

# Erkennung von Routing-Problemen

Richard Hartmann  
(hartmanr@in.tum.de)

Hauptseminar „Internet Measurement“ ,  
Technische Universität München Lehrstuhl Feldmann

SS 2005 (Version vom 27. Juni 2005)

## Zusammenfassung

In diesem Papier soll erläutert werden, wie man so genannte Routing Loops erkennen kann und wie sie sich auf die Performanz des End-to-End-Verkehrs und das Verkehrsaufkommen zwischen den beteiligten Routern auswirken. Routing Loops entstehen, wenn die Forwarding-Tabellen zweier oder mehrerer Router widersprüchliche Informationen über den Weg, den die weitergeleiteten Pakete nehmen sollen, enthalten. Da jeder Router versuchen wird, die Pakete entlang der vermeintlich bestmöglichen Route zu schicken, entstehen Rundwege, entlang derer die Pakete geschickt werden. Dadurch entstehen hohe Latenzen oder Paketverluste, die sich nachteilig auf den Transfer der Daten auswirken. Die Erkennung von transienten<sup>1</sup> Routing Loops, ihrer Herkunft und ihrer Dauer sind wichtige Aufgaben in der Wartung von Netzwerken.

## 1 Einleitung

Zu den wichtigsten Aufgaben eines Internet Service Providers gehört es, die schnellstmögliche und beste Übertragung von in sein Netzwerk geschickten Daten sicher zu stellen. Wesentliche Eigenschaften der Datenübertragung werden von Routing Loops direkt beeinflusst. Jitter, Latenz, Auslastung der Inter-Router-Links wirken sich direkt auf den Datendurchsatz der Endknoten untereinander aus. Durch erhöhte oder variierte Übertragungszeiten oder Paketverluste werden die Flow-Control-Mechanismen von TCP ausgelöst, welche wiederum die Übertragungsraten der Verbindungen herabsetzen. Andere Protokolle wie zum Beispiel UDP müssen entweder auf einer höheren Ebene mit entsprechenden Mechanismen reagieren, oder die verschlechterten Übertragungseigenschaften unkompensiert hinnehmen.

Es soll versucht werden mit den von [Hengartner et. al. 2002] vorgestellten Methoden die transienten Loops auf Ebene der Router zu entdecken. Andere Arbeiten auf diesem Gebiet beschäftigten sich mit der Erkennung von Routing Loops auf der Ebene der Netzendpunkte. Indem die Header aller Pakete, die über einen gewissen Zeitraum den Router passieren, gespeichert werden, können diese danach zu jedem beliebigen Zeitpunkt bearbeitet und ausgewertet werden. Die vier Router, auf denen das Sammeln der Daten stattgefunden hat, befinden sich im Netz von Sprint, einem Tier 1<sup>2</sup>.

---

<sup>1</sup>Transiente Fehler sind temporär begrenzte, eher kurzzeitige Fehler. Eine Unterscheidung wird in Kapitel 3 gemacht.

<sup>2</sup>siehe Definitionen in Kapitel 2.

Zunächst soll in Kapitel 2 mit einigen Begriffsdefinitionen eine Grundlage zum leichten Verständnis dieses Papiers geschaffen werden. In Kapitel 3 geht es um Entstehung und Bedeutung von Routing Loops und warum sie in einem realen und skalierbaren Netzwerk de facto unvermeidlich sind. Kapitel 4 folgt mit einem Vergleich der Erkennung von Routing Loops durch End-to-End-Überwachung und Überwachung von zentralen Routern im Backbone eines Tier 1. Anschließend wird in Kapitel 5 betrachtet, wie man Replica Streams über längere Zeiträume aus kurzzeitigen Replica Streams aufbauen kann. Diese Replica Streams werden daraufhin in Kapitel 6 auf Besonderheiten untersucht und diese, soweit möglich, erklärt. Die Zusammenfassung der Ergebnisse in Kapitel 7 wird von Anmerkungen zu [Hengartner et. al. 2002] und Vorschlägen für mögliche Verbesserungen mit Kapitel 8 abgeschlossen.

