

Comparação entre abordagens *multi-hop* de IP Fast Reroute: E-CER nível SIG x ED-NotVia

Fernando Barreto, Emílio Carlos Gomes Wille e Luiz Nacamura Júnior

Resumo—As infraestruturas de rede IP necessitam de alta confiabilidade. Abordagens de *IP Fast Reroute* (IPFRR) auxiliam os protocolos de roteamento durante a ocorrência de falha com métodos rápidos de contorno de falha para amenizar a instabilidade causada pelo período de convergência. O *Esquema de Caminhos Emergenciais Rápidos* (E-CER), desenvolvido pelos autores, é uma abordagem IPFRR que se provou ser mais eficiente que a abordagem *NotVia*. Uma abordagem recente, nomeada *ED-NotVia*, aperfeiçoa o método *NotVia*. Esse artigo compara o E-CER e *ED-NotVia*, e os resultados revelam o E-CER mais robusto e com menos recursos necessários na tabela de encaminhamento que o *ED-NotVia*.

Palavras-Chave—OSPF, IP, roteamento, confiabilidade.

Abstract—The current IP network infrastructures require high reliability. IP Fast Reroute (IPFRR) approaches aid routing protocols during failure in order to reduce the instability from convergence period with a fast failure recovery method. The *Fast Emergency Paths Scheme* (E-CER), deployed by the authors, is an IPFRR approach which was proved to be more efficient than *NotVia*. A recent approach, named *ED-NotVia* improves *NotVia* failure recovery method. This article compares E-CER and *ED-NotVia* approach. The results reveal E-CER more robust and demands less resources in the forwarding table than *ED-NotVia*.

Keywords—OSPF, IP, rerouting, reliability.

I. INTRODUÇÃO

A maioria das infraestruturas de rede IP dos sistemas autônomos utilizam o *Open Shortest Path First* (OSPF) [1] como protocolo de roteamento. O seu objetivo é encontrar rotas para o tráfego passante na infraestrutura e ser capaz de encontrar novas rotas na presença de falhas. Um rompimento de enlace ou grupo de enlaces nomeado *Shared Risk Link Group* (SRLG), pane em um roteador, ou atividade de manutenção (ex: reinicialização de roteador) são considerados ocorrência de falha [11]. Um SRLG é um grupo de enlaces, onde a falha de um enlace deve ser tratada como uma falha do grupo de enlaces (ex: o corte de um conduto ou falha de uma interface de rede). Na ocorrência de falhas, o OSPF é sinalizado e reage para encontrar novas rotas, necessitando de vários segundos a minutos [2][11][13] para terminar o período de convergência e assim disponibilizar novas rotas. Durante esse período, grandes quantidades de pacotes são descartados devido a rotas inconsistentes. Alguns trabalhos procuraram reduzir o período de convergência do OSPF para centenas de milissegundos [2], no entanto essa abordagem pode ocasionar mais instabilidade se a falha for transitória ou de um roteador, causando instabilidades nas rotas [8]. Além disso, mesmo poucas centenas de milissegundos pode ocasionar degradação

em aplicações sensíveis ao tráfego como VoIP e Vídeo. Como a ocorrência de falhas é comum no dia a dia de operação de gerência de uma rede, e uma grande porcentagem delas corresponde a uma única falha (aproximadamente 70% das falhas) [11], lidar com esse quesito torna-se crucial para manter a confiabilidade da infraestrutura de rede IP. Para atender a esse problema, a IETF definiu um *framework* nomeado IPFRR [3], o qual propõe um esquema teórico para um ambiente de recuperação imediato (a partir do momento que o *hardware* sinaliza uma falha, em torno de 50ms), com rotas alternativas antecipadas para os tráfegos afetados pelo aparecimento de falha. Esse ambiente deve atuar até que o protocolo de roteamento, no caso o OSPF, termine seu período de convergência.

