



Untersuchungen zum Betriebszustand des Internets

Niels Lepperhoff

Systemforschung und Technologische Entwicklung (STE)
Forschungszentrum Jülich GmbH
52425 Jülich
n.lepperhoff@fz-juelich.de

Zusammenfassung: Weil das Internet für Wirtschaft und Gesellschaft eine immer unverzichtbarere Rolle einnimmt, steigt das Bedürfnis die Zuverlässigkeit des Internets zu bestimmen und zu bewerten. Eine Messung der Round Trip Time (RTT) und des Paketverlusts ist nur ein erster Schritt. Die Interpretation der Messungen ist der oft vernachlässigte zweite Schritt, der wegen des dynamischen Routings im Internet unverzichtbar bleibt. Die Interpretation der Messungen eine eigenständige Herausforderung, die in der Literatur kaum behandelt wird. Erste Abhilfe schafft der vom Forschungszentrum Jülich entwickelte „Internet Monitor“, der die Zuverlässigkeit ausgewählter Router, DNS-Sever und WWW-Server beobachtet. Besonderes Augenmerk bei der Entwicklung gilt der automatischen Datenanalyse. Am Beispiel von Erreichbarkeitsmessungen für 13 DNS-Rootserver und den 11 DeNIC-DNS-Server wird der Nutzen des Internet Monitors vorgestellt. Er demonstriert, wie häufige Vorkommnisse von den ungewöhnlichen Ereignissen getrennt werden können.



1 Einleitung

Die Funktionsfähigkeit von Computernetzen, insbesondere des Internets, gerät zunehmend in den Blick, weil immer mehr Unternehmen und Bürger diese nutzen und deshalb auf einen störungsarmen Betrieb angewiesen sind. Damit geht der Wunsch einher, die Zuverlässigkeit von Computernetzen, insbesondere des Internets, zu kennen, d.h. zu messen.

Ein wichtiges Anwendungsfeld für eine Zuverlässigkeitsüberwachung von Computernetzen in Unternehmen ist die Überwachung von Service Level Agreements. Für das Internet steht im Vordergrund zu verstehen, wie sich Störungen (Kabelschäden, Routerausfälle und Wurminfektionen) auf das Internet auswirken, und wie sich ihre Wirkungen räumlich verteilen.

Als einen ersten Schritt in diese Richtung hat das Forschungszentrum Jülich den „Internet Monitor“ entwickelt, der die Zuverlässigkeit ausgewählter Router, DNS-Sever und WWW-Server beobachtet. Besonderes Augenmerk bei der Entwicklung galt der automatischen Datenanalyse (siehe Abschnitt 4).

Aufgrund seiner Bedeutung eignet sich das Domain Name System (DNS) hervorragend, um den Nutzen einer Zuverlässigkeitsüberwachung mit Hilfe des Internet Monitors deutlich zu machen. Das DNS wandelt Adressen „www.fz-juelich.de“ in IP-Nummern um, damit Datenpakete adressiert werden können. Jedes Paket im Internet benötigt die IP-Nummer seines Ziels, um es zu erreichen. Für die Funktionsfähigkeit des Internets ist das DNS damit zentral. Um eine ausreichende Redundanz und Lastverteilung zu ermöglichen



weist das DNS eine hierarchische Architektur auf. An der Spitze stehen die 13 Rootserver, die über den gleichen Datenbestand verfügen. Sie beantworten die Anfragen nicht selbst, sondern verweisen auf die DNS-Server der Top Level Domain. Für die deutsche TLD „de“ sind das die DNS-Server von DeNIC, die ihrerseits auf die DNS-Server des Eigentümers der IP-Nummer oder des Domainnamens verweisen. Für die Funktionsfähigkeit des DNS sind sowohl die Rootserver wie auch die DNS-Server von DeNIC wichtig.

2 Verwandte Arbeiten

Bisher kennt nur jeder Netzbetreiber den Zustand seines Netzes (als Beispiel [Cà00]). In der Regel werden diese Angaben vertraulich behandelt. Den Zustand des gesamten Internets, im folgenden Betriebszustand genannt, kennt keiner. Paxson et al. [Pa98] schlugen deshalb vor, ein weltweites Beobachtungssystem zu installieren. Der Autor hat keinen Hinweis gefunden, dass der von Paxson et al. [Pa98] vorgestellte Prototyp heute im Regelbetrieb arbeitet.

Einen ersten Ansatz macht der „Internet Traffic Report“¹, der Paketverlustrate und Übertragungszeit (Round Trip Time (RTT) genannt) einiger weniger Router weltweit sammelt. Die Anzahl der Router ist für eine repräsentative Aussage viel zu klein. So wird Deutschland bspw. durch einen einzigen Router in Frankfurt repräsentiert. Auch werden die Messungen nicht interpretiert, d.h. es bleibt unklar, ob ein Messergebnis nun einen gewöhnlichen Betriebszustand widerspiegelt oder auf eine Störung hindeutet.