## 2 Begriffsdefinitionen

**Definition 1 (Routing Loop)** Eine Routing Loop wird definiert als eine widersprüchliche, temporäre Inkonsistenz in den Forwarding-Tabellen der Router, durch die Pakete im Kreis geschickt werden. Sie kann durch Updates der Routen oder durch Fehlkonfiguration entstehen.

**Definition 2 (IP Adresspräfix)** Ein IP Adresspräfix bezeichnet die Größe des Adressraums, innerhalb der sich die Adresse befindet. Üblicherweise wird die Syntax *a.b.c.d/e* verwendet, also zum Beispiel 192.168.0.0/24 oder 192.168.0.0/16. Im ersten Fall wären die ersten 24 Bit festgelegt und die letzten 8 Bit der Adresse variabel, was in 192.168.0.x resultieren würde. Im zweiten Fall wären nur die ersten 16 Bit festgelegt, die anderen 16 frei, sprich 192.168.y.z. Eine andere, veraltete, Bezeichnung ist Netzmaske. Diese wäre im ersten Fall 255.255.255.0, im zweiten 255.255.0.0.

**Definition 3 (Replica Stream)** Als Replica Stream werden alle Vorkommnisse desselben Pakets innerhalb der Logfiles bezeichnet, die folgende Eigenschaften erfüllen:

- 1) Das Paket kommt mehr als zweimal vor.
- 2) Es gibt während des Zeitraums, in dem der Replica Stream stattfindet, keine nicht in einer Routing Loop befindlichen Pakete desselben Zieladresspräfixes( in diesem Fall werden nur /24 oder mehr betrachtet)

**Definition 4 (ISP)** Ein ISP ist ein Internet Service Provider, was sowohl Firmen, die Endkundenanschlüsse zur Verfügung stellen, als auch Backbone Provider bezeichnet.

**Definition 5 (AS)** Ein Autonomes System bezeichnet eine eigenständige Verwaltungseinheit innerhalb des Internets. Sie wird an Hand ihrer AS Nummer eindeutig identifiziert. Typischerweise hat ein ISP genau eine AS Nummer.

**Definition 6 (Tier 1)** Mit Tier (engl. Rang) 1, 2 oder 3 bezeichnet man die relative Größe eines ISP. Bei einem Tier 1 handelt es sich um einen sehr großen, stark vernetzten, multikontinentalen ISP. Um eine Größenvorstellung zu bekommen, die Deutsche Telekom ist nicht immer als Tier 1 angeführt.

**Definition 7 (Jitter)** Bei Jitter (engl. Fluktuation, Schwankung) handelt es sich um Wechsel von Amplitude oder Frequenz in der Datenübertragung. In diesem Papier bedeutet Jitter eine unterschiedliche Paketlaufzeit von konsekutiven Paketen.

**Definition 8 (TTL)** Die TTL (Time to live) ist ein Counter mit 8 Bit, der von jedem vom Paket zu passierenden Router, Bridge etc. um eins dekrementiert wird. Erreicht die TTL null wird das Paket verworfen und eine ICMP Nachricht über den Verlust des Pakets an den Absender geschickt.

**Definition 9 (TTL Delta)** Wenn ein Paket zweimal durch einen Router geschickt wird, dann muss die TTL zwischen dem ersten und zweiten Mal verringert worden sein. Der Betrag der Differenz zwischen beiden TTLs ergibt das TTL Delta.

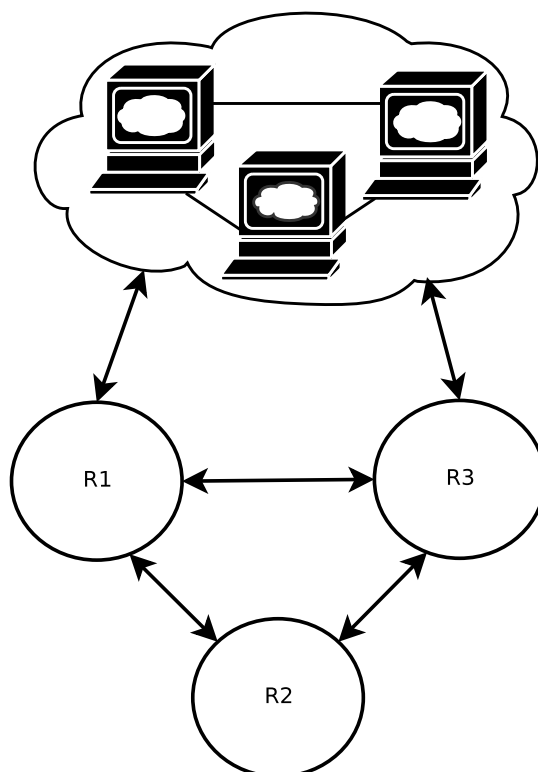
**Definition 10 (ACK Paket)** Ein ACK Paket bestätigt die Ankunft eines gesendeten Pakets. Bei ausbleibenden ACKs wird der Sender erneut senden, nach einiger Zeit aber die Verbindung einseitig beenden.

**Definition 11 (SYN Paket)** Ein SYN Paket wird zum Aufbau einer TCP beidseitigen Verbindung gesendet. Es wird entweder mit einem SYN ACK oder einem SYN und einem ACK beantwortet, woraufhin das SYN wieder vom ersten Sender mit einem ACK beantwortet wird (Three Way Handshake)

**Definition 12 (FIN Paket)** Ein FIN Paket wird zum einseitigen Verbindungsabbau versendet. Es wird mit einem FIN ACK oder mit einem FIN und einem ACK beantwortet, dieses FIN wieder mit ACK beantwortet. Der andere Kommunikationspartner muss zum Abbau seiner Verbindungsseite analog ein FIN senden. (Four Way Handshake)

### 3 Entstehung und Bedeutung von Routing Loops

Routing Loops entstehen, wenn zwei oder mehr Router widersprüchliche Informationen über die optimale Route, die ein Paket zu gehen hat, in ihren Forwarding-Tabellen vorhalten.



**Abbildung 1:** Die Router in der Beispielkonfiguration.

Angenommen die Router R1, R2 und R3 stehen, wie in Abbildung 1 gezeigt, in einer Dreiecksverbindung, R1 und R3 haben eine Verbindung zur Außenwelt. Bisher wurde Verkehr von R2 und R3 über R1 geleitet. Die Forwarding-Tabelle sieht aus wie in Tabelle 1<sup>3</sup>. Nun fällt der Link von R1 zur Außenwelt aus und R1 erneuert seine Forwarding-

R1	R1
R2	R1
R3	R1

**Tabelle 1:** Die Forwarding-Tabelle am Anfang.

Tabellen entsprechend. Da R1 weiß, dass R3 auch eine Verbindung nach außen hat, wird R1 seinen Verkehr über R3 leiten wollen. In diesem Moment befindet sich die Forwarding-Tabelle im Zustand wie in Tabelle 2 gezeigt. R2 empfängt das Update der Forwarding-

R1	R3
R2	R1
R3	R1

**Tabelle 2:** Die Forwarding-Tabelle nach dem Ausfall des Links von R1 nach außen.

Tabellen, erneuert seine Forwarding-Tabelle und leitet den nach außen gerichteten Verkehr von nun an auch über R3 wie in Tabelle 3 gezeigt. R3 hat von der Veränderung noch

R1	R3
R2	R3
R3	R1

**Tabelle 3:** Die Forwarding-Tabelle nachdem R2 seinen Eintrag aktualisiert hat.

nichts bemerkt. In dieser Konfiguration schicken R1 und R2 allen nach außen gerichteten Verkehr zu R3. R3 leitet die empfangenen Pakete nach R1 weiter. Ab diesem Zeitpunkt werden R1 und R3 sich gegenseitig immer wieder die gleichen Pakete schicken bis ihre Puffer voll sind, die TTL einzelner Pakete auf null sinkt oder die Routing Loop mit einem Update der Forwarding-Tabelle von R3 behoben wird. Die Pakete haben in diesem Fall ein TTL Delta von 2, dem kleinsten möglichen TTL Delta. Nachdem R3 als letztes seine Forwarding-Tabelle angepasst hat, ist das Netzwerk auf die neue Konfiguration konvergiert. Mit den neuen Forwarding-Tabellen wie in Tabelle 4 ist wieder ein arbeitsfähiger Zustand hergestellt.

Grundsätzlich wird zwischen transienten, also eher kurzfristigen, und persistenten Routing Loops unterschieden. Transiente Routing Loops entstehen im normalen Netzwerkverkehr durch veränderte Bedingungen innerhalb des Netzwerks und lösen sich typischerweise selbst durch Konvergierung des Netzwerks zu einem globalen Zustand aller Forwarding-Tabellen auf. Persistente Routing Loops werden zumeist durch Fehlkonfigurationen hervorgerufen und bedürfen zu ihrer Auflösung der manuellen Intervention einer realen Person. Im Rahmen dieses Papiers werden ausschliesslich transiente Routing Loops betrachtet.

<sup>3</sup>Diese globale Forwarding-Tabelle ist natürlich stark vereinfacht und stellt ausschließlich die Pfade nach außen dar.

R1	R3
R2	R3
R3	R3

**Tabelle 4:** Die konvergierte Forwarding-Tabelle.

Die Auswirkungen dieser Routing Loops sind breit gefächert und haben, je nach verwendetem Protokoll, unterschiedliche Auswirkungen. Die offensichtlichen Beeinträchtigungen des Paketflusses sind erhöhte Übertragungszeiten und Paketverluste. Durch das zirkelartige Weiterleiten der Daten steigt der Bandbreitenverbrauch auf den an der Routing Loop beteiligten Leitungen sprunghaft an. Die normalerweise nur einmalig zu versendenden Pakete belasten einen unidirektionalen Link im ungünstigsten Fall 128<sup>4</sup>, einen bidirektionalen Link 256 mal. Durch den stärkeren Jitter sinkt die Performanz von Echtzeitanwendungen wie VoIP oder von Out of Order fähigen Protokollen.

All diese Auswirkungen sind aus der Sicht des Netzwerks von den Endknoten, die ja über keinerlei direkten Informationen über das Netzinnere verfügen, nicht von schlechten Verbindungen, Bandbreitenbeschränkungen, vollen Puffern der Router oder praktisch allen anderen möglichen Netzwerkfehlern zu unterscheiden<sup>5</sup>, womit die ganz normalen Flow Control Mechanismen der Endknoten und ihrer Protokollstacks, soweit vorhanden, in Aktion treten.

Wie einleitend angedeutet, wird TCP die Datenübertragungsrate der Verbindungen soweit reduzieren, bis die Routing Loop entweder behoben oder die Verbindung durch das Verwerfen all ihrer Pakete zwangsweise beendet wird. Besonders im Fall von notwendigerweise langfristigen TCP-Verbindungen wie Links von IRC Servern oder VPNs kann sich dies als sehr nachteilig erweisen. Während die eingebaute Selbstregelung von TCP automatisch vor einer Verschwendung der Sende- und Empfangskapazität schützt, fehlt UDP als prominentesten Vertreter dieser Kategorie jede Art von Flow Control. Der Sender der Daten hat keine Möglichkeit, vom Verlust seiner Pakete zu erfahren, sendet also mit gleichbleibender Geschwindigkeit, obwohl der Empfänger diese bestenfalls verspätet, meist überhaupt nicht erhält. Andererseits ist bei einer Routing Loop zwischen Empfänger und Sender TCP durch den Verlust von ACKs trotz Erreichen des Empfängers genauso beeinträchtigt wie bei einer Routing Loop zwischen Sender und Empfänger. UDP bleibt von den Auswirkungen der Routing Loops von Empfänger zu Sender gänzlich verschont.

Ein Spezialfall von TCP-Verbindungen ist der Verlust von SYN Paketen. Zwingenderweise werden verloren gegangene SYN Pakete mindestens eine Verzögerung des Verbindungsaufbaus bis zum Timeout oder einer manuellen Neuübertragung erzeugen. Zumindest bei länger bestehenden Routing Loops fällt dies aber nicht zu sehr ins Gewicht, da dann auch alle anderen Verbindungen abgebrochen werden. Auch der Verlust des letzten FIN ACKS kann bei einem der Teilnehmer an der TCP-Verbindung zu Overhead führen, da die Verbindung auf der Empfängerseite nutzloserweise weiterhin offen gehalten werden muss.

