IP Fast Reroute

Deniz Ugurlu
Betreuer: Nils Kammenhuber
Seminar Future Internet WS09/10
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München
Email: ugurlu@in.tum.de

***Kurzfassung*— Diese Arbeit beschreibt, wie lokaler Schutz für Datenverkehr in rein IP-basierten Netzwerken bei Auftreten einzelner Verbindungs- oder Routerausfälle erreicht werden kann. Das Ziel dabei ist, Ausfallzeiten und damit zusammenhängende Datenverluste im Falle solcher Fehler zu minimieren, während durch die Router neue optimale Pfade für die geänderte Netzwerktopologie berechnet werden. IP Fast Reroute beschreibt Techniken, welche ein schnelles Reagieren auf Ausfälle im Netzwerk durch Verwendung zuvor berechneter alternativer Next-Hops oder über Not-Via Adressen ermöglichen. Das Ausmaß des Schutzes (Node- und/oder Linkprotection) hängt dabei von der Topologie des jeweiligen Netzwerkes ab.**

***Schlüsselworte*— IPFRR, Fast Reroute, Link-Protection, Node-Protection, Micro Loop, Downstream Pfad**

I. Einleitung

Nach einer Verbindungsunterbrechung in rein IP-basierten Netzwerken benötigen Router mit aktuellen Methoden noch Zeiträume in der Größenordnung mehrerer hundert Millisekunden, um Reparaturpfade zu initialisieren und Daten über diese umzuleiten. Für z.B. multimediale Anwendungen wie VoIP oder Business-Lösungen reicht dies oft nicht aus, da diese empfindlich auf Datenverluste reagieren können, welche über zehntel Millisekunden hinausgehen.

Als IP Fast Reroute, folgend abgekürzt als IPFRR, werden Techniken bezeichnet, die eine möglichst schnelle Erholung von solchen Ausfällen ermöglichen. Dazu werden Alternativen für Verbindungen zwischen Routern berechnet, um Datenverkehr im Fehlerfall über diese abgespeicherten Reparaturpfade zu leiten. Andere Methoden verwenden Not-Via Adressen, um dadurch anzuzeigen, über welchen Punkt des Netzwerks ein Router, bei Störung einer gegebenen Verbindung, erreichbar ist. IPFRR dient dabei als übergangsweise Notlösung, während für die geänderte Netzwerktopologie neue optimale Pfade berechnet und eingesetzt werden können. Ziel beim Einsatz von IPFRR sind Datenverluste im Bereich von wenigen Zehntel Millisekunden.

Durch Verwendung alternativer Next-Hops soll ein Maximum an Fehlerfällen, etwa Link- oder Nodeausfälle, abgedeckt werden, wobei die Wahl der Absicherung von der Netzwerktopologie und dem aufgetretenen Fehler abhängt. Meist kann dadurch kein vollkommener Schutz eines Netzwerks gewährleistet werden.

Mittels der Not-Via Adressen hingegen ist eine Abdeckung von 100% des Netzwerkes möglich, allerdings wird hierfür ein deutlich höherer Rechenaufwand benötigt.

Im Folgenden wird in Abschnitt II die Terminologie erklärt, gefolgt von den unterschiedlichen Fehlerszenarios einschließlich der Zusammensetzung der Ausfallzeit in Abschnitt III. Die Abschnitte IV und V stellen IPFRR Verfahren im Detail vor, und veranschaulichen diese an ausgewählten Beispielen. Abschließend werden Vor- und Nachteile der Techniken gegenübergestellt und ein Ausblick auf die weitere Entwicklung gegeben.

II. Terminologie

Die in dieser Arbeit verwendeten Begriffe und Abkürzungen im Bezug auf IP Fast Reroute entsprechen den im IPFRR Framework von M. Shand und S. Bryant Eingeführten. [1]