Das RIPE Network Coordination Centre (RIPE NCC)² baut eine Überwachungssystem für Server des Domain Name Systems der nationale Registries und die DNS-Rootserver auf. RIPE NCC beschränkt sich aus nahe liegenden Gründen auf das DNS. Wichtige WWW-Server oder zentrale Router bleiben unberücksichtigt. Die Messungen werden von RIPE NCC nicht interpretiert.

Einige Autoren haben über begrenzte Zeiträume die Zuverlässigkeit des Pakettransportes untersucht. Bolot [Bo93] untersuchte den Paketverlust für Verbindungen. Paxson [Pa97] untersucht die Stabilität des Routing zwischen 34 Messstellen. Labovitz et al. [La00, LAJ99, La01, LMJ98] analysierten die Routingstabilität. Duffield und Grossglauser [DG01] beschreiben ein Messverfahren, um den Weg von Paketen innerhalb eines Netzes zu verfolgen und dabei die Auslastung des Netzes zu messen. Der Ansatz basiert auf Kennzeichnung von Paketen und kann deshalb nur dort eingesetzt werden, wo der Zugang zu den transportierten Paketen gegeben ist, d.h. es eignet sich nur für Netzbetreiber zur Optimierung der eigenen Netze.

Diese Ansätze konzentrieren sich auf die Datenerhebung. Natürlich ist die Datenerhebung nicht trivial und notwendig. Hindernisse, wie Filterungen, müssen überwunden werden (Abschnitt 3). Zu kurz gekommen ist jedoch die Interpretation der Messergebnisse (Abschnitt 4). Abschnitt 5 zeigt, wie die vorgestellte Methode auf DNS-Rootserver und DeNIC-DNS-Server angewandt wird. Als Grundlage dienen Messergebnisse, die mit dem „Internet Monitor“ des Forschungszentrums Jülich erhoben worden sind. Anschließend fasst Abschnitt 6 die Überlegungen zusammen.

¹ <http://www.internettrafficreport.com/>

² <http://dnsmon.ripe.net/dns-servmon/>

3 Messung des Betriebszustandes

Das ICM-Protokoll stellt mit „Ping“ den klassischen Dienst zur Messung der Funktionsfähigkeit eines Beobachtungszieles zur Verfügung [RFC 792]. Ping misst die Zeit, die zwischen der Echoanfrage und ihrer Beantwortung verstreicht. Diese Zeitspanne heißt Round Trip Time (RTT).

Ping hat zwei Vorteile: Zum ersten ist die transferierte Datenmenge mit zwei Paketen pro Messung minimal. Zum zweiten können Router, DNS-Rootserver und WWW-Server mit der gleichen Methode beobachtet werden. Dadurch bleibt die Vergleichbarkeit der RTT erhalten.

Leider antworten nicht mehr alle Router und Server auf Pinganfragen. Dadurch verlieren Ping und das auf Ping aufbauende Traceroute ihre Wirksamkeit. Der „Internet Monitor“ kombiniert zur Beobachtung der 13 DNS-Rootserver Ping mit einer DNS-Anfrage. Antwortet ein Rootserver auf Pinganfragen nicht, weil gefiltert wurde, beantwortet er noch die DNS-Anfragen. Deshalb kann von einem Paketverlust bei Pinganfragen nicht auf eine Funktionsstörung geschlossen werden. Werden Pinganfragen beantwortet, nutzt der Internet Monitor sie, um die RTT festzustellen.

4 Bewertung der Messergebnisse

Eine ausführliche Erläuterung, wie die Messergebnisse analysiert werden, findet sich in [Le04]. Um die Qualität von Verbindungen zu einem oder mehreren Beobachtungszielen abzuschätzen, muss die gemessene RTT und der Paketverlust interpretiert werden. Wegen des dynamischen Routings ändern sich die Pfade zu den Beobachtungszielen und damit auch ihre RTT, d.h. eine fast konstante RTT ist nicht zu erwarten. Wechselnde Routen bedeuten für den normalen Betriebszustand, dass dieser sich nicht durch einen Wert ausdrücken lässt, sondern nur als Intervall. Ein solches Intervall kann sich im Tagesverlauf ändern.

Ein Beobachtungsziel kann durchaus im normalen Betriebszustand Paketverlust ausweisen. „Normal“ darf nicht als normatives Konzept verstanden werden, das beschreibt wie die RTT und der Paketverlust sein sollte. Ein Beobachter weiß nicht, welchen Grad an Zuverlässigkeit die Betreiber von Beobachtungszielen anstreben. Ihm interessiert, was ohne bekannte große Störungen täglich passiert.

Ein normaler Zustand ist ein häufig beobachteter Zustand. Beobachtungen über einen längeren Zeitraum erlauben es, die Häufigkeiten von RTT und verlorenen Paketen festzustellen. Aus diese Häufigkeiten wird eine Referenzwoche konstruiert, die beschreibt, welche RTT und Paketverlustrate als „normal“ angesehen werden kann, d.h. in der Vergangenheit häufig auftrat.

Die beobachteten RTT werden durch die Nutzung des Internets geprägt. Damit sind zwei Perioden zu erwarten: Eine 24stündige Periode, die den Tagesverlauf der Nutzung widerspiegelt, und eine Periode, die zwischen Werktagen und Wochenende unterscheidet. