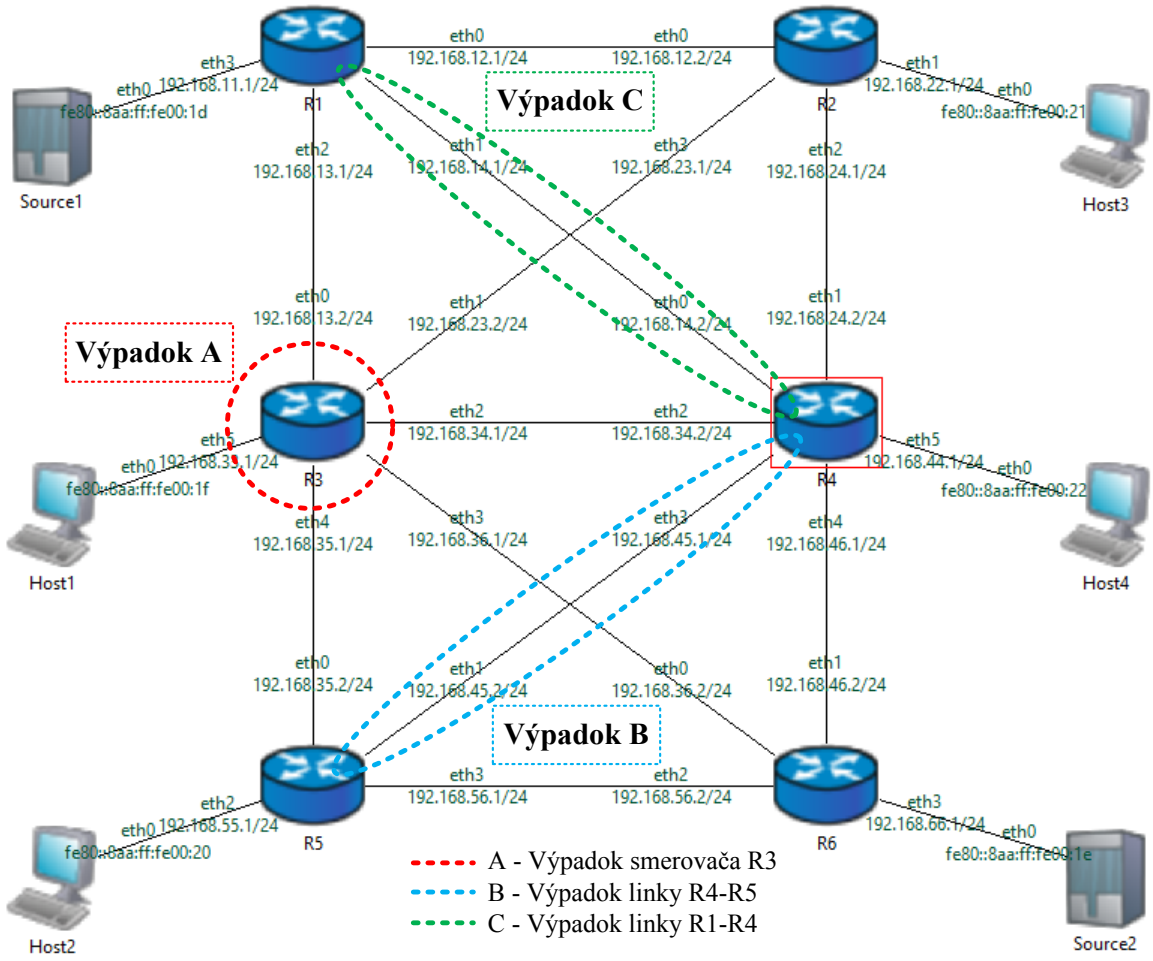
Predpokladaný výsledok simulácie je taký, že M-REP mechanizmus by mal obnoviť komunikáciu aj po viacnásobných výpadkoch v sieti v rôznych časoch. Dôležitou časťou testu bude moment, kedy dôjde k výpadku na alternatívnej trase už po vytvorení multicastového distribučného stromu. Je nutné podotknúť, že komunikácia sa obnoví až po obnovení alternatívnej cesty, čo v našom prípade znamená obnovenie špecifického (Source, G) multicastového distribučného stromu.

Zdroj $Source_1$ začne odosielať dáta v pravidelných intervaloch na adresu $Host_2$. Bude sa simulovať výpadok smerovača R_3 a neskôr aj postupný výpadok liniek na alternatívnej multicastovej distribučnej ceste, ktorá už bola vytvorená na základe pravidla prvého príchodu.

Č.	Čas (sims)	Sieťový komponent	Akcia
1	50	Source1	Odoslanie dát na adresu Host2, perióda 1sims
2	52	R3	Výpadok uzla R3, odpojenie všetkých liniek
3	54	Linka R4-R5	Odpojenie linky
4	56	Linka R1-R4	Odpojenie linky
5	58	R3	Pripojenie všetkých odpojených linky

Tabuľka 6: Popis scenáru 3

Po simulácii výpadku smerovača R_3 (obrázok 39, výpadok A), $Source_1$ odošle dáta na adresu $Host_2$. Smerovač R1 zistí výpadok na výstupnom rozhraní originálnej cesty a zmení cieľovú IP adresu paketov na multicastovú IP (226.1.1.1). Alternatívna cesta, ktorá vznikne na základe pravidla prvého príchodu, je $R_1 \rightarrow R_4 \rightarrow R_5$ (tabuľka 7, riadky 9 až 16, riadky 25 až 28). Rozhrania na smerovačoch R_2, R_4, R_5 a R_6, ktoré príjmu nadbytočnú multicastovú komunikáciu, sa odhlásia od odberu multicastu správou PIMJoinPrune (tabuľka 7, riadky 19 až 24).



Obrázok 39: Viacnásobný výpadok liniek v rôznych časoch

Ďalej bude nasledovať výpadok linky medzi smerovačmi R_4 a R_5 (obrázok 39, výpadok B). Smerovač R_5 stratí RPF rozhranie prvého príchodu a musí odoslať správu PIMGraft všetkými výstupnými PIM rozhraniami (okrem pôvodného RPF rozhrania). V tomto prípade smerovač R_5 odošle správu PIMGraft smerovaču R_6 (tabuľka 7, modrá farba, riadok 31). Smerovač R_6 príjme správu PIMGraft, nastaví rozhranie eth_2 na stav forward a odošle správu PIMGraft RPF rozhraním nadradenému smerovaču R_4.

Smerovač R_4 príjme správu PIMGraft a nastaví rozhranie eth_4 na forward. Týmto spôsobom sa vytvorí nová alternatívna cesta $R_1 \rightarrow R_4 \rightarrow R_6 \rightarrow R_5$ a komunikácia bude opäť obnovená (tabuľka 7, zelená farba, riadky 35 až 39).

Posledný výpadok bude simulovaný na linke medzi smerovačmi R_1 a R_4 (obrázok 39, výpadok C). Tento výpadok zapríčiní, že v sieti bude existovať **len jedna cesta od zdroja k cieľu**. Ako v predchádzajúcom prípade, bude sa opakovať rovnaký princíp obnovenia alternatívnej cesty.

Smerovač R_4 zistí výpadok RPF rozhrania, čo znamená, že musí odoslať správu PIMGraft na všetky PIM výstupné rozhrania (okrem pôvodného RPF rozhrania), t.j. smerovačom R_2 a R_6 (tabuľka 7, modrá farba, riadky: 41, 44). Smerovač R_2 príjme správu PIMGraft, nastaví rozhranie eth_2 na stav forward a odošle správu PIMGraft smerovaču R_1. Smerovač R_1 po prijatí správy PIMGraft nastaví rozhranie eth_0 na stav forward. Alternatívna cesta od $Source_1$ k $Host_2$ sa obnoví a bude $R_1 \rightarrow R_2 \rightarrow R_4 \rightarrow R_6 \rightarrow R_5$ (tabuľka 7, zelená farba, riadky 49 až 54).

Č.	Čas (sims)	Akcia	Typ správy
1	50.00001162	Source1 --> R1	appData
2	50.00003497	R1 --> R3	appData
3	50.00005832	R3 --> R5	appData
4	50.00008167	R5 --> Host2	appData
5	51	Source1 --> R1	appData
6	51.00001173	R1 --> R3	appData
7	51.00002346	R3 --> R5	appData
8	51.00003519	R5 --> Host2	appData
9	52	Source1 --> R1	appData
10	52.00001173	R1 --> R2	appData
11	52.00001173	R1 --> R4	appData
12	52.00002346	R2 --> R4	appData
13	52.00002346	R4 --> R2	appData
14	52.00002346	R4 --> R5	appData
15	52.00002346	R4 --> R6	appData
16	52.00003519	R5 --> Host2	appData
17	52.00003519	R5 --> R6	appData
18	52.00003519	R6 --> R5	appData
19	52.000036099999	R2 --> R4	PIMJoinPrune
20	52.000036099999	R4 --> R2	PIMJoinPrune
21	52.000041909999	R2 --> R1	PIMJoinPrune
22	52.000047829999	R5 --> R6	PIMJoinPrune
23	52.000047829999	R6 --> R5	PIMJoinPrune
24	52.000053639999	R6 --> R4	PIMJoinPrune
25	53	Source1 --> R1	appData
26	53.00001173	R1 --> R4	appData
27	53.00002346	R4 --> R5	appData
28	53.00003519	R5 --> Host2	appData
29	54	Source1 --> R1	appData
30	54.00001173	R1 --> R4	appData
31	54.060855252323	R5 --> R6	PIMGraft
32	54.060861062323	R6 --> R5	PIMGraftAck
33	54.060872682323	R6 --> R4	PIMGraft
34	54.060878492323	R4 --> R6	PIMGraftAck
35	55	Source1 --> R1	appData

36	55.00001173	R1 --> R4	appData
37	55.00002346	R4 --> R6	appData
38	55.00003519	R6 --> R5	appData
39	55.00004692	R5 --> Host2	appData
40	56	Source1 --> R1	appData
41	56.088325558276	R4 --> R6	PIMGraft
42	56.088331368276	R6 --> R5	PIMGraft
43	56.088331368276	R6 --> R4	PIMGraftAck
44	56.088337178276	R4 --> R2	PIMGraft
45	56.088337178276	R5 --> R6	PIMGraftAck
46	56.088342988276	R2 --> R4	PIMGraftAck
47	56.088354608276	R2 --> R1	PIMGraft
48	56.088360418276	R1 --> R2	PIMGraftAck
49	57	Source1 --> R1	appData
50	57.00001173	R1 --> R2	appData
51	57.00002346	R2 --> R4	appData
52	57.00003519	R4 --> R6	appData
53	57.00004692	R6 --> R5	appData
54	57.00005865	R5 --> Host2	appData
55	58	Source1 --> R1	appData
56	58.00002335	R1 --> R3	appData
57	58.0000467	R3 --> R5	appData
58	58.00005843	R5 --> Host2	appData

Tabuľka 7: Priebeh komunikácie v sieti počas postupných výpadkoch

Výsledok simulácie bol podľa očakávaní a M-REP mechanizmus zotavil sieť aj po viacnásobnom výpadku v sieti.

5.4 Vyhodnotenie simulácií

V simulátore OMNeT++ bol otestovaný M-REP IPFRR mechanizmus na troch rôznych kritických situáciách zadefinovaných v troch scenároch s rôznymi úrovňami obťažnosti. Od scenára 1 s výpadkom jednej linky, cez scenár 2 s výpadkom celého smerovača až po scenár 3 s viacnásobným výpadkom liniek a smerovača. Všetky tieto scenáre môžu nastať aj v reálnej sieti. Vo všetkých scenároch bol najprv zaznamenaný tok komunikácie v skonvergovanej sieti pred zlyhaním linky, počas výpadku a teda konštrukcia záložného riešenia vo forme multicastového stromu, ako aj po obnovení pôvodnej originálnej cesty a návrat do východzieho stavu.

Priebeh a výsledky simulačných testov overili funkčnosť a implementovatelnosť nami navrhnutého IPFRR mechanizmu M-REP. Na základe ich výsledkov môžeme

konštatovať, že mechanizmus M-REP sa vo všetkých prípadoch správal podľa očakávania, t.j. vždy, ak existuje cesta do cieľa, mechanizmus M-REP ju nájde a vybuduje na nej multicastový distribučný strom, ktorým sa chránená prevádzka dostane až do cieľa. Mechanizmus M-REP sa osvedčil aj v prípade, keď sme simulovali postupné výpadky v sieti, čo predstavuje jeden z najťažších testov.

Existujúce IPFRR mechanizmy sa testujú len voči výpadkom liniek alebo smerovača v jednom okamihu. Je nutné podotknúť, že niektoré z existujúcich IPFRR mechanizmov by nedokázali zotaviť sieť po postupných výpadkoch (napr. RLFA [**30**]), ako je tomu v prípade mechanizmu M-REP.

Súčasné IPFRR mechanizmy majú alternatívnu cestu predpočítanú a po zistení výpadku linky prepnutie na alternatívnu trasu trvá minimálnu dobu. Navrhnutý M-REP IPFRR mechanizmus po zistení výpadku linky v reálnej sieti zapuzdri unicastovú komunikáciu na špecifický multicastový (Source, G) tok. Zapuzdrenie komunikácie na špecifickú multicastovú skupinu trvá takisto minimálny čas. Je nutné povedať, že princíp zapuzdrenia komunikácie využívajú aj niektoré z existujúcich IPFRR mechanizmov (napr. RLFA, Not-Via Addresses).

Princíp nášho mechanizmu M-REP v porovnaní s existujúcimi IPFRR mechanizmami je diametrálne odlišný. Treba zdôrazniť, že najdlhší čas pri existujúcich IPFRR mechanizmoch, ako aj pri mechanizme M-REP je vlastne daný detekciou výpadku linky na suseda. Táto však závisí od spôsobu prevedenia detekcie.

Na priloženom DVD (strana 114) nájdete všetky zdrojové súbory vrátane výstupov z jednotlivých simulácii. V práci sú simulácie realizované na testovacej topológii, ktorá obsahuje šesť smerovačov. Test na rozšírenej topológii s deviatimi smerovačmi je umiestnený na DVD.

6 PRÍNOSY DIZERTAČNEJ PRÁCE

Hlavný prínos nového M-REP IPFRR mechanizmu je skutočnosť, že nie je závislý na prípravných výpočtoch (pre-computing). Alternatívna cesta nie je vypočítaná vnútorným algoritmom, ako je to u konkurenčných IPFRR mechanizmov [**13**] [**30**] [**41**] [**75**] [**43**]. Vzhľadom na túto vlastnosť môžeme tvrdiť, že M-REP mechanizmus je v súčasnosti oproti analyzovaným riešeniam unikátny.

V porovnaní s existujúcimi IPFRR mechanizmami koncepcia M-REP mechanizmu prináša okrem spomínanej výhody aj radu ďalších. Prehľad výhod a nevýhod mechanizmu M-REP sumarizuje tabuľka 8.

