ŽILINSKÁ UNIVERZITA V ŽILINE

AUTOREFERÁT
DIZERTAČNEJ PRÁCE

Žilina, apríl 2015

Ing. Jozef Papán

Žilinská univerzita v Žiline
Fakulta riadenia a informatiky

Ing. Jozef Papán

Autoreferát dizertačnej práce

Rýchle zotavenie siete – IP Fast Reroute

na získanie akademického titulu **„philosophiae doctor“ (v skratke PhD.)**
v študijnom programe doktorandského štúdia
aplikovaná informatika

v študijnom odbore:
9.2.9 aplikovaná informatika

Žilina, apríl 2015

Dizertačná práca bola vypracovaná v dennej forme doktorandského štúdia na Katedre informačných sieti, Fakulte riadenia a informatiky Žilinskej univerzity v Žiline.

Školiteľ:	Doc. Ing. Pavel Segeč, PhD. Katedra informačných sieti Fakulta riadenia a informatiky Žilinská univerzita v Žiline
Školiteľ špecialista:	Ing, Peter Palúch, PhD. Katedra informačných sieti Fakulta riadenia a informatiky Žilinská univerzita v Žiline
Oponenti:	

Autoreferát bol rozoslaný dňa: .....

Obhajoba dizertačnej práce sa koná dňa ..... o ..... h. pred komisiou pre obhajobu dizertačnej práce schválenou odborovou komisiou v študijnom **odbore 9.2.9 aplikovaná informatika, v študijnom programe aplikovaná informatika**, vymenovanou dekanom Fakulty riadenia a informatiky Žilinskej univerzity v Žiline dňa .....

prof. Ing.Martin Klimo, PhD.
predseda odborovej komisie
študijného programu **aplikovaná informatika**
v študijnom odbore **9.2.9 aplikovaná informatika**
Fakulta riadenia a informatiky
Žilinská univerzita
Univerzitná 8215/1
010 26 Žilina

OBSAH

ÚVOD

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. Táto doba je závislá od viacerých faktorov, ako sú napríklad fyzická topológia siete, čas detekcie výpadku linky či suseda, ako aj od použitého typu smerovacieho protokolu a jeho vnútorného algoritmu výberu najkratších ciest. Počas procesu konvergencie siete 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, kde smerovače bez potreby dodatočnej technológie nad IP, alebo len s minimálnym nárokmi na dodatočné služby v IP sieti dokážu realizovať rýchle zotavenie.

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 súčasnosti existuje niekoľko funkčných IPFRR mechanizmov, ktoré využívajú rôzne metódy výpočtu náhradnej smerovacej cesty pre obídenie časti siete s výpadkom spojenia. Medzi najrozšírenejšie mechanizmy sa radia tie, ktoré využívajú alternatívny nasledujúci bezslučkový smerovač (tzv. next-hop smerovač) alebo využívajú tunelovanie sieťovej komunikácie.

V dizertačnej 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.

Dizertačná práca sa skladá z šiestich hlavných 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 dizertačnej práce je vytvorenie nového mechanizmu v oblasti rýchleho zotavenia siete.

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.

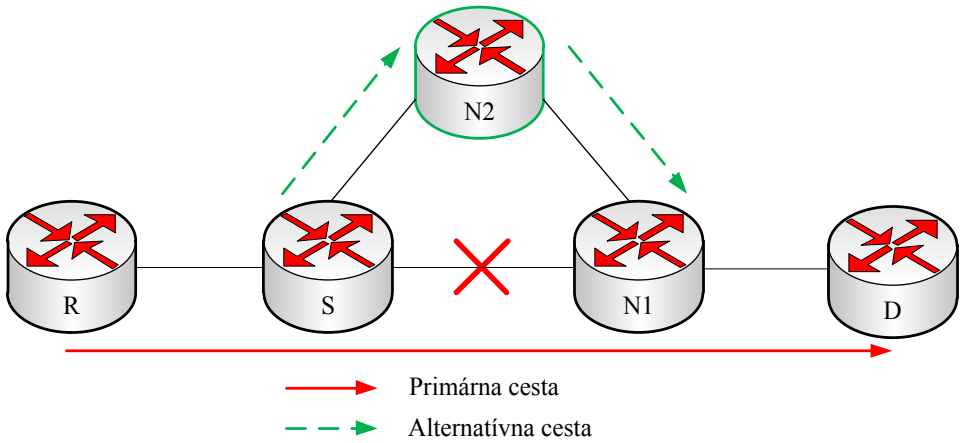
Piata kapitola ponúka matematické overenie a simulačné otestovanie funkčnosti návrhu M-REP IPFRR mechanizmu. Táto kapitola obsahuje matematicky dôkaz, ktorý dokázal korektnosť v práci navrhnutej modifikácie originálneho PIM RPF mechanizmu. Ďalej je v kapitole rozobraná problematika výberu vhodného simulačného nástroja, v ktorom bol navrhnutý mechanizmus testovaný v rôznych scenároch s výpadkami v sieti. Simulácie boli realizované v simulačnom nástroji OMNeT++.

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 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

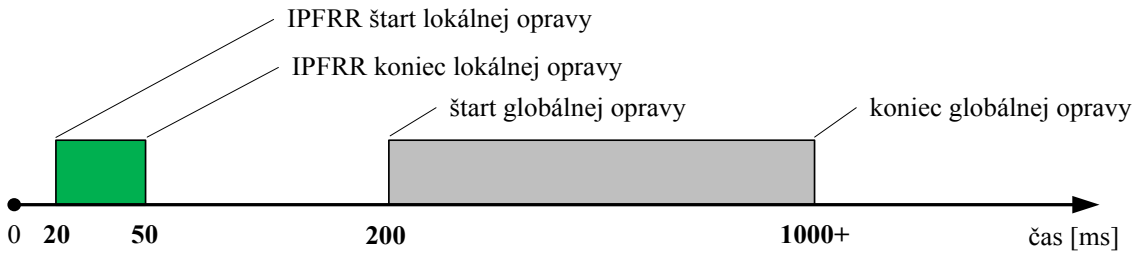
V oblasti IPFRR sa používajú špecifické označenia pre smerovače, ktoré majú špeciálny význam:

- **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** (**destination router**), je cieľovým smerovačom pôvodného toku dát.

Elementárny popis priebehu rýchleho zotavenia v sieti na smerovači S vyzerá 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)

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** [**1**] , [**2**], [**3**].

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**. V súčasnosti existujú viaceré mechanizmy IPFRR, ktoré sa vzájomne odlišujú spôsobom výpočtu záložných alternatívnych ciest. 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.

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.

2 ZHRNUTIE PROBLEMATIKY

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 Loop-Free Alternates (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. Nedá sa jednoznačne prehlásiť, ktorý z existujúcich IPFRR mechanizmov je najlepší. Každý z jednotlivých mechanizmov má svoje výhody a nevýhody.

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.

IPFRR mechanizmus	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.

2.1 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.

Prípravné 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?

2.2 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**.

3 CIELE PRÁCE

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 dizertačnej práce:

Hlavným cieľom 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

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 sme využili pri návrhu nového IPFRR mechanizmu.**

4.1 Modifikácia RPF

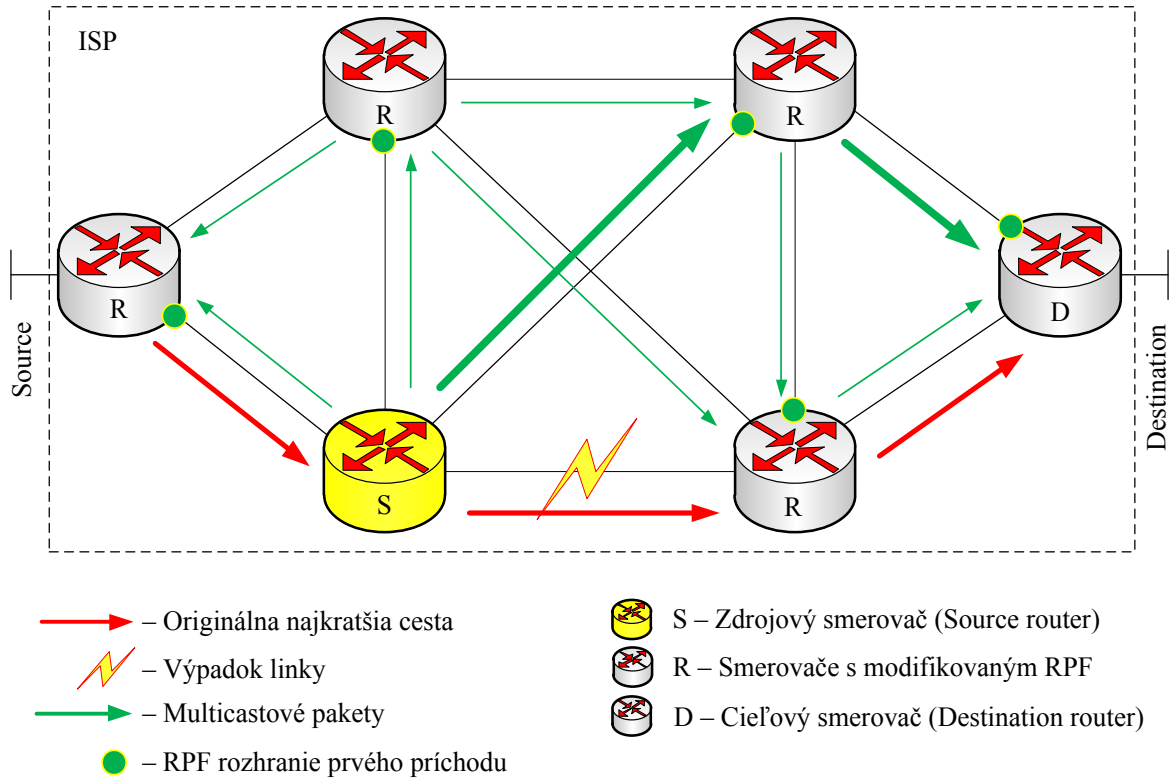
Originálne správanie sa RPF mechanizmu v PIM-DM **nie je vhodné** pre naše využitie v oblasti IPFRR. RPF mechanizmus v pôvodnom PIM-DM využíva informácie z unicastovej smerovacej tabuľky pre výber korektného RPF rozhrania pre špecifický multicastový (S, G) tok. Avšak v sieti, kde nastal výpadok linky 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 3).

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 3: Modifikované RPF v PIM-DM