---

<sup>4</sup>Die maximale TTL 256 / minimales TTL Delta 2 = 128. Das Paket kann auf der kürzesten möglichen Routing Loop nur maximal 128 mal kreisen bevor es verworfen wird.

<sup>5</sup>Es ist zwar durchaus möglich und üblich traceroute und ähnliche Programme zu verwenden, um Routing Loops oder andere Netzwerkfehler zu entdecken und zu unterscheiden. Dies wird aber meist durch reale Personen im Bedarfsfall oder von dedizierten Testsuiten im normalen Regelbetrieb durchgeführt. Dadurch stehen diese Informationen den Endknoten nicht zur Verfügung.

## 4 Vergleich von End-to-End-Überwachung und Überwachung von zentralen Routern

Bei der Suche nach Routing Loops gibt es zwei grundsätzlich verschiedene Ansätze. Der eine Ansatz ist das Überwachen des Netzes von möglichst vielen Endpunkten des Netzwerks aus, die so genannte End-to-End-Überwachung. Der andere Ansatz ist, das Netzwerk an idealerweise zentral gelegenen Knotenpunkten zu überwachen. Aus Gründen des Datenschutzes<sup>6</sup> und der technischen Machbarkeit werden nur die Header der Pakete gespeichert.

Vorteilhaft am ersten Verfahren ist, dass sich diese Art der Netzkontrolle kostengünstig ohne viel Aufwand oder Genehmigungsverfahren in kürzester Zeit aufbauen lässt. Auf der anderen Seite kann man auf diese Weise nur dann von Routing Loops erfahren, wenn sich die an dem System beteiligten Endknoten in einem Präfix befinden, das von den Routing Loops betroffen ist. Außerdem kann nur dann eine Unterscheidung von Routing Loops von anderen Netzwerkfehlern getroffen werden, wenn die ICMP Nachrichten über das Verwerfen der Pakete nach Ablauf der TTL nicht auch von einer Routing Loop betroffen sind. Gänzlich unmöglich sind Aussagen über die Tragweite der Routing Loops, wie die Anzahl der insgesamt betroffenen Pakete, das Verhältnis des betroffenen Verkehrs im Vergleich zum anderen Verkehr oder die zusätzlich entstehende Belastung der Netzwerkverbindungen.

[Hengartner et. al. 2002] ziehen den Ansatz vor, die Überwachung des Netzwerkverkehrs direkt an möglichst zentralen Routern im Backbone des Internet durchzuführen. Durch den direkten Zugriff auf alle Header sämtlicher Pakete, die den Router im Überwachungszeitraum passiert haben, wird ein lokal vollständiges Abbild des Zustands des Netzwerks ermöglicht. Dies ermöglicht eine Tiefe der Auswertung der gesammelten Informationen, die mit dem ersten Verfahren nur unter unverträglich hohem Aufwand realisierbar wäre. Die Gewinnung dieser Daten ist aber auch mit entschieden höherem Aufwand versehen. Da die Router der ISPs sich im produktiven Einsatz befinden, ist ein auch noch so kurzer Ausfall nicht, eine Leistungsbeeinflussung nur unter bestimmten Voraussetzungen akzeptabel. Die Gewinnung der Daten ist dem laufenden Betrieb unterzuordnen. Ein direkter Zugriff auf die Router für Außenstehende ist unmöglich, man muss entweder auf bestehende Daten zurückgreifen oder versuchen, einen Tier 1 ISP zur Kooperation zu bewegen.

## 5 Zusammenführen von Replica Streams

Die gewonnenen Rohdaten müssen erst gefiltert, verarbeitet und zusammengeführt werden, bevor man mit der Analyse beginnen kann. Zunächst fallen alle Paketströme aus den potentiellen Replica Streams heraus, deren IP ID nur einmal vorkommt, bei den typischen Zeitspannen<sup>7</sup> in denen Routing Loops auftreten ist ein Wrap-Around<sup>8</sup> auszuschließen. Zu Vergleichszwecken werden diese Pakete aber später noch benötigt. Die übrig gebliebenen Pakete haben den betrachteten Router mindestens zweimal passiert. Alle Pakete, die exakt zweimal beobachtet wurden, werden auch aus der Betrachtung ausgeschlossen. Dies ist notwendig um eventuell durch Token Ring oder SONET er-

---

<sup>6</sup>Auch ohne Nutzdaten können noch weitläufige Rückschlüsse über das Verhalten der Nutzer getroffen werden. Durch Löschen der Least Significant Bits kann man aber auch diese Informationen zumindest teilweise vernichten und trotzdem mit realen Daten arbeiten.

<sup>7</sup>90% aller in [Hengartner et. al. 2002] beobachteten Routing Loops dauerten zehn Minuten oder kürzer.

<sup>8</sup>Der Zähler für die IP ID ist endlich. Nach einer gewissen Verbindungsdauer muss erneut bei null begonnen werden.

zeugte Zwillinge sicher auszuschließen.<sup>9</sup> Nun werden alle Präfixe (/24) zusammengefasst und sicher gestellt, dass sämtliche Pakete aus demselben Prefixes innerhalb der Dauer des Replica Streams in der Routing Loop gefangen waren<sup>10</sup>. Falls Pakete dieses Präfixes erscheinen, die nicht mindestens zweimal aufgetreten sind vorkommen, muss es sich um eine Lücke der Routing Loop und damit zwei verschiedene Replica Streams handeln. In einem letzten Schritt werden alle Replica Streams, die sich zeitlich überschneiden, auf das gleiche Präfix lauten und wie oben keine nicht in der Routing Loop gefangenen Pakete im gleichen Zeitraum aufweisen, zu großen Replica Streams zusammengeführt. Um nicht erkennbare Routing Loops, in denen kurzzeitig keine Pakete kreisten nicht fälschlicherweise auszuschließen wurden bei Pausen zwischen zwei Replica Streams von weniger als einer Minute selbige nach obigen Regeln zusammengesetzt<sup>11</sup>.

## 6 Betrachtungen der Replica Streams

### 6.1 Allgemeine Betrachtungen

In [Hengartner et. al. 2002] wurden drei grundsätzliche Metriken verwendet:

- 1) TTL Delta
- 2) Anzahl der Replica im Replica Stream
- 3) Inter Replica Spacing (Zwischenankunftszeiten)

Das TTL Delta bezeichnet die Größe der Routing Loop. Das TTL Delta ist auch die Anzahl der Router die das Paket auf seiner letzten Runde durch die Routing Loop passiert hat<sup>12</sup>. Der Großteil, knapp 90%, aller Routing Loops in den betrachteten Daten hatte ein TTL Delta von zwei, es waren also nur direkt zwei Router betroffen. Die Autoren von [Hengartner et. al. 2002] erklären diesen Umstand damit, dass alle vier Router an denen von ihnen Messungen durchgeführt wurden, an der Verbindung zu einem anderen AS stehen. Dadurch, dass Routeninformationen innerhalb des eigenen Netzwerks per Flooding verteilt werden können, zwischen zwei AS aber nicht, entstehen Timingunterschiede mit höherer Wahrscheinlichkeit als in internen Netzen.

Die Anzahl der Replica im Replica Stream gibt Auskunft über die Gesamtverweildauer der Pakete in der Routing Loop. Spätestens bei 128 Wiederholungen wird das Paket in der Routing Loop verworfen. In den Daten gibt es zwei markante und offensichtlich signifikante Sprünge bei circa 30 und circa 60 Wiederholungen. Diese beiden Sprünge sind leicht zu erklären. Die Standard TTL im Linuxkernel ist 64<sup>13</sup>, die in Windows 2000 128. Windows XP war zum Zeitpunkt der Messungen noch nicht erschienen. Durch diese beiden Sprünge wird bereits ersichtlich, was die Autoren von [Hengartner et. al. 2002] am Schluss folgern: Die meisten in Routing Loops gefangenen Pakete werden von den Routern verworfen.