Dentre as abordagens consideradas IPFRR, temos a *Equal Cost Multi-Paths* (ECMP) [1], *Failure Insensitive Routing* (FIR) [13], *NotVia* [6], *Loop-Free Alternates* (LFA) [4], *Tunnels* [14] e *Multiple Routing Configurations* (MRC) [12]. Essas abordagens previamente adicionam informações extras na *Forwarding Information Base* (FIB) dos roteadores além de alterações no processo de encaminhamento dos mesmos. Essas informações na FIB são utilizadas em caso de falha para guiar os fluxos de pacotes comprometidos de forma a contornar a falha. Dentre as abordagens IPFRR citadas, ECMP e LFA são consideradas as mais simples e devem ser utilizadas quando for viável [3]. O ECMP permite o uso de rotas de recuperação com mesmo custo que a rota principal, no entanto essas rotas não devem conter o ponto de falha em seu caminho até o destino. O LFA procura identificar qual roteador vizinho consegue, a partir dele, ter uma rota capaz de contornar o ponto de falha. Na existência de uma falha, o LFA encaminha o fluxo de tráfego afetado para esse roteador vizinho. As abordagens ECMP e LFA não alcançam 100% de cobertura de falhas em uma topologia, e nesses casos o *framework* IPFRR recomenda uma abordagem *multi-hop*. Dentre as abordagens citadas, a abordagem *NotVia* [6] é a única abordagem *multi-hop* que consegue atingir 100% de cobertura para falha de um enlace, roteador ou SRLG.

A abordagem *NotVia* utiliza o conceito de endereço *not-via*, que indica um componente de rede (enlace ou roteador) a ser contornado quando estiver com falha. Todos os roteadores utilizam endereços *not-via* para cálculo de uma rota através do *Shortest Path First* (SPF) para contornar os componentes que eles representam. Para que um roteador consiga identificar qual endereço *not-via* deve ser utilizado na presença de falha adjacente, um campo adicional em cada entrada da FIB armazena a informação de *next-next-hop*. Essa informação revela qual o endereço *not-via* deve ser usado para encapsular os pacotes e desviá-los da falha. Os demais roteadores, ao

Fernando Barreto, Coordenadoria de Gestão e Tecnologia da Informação, Universidade Tecnológica Federal do Paraná, Apucarana (PR), Brasil, E-mail: fbarreto@utfpr.edu.br. Emílio C. G. Wille e Luiz Nacamura Jr., Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná, Curitiba (PR), Brasil, E-mail: ewille@utfpr.edu.br, nacamura@utfpr.edu.br.

receberem esse pacote encapsulado conseguem encaminhá-lo com base nas rotas já calculadas para esse endereço *not-via*. Mesmo sendo a única abordagem a atingir 100% de cobertura de falha, ela é dependente da técnica de encapsulamento, necessita de uma extensão relativamente grande na FIB (muitas entradas para endereços *not-via* e o uso do campo adicional *next-next-hop* por cada entrada na FIB). Também, define uma rota de recuperação mais longa que o necessário (ocasiona *loops* transitórios), pode causar congestionamentos (compromete tráfegos não afetados pela falha) e não considera a possibilidade de múltiplas falhas. Mesmo a ocorrência de múltiplas falhas sendo inferior a 30% [11] e o *framework* IPFRR não exigir que uma abordagem IPFRR lide com essa ocorrência, o fato de considerá-lo mostra-se importante para evitar que uma abordagem IPFRR cause mais instabilidades na rede devido a múltiplas ações de contorno de falha.

Um ambiente completo e robusto de IPFRR nomeado *Esquema de Caminhos Emergenciais Rápidos* (E-CER) [5] foi desenvolvido pelos autores deste artigo. O E-CER é capaz de atingir 100% de cobertura de falha, ser superior ao *NotVia* ao prover rotas de recuperação próximas das rotas das oferecidas pelo OSPF após o período de convergência [5], ser independente da técnica de encapsulamento, necessitar poucas informações extras na FIB, impedir o surgimento de congestionamentos e considerar a ocorrência de múltiplas falhas.

Várias abordagens tentam resolver esses problemas da abordagem *NotVia*, como [9] [10] [7]. A abordagem [9] melhora a eficiência do algoritmo *NotVia* porém consegue reduzir apenas uma parte dos endereços *notvia* na FIB. A abordagem [10] propõe o *Lightweight NotVia*, que usa o conceito de árvores redundantes para criar rotas de recuperação, conseguindo reduzir significativamente a quantidade de endereços *not-via* necessários na FIB, no entanto adiciona novos problemas de congestionamento com a duplicação dos pacotes *not-via* para diferentes rotas. A abordagem [7] apresenta o *ED-NotVia*, sendo essa abordagem mais promissora, pois além de aperfeiçoar o *NotVia* com rotas de recuperação curtas e sem *loops* transitórios, consegue ainda uma redução significativa da extensão necessária na FIB para os endereços *not-via*.

Este artigo apresenta o E-CER e o *ED-NotVia* e realiza uma comparação das abordagens. Na sequência, apresenta os resultados obtidos das abordagens comparando as rotas de recuperação geradas e a quantidade de informação extra adicionada na FIB. Os resultados da comparação são obtidos por meio de simulação utilizando configurações de topologias reais e artificiais (criadas por geradores de topologias).

II. ESQUEMA DE CAMINHOS EMERGENCIAIS RÁPIDOS

A abordagem E-CER, apresentada em [5], fornece uma solução completa de IPFRR. Cada roteador que executa o E-CER é nomeado roteador origem (*RO*). Em todos os níveis o E-CER simula uma falha adjacente e utiliza o *Incremental SPF (I-SPF)* [15] para encontrar a nova árvore de menores caminhos e a partir dela definir previamente uma rota de recuperação na FIB. Nessa busca, a abordagem sempre tenta contornar o roteador adjacente (*RA*), o que implica em contornar também o

enlace adjacente (*RO, RA*). Essa medida é necessária pois não há como identificar imediatamente se uma falha adjacente sinalizada pelo *hardware* é do (*RO,RA*) ou do *RA*. Caso o roteador destino (*RD*) seja o *RA*, então contorna-se o (*RO,RA*) apenas. Ao optar por contornar o *RA*, obtém-se uma solução com maior garantia de desvio de tráfego, além de ser a opção recomendada pelo *framework* IPFRR.

O E-CER foi planejado como uma adaptação do *framework* IPFRR definindo 3 níveis para obter as rotas de recuperação: ECMP, LFA e SIG. O Nível ECMP verifica se existe outra rota de mesmo custo que a rota original, mas que não utilize a falha adjacente. O Nível LFA adapta a abordagem original LFA [4] minimizando o custo do caminho obtido pela rota de recuperação considerando também o número de roteadores usados até o roteador destino (*RD*). O número de roteadores é considerado somente se existir uma ou mais rotas de recuperação com mesmo custo a partir do roteador vizinho. Em ambas as abordagens, o roteador vizinho já possui rotas OSPF que conseguem contornar a falha. Para maiores detalhes dos níveis ECMP e LFA ver [5].

Como o Nível SIG e o *ED-NotVia* enquadram-se no *multi-hop* do *framework* IPFRR, o presente artigo apresentará mais detalhes apenas do nível SIG para comparar com *ED-NotVia*.

Formulação 1 (E-CER - Nível SIG): Considere o processo de minimização

$$\begin{aligned} & \text{Min}(1000\text{DistRR}(RO, R_{TMP}) + \text{NumRotRR}(RO, R_{TMP})) \\ & \text{Sujeito a:} \\ & D_{OSPF}(R_{TMP}, RD) < D_{OSPF}(R_{TMP}, RO) + D_{OSPF}(RO, RD) \\ & RA \notin \text{Roteadores}_{OSPF}(R_{TMP}, RD), \text{ se } RA \neq RD \\ & \text{Enlaces}_{OSPF}(R_{TMP}, RD) \cap \begin{cases} \text{SRLG}(RO, RA) = \emptyset, \text{ se } RA = RD \\ \text{SRLG}(RA, ?) = \emptyset, \text{ se } RA \neq RD \end{cases} \end{aligned} \quad (1)$$

O Nível SIG procura encontrar um roteador, além do roteador vizinho, nomeado R_{TMP} , minimizando o custo da rota de recuperação (*DistRR*) de *RO* até R_{TMP} e considerando o número de roteadores na rota de recuperação (*NumRotRR*) de *RO* até R_{TMP} . O número de roteadores somente é considerado se existem múltiplas rotas de recuperação de mesmo custo devido ao fator de multiplicação 1000. Esse número é considerado suficiente, pois é improvável que exista mais de 1000 roteadores em uma rota de recuperação dentro de uma área do OSPF. Ao considerar o número de roteadores torna-se possível reduzir a quantidade de roteadores com informações extras na FIB. O processo de minimização tem como restrição o custo da rota original OSPF (D_{OSPF}) do R_{TMP} para o *RD*, devendo ser menor que o custo da rota de R_{TMP} até *RO* acrescido do custo da rota de *RO* até *RD* para evitar *loop* de roteamento. Além dessa restrição, se $RA \neq RD$, então $RA \notin$ aos roteadores da rota original OSPF (Roteadores_{OSPF}) de R_{TMP} até *RD*, o que evita o uso do *RA* na rota de recuperação. Caso exista SRLG, nenhum dos enlaces da rota original OSPF de R_{TMP} até *RD* deve pertencer ao grupo SRLG do (*RO,RA*), se $RA = RD$, ou SRLG do (*RA, ?*), onde *?* significa qualquer roteador adjacente ao *RA*, se $RA \neq RD$.