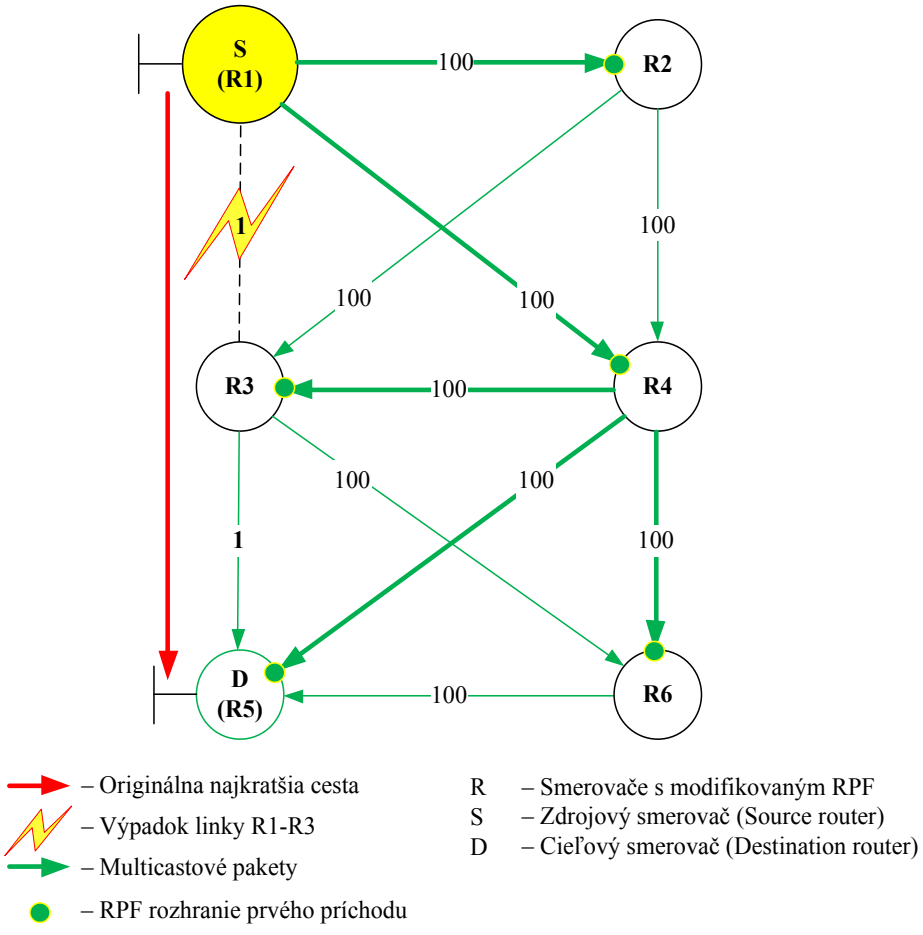
Od momentu, v ktorom nastane v sieti výpadok linky na pôvodnej najkratšej ceste medzi zdrojom a cieľom, smerovacie informácie v smerovacích tabuľkách smerovačov nie sú aktuálne. Dôsledkom je, že smerovače nemajú aktuálne informácie o korektnom RPF rozhraní, kým sa proces konvergencie unicastového smerovacieho 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 (obrázok 4).

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 hlavnej práci.

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.



Obrázok 4: Pravidlo prvého príchodu

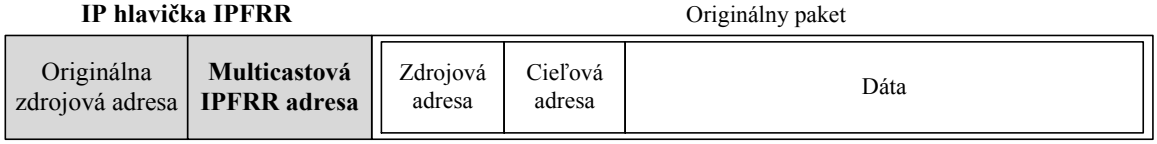
Zapuzdrené IPFRR pakety musia byť pri odchode z chránenej sieťovej domény opäť obnovené do originálneho stavu. Proces obnovenia komunikácie zaisťuje smerovač D, ktorý vykonáva potrebnú dekapsuláciu. To znamená, že koniec IPFRR multicastového toku je na tomto smerovači. Následne po tomto procese dekapsulácie 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 5). Zapuzdrenie unicastovej komunikácie s originálnou zdrojovou a novou multicastovou adresou zabezpečí, že takto upravená komunikácia je pripravená pre multicastový proces šírenia.