Výhody	**Nevýhody**
+ Nezávislosť na prípravných výpočtoch	– Len v sieti s linkami typu bod-bod
+ Nezávislosť na veľkosti siete	– Náhodná cesta
+ Nezávislosť na smerovacích protokoloch	– Modifikácia paketov (tunelovanie)
+ 100% repair coverage	– Proces šírenia/odhlásenia v PIM-DM
+ Schopnosť riešiť viacnásobné výpadky	– Náhodná cesta
+ Relatívne jednoduchá implementácia	

Tabuľka 8: Výhody a nevýhody nového M-REP IPFRR mechanizmu

Z analýzy súčasných IPFRR mechanizmov v kapitole 2 vyplynulo, že iba niektoré existujúce IPFRR mechanizmy našli uplatnenie v operačných systémoch smerovačov. Vďaka využitiu existujúceho multicastového protokolu PIM-DM a jeho minimálnej modifikácii logiky RPF a použitia správ Graft je možné využiť nový M-REP IPFRR mechanizmus aj v reálnych zariadeniach.

V nasledujúcich podkapitolách sa budeme venovať jednotlivým prínosom dizertačnej prace, problémovým oblastiam a budúcnosti výskumu.

6.1 Nezávislosť na prípravných výpočtoch

Väčšina existujúcich IPFRR mechanizmov je založená na prípravných výpočtoch (pre-computing) alternatívnej cesty. **M-REP mechanizmus nevyžaduje prípravné výpočty alternatívnej cesty**. Používame špecifickú multicastovú adresu a proces

šírenia/odhlásenia (flooding/pruning) PIM-DM pre odoslanie chránenej komunikácie okolo zlyhanej linky alebo smerovača.

Pri existujúcich IPFRR mechanizmoch veľkosť siete vplýva na množstvo prípravných výpočtov, ktoré musia smerovače realizovať. To znamená, že s veľkosťou siete stúpa aj množstvo prípravných výpočtov pre výpočet alternatívnych ciest.

Ak by sme zobrali do úvahy mechanizmus LFA, autori v [**5**] uvádzajú, že špecifický smerovač s LFA vykoná rádovo *O(k)* výpočtov SPF, kde k je počet susedných smerovačov. Pri mechanizme RLFA podľa [**5**] môže smerovač s aktívnym RLFA vykonať až $O(k^2)$ výpočtov SPF. Z týchto faktov je zrejmé, že s rastúcim počtom smerovačov v sieti stúpa aj počet prípravných výpočtov.

Avšak navrhnutý M-REP IPFRR mechanizmus nevyžaduje prípravné výpočty, čo znamená, že **mechanizmus M-REP nie je vo svojom princípe ovplyvnený veľkosťou siete**.

6.2 Nezávislosť na smerovacích protokoloch

S prípravnými výpočtami (pre-computing) alternatívnej cesty súvisí aj závislosť na smerovacích protokoloch. Niektoré súčasné IPFRR mechanizmy vyžadujú pre výpočet alternatívnej cesty topologické informácie z link-state smerovacích protokolov. Sú teda závislé na link-state smerovacích protokoloch.

M-REP mechanizmus nevyžaduje prípravné výpočty alternatívnej cesty, ani pri konštrukcii multicastového distribučného stromu nevychádza zo smerovacej tabuľky, čo znamená, že je **nezávislý od smerovacieho protokolu**.

6.3 100% repair coverage

Ďalšou výhodou M-REP IPFRR mechanizmu je, že rieši problematiku viacnásobného zlyhania v sieti. Unicastový chránený tok, ktorý je zapuzdrený do špecifického multicastového toku, sa šíri po funkčných linkách.

Ak v sieti dôjde v jednom okamihu k veľkému výpadku liniek resp. smerovačov a bude existovať iba jedna možná cesta od zdroja k cieľu, M-REP mechanizmus túto cestu

nájde a použije. Inými slovami, nový M-REP mechanizmus poskytuje **100% repair coverage**.

6.4 Postupné výpadky liniek v sieti

Existujúce IPFRR mechanizmy sa testujú **najčastejšie voči výpadkom liniek alebo zariadení (smerovačov)** [**6**] [**45**]. V tejto dizertačnej práci sme ukázali, že navrhnutý mechanizmus M-REP dokáže poskytnúť vysokú mieru ochrany pred výpadkami liniek v sieti, a zamerali sme sa aj na simuláciu postupných výpadkov na alternatívnej trase. Simulácie v OMNeT++ preukázali, že **mechanizmus vie poskytnúť alternatívnu cestu po postupných výpadkoch liniek alebo smerovačov v sieti**.

6.5 Jednoduchá implementácia

M-REP IPFRR mechanizmus využíva existujúci multicastový protokol PIM-DM. Jednoduchou modifikáciou logiky pre výber RPF rozhrania ako aj modifikáciou používania správy Graft v tomto protokole sme využili jeho natívne správanie v novej oblasti IPFRR. Protokol PIM-DM je v súčasnosti podporovaný smerovačmi mnohých výrobcov. Jednou z výhod M-REP mechanizmu je preto jeho **jednoduchá implementácia**.

6.6 Problémové oblasti a budúcnosť výskumu

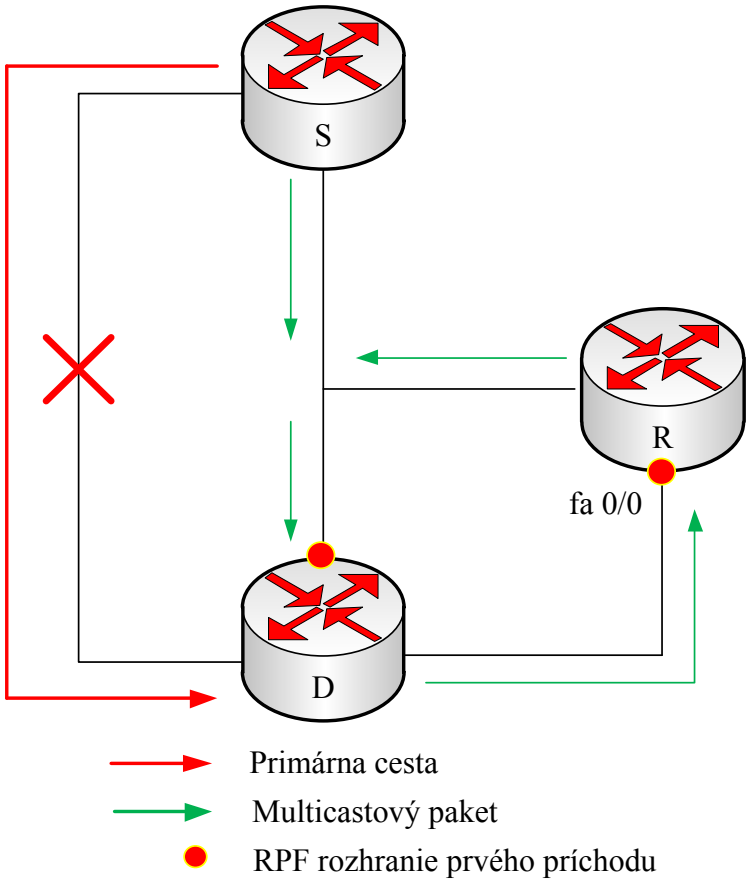
Problémové oblasti M-REP mechanizmu priamo súvisia aj so stanovenými požiadavkami na topológiu, v ktorej je mechanizmus M-REP použiteľný. Prvou požiadavkou na topológiu siete sú linky typu bod-bod medzi smerovačmi. Táto požiadavka nateraz vylučuje použitie M-REP IPFRR mechanizmu v sieťach s viacnásobným prístupom (tzv. multi-access siete). Prečo je to tak, vysvetlíme v nasledujúcej podkapitole.