Para cada *RD* de nível SIG, encontra-se um R_{TMP} e consequentemente uma rota de recuperação de *RO* até R_{TMP} . Cada rota de recuperação para um *RD* possui um identificador

de 6 bits (detalhado mais adiante). Se existir uma mesma rota de recuperação para vários diferentes RDs então utiliza-se apenas uma única rota de recuperação com único identificador (para mais detalhes, ver seção *Extensão E-CER na FIB* em [5]). Para que os pacotes possam ser desviados de RO até R_{TMP} , a abordagem *E-CER* realiza uma marcação padronizada dos pacotes nomeada CER_Marca . Essa marca consiste de 16 bits divididos em 10 bits para identificar o RO (limita a 1024 roteadores por área OSPF, sendo suficiente, pois em situações reais, mais que 200 roteadores já produzem *overhead* de tráfego OSPF [16]) e 6 bits para identificar a rota de recuperação de RO até R_{TMP} (limita a 64 rotas de recuperação, sendo também suficiente uma vez que necessitou em média 16 identificadores por roteador e alguns roteadores necessitou-se de no máximo 40). No entanto, o E-CER pode ser adaptado para aumentar ou diminuir o número de bits entre os identificadores de RO e da rota de recuperação. Os campos utilizados para inserir a CER_Marca nos cabeçalhos dos pacotes IP são o *Fragment Offset* no IPv4 ou *Flow Label* no IPv6. Somente nos casos que esses campos estejam utilizados pelo protocolo IP (ver em [5]), adota-se a técnica de encapsulamento para então realizar a marcação.

Para que o processo de encaminhamento consiga direcionar um pacote marcado, existe um campo extra para indicar qual interface de rede (IR) deve ser utilizada, formando o par CER_Marca/IR . A IR consiste inicialmente de 8 bits, limitado a representar 256 interfaces por roteador (número considerado suficiente para os equipamentos atuais). Caso for necessário aumentar o número de bits de IR , o E-CER possibilita esse aumento dinamicamente conforme for necessário o que não influencia de forma significativa (ex: 2 bits já aumenta para 1024 interfaces) na quantidade de informações extras na FIB.

Para identificar qual CER_Marca o processo de encaminhamento no roteador RO deve utilizar, é adicionado um campo extra em cada entrada na tabela de encaminhamento de RO , nomeado Ref , que referencia qual CER_Marca/IR deverá ser aplicado se a rota original estiver comprometida. O campo Ref ocupa 1 byte, sendo suficiente para representar todas as marcas necessárias em um roteador, pois em média são necessários 4 bits por roteador e, em alguns casos apenas, no máximo 6 bits.

Os demais roteadores na rota de recuperação $\neq RO$ possuem na FIB o registro do par CER_Marca/IR . Para isso, cada roteador, além de efetuar o cálculo do nível SIG do seu roteador, simula o cálculo do nível SIG dos demais roteadores de rede e assim torna possível a identificação de quais CER_Marca/IR devem estar na sua FIB [5]. Cada roteador então terá apenas os registros de CER_Marca/IR necessários na FIB, e com isso os pacotes marcados com CER_Marca serão encaminhados pela IR para atingirem o R_{TMP} . A partir do R_{TMP} , os pacotes continuam marcados só que são encaminhados utilizando a rota OSPF original até atingir RD . Isso é possível pois os demais roteadores a partir de R_{TMP} até RD não possuem na FIB um registro da respectiva CER_Marca . Ao atingir RD , a marca é removida. A manutenção da marca de RO até RD tem por objetivo evitar a ocorrência de congestionamento, uma vez que ao encaminhar um pacote marcado e a fila da interface de rede estiver saturada, descarta-se o pacote marcado para evitar instabilidade em demais fluxos de tráfego não afetados pela

falha. A marca também tem por objetivo evitar instabilidades na rede através de múltiplas recuperações, que podem ser causadas por múltiplas falhas. Quando um roteador tenta encaminhar um pacote marcado e a interface de saída apresenta uma falha, o roteador descarta o pacote marcado pois indica a ocorrência de múltiplas falhas na topologia.