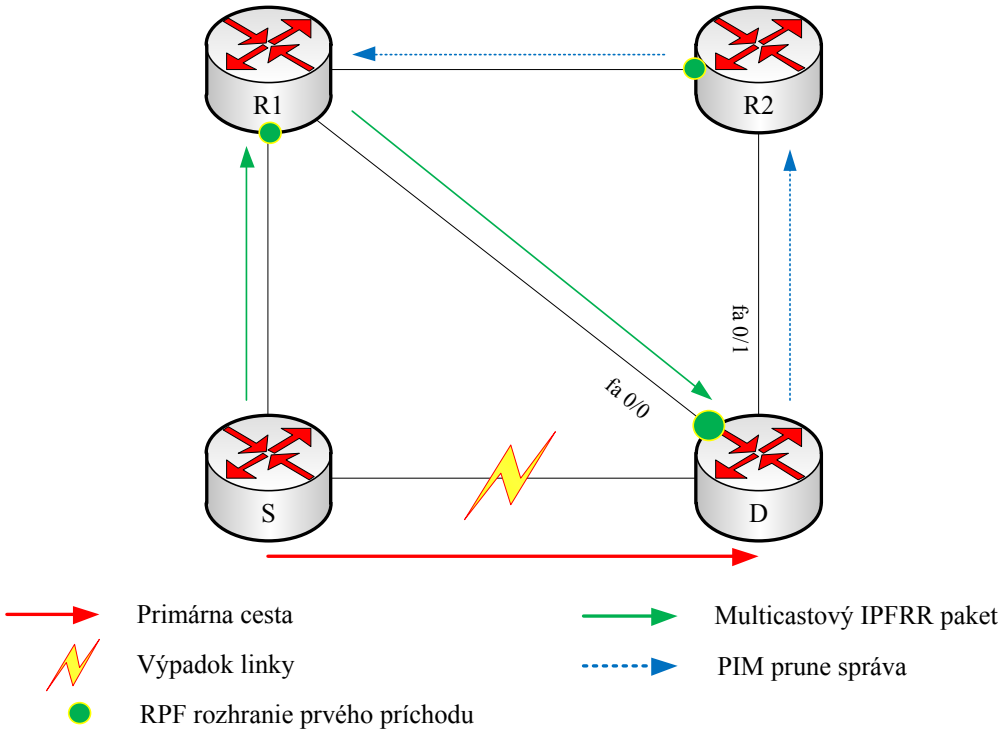
Obrázok 5: Zapuzdrenie unicastovej komunikácie

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 6, 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→R_1→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.

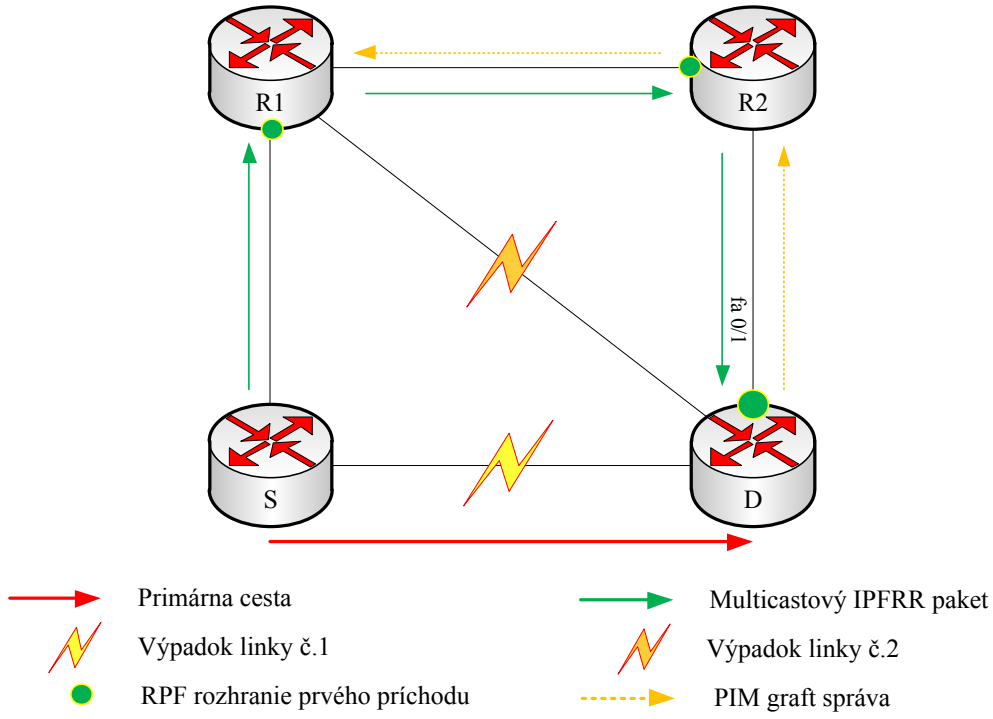


Obrázok 6: Viacnásobné zlyhanie liniek v rôznych časoch

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 7).