Für den aktuell berechnenden Router, dem Ausgangspunkt also, wird die Bezeichnung S(ource), für den Router am Zielpunkt entsprechend D(estination) verwendet. Der primäre Next-Hop, also die Übertragung zum erste Knotenpunkt bzw. Router auf dem kürzesten Pfad von S zu D, wird als E notiert. Existieren mehrere kürzeste Pfade nennt man diese ECMP (equal cost multi-path) und deren primäre Next-Hops E1, E2, E3 etc. Der i-te Nachbar-Router zu S heißt Ni. Darüber hinaus werden die Abkürzungen LFA (loop-free alternate), SPF (shortest path first) und SPT (shortest path tree) verwendet. LFA steht dabei für einen kreisfreien Ersatz, dessen Berechnung und Funktionsweise in Abschnitt III erklärt wird. Mittels SPF werden von jedem Router individuell optimale Pfade aufgrund von Wegekosten bestimmt. Häufig wird dazu der Dijkstra-Algorithmus verwendet. Der resultierende Baum mit dem jeweils berechnenden Router als Wurzel ist der SPT. Um die optimale und kürzeste Distanz zwischen zwei Punkten A und B zu bestimmen, wird die Notation D_opt(A, B) eingeführt.

Abbildung 1 zeigt eine Beispieltopologie. Der kürzeste Pfad von S nach D läuft in diesem Fall über E.

III. Fehlerszenarios

IP Fast Reroute kann in einem Netzwerk Schutz gegen einzelne Ausfälle verschiedener Komponenten bieten. Dabei treten jedoch, abhängig von der Topologie des Netzwerks, unterschiedliche Problematiken auf, wenn maximaler Schutz gewährleistet werden soll. Um den Grad an Absicherung differenzieren zu können, werden verschiedene Arten von Fehlern unterschieden.

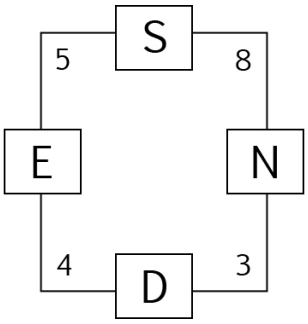

Abbildung 1. Einfache Topologie

A. Linkausfälle

Kommt es zum Ausfall einer Verbindung zwischen zwei Routern, also einem Linkausfall, gehen alle Daten verloren, welche weiterhin über diese Verbindung weitergeleitet werden.

B. Nodeausfälle

Von einem Nodeausfall spricht man, wenn ein Router nicht mehr erreichbar ist. Das führt dazu, dass alle Verbindungen zwischen diesem und anderen Routern oder Präfixen unterbrochen werden.

C. Fehlerdauer

Tritt einer dieser Fehler im Netzwerk auf, kommt es unwiederbringlich zu Verlust von Daten, da angrenzende Router den Fehler erst erkennen und dann den entsprechenden Datenverkehr umleiten müssen. Die Ausfallzeit setzt sich dabei aus den Zeiten zusammen, die vergehen, bis benachbarte Router den Fehler erkennen, den Ursprung identifizieren, die Informationen über den Fehler im Netzwerk verbreiten, neue SPF-Berechnungen durchführen und die Ergebnisse in den Routingtabellen installieren. Dabei entfallen weniger als 20ms auf das Feststellen des Fehlers, das Orten dauert unter 10ms. Bis die Information über die neue Topologie an alle Router im Netzwerk weitergeleitet, entsprechende SPF-Berechnungen neu durchgeführt und Routingtabellen aktualisiert wurden, verstreichen mit bisherigen Methoden mehrere 100ms, je nach Anzahl an Knoten und Präfixen. [2]

Mittels der IPFRR-Techniken soll an dieser Stelle erreicht werden, dass die Zeit nach dem Erkennen eines Fehlers bis zur Übernahme der SPF-Ergebnisse durch zuvor berechnete alternative Reparaturpfade ohne Datenverlust überbrückt werden kann.

IV. Loop Free Alternates

Tritt in einem Netzwerk ein Fehler auf, wird dieser zuerst von den direkt benachbarten Routern bemerkt. Unterstützen diese Router IPFRR, können deren gespeicherte Reparaturpfade verwendet werden, ohne dass andere Router über die Änderung informiert werden müssen.

Als Beispiel dient eine Topologie wie in Abbildung 1 zu sehen. Bei Berechnung des kürzesten Pfades von Router S zu D ergibt sich E als primärer Next-Hop. Da Router S IPFRR verwendet, versucht dieser, einen zusätzlichen alternativen Pfad zu D zu finden, bei dem die Verbindung zwischen S und E nicht durchlaufen wird. Ermöglicht wird das durch Router N. Kommt es zum Ausfall der Verbindung zwischen S und E und hat S dies bereits erkannt, wird der abgespeicherte alternative Next-Hop zu N als neuer primärer Next-Hop für Traffic mit Ziel D installiert. Diese Berechnung von alternativen Next-Hops wird analog von allen Routern und für alle Zieladressen durchgeführt.

A. Definition + Absicherung

Ein kreisfreier Pfad über einen alternativen Next-Hop (LFA) kann genau dann gefunden werden, wenn ein Nachbar des primären Next-Hop die Bedingung aus Ungleichung (1) erfüllt. [3]

$$D\_opt(N, D) < D\_opt(N, S) + D\_opt(S, D) \qquad (1)$$

Im o.g. Beispiel trifft dies auf Router N bereits zu, da $3 < 8 + 9$. Geht man aber von geänderten Wegekosten 30 zwischen N und D aus, ändert sich die Ungleichung zu $30 \not< 8+9$ und Router N kann keine Kreisfreiheit mehr garantieren. Alternative Next-Hops können einen unterschiedlichen Grad an Absicherung gegen Ausfälle bieten. Unterschieden wird dabei zwischen Absicherung gegen Verbindungsausfälle, was als Link-Protection bezeichnet wird, und Absicherung gegen Routerausfälle, auch Node-Protection genannt. Probleme bei Ausfällen können dann auftreten, wenn beispielsweise ein Routerausfall eintritt, der alternative Next-Hop aber nur Link-Protection bietet. In solchen Fällen können sich sogenannte Micro Loops bilden, bei denen Daten zwischen Routern im Kreis hin- und hergeleitet werden, bis diese verworfen werden.

B. Micro Loops

Anhand von Abbildung 2 lässt sich dies verdeutlichen.

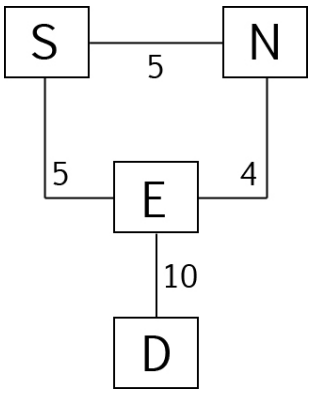

Abbildung 2. Entstehung von Micro Loops

Die Berechnung von Router S hat E als primären Next-Hop und N als alternativen Next-Hop zum Ergebnis. Diese werden abgespeichert und in seiner Routingtabelle eingetragen. Router N kann den Traffic dabei im Fall eines Verbindungsfehlers zwischen S und E absichern. Fällt aber Router E vollständig

aus, kann auch über den alternativen Next-Hop N keine Reparatur erfolgen. Tritt der Fall ein, dass E ausfällt, bemerken sowohl S als auch N dies und leiten ihren Traffic über die jeweils abgespeicherten Alternativen um. Das hat zur Konsequenz, dass S versucht, über N weiterzuleiten, während N versucht, Daten über S zu senden. Dieses Verhalten bezeichnet man als Micro Loop. [4]

Wie in [3] beschrieben, können nicht nur Fehler, die größere Ausmaße als geplant annehmen, sondern auch das gleichzeitige Auftreten mehrerer Fehler dazu führen, dass sich Micro Loops bilden, in denen Daten mit hoher Wahrscheinlichkeit verloren gehen.

1) Downstream Pfade: Eine Möglichkeit, die Bildung von Micro Loops zu verhindern, besteht darin, die Auswahl alternativer Next-Hops auf Router zu beschränken, welche sich auf Downstream Pfaden zwischen S und D befinden. Ein alternativer Next-Hop verläuft auf einem Downstream Pfad, falls Ungleichung (2) von dem Router erfüllt wird.

$$D\_opt(N, D) < D\_opt(N, S) + D\_opt(S, D) \qquad (2)$$

Alle Router entlang eines Downstream Pfades müssen also näher am Zielpunkt liegen bzw. haben geringere Wegekosten zum Ziel als ihr jeweiliger Vorgänger. Bezogen auf das Beispiel in Abbildung 2 bedeutet dies, dass von S zwar Router N als Downstream Alternative gewählt werden kann, jedoch umgekehrt N nicht S als Downstream Alternative verwenden darf. N hat deshalb keine Möglichkeit einen kreisfreien alternativen Next-Hop zu finden, weshalb der Traffic im Fehlerfall von N verworfen und die Entstehung eines Micro Loops verhindert wird. Es zeigt sich, dass in einem Netzwerk, in dem ausschließlich Downstream Pfade verwendet werden sollen, die Auswahl an alternativen Next-Hops drastisch eingeschränkt sein kann. Dadurch vermindert sich auch gleichzeitig die Anzahl an Reparaturwegen. Abgesehen von Downstream Pfaden bieten alternative Next-Hops mit Node-Protection eine weitere Möglichkeit, solche Micro Loops zu vermeiden.