III. ED-NOTVIA

A abordagem *ED-NotVia*, descrita em [7], utiliza o mesmo procedimento de recuperação realizado pela abordagem *NotVia*, porém propõe melhorias que consistem de dois aperfeiçoamentos. O primeiro consiste em identificar apenas os endereços *not-via* necessários em cada roteador. Isso se justifica pelo fato de um roteador não necessitar de um endereço *not-via* se os pacotes encapsulados com esse endereço não o utilizarem em sua rota de recuperação. Para tanto, a abordagem *ED-NotVia* apresenta duas definições para que um roteador esteja de acordo com uma nomeada *Condição RS* [7]. Essa *Condição RS* basicamente possibilita que um roteador consiga identificar, em cada cálculo de árvore de menores caminhos que ele realiza para cada enlace ou roteador falho da topologia, quais endereços *not-via* o utilizam como rota de recuperação. Dessa forma, apenas os endereços *not-via* necessários são preenchidos na FIB.

O segundo aperfeiçoamento é a diminuição do caminho de recuperação necessário em relação ao *NotVia* original. Isso é possível realizando o desencapsulamento dos pacotes *not-via* antes de chegarem ao roteador que detém o endereço *not-via*, nomeado *Early Decapsulation*. Para tanto, o roteador deve, além da *Condição RS*, verificar se a rota original OSPF para o endereço *not-via* não contém a falha. A condição para essa verificação é apresentada na formulação abaixo.

Formulação 2 (Early Decapsulation): Considere a equação

$$\text{custo}(R,D) < \text{custo}(R,F) + \text{custo}(F,D) \quad (2)$$

A função $\text{custo}()$ retorna o custo da rota OSPF. R seria o roteador que verifica se pode ou não desencapsular pacotes com endereço *not-via*. F é o roteador considerado falho. D é o roteador destino.

Esses dois aperfeiçoamentos (*Condição RS* e *Early Decapsulation*) devem ser aplicados em conjunto e possibilitam reduzir o número de endereços *not-via* necessários para definir uma rota de recuperação. Isto é possível pois os demais roteadores a partir de R não precisam ter o endereço *not-via* na FIB, bastando encaminhar utilizando a rota original OSPF para D . No entanto, a abordagem não demonstra como um roteador identifica no processo de encaminhamento quando um endereço é ou não *not-via* para poder desencapsular os pacotes, uma vez que o roteador não tem essa informação da FIB. Para fins de implementação no simulador, realizamos essa identificação dos endereços *not-via* no simulador. A abordagem também deixa explícito que realiza contorno apenas do enlace adjacente, justificando que, pelo fato de 70% das falhas serem desse tipo [11], não contornam o roteador adjacente, contrariando as recomendações IPFRR [3]. No entanto, o *ED-NotVia* apresenta indícios de como realizar esse processo e a adotamos quando realizamos sua implementação no simulador para confrontar com o E-CER.

IV. E-CER (NÍVEL SIG) X ED-NOTVIA

O *ED-NotVia* melhora a abordagem *NotVia* reduzindo o tamanho da rota de recuperação percorrida e a quantidade de endereços *not-via* na FIB de cada roteador, no entanto depende da técnica de encapsulamento, não evita congestionamentos causados pelo desvio e não evita instabilidades na rede na presença de múltiplas falhas.

O E-CER de Nível SIG adota uma abordagem que independe da técnica de encapsulamento, obtém rotas de recuperação com extensão reduzida pelo processo de minimização, necessita de poucas informações extras na FIB para aplicar o roteamento dos pacotes, consegue evitar congestionamentos e consegue detectar a ocorrência de múltiplas falhas.