Die Zwischenankunftszeiten der Replica geben ein ungefähres Maß der Ausdehnung der Routing Loop. Natürlich überwiegen die kurzen Inter Replica Spacings analog zu den TTL Deltas von zwei. Der Hauptteil aller Inter Replica Spacings liegt unter 100 ms, fast alle unter 200 ms. Inter Replica Spacings von mehr als 250 ms treten praktisch nicht

---

<sup>9</sup>In Kapitel 8 wird betrachtet, wie man dieses Verfahren verbessern könnte.

<sup>10</sup>Es ist in der Arbeit von [Hengartner et. al. 2002] nicht ersichtlich, ob ein nur zweimal vorkommendes Paket als Ausschlusskriterium angenommen wurde, der Replica Stream also verworfen wurde. Der Autor nimmt dies aber nicht an.

<sup>11</sup>Die Autoren von [Hengartner et. al. 2002] legten eine Minute willkürlich als Zeitraum fest, nachdem Versuche mit Zeiträumen von 1, 2 und 5 Minuten keine signifikanten Unterschiede ergaben.

<sup>12</sup>Jeder Router zieht eins von der TTL des Pakets ab. Damit ist die Anzahl der Dekrementationen die Anzahl der Router.

<sup>13</sup>Das ist seit mindestens Kernel 2.2.0 der Fall. Zum aktuellen Zeitpunkt ist Kernel 2.6.12.1 die neueste Version, bei welcher dies auch der Standardwert ist.

auf. Das Inter Replica Spacing ist gleichzeitig die kleinste mögliche Verzögerung, die auf die Laufzeit der Pakete aufgerechnet werden muss. Zusätzliche Verzögerungen können durch Puffer in den Routern, Verarbeitungszeiten und ähnlichen Faktoren auftreten. In Verbindung mit der Anzahl der Replicas kann man versuchen, die zusätzliche Gesamtverzögerung abzuschätzen, was die Autoren von [Hengartner et. al. 2002] aber nicht versuchen.

## 6.2 Eigenschaften der Replica

Um eine ungefähre Vorstellung davon zu bekommen, wie sich die vorgenannten Faktoren auswirken, muss man auch die Art des Verkehrs kennen, der über die Router gesendet wird. Mit circa 80% macht TCP-basierter Verkehr den größten Teil des gesamten Datenvolumens aus. UDP-basierter Verkehr ist mit 10-15% an zweiter Stelle des Verkehrsaufkommens. An dritter Stelle stehen ICMP Pakete, hauptsächlich Ping und Time Exceeded-Meldungen.

Am Gesamtvolumen entfallen knapp 10% allein auf die TCP SYN und FIN Pakete. SYN Pakete sind im Verkehr innerhalb der Routing Loop im Vergleich zum normalen Verkehr überrepräsentiert. Durch die Tendenz der Pakete in den Routing Loops verworfen zu werden, werden zwar viele Verbindungsersuche gesandt, diesen Folgen aber logischerweise keine Daten, da nie eine Verbindung zu Stande kommt. ICMP ist genau wie SYN auch in den Replica Streams überrepräsentiert. Durch die verhungerten Verbindungen werden vermehrt Untersuchungen über das Netz von außen angestellt, und sowohl die Pings mit stetig steigender TTL als auch die Time Exceeded für trace-route sind ICMP Nachrichten<sup>14</sup>. Pakete mit Präfixen in Klasse C Netze<sup>15</sup> sind häufiger in Routing Loops als Pakete mit anderen Präfixen. Dies ist wahrscheinlich auf die eher veränderliche Natur der Klasse C Netze zurückzuführen<sup>16</sup>.

## 6.3 Dauer und Größe der Routing Loops

Die meisten Replica Streams haben wie erwartet eine zeitliche Länge von unter 500 ms<sup>17</sup> was eine grobe Schätzung auf eine durchschnittliche Gesamtzusatzlatenz von unter 750 ms für den Fall, dass das Paket die Routing Loop verlassen kann, zulässt. Eine relativ kleine Anzahl von Routing Loops ist für eine relativ große Anzahl an Replica Streams verantwortlich. Auf mehrere hundert Routing Loops kommen mehrere zehntausend Replica Streams. Routing Loops dauern zu 90% weniger als zehn Sekunden. Dies ist in Übereinstimmung mit Untersuchungen, dass die typische Konvergenzzeit im Internet bei fünf bis zehn Sekunden liegt.