C. Berechnung von Alternativen

Um für ein bestimmtes Ziel D eine LFA zu berechnen, benötigt ein Router diverse Informationen über kürzeste Pfade und deren Wegekosten. Die kürzeste Distanz zwischen S und D, D_opt(S, D), ist in der Regel nach der SPF-Berechnung durch das Routing-Protokoll direkt verfügbar. Entfernungen aus Sicht eines Nachbarrouters N, also D_opt(N, D) und D_opt(N, S), erhält man durch zusätzliche SPF-Berechnungen, welche aus Sicht von N durchgeführt werden. Das bedeutet, dass N als Wurzel des SPT angenommen wird und somit von N aus alle kürzesten Pfade im Netzwerk errechnet werden.

Um kreisfreie alternative Next-Hops nach [3] zu garantieren, muss mindestens Ungleichung (1) durch einen Nachbarrouter erfüllt sein. Dadurch wird sichergestellt, dass weitergeleiteter Traffic keinen Kreis bildet, falls eine Verbindung zwischen Routern ausfällt. Um gegen Ausfälle eines ganzen Routers E Schutz bieten zu können, ist es erforderlich, dass ein Nachbar N kreisfrei bezüglich E und D ist. Der Pfad von N zu D führt also nicht über E. Bietet N eine kreisfreie Alternative und wird zusätzlich Gleichung (3) erfüllt, nennt man N eine Node-Protecting LFA.

$$D\_opt(N, D) < D\_opt(N, E) + D\_opt(E, D) \qquad (3)$$

Wird hingegen Gleichung (4) erfüllt, ist es möglich, dass mehrere Pfade mit gleich niedrigen Wegekosten existieren. Es besteht somit auch die Möglichkeit, dass einer dieser Pfade Schutz bei Ausfall von E bietet. Gleich wahrscheinlich ist aber auch, dass ein anderer Pfad dies nicht gewährleistet. Da der berechnende Router keinerlei Einfluss auf die Wahl eines konkreten Pfades hat, muss davon ausgegangen werden, dass ein alternativer Next-Hop keine Node-Protection Eigenschaft besitzt, wenn Gleichung (3) erfüllt wird.

$$D\_opt(N, D) = D\_opt(N, E) + D\_opt(E, D) \qquad (4)$$

D. Equal-Cost Multipath

Existiert ein Equal-Cost Multipath (ECMP), folgt daraus, dass auch mehrere primäre Next-Hops verwendet werden, um Traffic zu einem bestimmten Ziel weiterzuleiten. Fällt einer dieser primären Next-Hops aus, sollte dessen alternativer Next-Hop verwendet werden. Die Alternative wiederum kann selbst einer der anderen primären Next-Hops sein, muss es aber nicht. Der Schutz anderer primärer Next-Hops reicht gegebenenfalls nicht aus, um den aktuell aufgetretenen Ausfall abzufangen.

In Abbildung 3 ist ein Aufbau mit drei primären Next-Hops E1, E2 und E3 zu sehen, bei denen sich die primären Next-Hops untereinander unterschiedlich starken Schutz bieten können.

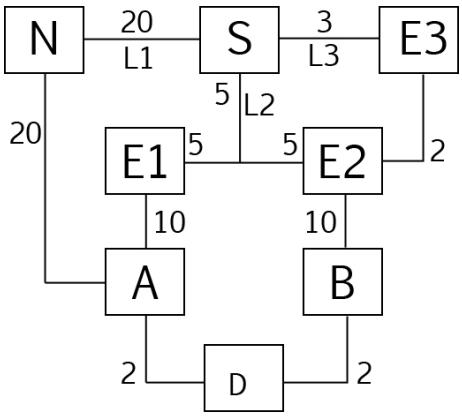

Abbildung 3. ECMP

Die Pfade über E1, E2 und E3 zu D bieten alle die selben Wegekosten. Die möglichen Absicherungen gegen Fehler verhalten sich dabei wie folgt:

- Der primäre Next-Hop L2 zu E1 kann von L3 zu E3, einem anderen primären Next-Hop, gegen Link- und Routerausfälle abgesichert werden.