Obrázok 7: Odoslanie PIM graft správy

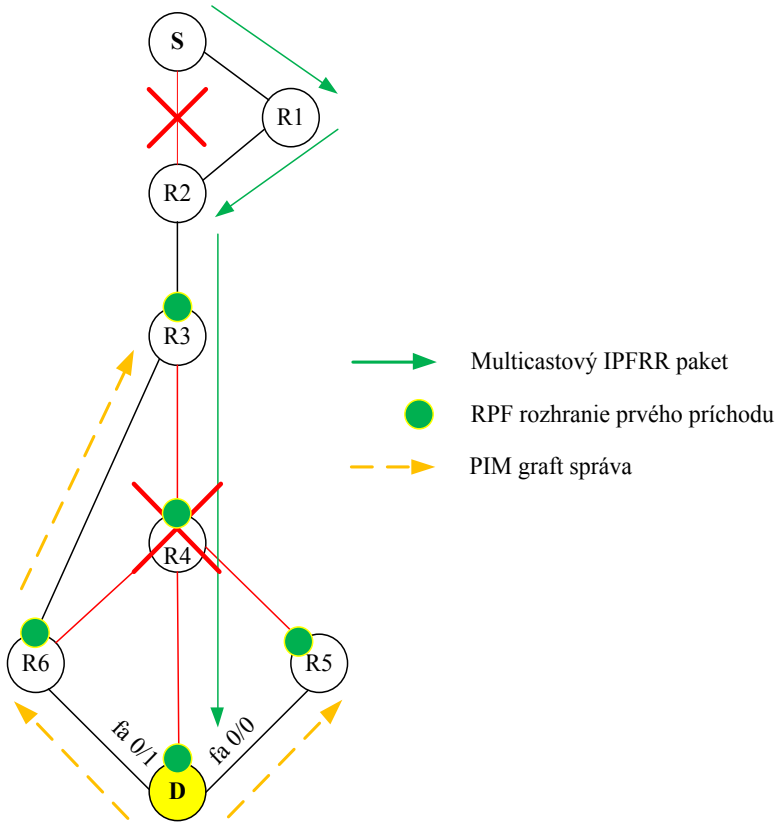
Protokol PIM-DM na re-inicializáciu distribučného stromu a pre zrušenie stavu odhlásenia používa správu Graft. V klasickom PIM-DM sa správa Graft posiela RPF rozhraním. V prípade nášho mechanizmu však musíme riešiť práve stratu RPF rozhrania, preto pravidlá pre použitie správy Graft budú v našom mechanizme 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 [**4**] odosiela RPF rozhraním pre špecifický (S, G) strom. V našom prípade (obrázok 7) 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 7), 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 $S \rightarrow R_1 \rightarrow R_2 \rightarrow D$.