Os dois aperfeiçoamentos apresentados por *ED-NotVia* adotam regras semelhantes com as descritas pela abordagem E-CER de Nível SIG. Em ambas as abordagens os pacotes são desviados no roteador adjacente à falha e seguem pela rota de recuperação predefinida até atingir um roteador que, a partir dele, consegue encaminhar com rotas OSPF até o destino sem passar pelo ponto falho. A diferença entre as abordagens para guiar os pacotes na rota de recuperação até esse roteador está na metodologia de desvio. O E-CER realiza um processo de marcação com *CER_Marca* e o *ED-NotVia* realiza um processo de encapsulamento com endereço *not-via*. O processo de marcação do E-CER, ao contrário do *ED-NotVia*, evita uma possível fragmentação dos pacotes que ocorreria no encapsulamento se o tamanho original do pacote estiver próximo da *Maximum Transfer Unit* (MTU). O E-CER reusa a *CER_Marca* para evitar congestionamentos que possam ocorrer devido ao desvio do tráfego, descartando-os para evitar instabilidades em fluxos de tráfego não afetados pela falha. Além disso, a *CER_Marca* é utilizada para detectar múltiplas falhas na topologia, e nesse caso, o E-CER atua descartando os pacotes marcados para evitar múltiplas recuperações de falha. Tanto o *NotVia* quanto o *ED-NotVia* não fornecem essas opções em suas abordagens de recuperação, e nesses casos, causam mais instabilidades durante o período de convergência do OSPF.

Ambas as abordagens necessitam de alterações no plano de roteamento e encaminhamento dos roteadores para que possam aplicar os seus métodos de recuperação de falha. Nesse quesito, a *ED-Notvia* apresenta a abordagem mais simplificada para ser implementada principalmente por utilizar sempre a técnica de encapsulamento (já está implementado no software dos roteadores), porém a abordagem E-CER pode ser mais econômica no uso de recursos na FIB, ser robusta e eficiente para criar uma rota de recuperação, além de evitar instabilidades nos fluxos dos demais tráfegos passantes.

A. Avaliação das Rotas de Recuperação e das Informações Extras na FIB

Tanto a E-CER de Nível SIG quanto *NotVia* e *ED-NotVia*, foram implementados como módulos no simulador J-Sim (<http://sites.google.com/site/jsimofficial/>). As abordagens foram adicionadas ao cálculo de rotas OSPF e ao processo de encaminhamento de pacotes. A escolha desse simulador deve-se ao fato do código fonte do OSPF ser portado do software de

roteamento GNU/Zebra, o qual possui um comportamento semelhante ao definido pela IETF [1]. Os resultados obtidos nessa avaliação são determinísticos devido aos resultados do cálculo de caminhos *I-SPF*, que é utilizado pelas abordagens.

Para fins de comparação com o E-CER, foi considerada uma taxa de cobertura de falha de 100% no algoritmo do *ED-NotVia*.

Foram utilizadas no simulador as mesmas topologias reais (Servint, Qwest, AT&T, AT Home, Abilene, GEANT2, AGIS e CAIS) e as 50 topologias com 32 roteadores e 64 enlaces obtidas pelo gerador *BRITE* (<http://www.cs.bu.edu/brite/>), utilizadas em [5]. Os custos dos enlaces das topologias foram definidos de acordo com a velocidade dos enlaces, como recomendado pela Cisco [16].

A primeira avaliação realizada corresponde ao comprimento das rotas de recuperação desde o roteador início do desvio até o roteador destino da topologia. A Tabela I apresenta o comprimento médio, mínimo e máximo obtido pelas rotas de recuperação para cada uma das topologias avaliadas. O comprimento mínimo em todas as abordagens é 2 por ser o menor número de uma abordagem *multi-hop* do *framework* IPFRR.

TABELA I. COMPRIMENTO DAS ROTAS DE RECUPERAÇÃO EM NÚMERO DE ROTEADORES

	E-CER			NotVia			ED-NotVia		
	Méd	Min	Max	Méd	Min	Max	Méd	Min	Max
Servint	4,4	2	10	4,6	2	12	4,4	2	10
Qwest	3,5	2	8	3,6	2	10	3,5	2	8
AT & T	3,6	2	7	3,8	2	8	3,6	2	7
ATHome	9,5	2	20	11,6	2	26	9,6	2	21
BRITE	3,3	2	6	3,4	2	7	3,3	2	6
Abilene	4,2	2	8	4,3	2	8	4,2	2	8
GEANT2	4,2	2	9	4,4	2	10	4,2	2	9
AGIS	8,0	2	19	9,4	2	24	8,1	2	20
CAIS	8,8	2	18	10,7	2	24	8,9	2	19

Na Tabela I, tanto o E-CER de Nível SIG quanto o *ED-NotVia* fornecem resultados parecidos por adotarem abordagens semelhantes (ver seção IV). A vantagem do E-CER ocorre em alguns casos onde existem múltiplas rotas de recuperação de *RO* até R_{TMP} com mesmo custo, pois o E-CER realiza um processo de minimização na escolha da rota de recuperação considerando o número de roteadores até R_{TMP} . Esses casos ocorrem com maior chance em topologias maiores devido à grande combinação de caminhos, o que justifica a leve vantagem do E-CER nas topologias AT Home, CAIS e AGIS.