- Verbindung L2 zu E2 wird von L2 zu E1 lediglich gegen Routerausfälle und durch L3 zu E3 gegen Linkausfälle abgesichert.
- L3 zu E3 kann von L2 zu E1 und auch L2 zu E2 gegen beide Fehlerarten geschützt werden.
- Mit L1 als alternativem Next-Hop werden sowohl für L2 zu E1 als auch für L2 zu E2 Link- und Routerausfälle abgedeckt.

E. Broadcast Links

Bei Punkt-zu-Punkt Interfaces gilt für kreisfreie alternative Next-Hops, dass ein Router mit Node-Protection Eigenschaft immer auch Link-Protection liefert. Ein Problem tritt allerdings bei sog. Broadcast Links auf, d.h. eine Verbindung von einem zu mehreren anderen Routern. Abbildung 4 zeigt eine Topologie, bei der von S ausgehend ein Broadcast Link zu N und E besteht. Dieser Link wird als Pseudonode(PN) dargestellt, dessen Wegekosten zu angrenzenden Routern 0 sind, um eine Berechnung von kreisfreien Alternativen zu ermöglichen.

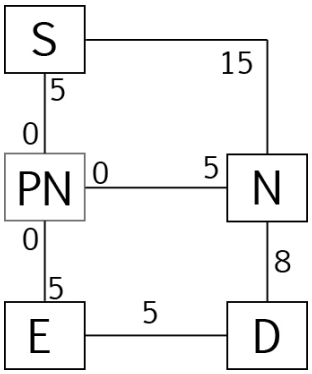

Abbildung 4. Broadcast Link

In Topologien mit Broadcast Links muss zur Untersuchung und zum Nachweis von möglichen Absicherungen eine genauere Betrachtung als bei simplen Punk-zu-Punkt Netzwerken erfolgen. Im o.g. Beispiel zeigt sich, dass Router N eine kreisfreie Link-Protecting Alternative bezüglich S und der Pseudonode darstellt. Allgemein lässt sich für einen Router N, der einen Broadcast Link kreisfrei absichern soll, folgende Bedingung aufstellen:

$$D\_opt(N, D) = D\_opt(N, PN) + D\_opt(PN, D) \qquad (5)$$

Der kürzeste Pfad der Pseudonode zu D verläuft über Router E, daher ist ein Nachbarrouter, der den Ausfall von E absichert, gleichzeitig auch kreisfreie Link-Protecting Alternative. Eine Ausnahme davon besteht nur, wenn der einzig mögliche Pfad von Router S zu Router N über die selbe Pseudonode führt. Dies ist der einzige Fall, in dem Node-Protection nicht aber Link-Protection durch einen Router vorliegt. Um in solch einer Topologie Absicherung gegen Verbindungsausfälle zu ermöglichen, ist es notwendig, dass sowohl der Pfad des ausgewählten alternativen Next-Hop als auch die Verbindung zwischen S und dieser Alternative nicht über den Broadcast Link verlaufen. Da bei Netzwerken mit Punkt-zu-Punkt Verbindungen Letzteres nicht möglich ist, muss für primäre Next-Hops, welche über Broadcast Links erreicht werden, bei der Auswahl der Alternativen beachtet werden, ob diese gegen Verbindungsausfälle absichern können. Anhand von Abbildung 4 kann dies beispielhaft erläutert werden.

Um über N gegen Verbindungsausfall des Broadcast Links abzusichern, darf der kürzeste Pfad von N nach D nicht über die Pseudonode verlaufen. Des Weiteren darf auch der von S gewählte alternative Next-Hop die Pseudonode nicht durchlaufen. Der kürzeste Pfad von S zu N verläuft im Beispiel allerdings über die Pseudonode, das heißt, S muss einen Next-Hop zu N finden, der die Pseudonode vermeidet, dafür aber höhere Wegekosten in Anspruch nehmen.