6.6.1 Siete s viacnásobným prístupom

Nami navrhnutý mechanizmus využíva pozmenenú RPF logiku tak, že RPF rozhranie na smerovači je určené na základe pravidla prvého príchodu. To znamená, že pre našu špecifickú IPFRR multicastovú skupinu nevyužívame informácie z unicastovej smerovacej tabuľky. Tieto smerovacie informácie v smerovacej tabuľke sú založené na najkratších vzdialenostiach k cieľu. Ak by sme použili M-REP mechanizmus v sieťach s viacnásobným prístupom, mohlo by dôjsť k smerovacím slučkám.

Pri posielaní multicastových paketov na sieťach s viacnásobným prístupom je nutné jednoznačne vybrať len jeden smerovač, ktorý bude mať právo posielať multicastové pakety smerom k cieľu. Ostatné smerovače, ktoré sú na tejto sieti, nebudú môcť ďalej doručovať multicastové pakety.

Doručovanie multicastových paketov v sieťach s viacnásobným prístupom v protokole PIM-DM rieši mechanizmus Assert. Tento mechanizmus vyberie len jeden smerovač z daného segmentu (nazýva sa Assert Winner), ktorý má právo doručovať multicastové dáta smerom k cieľu.



Obrázok 40: Vznik smerovacej slučky v sieti s viacnásobným prístupom

Máme danú topológiu na obrázku 40, kde smerovač S odošle IPFRR multicastový paket na sieť s viacnásobným prístupom. Ak by smerovač R prijal prvý IPFRR multicastový paket rozhraním fa 0/0 od smerovača D, podľa pravidla prvého príchodu by bolo toto rozhranie zvolené za RPF rozhranie. Medzi smerovačmi D a R by teda mohla vzniknúť smerovacia slučka.

Proces Assert by v tomto prípade vyberal doručovateľa na segment s viacnásobným prístupom zo smerovačov S a R. Podľa [**59**] víťaz procesu Assert je určený nasledovnými podmienkami:

1. Ak smerovače majú cesty ku zdroju multicastového vysielania s rovnakou metrikou, vyhráva ten, ktorý má cestu s najnižšou Administrative distance (AD).
2. Ak smerovače majú cesty k zdroju multicastu s rôznymi metrikami, vyhráva smerovač s najmenšou metrikou.
3. Ak majú smerovače rovnaké cesty k zdroju, vyhráva smerovač s najvyššou IP adresou.

Mechanizmus Assert využíva pre výber doručovateľa multicastovej komunikácie unicastové smerovacie informácie zo smerovacej tabuľky, ktoré sú založené na cenách liniek k zdroju multicastového vysielania. Tento výber je avšak v **rozpore** s naším výberom RPF rozhrania na základe prvého príchodu.

Preto si táto problematika vyžaduje v budúcnosti ďalšie skúmanie. Je nutné poznamenať, že aj niektoré existujúce IPFRR mechanizmy majú problémy v sieťach s viacnásobným prístupom, ako napr. Remote LFA [**30**].

6.6.2 Náhodná alternatívna cesta

Existujúce mechanizmy IPFRR používajú SPF algoritmus pre výpočet najkratšej alternatívnej cesty od zdroja k cieľu. Tieto výpočty vyžadujú výpočtový výkon smerovača, ale vypočítaná alternatívna cesta je najkratšou možnou cestou.

Originálny protokol PIM-DM vytvára stromy najkratších ciest (inak nazývané aj Shortest Path Tree - SPT). Vytvorenie týchto stromov najkratších ciest zabezpečuje mechanizmus RPF v PIM-DM.

RPF mechanizmus v mechanizme M-REP nevyužíva unicastové smerovacie informácie pre overovanie korektného RPF rozhrania, ale RPF rozhranie je zvolené na základe pravidla prvého príchodu multicastového paketu so špecifickou IPFRR multicastovou adresou. Multicastové pakety sa modifikovaným RPF mechanizmom dostanú do cieľa, avšak garancia najkratšej cesty nie je možná. Multicastové dáta sa môžu, ale nemusia dostať do cieľa najkratšou cestou.

Druhou požiadavkou M-REP IPFRR mechanizmu je, aby cieľový smerovač D mal na svojom výstupnom rozhraní priamo pripojenú cieľovú stanicu. Tejto stanici je doručovaný pôvodný unicastový tok dát. Cieľový smerovač je identifikovaný na základe tejto požiadavky. Inak povedané, cieľovým smerovačom D sa stane taký smerovač, ktorý bude mať priamo pripojenú cieľovú stanicu. Multicastový špecifický (Source, G) strom je vytvorený od zdroja multicastového vysielania po cieľový smerovač D.

6.6.3 Zapuzdrenie dát

Náš mechanizmus používa zapuzdrenie IPv4 unicastového paketu chráneného toku ďalšou IP hlavičkou (multicastové tunelovanie). V IPv6 môže byť využitý ten istý princíp alebo môže byť na tento účel navrhnutá nová IPv6 rozširujúca hlavička. Modifikácia originálnych paketov prináša so sebou rôzne problémy s MTU (navyšovanie veľkosti paketu o hlavičku multicastového tunela), zvýšenie výpočtovej náročnosti CPU smerovača a iné.

Avšak je nutné poznamenať, že väčšina existujúcich IPFRR mechanizmov (okrem klasického LFA a ECMP) takisto zapuzdruje komunikáciu, či modifikuje špecifické bity v hlavičke paketu. Modifikácia paketov je jedna z nevýhod IPFRR mechanizmov, ale v súčasnosti je táto technika najpoužívanejšia.

6.6.4 Proces šírenia/odhlásenia v PIM-DM

Protokol PIM-DM na začiatku multicastového vysielania rozposiela multicastové pakety všetkým smerovačom v administratívnej doméne (flooding proces). Smerovače, ktoré nemajú príjemcov pre túto multicastovú komunikáciu, sa odhlásia od príjmu (pruning proces). Okrem spomínaných procesov PIM-DM protokol posiela periodicky "Hello" správy ostatným smerovačom. Procesy šírenia a odhlásenia (flooding, pruning) sa v sieti periodicky opakujú pre každý multicastový distribučný strom, čo prináša nadbytočné zaťaženie na sieť.

Avšak M-REP IPFRR mechanizmus zapuzdruje chránenú unicastovú komunikáciu na špecifický multicastový (Source, G) tok len dovtedy, kým nie je proces konvergencie kompletný. Po dokončení procesu konvergencie v sieti, je smerovanie komunikácie riadené smerovacím protokolom.

6.7 Budúcnosť výskumu

Spoločnosti ako Cisco Systems alebo Juniper Network sa čoraz viac zaujímajú o technológie rýchleho zotavenia siete, pretože nároky na ISP sa stále zvyšujú. V budúcnosti

by sa mal výskum zamerať na ďalšie overenie navrhnutého mechanizmu M-REP, odstránenie jeho problémových oblastí a implementáciu do experimentálneho prostredia Quagga. Súčasné požiadavky M-REP mechanizmu na linky typu bod-bod alebo priamo pripojená cieľová stanica k špecifickému smerovaču môže byť v niektorých prípadoch limitujúca.

Mechanizmus M-REP je navrhnutý pre ochranu špecifického unicastového toku. Preto by sa mal výskum sústrediť aj na overenie, či je možné chrániť mechanizmom M-REP všetky toky, ktoré mali primárnu cestu cez zlyhanú linku resp. smerovač.