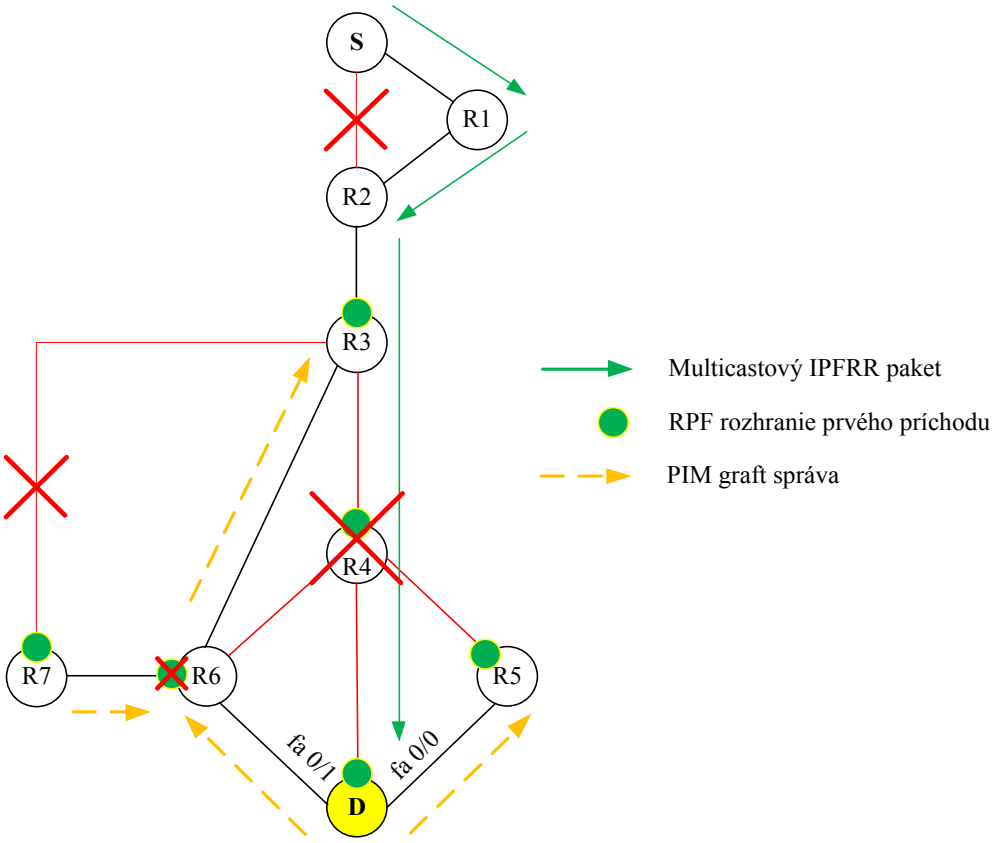
Ukážme si aplikáciu modifikovanej procedúry RPF a Graft mechanizmu M-REP na nasledujúcom zložitejšom príklade. Majme danú topológiu podľa obrázku 8, kde nastane prvý výpadok linky na smerovači R_2. Smerovač, ktorý zistí tento výpadok, sa stane smerovačom S a začne zapuzdrovať unicastovú komunikáciu na 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 8: 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 8 na topológiu v obrázku 9, 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 9: 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 Overenie riešenia

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 (dôkaz sporom).

Druhým krokom bolo overenie implementovatelnosti a funkčnosti navrhnutého M-REP IPFRR mechanizmu v simulátore OMNeT++.

Naším primárnym zámerom bolo testovanie mechanizmu na rôznych kritických situáciách, ktoré môžu nastať aj v reálnych podmienkach. Mechanizmus bol 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 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 [**5**] [**6**] [**7**] [**8**] [**9**]. 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 2.

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 2: Výhody a nevýhody nového M-REP IPFRR mechanizmu

Z analýzy súčasných IPFRR mechanizmov 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.

5.1 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 [**10**] uvádzajú, že špecifický smerovač s LFA vykoná rádovo $O(k)$ výpočtov SPF, kde k je počet susedných smerovačov. Pri mechanizme RLFA podľa [**10**] 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**.

5.2 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**.

5.3 100% 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**.

5.4 Postupné výpadky liniek v sieti

Existujúce IPFRR mechanizmy sa testujú **najčastejšie voči výpadkom liniek alebo zariadení (smerovačov)** [**1**] [**11**]. V 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**.

5.5 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**.