F. Auswahlverfahren

Bei der Auswahl der alternativen Next-Hops durch Router, welche die Spezifikation [3] unterstützen, soll für jeden primären Next-Hop versucht werden, mindestens eine LFA zu ermitteln. Gleichzeitig soll eine maximal mögliche Abdeckung von Fehlerfällen durch diese LFA erzielt werden. Dies wird dadurch erreicht, dass Router S bei der Berechnung diejenige LFA bevorzugt wählt, welche Node-Protection bietet. Ist solch eine LFA nicht verfügbar, kann eine kreisfreie Alternative gewählt werden, die Verbindungsausfälle absichert. Für den Fall, dass eine kreisfreie Alternative sowohl Link- als auch Node-Protection bietet, und eine zweite Alternative nur mit Node-Protection nicht aber Link-Protection zur Auswahl steht, sollte die Link- und Node-Protecting LFA von S gewählt werden.

Existieren mehrere primäre Next-Hops, sollte entweder einer der anderen primären Next-Hops oder eine kreisfreie Alternative mit Node-Protection als LFA gewählt werden. Ist solch eine Alternative nicht verfügbar und kann keiner der anderen primären Next-Hops die Verbindung schützen, sollte eine kreisfreie Alternative Link-Protection verwendet werden. Durch Anwendung dieser Priorisierung wird ein größtmöglicher Ausfallschutz ermöglicht.

G. Einsatzdauer der Reparaturpfade

Die Dauer, über die ein Router einen alternativen Next-Hop verwenden sollte, sobald sein primärer Next-Hop ausgefallen ist, muss begrenzt werden. Dadurch wird sichergestellt, dass die optimalen Pfade durch die SPF-Berechnung der geänderten Netzwerktopologie installiert und verwendet werden.

Bei der Umstellung der alternativen Next-Hops auf die neu berechneten primären Next-Hops muss jedoch beachtet werden, dass sich Micro Loops bilden können, wenn Router S den neuen primären Next-Hop sofort verwendet, während bei anderen Routern noch SPF-Berechnungen andauern. Geht man z.B. von einer Topologie wie in Abbildung 5 aus und die Verbindung von S zu E wird unterbrochen, kommt N1 als alternativer Next-Hop zum Einsatz.

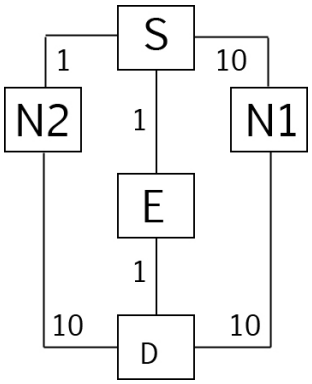

Abbildung 5. Einsatzdauer von LFAs

Bei der darauf folgenden SPF-Berechnung ergibt sich N2 als neuer primärer Next-Hop für das Ziel D. Wird in Router S sofort nach Berechnung N2 als neuer primärer Next-Hop installiert, ist es wahrscheinlich, dass bei N2 noch die primären Next-Hops der alten, fehlerfreien Topologie im Einsatz sind. Dies resultiert darin, dass S seinen Traffic für D über N2 weiterleitet, während bei N2 der optimale Pfad zu diesem Ziel noch über S installiert ist und somit ein Micro Loop entsteht. Dieser Kreis besteht solange, bis in N2 die aktualisierten primären Next-Hops übernommen wurden. Unter der Annahme nur einzeln auftretender Fehler kann solch ein Verhalten unterbunden werden, indem die Verwendung der neuen primären Next-Hops von Router S verzögert, und der Traffic solange weiter über die alternativen Next-Hops geleitet wird. Die alternativen Next-Hops können durch die neu Berechneten ersetzt werden, falls der neue primäre Next-Hop kreisfrei bezüglich der Topologie vor Auftreten des Fehlers ist oder eine vorher definierte Zeitspanne abgelaufen ist. Diese Zeitspanne sollte eine Obergrenze für die worst-case Laufzeit des Übergangs während der Netzwerkkonvergenz darstellen. Abgesehen davon kann der neue primäre Next-Hop sofort verwendet werden, falls der betroffene Router über einen unabhängigen neuen Fehler im Netzwerk informiert wurde.

H. Präfixe in Multihomed Netzwerken

Bei Multihomed Präfixen, d.h. Präfixe, die über mehrere verschiedene Router erreichbar sind, kann es bei der Berechnung der Alternativen zu einer nicht optimalen Lösung kommen.