ZÁVER

Hlavným cieľom predkladanej dizertačnej práce bolo navrhnutie nového IPFRR mechanizmu s ohľadom na odstránenie niektorých problémových oblasti existujúcich IPFRR mechanizmov. Práca predstavuje nový M-REP IPFRR mechanizmus, ktorý vychádza z inovatívneho spôsobu využitia multicastového protokolu PIM-DM. Protokol PIM-DM na začiatku procesu šírenia multicastového vysielania (flooding) doručí multicastové dáta ku každému PIM smerovaču v sieti (nezávisle od výpadku). Práve túto špecifickú vlastnosť protokolu PIM-DM sme využili pri návrhu nového mechanizmu M-REP. Tento mechanizmus je primárne určený pre ochranu špecifického unicastového toku prostredníctvom výstavby záložného multicastového distribučného stromu, definovaného unikátnou multicastovou adresou.

Ako už bolo spomenuté v analýze dnešných IPFRR mechanizmov, väčšina mechanizmov v oblasti IPFRR vyžaduje prípravné výpočty alternatívnej trasy pre prípad rôznych zlyhaní liniek alebo smerovačov v sieti (pre-computing). Nutnosť vykonávania prípravných výpočtov spôsobuje neželané efekty ako napr. zaťaženie CPU smerovača, závislosť na link-state smerovacích protokoloch a iné.

M-REP mechanizmus nevyžaduje vykonávanie prípravných výpočtov záložnej cesty, pretože využíva proces záplavového šírenia multicastovej komunikácie v protokole PIM-DM. S ohľadom na špecifické podmienky a účel, v ktorých má tento mechanizmus pracovať, bolo nevyhnutné modifikovať RPF mechanizmus v PIM-DM. RPF rozhranie je zvolené na základe prvého príchodu paketu so špeciálnou multicastovou adresou. Všetky smerovače v administratívnej doméne musia mať práve jedno RPF rozhranie pre špecifický (Source, G) tok.

Protokol PIM-DM s modifikovaným RPF mechanizmom explicitne vytvára strom, čo znamená, že smerovacie slučky medzi smerovačmi nemôžu vzniknúť. Alternatívna cesta je vytvorená pravidlom prvého príchodu špecifického multicastového paketu. Zapuzdrovanie chránenej unicastovej komunikácie na multicastovú je realizované dovtedy, kým proces konvergencie v sieti nie je kompletný.

Nový M-REP IPFRR mechanizmus rieši problematiku vykonávania prípravných výpočtov existujúcich IPFRR mechanizmov, závislosti na smerovacích protokolov a problematiku viacnásobného výpadku v sieti, resp. postupných výpadkov. Ďalšou výhodou

je 100% repair coverage a možnosť jednoduchej implementácie do existujúcich operačných systémov smerovačov.

V práci sme poukázali aj na problémové oblasti nového M-REP IPFRR mechanizmu, ako je použitie len v topológiách s linkami typu bod-bod, náhodnosť identifikovanej alternatívnej cesty či problematika zapuzdrenia dát. Väčšina uvedených problémových oblastí sa týka aj existujúcich IPFRR mechanizmov.

Keďže originálny mechanizmus RPF v PIM-DM bol modifikovaný, v predloženej práci je predstavený formálny dôkaz, že navrhnutá modifikácia nespôsobí smerovaciu slučku. Okrem overenia matematickým dôkazom sme realizovali úspešné simulácie v simulačnom prostredí OMNeT++, čím sme overili implementovatelnosť a funkčnosť nového mechanizmu M-REP.

ZOZNAM POUŽITEJ LITERATÚRY

1. CISCO SYSTEMS. CCNP 1: Advanced Routing Companion Guide (Cisco Networking Academy Program), 2nd Edition. Cisco Press, 2004, s. 93-94 [cit. 2014-12-29]. ISBN: 1-58713-135-8. Dostupné z: http://www.ciscopress.com/store/ccnp-1-advanced-routing-companion-guide-cisco-networking-9781587131356

2. SHAND, M. S. BRYANT a CISCO SYSTEMS. IP Fast Reroute Framework [RFC 5714]. Internet Engineering Task Force, 2010, s. 1-12 [cit. 2014-09-25]. ISSN: 2070-1721. Dostupné z: https://tools.ietf.org/html/rfc5714

3. PALÚCH, S. Algoritmická teória grafov. Žilina: Žilinská univerzita, 2008, s. 71-82 [cit. 2014-08-10]. Dostupné z: http://frcatel.fri.uniza.sk/users/paluch/grafy.pdf

4. SHAND, M. S. BRYANT a CISCO SYSTEMS. A Framework for Loop-Free Convergence [RFC 5715]. IETF, 2010, s. 10-18 [cit. 2014-12-19]. ISSN: 2070-1721. Dostupné z: https://tools.ietf.org/html/rfc5715

5. GJOKA, M. V. RAM a X. YANG. Evaluation of IP Fast Reroute Proposals. University of California, Irvine: IEEE, 2007, s. 1-7 [cit. 2014-11-23]. ISBN: 1-4244-0613-7. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4268086

6. GJOKA, M. V. RAM a X. YANG. Evaluation of IP Fast Reroute Mechanisms. Irvine: University of California, 2007, s. 3-6 [cit. 2014-10-11]. Dostupné z: www.minasgjoka.com/papers/ipfrr06-slides.ppt

7. ANTONAKOPOULOS, S. Y. BEJERANO a P. KOPPOL. A simple IP fast reroute scheme for full coverage. Belgrade (Belgrade): IEEE, 27. 6. 2012, s. 1 [cit. 2014-11-05]. ISBN: 978-1-4577-0831-2. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6260822

8. SZILAGYI, P. a Z. TOTH. Design, Implementation and Evaluation of an IP Fast ReRoute Prototype. Budapest: Budapest University of Technology and Economics, 2008, s. 3-6 [cit. 2014-10-05]. Dostupné z: http://opti.tmit.bme.hu/~enyedi/ipfrr/tdk_szilagyi.pdf

9. KATZ, D. D. WARD a JUNIPER NETWORKS. Bidirectional Forwarding Detection (BFD) [RFC 5882]. Internet Engineering Task Force, 2010, s. 1-14 [cit. 2014-09-30]. ISSN: 2070-1721. Dostupné z: https://tools.ietf.org/html/rfc5882

10. CISCO SYSTEMS, INC. OSPF Support for Fast Hellos. Cisco Systems, 2005 [cit. 2014-12-12]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fasthelo.html#wp1027129

11. SCHOLL, T. a AT&T LABS. BFD (Bidirectional Forwarding Detection) Does it work and is it worth it? NANOG 45, 2009, s. 2-11 [cit. 2014-12-20]. Dostupné z: https://www.nanog.org/meetings/nanog45/presentations/Monday/Scholl_BFD_N45.pdf

12. ENYEDI, G. Novel Algorithms for IP Fast ReRoute. Budapest, Hungary: Department of Telecommunications and Media Informatics, 2011, s. 85-86 [cit. 2014-10-21]. Dostupné z: http://www.omikk.bme.hu/collections/phd/Villamosmernoki_es_Informatikai_Kar/2011/Enyedi_Gabor/ertekezes.pdf

13. ATLAS, ZININ a ALCATEL-LUCENT. Basic Specification for IP Fast Reroute: Loop-Free Alternates [RFC 5286]. Network Working Group, 2008, s. 1-20 [cit. 2014-09-28]. Dostupné z: http://tools.ietf.org/html/rfc5286