A segunda avaliação realizada apresenta a quantidade de informações extras adicionadas na FIB, ou seja, além da tabela de encaminhamento já gerada pelo OSPF. Nessa avaliação a abordagem E-CER possui vantagem significativa sobre a *ED-NotVia* em todas as topologias, uma vez que essas informações são minimizadas na definição da *CER_Marca* quando comparado com a definição dos endereços *not-via*. A Tabela II apresenta a quantidade média de informações extras adicionadas por roteador nas topologias. Nessa tabela utiliza-se a seguinte nomenclatura: o número de entradas OSPF

existentes na FIB (nEO), *CER_Marca/IR* com 3 bytes (16 bits da marca + 1 byte do *IR*), *Ref* com 1 byte, 12 bytes para cada nova entrada na FIB (nFIB) referente aos endereços *not-via* [1], e cada *next-next-hop* (n-n-h) é um endereço IP com 4 bytes acrescidos em cada entrada OSPF na FIB [6][7].

V. CONCLUSÕES

Foi apresentado nesse artigo o funcionamento das abordagens de IPFRR: *E-CER* e *ED-NotVia*. O *E-CER* fornece uma abordagem completa que adapta o *framework* IPFRR de modo a produzir rotas de recuperação curtas e eficientes e com um processo de encaminhamento capaz de evitar instabilidades na rede decorrente do desvio do tráfego. É detalhado o nível SIG da abordagem *E-CER*, que pertence à definição *multi-hop* do *framework* IPFRR, a fim de comparar com a abordagem *ED-NotVia*. A abordagem *ED-NotVia* propõe melhorias na abordagem *NotVia* afim de reduzir a quantidade de informação extra na FIB e o comprimento das rotas de recuperação. Ao confrontar as duas abordagens, verificou-se que a *E-CER* de nível SIG consegue ter melhores resultados em termos de comprimento das rotas de recuperação quando existem múltiplas rotas de recuperação de mesmo custo e assim são minimizadas considerando a quantidade de roteadores. O *E-CER* também possui grande vantagem ao confrontar a quantidade de informações extras na FIB, pois o uso da marca *CER_Marca/IR* ocupa significativamente menos espaço que os endereços *not-via* da abordagem *ED-NotVia*. Ao contrário do *ED-NotVia*, o *E-CER* independe da técnica de encapsulamento, o que evita a chance de fragmentação de pacotes, impede a ocorrência de congestionamentos que possam ser causados pela rota de recuperação, e impede o surgimento de instabilidades na rede ao evitar múltiplas recuperações se existir várias falhas na topologia. O *E-CER*, no entanto, dependente atualmente do protocolo de roteamento OSPF, entretanto este é o protocolo de roteamento indicado pela IETF e mais adotado na prática.