5.6 Problémové oblasti a budúcnosť výskumu

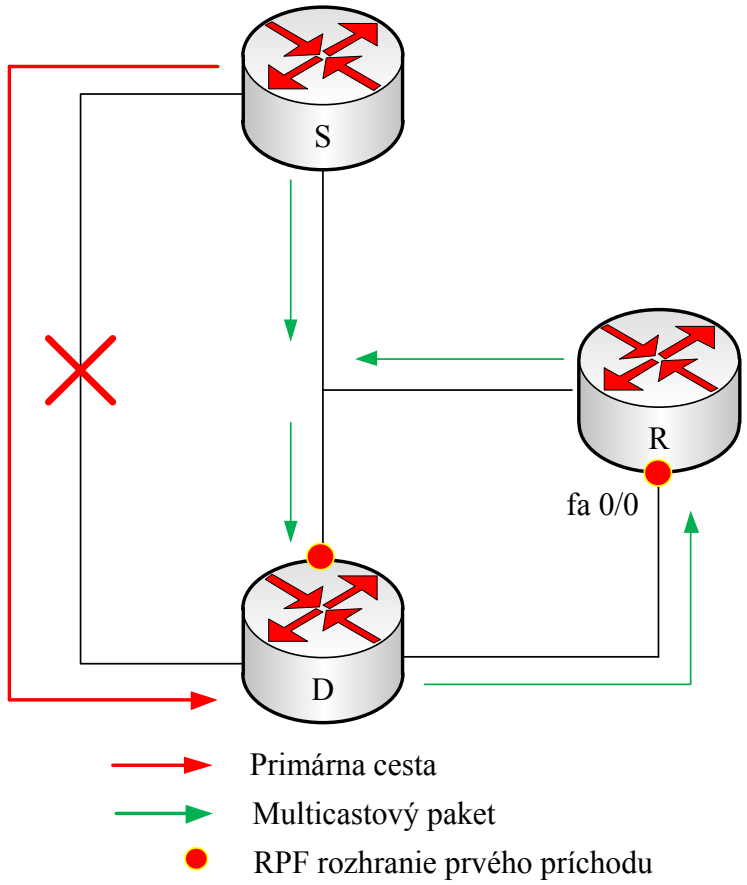
Problémové oblasti M-REP mechanizmu priamo súvisia aj so stanovenými požiadavkami na topológiu, v ktorej je mechanizmus M-REP použiteľný. Prvou požiadavkou na topológiu siete sú linky typu bod-bod medzi smerovačmi. Táto požiadavka nateraz vylučuje použitie M-REP IPFRR mechanizmu v sieťach s viacnásobným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

5.6.1 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 10: Vznik smerovacej slučky v sieti s viacnásobným prístupom

Máme danú topológiu na obrázku 10, 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 [**4**] 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 [**6**].

5.6.2 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.

5.6.3 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.

5.6.4 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.

5.7 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 dizertačnej 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.

PUBLIKOVANÉ ČLÁNKY

J. Papan, P. Segec, P. Paluch. **Utilization of PIM-DM in IP Fast Reroute**. ICETA 2014: 12th IEEE International Conference on Emerging eLearning Technologies and Applications, pp. 373–378, ISBN 978-1-4799-7739-0, 2014, IEEE.

J. Papan, P. Segec, P. Paluch. **Tunnels in IP Fast Reroute**. Digital Technologies: The 10th International Conference, pp. 281–285, ISBN 978-1-4799-3301-3, 2014, IEEE.

J. Papan, P. Segec, P. Paluch. **Multicast in IP Fast Reroute**. ELEKTRO 2014: Proceedings of 10th International Conference, pp. 81–85, ISBN 978-1-4799-3720-2, 2014, IEEE.

P. Segec, P. Paluch, J. Papan, M. Kubina. **The integration of WebRTC and SIP: Way of Enhancing Real-time, Interactive Multimedia Communication**. ICETA 2014: 12th IEEE International Conference on Emerging eLearning Technologies and Applications, pp. 437–442, ISBN 978-1-4799-7739-0, 2014, IEEE.

J. Papan, M. Jurecka, J. Milanova. **WSN for Forest Monitoring to Prevent Illegal Logging**. FedCSIS: Proceedings of the Federated Conference on Computer Science and Information Systems, pp. 809–812, ISBN 978-83-60810-51-4, 2012, IEEE.

M. Drozdova, M. Mokrys, M. Kardos, Z. Kurillova, J. Papan. **Change of Paradigm for Development of Software Support for eLearning**. ICETA 2012: 10th IEEE International Conference on Emerging eLearning Technologies and Applications, ISBN 978-1-4673-5123-2, 2012, IEEE.

ZOZNAM DÔLEŽITEJ LITERATÚRY

1. 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
2. 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
3. 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
4. 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
5. 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
6. 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
7. 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
8. 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
9. 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
10. 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
11. 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
12. 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

13. 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

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

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

16. 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

17. 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

18. 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

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. 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

21. 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

22. 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

23. 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

24. 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

25. 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

26. 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