Diese Daten und Erkenntnisse zusammengefasst ergeben ein zweigeteiltes Bild von Routing Loops. Es existieren die kurzen, bemerkbaren aber nicht zu schwer ins Gewicht fallenden Routing Loops welche aber in der Unterzahl sind. Der Großteil aller Routing Loops in den betrachteten Daten führte zum Verwerfen der Pakete. Zwischen 0,6% und 11% aller in eine Routing Loop gelangten Pakete entkommen dieser und haben eine zusätzliche Latenz von 25 ms bis 1300 ms.

---

<sup>14</sup>Es gibt auch ein traceroute welches auf TCP basiert. Außerdem erzeugen auch alle anderen verhungerten Pakete Time Exceeded Meldungen.

<sup>15</sup>192.0.0.0 bis 233.255.255.255

<sup>16</sup>Die meisten DSL und Dialup-Verbindungen mit dynamischen Verbindungen haben IP Adressen aus Klasse C Netzen

<sup>17</sup>Da, wie erwähnt, die meisten Routing Loops eine Größe von 2 haben und die Inter Replica Spacings meist bei 200 ms liegen, gilt  $TTL \Delta 2 * 200 \text{ ms}$ .

## 7 Zusammenfassung

Es wurde in die Materie von Routing Loops eingeführt und betrachtet, welche Arten der Entdeckung man wählen kann. Dieses Wissen wurde an Hand einer praktischen Ausarbeitung mit Daten aus der realen Welt erweitert. Die negative Auswirkung von Routing Loops wurde aufgezeigt, um zu unterstreichen, wie wichtig eine funktionierende Infrastruktur ist.

## 8 Kritik und Verbesserungsvorschläge

Im Allgemeinen lässt sich sagen, dass [Hengartner et. al. 2002] und [IMW2002] solide geschrieben sind. Es finden sich aber einige Fehler, die über bloße Rechtschreibfehler hinaus gehen. Im Beispiel zu Fig.1 wird vom Ausfall des Routers R1, und nicht dem seiner Verbindung in die Außenwelt gesprochen. In Fig. 3 wurde statt Anzahl der Pakete die Größe der Pakete als Maßstab genommen. Es wurde versäumt zu definieren, welche Rolle die Replica Streams mit zwei Replica in der Bewertung der anderen Replica spielen. In der Ergebnisbesprechung ist von einem Backbone 5 die Rede, der in keiner Grafik oder auch nur an einer anderen Stelle des Papiers nochmals erscheint.

Verbessern könnte man an der Vorgehensweise, dass man, wie im Papier erwähnt die Updateinformationen für die Forwarding-Tabellen mitprotokolliert und damit feinere Auswertungen, insbesondere über fließende Verläufe in den Routing Loops oder sich ändernde Präfixe, machen kann. Außerdem wäre damit eine genaue Einordnung der Replica Streams mit nur zwei Replicas möglich. Auch eine langfristige Protokollierung könnte interessante Ergebnisse liefern. Nicht zuletzt wäre es interessant Information über den gleichen Zeitraum von weltweit verteilten Routern aus verschiedenen AS möglichst in den zentralen Knotenpunkten auszuwerten, um auf diesem Weg die Bewegung der Routing Loops durch das Netzwerk verfolgen zu können.

Alles in Allem ein interessantes Thema, welches Lust auf mehr macht.

## Literatur

- [Hengartner et. al. 2002] Urs Hengartner, Sue Moon, Richard Mortier, Christophe Diot: *Detection and Ananalysis of Routing Loops in Packet Traces*; 2002 - Das Papier
- [IMW2002] Urs Hengartner, Sue Moon, Richard Mortier, Christophe Diot: *Detection and Ananalysis of Routing Loops in Packet Traces*; 2002 - Die Präsentation