14. LAPPETELAINEN, A. Equal Cost Multipath Routing in IP Networks [Master's thesis]. Aalto University School of Science, 2011, s. 50-51 [cit. 2014-11-06]. Dostupné z: http://lib.tkk.fi/Dipl/2011/urn100416.pdf

15. PREVIDI, S. Fast Convergence and IP Fast Reroute. Bareclona, Spain: Cisco Systems, 2009, s. 3-28 [cit. 2014-09-26]. Dostupné z: http://files.netcore.be/Cisco%20Networkers%202009%20-%20All%20Sessions/Breakouts/BRKIPM/BRKIPM-3019/BRKIPM-3019.pdf

16. PREVIDI, S. IP Fast ReRoute Technologies. Cisco Systems, 2006, s. 2-11 [cit. 2014-11-10]. Dostupné z: http://www.apricot.net/apricot2006/slides/conf/thursday/Stefano_Previdi_IPFRR-Apricot.pdf

17. KVALBEIN, A. IP fast reroute - Solutions and challenges. Simula Research Laboratory, 2013, s. 2-4 [cit. 2014-09-26]. Dostupné z: folk.uio.no/amundk/frr_workshop/ipfrr.kvalbein.ppt

18. FRANCOIS, P. IP Fast ReRoute What should be done ? [IP-FRR Workshop]. Oslo: UCL INGI, 2007, s. 4-21 [cit. 2014-10-15]. Dostupné z: http://folk.uio.no/amundk/frr_workshop/ipfrr-ws-oslo-francois.pdf

19. FILSFILS, C. E. et al. Loop-Free Alternate (LFA) Applicability in Service Provider (SP) Networks. 2012, s. 1-8 [cit. 2015-01-10]. ISSN: 2070-1721. Dostupné z: https://tools.ietf.org/html/rfc6571

20. CSIKOR, L. a G. RETVARI. IP Fast Reroute with Remote Loop-Free Alternates: the Unit Link Cost Case. Budapest University of Technology and Economics: High Speed Networks Laboratory, Department of Telecommunications and Media Informatics, s. 1-2 [cit. 2014-08-16]. ISBN: 978-1-4673-2016-0. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6459750

21. CISCO SYSTEMS, INC. Remote Loop-Free Alternate - Fast Reroute. San Jose, CA 95134-1706: 2014, s. 5-8 [cit. 2014-11-13]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/wireless/asr_901/Configuration/Guide/b_asr901-scg/b_asr901-scg_chapter_0100111.pdf

22. CICO SYSTEMS. Routing Resiliency - Latest Enhancements. Cico Systems, 2010, s. 20 [cit. 2014-10-23]. Dostupné z: http://stor.balios.net/Live2011/BRKIPM-2000.pdf

23. CISCO SYSTEMS. OSPFv2 Loop-Free Alternate Fast Reroute. Cisco Systems, 2011, s. 3-4 [cit. 2014-10-23]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-3s/iro-lfa-frr-xe.pdf

24. JUNIPER NETWORKS. Understanding and Deploying Loop-Free Alternate. Juniper Networks, 2009, s. 5 [cit. 2014-10-23]. Dostupné z: http://kb.juniper.net/library/CUSTOMERSERVICE/GLOBAL_JTAC/technotes/8010056-001-EN.pdf

25. HOPS, C. a NEXTHOP TECHNOLOGIES. Analysis of an Equal-Cost Multi-Path Algorithm [RFC 2992]. Network Working Group, 2000, s. 1-6 [cit. 2014-12-05]. Dostupné z: http://tools.ietf.org/html/rfc2992

26. NEMETH, K. A. KOROSI a G. RETVARI. Optimal OSPF Traffic Engineering using Legacy Equal Cost Multipath Load Balancing. Brooklyn, NY: IFIP Networking

Conference, 2013, 2013, s. 1-7 [cit. 2014-10-30]. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6663529

27. ATLAS, A. a GOOGLE INC. U-turn Alternates for IP/LDP Fast-Reroute [draft-atlas-ip-local-protect-uturn-03]. Network Working Group, 2006, s. 1-12 [cit. 2014-09-10]. Dostupné z: http://tools.ietf.org/html/draft-atlas-ip-local-protect-uturn-03

28. YANG, X. a D. WETHERALL. Source Selectable Path Diversity via Routing Deflections. University of California, University of Washington: ACM New York, 2006, s. 1-2 [cit. 2014-11-10]. ISBN: 1-59593-308-5. Dostupné z: http://www.cc.gatech.edu/classes/AY2007/cs7260_spring/papers/deflections.pdf

29. ATLAS, A. et al. U-Turn Alternates for IP/LDP Local Protection. IETF-60 Routing Area WG, 2006, s. 14-15 [cit. 2014-11-06]. Dostupné z: http://www.ietf.org/proceedings/60/slides/rtgwg-1/rtgwg-1.ppt

30. BRYANT, S. et al. Remote Loop-Free Alternate Fast Re-Route [Internet-Draft]. Network Working Group, 2015, s. 1-23 [cit. 2015-01-11]. Dostupné z: https://tools.ietf.org/html/draft-ietf-rtgwg-remote-lfa-10

31. YANG, Y. M. XU a Q. LI. A Lightweight IP Fast Reroute Algorithm with Tunneling. Tsinghua University (Cape Town): Department of Computer Science & Technology, 2010, s. 1-4 [cit. 2014-10-16]. ISBN: 978-1-4244-6402-9. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5502386

32. BRYANT, S. et al. IP Fast Reroute using tunnels [Internet-Draft]. Network Working Group, 2007, s. 15-19 [cit. 2014-12-10]. Dostupné z: http://tools.ietf.org/html/draft-bryant-ipfrr-tunnels-03

33. JUNIPER NETWORKS. Configuring Remote LFA Backup Over LDP Tunnels in an IS-IS Network. 2014 [cit. 2014-11-13]. Dostupné z: http://www.juniper.net/documentation/en_US/junos14.2/topics/task/configuration/configuring-remote-lfa-over-ldp-in-isis-network.html

34. PAN, P. et al. Fast Reroute Extensions to RSVP-TE for LSP Tunnels [RFC 4090]. Network Working Group, 2005, s. 1-32 [cit. 2014-12-26]. Dostupné z: https://tools.ietf.org/html/rfc4090

35. JUNIPER NETWORKS. Constrained Shortest Path First. Juniper Networks, 2010 [cit. 2014-12-26]. Dostupné z: https://www.juniper.net/techpubs/software/junos-es/junos-es93/junos-es-swconfig-interfaces-and-routing/constrained-shortest-path-first.html

36. PIÓRO, M. et al. Optimized IP-based vs. explicit paths for one-to-one backup in MPLS fast reroute. Warsaw: IEEE, 2010, s. 1-6 [cit. 2015-01-08]. ISBN: 978-1-4244-6704-4. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5624923

37. CSE620. MPLS Part II - Recovery. 2011, s. 34 [cit. 2015-01-08]. Dostupné z: http://www.cse.buffalo.edu/~qiao/cse620/MPLS-II.pdf

38. PAPNEJA, R. et al. Methodology for Benchmarking MPLS Traffic Engineered (MPLS-TE) Fast Reroute Protection [RFC]. IETF, 2013, s. 1-29 [cit. 2014-12-11]. ISSN: 2070-1721. Dostupné z: https://tools.ietf.org/html/rfc6894

39. CISCO SYSTEMS. MPLS Traffic Engineering (TE)--Fast Reroute (FRR) Link and Node Protection. 2007 [cit. 2014-12-26]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/gslnh29.html