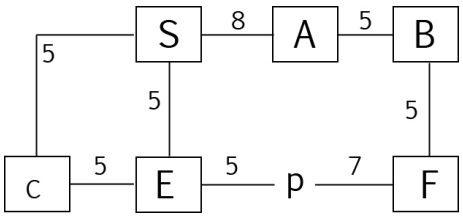

Abbildung 6. Multihomed Präfixe

Beispielsweise verläuft in Abbildung 6 der kürzeste Pfad zwischen S und p über Router E. Wird hierfür eine Alternative nur über den Router mit dem kürzesten Pfad zu p gesucht, erhält man C als LFA. Dieser ermöglicht Link-Protection, im Gegensatz zu A, welcher zwar einen längeren Pfad zu p hat, aber gegen kompletten Ausfall von E absichern kann. Daher ist es bei Multihomed Präfixen wichtig, alternative Pfade auch über alle anderen Router zu suchen, an welche das Präfix angeschlossen ist. Durch dieses Verhalten kann wieder maximal möglicher Schutz erreicht werden.

I. Sicherheit

Bei Verwendung der LFA Mechanismen für IP Fast Reroute werden keinerlei Änderungen an den Nachrichten des Routing-Protokolls vorgenommen. Es entstehen dadurch also keine zusätzlichen Sicherheitslücken bezüglich z.B. Paket-Änderungen oder Replay-Attacken. [3]

Auch die übergangsweise Verwendung von Next-Hop Routern, welche bei einer Änderung im Netzwerk ohne IPFRR nicht eingesetzt würden, kann nicht als zusätzliche Gefährdung betrachtet werden, da diese bei entsprechenden Ausfällen ohnehin verwendet werden. Mittels der beschriebenen Technik zur Verwendung von LFAs kann laut [1] in 80% der Fehlerfälle ein Reparaturpfad gefunden werden.

V. Not-Via Adressen

IPFRR mittels LFAs bietet keine Möglichkeit, den Ursprung eines Fehlers aufzuzeigen, an andere Router weiterzuleiten und Reparaturpfade explizit um diesen Punkt herum zu leiten. Dies beeinflusst auch die Abdeckung an Fehlerfällen in Abhängigkeit der Topologie eines Netzwerks.

Die im Folgenden vorgestellte Technik der Not-Via Adressen ermöglicht es, Pakete im Fehlerfall zu kapseln und an eine Netzwerkkomponente zu senden, welche vom betroffenen Router über seine Not-Via Adresse angegeben ist. Wird das Netzwerk durch den Ausfall nicht partitioniert, ist mit Hilfe von Not-Via Adressen in jedem Fall eine Reparatur möglich.

Not-Via Adressen werden von jedem Router in einem Netzwerk für jede Verbindung einzeln angegeben. So erhält ein Router B für die Verbindung zwischen A und B zusätzlich zu seiner regulären IP Adresse eine sog. Not-Via Adresse. Diese Adresse zeigt an, über welchen Knoten im Netzwerk Router B erreichbar ist, ohne dass die Verbindung von A zu B verwendet wird.

A. Berechnung mittels Not-Via Adressen

Bei diesem Mechanismus ist es notwendig, dass jeder Router für einen Ausfall jedes anderen Routers einen Pfad über dessen Not-Via Adresse berechnet, den er dann im Fehlerfall sofort verwenden kann. Dazu simuliert ein Router X nacheinander Ausfälle der anderen Router im Netzwerk und berechnet einen neuen SPF mittels der Not-Via Adresse. Für ein Netzwerk mit n Routern bedeutet dies, dass jeder Router n-1 zusätzliche SPF-Berechnungen durchführen muss, weshalb diese Methode vergleichsweise rechenintensiv ist.

In [2], [5] werden jedoch Optimierungen zur Reduzierung des Rechenaufwandes bei der alternativen Wegfindung vorgestellt. Dazu wird in einem ersten Schritt überprüft, ob die

zugehörige Verbindung der fraglichen Not-Via Adresse in der aktuellen Topologie verwendet wird. Ist dies nicht der Fall, muss natürlich keine neue Berechnung von kürzesten Pfaden hierfür erfolgen. Eine weitere deutliche Reduktion der Komplexität bietet der Einsatz des ISPF Algorithmus (Incremental SPF, [6]) in Verbindung mit vorzeitiger Terminierung statt einer normalen SPF-Berechnung.