REFERENCES

[1] J. Moy. "OSPF version 2". *Internet RFC* 2328, 1998.
 [2] P. Francois, C. Filfis, C. Evans, e O. Bonaventure. "Achieving subsecond IGP convergence in large IP networks". *In ACM SIGCOMM*, 2005.
 [3] M. Shand e S. Bryant. "IP Fast Reroute Framework". *Internet RFC* 5714. 2010.
 [4] A. Atlas e A. Zinin "Basic Specification for IP Fast-Reroute Loop-Free Alternate". *Internet RFC* 5286. 2008.
 [5] F. Barreto, E. C. G. Wille, L. Nacamura Jr, "E-CER: An Approach to Deviate Packets during Failure in IP Backbones with OSPF", *Revista IEEE América Latina*, 2009.
 [6] S. Bryant, M. Shand, e S. Previdi. "IP Fast Reroute Using Not-via Address". *Internet Draft. IETF Routing-WG*. 2010.
 [7] Q. Li, M. Xu, Q. Li, D. Wang e Y. Cui, "IP Fast Reroute: NotVia with Early Decapsulation", *IEEE Global Communication Conference (GLOBECOM)*, 2010.
 [8] A. Basu e J. F. Riecke, "Stability Issues in OSPF Routing". *SIGCOM Applications, Technologies, Architecture, and Protocols for Communications*. 2001.
 [9] A. Li, P. Francois e X. Yang, "On Improving the Efficiency and Manageability of NotVia", *ACM CoNEXT conference* , 2007.
 [10] G. Enyedi, G. Rétvári, P. Szilágyi e A. Császár, "IP Fast ReRoute: Lightweight Not-Via" *International Networking Conference*, 2009.
 [11] G. Iannaccone, C. Chuah, S. Bhattacharyya, e C. Diot. "Feasibility of IP Restoration in a Tier-1 Backbone". *IEEE Network Magazine*, 2004.
 [12] A. Kvalbein, A. F. Hansen, T. Cicic, S. Gjessing, e O. Lysne. "Fast IP Network Recovery using Multiple Routing Configurations". *IEEE INFOCOM Computer Communications*, 2006.
 [13] A. Nelakuditi, S. Lee, Y. Yu, e Z. Zang. "Fast Local Rerouting for Handling Transient Link Failures". *In IEEE Transactions on Networking*, 2007.
 [14] S. Bryant, S. FilsFils, S. Previdi, e M. Shand. "IP Fast Reroute Using Tunnels". *In Internet Draft. IETF Routing-WG*. 2005.
 [15] P. Narvaez, K. Y. Siu e H. Y. Tzeng, "New dynamic SPT algorithm based on a ball-and-string model", *IEEE Transactions on Networking*, 2001.
 [16] J. Doyle, CCIE Professional Development Routing TCP/IP – Volume1. Cisco Press, 1998.

TABELA II. INFORMAÇÕES EXTRAS ADICIONADAS NA FIB

	E-CER	NotVia	ED-NotVia
Servint	12(CER_Marca/IR) + nEO(Ref), Total: 36 + nEO bytes	58(nFIB) + nEO(n-n-h) , Total: 696 + 4(nEO) bytes	20(nFIB) + nEO(n-n-h), Total: 240 + 4(nEO) bytes
Qwest	10(CER_Marca/IR) + nEO(Ref), Total: 30 + nEO bytes	93(nFIB) + nEO(n-n-h) , Total: 1116 + 4(nEO) bytes	20(nFIB) + nEO(n-n-h), Total: 240 + 4(nEO) bytes
AT & T	11(CER_Marca/IR) + nEO(Ref), Total: 33 + nEO bytes	72(nFIB) + nEO(n-n-h), Total: 864 + 4(nEO) bytes	19(nFIB) + nEO(n-n-h), Total: 228 + 4(nEO) bytes
AT Home	36(CER_Marca/IR) + nEO(Ref), Total: 108 + nEO bytes	106(nFIB) + nEO(n-n-h), Total: 1272 + 4(nEO) bytes	53(nFIB) + nEO(n-n-h), Total: 636 + 4(nEO) bytes
BRITE	10(CER_Marca/IR) + nEO(Ref), Total: 30 + nEO bytes	128(nFIB) + nEO(n-n-h), Total: 1536 + 4(nEO) bytes	19(nFIB) + nEO(n-n-h), Total: 228 + 4(nEO) bytes
Abilene	9(CER_Marca/IR) + nEO(Ref), Total: 27 + nEO bytes	30(nFIB) + nEO(n-n-h), Total: 360 + 4(nEO) bytes	14(nFIB) + nEO(n-n-h), Total: 168 + 4(nEO) bytes
GEANT2	12(CER_Marca/IR) + nEO(Ref), Total: 36 + nEO bytes	76(nFIB) + nEO(n-n-h), Total: 912 + 4(nEO) bytes	20(nFIB) + nEO(n-n-h), Total: 240 + 4(nEO) bytes
AGIS	31(CER_Marca/IR) + nEO(Ref), Total: 93 + nEO bytes	149(nFIB) + nEO(n-n-h), Total: 1788 + 4(nEO) bytes	46(nFIB) + nEO(n-n-h), Total: 552 + 4(nEO) bytes
CAIS	30(CER_Marca/IR) + nEO(Ref), Total: 90 + nEO bytes	88(nFIB) + nEO(n-n-h), Total: 1056 + 4(nEO) bytes	45(nFIB) + nEO(n-n-h), Total: 540 + 4(nEO) bytes