40. JUNIPER NETWORKS. MPLS Fast Reroute Network Operations Guide Junos OS. Juniper Networks, 2012 [cit. 2014-12-26]. Dostupné z: https://www.juniper.net/techpubs/en_US/junos12.1/information-products/topic-collections/nog-mpls-frr/index.html?topic-19291.html

41. BRYANT, S. et al. A Framework for IP and MPLS Fast Reroute Using Not-Via Addresses [RFC 6981]. Internet Engineering Task Force, 2013, s. 1-30 [cit. 2014-11-25]. ISSN: 2070-1721. Request for Comments: 6981. Dostupné z: https://tools.ietf.org/html/rfc6981

42. ENYEDI, G. et al. IP Fast ReRoute: Lightweight Not-Via without Additional Addresses. Rio de Janeiro: INFOCOM 2009, IEEE, s. 1-5 [cit. 2014-12-17]. ISBN: 978-1-4244-3512-8. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5062229

43. KVALBEIN, A. et al. Multiple Routing Configurations for Fast IP Network Recovery [Networking, IEEE/ACM Transactions]. Research Laboratory, Oslo, Norway, 2009, s.

1-13 [cit. 2014-09-08]. ISSN 1063-6692. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4579279

44. MEERAVALI, S. et al. Multiple Routing Configurations For Fast Ip Network Recovery. International Journal Of Engineering And Computer Science, 2013, s. 1-7 [cit. 2014-11-10]. ISSN: 2319-7242. Dostupné z: http://ijecs.in/issue/v2-i8/48%20ijecs.pdf

45. APELAND, O. K. a T. CICIC. Architecture and Performance of a Practical IP Fast Reroute Implementation. New Orleans, LO: Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE, 2008, s. 1-6 [cit. 2014-12-10]. ISBN: 978-1-4244-2324-8. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4698207

46. G. FINN, S. M. M. MDARD a R. A. BARRY. A Novel Approach to Automatic Protection Switching Using Trees. Montreal: Massachusetts Institute of Technology, 1997, s. 1-5 [cit. 2014-08-10]. ISBN: 0-7803-3925-8/97. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=605232

47. ENYEDI, G. et al. Algorithms for computing Maximally Redundant Trees for IP/LDP Fast-Reroute [Internet-Draft]. Arizona: University of Arizona, 2015, s. 1-19 [cit. 2015-04-04]. Dostupné z: https://tools.ietf.org/html/draft-ietf-rtgwg-mrt-frr-algorithm-03

48. MENTH, M. a W. BRAUN. Performance Comparison of Not-Via Addresses and Maximally Redundant Trees (MRTs). Germany: University of Tubingen, Department of Computer Science, 2013, s. 3 [cit. 2014-09-11]. ISBN 978-3-901882-50-0. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6572989

49. ITAI, A. a M. RODEH. The Multi-Tree Approach to Reliability in Distributed Networks. Academic Press, Inc. 1988, s. 1-17 [cit. 2014-11-28]. Dostupné z: http://www.cs.technion.ac.il/~itai/publications/TwoTrees/TwoTrees.pdf

50. PATEL, U. Redundant Trees for preplanned protection and multipath routing. CSC-772 Research Project Report,North Carolina State University, 2009 [cit. 2014-09-11]. Dostupné z: http://dutta.csc.ncsu.edu/csc772_fall09/wrap/Res_project/umang_Project_Report.pdf

51. ZHANG, W. et al. Linear time construction of redundant trees for recovery schemes enhancing QoP and QoS. INFOCOM, 2005, s. 1-8 [cit. 2014-11-28]. ISBN: 0-7803-8968-9. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1498553

52. CISCO SYSTEMS, INC. Multicast only Fast Re-Route. Cisco Systems, 2012 [cit. 2014-12-19]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_serv/configuration/xe-3s/asr1000/imc-serv-xe-3s-asr1000-book/imc_mofrr.html

53. KARAN, A. et al. Multicast only Fast Re-Route [draft-ietf-rtgwg-mofrr-06]. Network Working Group, 2015, s. 1-11 [cit. 2015-23-01]. Dostupné z: https://tools.ietf.org/html/draft-ietf-rtgwg-mofrr-06

54. JUNIPER NETWORKS, INC. Understanding Multicast-Only Fast Reroute. 2014 [cit. 2015-01-23]. Dostupné z: http://www.juniper.net/documentation/en_US/junos14.1/topics/concept/mcast-fast-reroute.html

55. SAE LOR, S. a M. RIO. Enhancing Repair Coverage of Loop-Free Alternates. University College London, 2010, s. 3 [cit. 2014-18-12]. Dostupné z: http://www.ee.ucl.ac.uk/lcs/previous/LCS2010/lens2010_submission_27.pdf

56. PORETSKY, S. et al. Benchmarking Terminology for Protection Performance [RFC 6414]. Internet Engineering Task Force, 2001, s. 1-30 [cit. 2014-12-11]. ISSN: 2070-1721. Dostupné z: https://tools.ietf.org/html/rfc6414

57. RIPE - RIPE NETWORK COORDINATION CENTRE. RIPE NCC Begins to Allocate IPv4 Address Space From the Last /8. NRO News, 2012 [cit. 2014-10-12]. Dostupné z: https://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8

58. DEERING, S. et al. Internet Protocol, Version 6 (IPv6) Specification [RFC 2460]. Internet Engineering Task Force, 1998, s. 4-24 [cit. 2014-10-15]. Dostupné z: http://www.ietf.org/rfc/rfc2460.txt

59. ADAMS, A. et al. Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised) [RFC 3973]. Network Working Group, 2005, s. 1-58 [cit. 2014-12-19]. Dostupné z: https://tools.ietf.org/html/rfc3973

60. DEERING, S. Host Extensions for IP Multicasting [RFC: 1112]. Stanford University: Network Working Group, 1989, s. 1-15 [cit. 2015-31]. Dostupné z: https://tools.ietf.org/rfc/rfc1112.txt

61. FENNER, B. et al. Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised) [RFC 4601]. Network Working Group, 2006, s. 4 [cit. 2015-01-03]. Dostupné z: https://tools.ietf.org/html/rfc4601

62. OMNET++ COMMUNITY. OMNeT++ Network Simulation Framework. 2013 [cit. 2014-12-30]. Dostupné z: http://www.omnetpp.org/

63. SIMULCRAFT INC. OMNEST - High-Performance Simulation for All Kinds of Networks. 2014 [cit. 2014-12-30]. Dostupné z: http://www.omnest.com/

64. OMNET++. INET Framework for OMNeT++. 2014 [cit. 2014-12-30]. Dostupné z: http://inet.omnetpp.org/

65. FAKULTA INFORMAČNÝCH TECHNOLÓGII, VUT BRNO. Automated Network Simulation and Analysis. 2014 [cit. 2014-12-30]. Dostupné z: https://nes.fit.vutbr.cz/ansa/pmwiki.php/Main/HomePage

66. FAKULTA INFORMAČNÝCH TECHNOLÓGII VUT BRNO. ANSA extension above INET framework for OMNeT++. 2014 [cit. 2014-12-30]. Dostupné z: https://github.com/kvetak/ANSA

67. RYBOVÁ, V. Modelování multicastového směrování v prostředí OMNeT++. Brno: FIT VUT v Brně, 2012 [cit. 2014-10-15]. Dostupné z: http://www.fit.vutbr.cz/study/DP/DP.php?id=14139