Der ISPF Algorithmus berechnet lediglich diejenigen Pfade neu, welche von der vorliegenden Topologieänderung betroffen sind. Vorzeitige Terminierung bedeutet in diesem Zusammenhang, dass die Berechnung abgebrochen wird, sobald der Pfad zur Not-Via Adresse gefunden wurde.

Möchte man Not-Via Adressen und LFAs zusammen verwenden, existiert noch eine weitere Möglichkeit zur Optimierung. Für einen Link, welcher durch die Not-Via Adresse gesichert werden soll, kann überprüft werden, ob bereits ein LFA berechnet wurde, welcher statt der Not-Via Adresse zu Reparaturzwecken verwendet werden kann. [5]

B. Vor- und Nachteile

Es zeigt sich also, dass sowohl der Einsatz von LFAs als auch Not-Via Adressen Vor- und Nachteile hinsichtlich Ressourcenaufwand und Größenordnung der Absicherung besitzen. Soll ein Netzwerk ausschließlich mittels Not-Via Adressen abgesichert werden, beträgt der erforderliche Rechenaufwand in einem realen Umfeld (Backbone mit 600 Nodes, alle Links abgesichert) etwa das 15-fache eines vollständigen SPF. [5] Andererseits ist es dadurch möglich, 100% aller Verbindungen in allen Topologien abzusichern (Ausnahme: Partitionierung des Netzwerks durch den Ausfall).

LFAs bieten dagegen eine Absicherung von etwa 70-80%, der benötigte Aufwand bei deren Berechnung ist allerdings signifikant niedriger.

VI. Zusammenfassung und Ausblick

Aufgrund der Vor- und Nachteile von kreisfreien Alternativen sowie Not-Via Adressen gibt es Ansätze, beide Methoden zu kombinieren. Dabei werden kreisfreie Alternativen berechnet, um den Großteil eines Netzwerkes abzusichern. Für die restlichen Verbindungen können danach Not-Via Adressen eingesetzt werden, um die vollständige Abdeckung an Fehlerfällen zu ermöglichen. Somit wird mit annehmbarem Aufwand die größtmögliche Sicherheit erreicht.

Da IPFRR eine vergleichsweise junge aufkommende Technologie darstellt, gibt es in realen Umgebungen meist Probleme, da nicht alle Router-Hersteller ISPF Implementierungen unterstützen und nicht alle Router über ausreichende Rechen- sowie Speicherkapazitäten verfügen. Davon abgesehen müssen für den Einsatz von Not-Via Adressen alle Router untereinander kompatibel sein.

Das Ziel, die Ausfallzeiten in Netzwerken zu verringern, kann IPFRR bei großer Fehlerabdeckung aus technischer Sicht bereits erreichen. Die Entwicklung von IPFRR wird z.B. von Cisco und der IETF vorangetrieben. Cisco unterstützt IPFRR LFA im seinem Routermodell CRS-1 [7], und viele IPFRR bezogene Drafts bzw. RFCs der IETF werden von Cisco Mitarbeitern mitgestaltet. [1], [5]

Weitere Verbesserungen an der Reaktionszeit zwischen dem Auftreten eines Fehlers und der Reparatur können durch Verringerung im Bereich der Fehlererkennung erreicht werden, welche die meiste Zeit beim IP Fast Rerouting beansprucht. [2]

Literatur

[1] M. Shand and S. Bryant, “IP Fast Reroute Framework,” IETF, draft-ietf-rtgwg-ipfrr-framework-12, June 2009.

[2] S. Previdi, “IP Fast reroute technologies,” Cisco-Talk, 2006.

[3] A. Atlas, “Basic specification for IP fast reroute: Loop-free alternates,” RFC 5286, September 2008.

[4] *IP Fast Reroute: Overview and Things We Are Struggling to Solve*. NANOG, January 2005.

[5] M. Shand, S. Bryant, and S. Previdi, “IP Fast reroute using not-via addresses,” IETF, draft-ietf-rtgwg-ipfrr-notvia-addresses-04, July 2009.

[6] J. McQuillan, I. Richer, and E. Rosen, “ARPANET routing algorithm improvements,” BBN Technical Report 3803, 1987.

[7] *IOS XR Routing Configuration Guide, Release 3.8*, Cisco.