68. Zebra. Free Software Foundation, Inc. 1999 [cit. 2015-01-28]. Dostupné z: https://www.gnu.org/software/zebra/

69. IPV6.CZ. Quagga. IPv6.cz, 2012 [cit. 2014-10-20]. Dostupné z: https://www.ipv6.cz/Quagga

70. Quagga Routing Suite [GPL licensed]. Quagga Routing Software Suite, 2013 [cit. 2014-10-18]. Dostupné z: http://www.nongnu.org/quagga/

71. FSF & GNU. GNU General Public License. 2014 [cit. 2015-01-02]. Dostupné z: http://www.gnu.org/copyleft/gpl.html

72. NSNAM. The Network Simulator - ns-2. 2009 [cit. 2014-01-02]. Dostupné z: http://www.isi.edu/nsnam/ns/

73. RUSSO, A. *Protocol Independent Multicast - Dense Mode for the ns-3 simulator*. 2013 [cit. 2015-01-02]. Dostupné z: https://github.com/trinacriax/pimdm

74. VARGA, A. INET Framework for OMNEST/OMNeT++. [cit. 2015-03-06]. Dostupné z: http://cs.txstate.edu/~qg11/2009nets/docs/inet/doc/walkthrough/tutorial.html

75. ATLAS, A. et al. An Architecture for IP/LDP Fast-Reroute Using Maximally Redundant Trees [Internet-Draft]. 2015, s. 1-36 [cit. 2015-03-15]. Dostupné z: https://tools.ietf.org/html/draft-ietf-rtgwg-mrt-frr-architecture-05

PRÍLOHY

Príloha A: Publikované články

1. **AFD** **IEEE**	Utilization of PIM-DM in IP Fast Reroute [Využitie PIM-DM v oblasti rýchleho zotavenia siete] / Jozef Papan, Pavel Segec, Peter Paluch. In: ICETA 2014 : 12th IEEE international conference on Emerging eLearning technologies and applications : December 4-5, 2014, Stary Smokovec, Slovakia. - [S.l.]: IEEE, 2014. - ISBN 978-1-4799-7739-0. - S. 373-378. [Papán Jozef (60%) - Segeč Pavel (20%) - Palúch Peter (20%)]
2. **AFD** **IEEE**	Tunnels in IP Fast Reroute [Technológia tunelov v rýchlom zotavení siete] / Jozef Papan, Pavel Segec, Peter Paluch. In: Digital technologies [elektronický zdroj] : the 10th international conference : 9-11 July 2014 Žilina, Slovakia. - [S.l.]: IEEE, 2014. - ISBN 978-1-4799-3301-3. - USB kľúč, s. 281-285. [Papán Jozef (60%) - Segeč Pavel (20%) - Palúch Peter (20%)]
3. **AFD** **IEEE**	Multicast in IP Fast Reroute [Technológia multicast v rýchlom zotavení siete] / Jozef Papan, Pavel Segec, Peter Paluch. In: ELEKTRO 2014 [elektronický zdroj] : proceedings of 10th international conference : Slovakia, May 19-20, 2014. - [S.l.]: IEEE, 2014. - ISBN 978-1-4799-3720-2. - CD-ROM, s. 81-85. [Papán Jozef (60%) - Segeč Pavel (20%) - Palúch Peter (20%)]
	Ohlasy:
	2014 [3] BAINGNE, M., PALANIVEL, K. Survey on fast IP network recovery. In (IJCSIT) International Journal of Computer Science and Information Technologies. ISSN 0975-9646, 2014, roč. 6, č. vol. 5 , 6, s. 8243-8245.
4. **AFD** **IEEE**	The integration of WebRTC and SIP: way of enhancing real-time, interactive multimedia communication [Integrácia WebRTC a SIP: rozšírenie interaktívnej komunikácie v reálnom čase] / Pavel Segeč ... [et al.]. In: ICETA 2014 : 12th IEEE international conference on Emerging eLearning technologies and applications : December 4-5, 2014, Stary Smokovec, Slovakia. - [S.l.]: IEEE, 2014. - ISBN 978-1-4799-7739-0. - S. 437-442. [Spoluautori: Palúch, Peter ; Papán, Jozef ; Kubina, Milan] [Segeč Pavel (70%) - Palúch Peter (10%) - Papán Jozef (10%) - Kubina Milan (10%)]
5. **AFC** **IEEE**	WSN for forest monitoring to prevent illegal logging / Jozef Papán, Matúš Jurečka, Jana Púchyová. In: FedCSIS [elektronický zdroj] : proceedings of the Federated conference on computer science and information systems : September 9-12, 2012, Wrocław, Poland. - [S.l.]: IEEE, 2012. - ISBN 978-83-60810-51-4. - USB kľúč, s. 809-812. - Spôsob prístupu: http://fedcsis.org/proceedings/fedcsis2012/pliks/208.pdf [Papán Jozef (30%) - Jurečka Matúš (35%) - Milanová Jana (35%)]

	Ohlasy:
	2014 [3] CZÚNI, L., VARGA, P.Z. Lightweight acoustic detection of logging in wireless sensor networks. In: SDIWC. [S.l. : s.n.], 2014. ISBN 978-0-9891305-6-1, 2014, s. 120-125.
	2014 [1] KOCHLÁŇ, M., MIČEK, J. Indoor propagation of 2.4GHz radio signal: Propagation models and experimental results. In: Digital technologies [USB] : the 10th international conference. [S.l.] : IEEE, 2014. ISBN 978-1-4799-3301-3, s. 136-140. SCOPUS
	2013 [3] KARPIŠ, O. Solar-cell based powering of a node for traffic monitoring. In IOSR Journal of Engineering. ISSN 2278-8719, 2013, vol. 3, iss. 4, s. 28-32.
	2013 [1] MARTINEZ, I. , RAMOS, V. Choosing a TCP version over static Ad Hoc wireless networks: Wired TCP or wireless TCP? In: Next Generation Mobile Applications, Services, and Technologies. [S.l..] : IEEE, 2013. ISBN 978-1-4799-2019-8, s. 170-174. SCOPUS
	2013 [4] ŠEVČÍK, P., KOVÁŘ, O. Power unit based on supercapacitors and solar cell module. In: SCIE-CONF 2013 : proceedings in scientific conference. Žilina : University of Žilina, 2013. ISBN 978-80-554-0726-5, s. 468-471.
6. AFD IEEE	Change of paradigm for development of software support for eLearning / Matilda Drozdová ... [et al.]. In: ICETA 2012 : 10th IEEE international conference on emerging eLearning technologies and applications : November 8-9, 2012, Stará Lesná, Slovakia. - [S.l.]: IEEE, 2012. - ISBN 978-1-4673-5123-2. - S. 81-84. Poznámka: Zborník vyšiel aj na CD-ROM s ISBN 978-1-4673-5121-8 [Spoluautori: Mokryš, Michal ; Kardoš, Martin; Kurillová, Zuzana ; Papán, Jozef] [Drozdová Matilda (30%) - Mokryš Michal (20%) - Kardoš Martin (20%) - Kurillová Zuzana (10%) - Papán Jozef (20%)]
	Ohlasy:
	2013 [1] BRDJANIN, D., MARIC, S. Model-driven techniques for data model synthesis. In: Electronics. ISSN 1450-5843, 2013, vol. 17, iss. 2, s. 130-136. SCOPUS

Príloha B: Obsah DVD

Priložené DVD obsahuje:

- Práca v elektronickej podobe (formát PDF)
- Simulátor OMNeT++ (verzia 4.5)
- Zdrojové kódy modifikovaného protokolu PIM-DM s knižnicou ANSA
- Realizované simulácie v OMNeT++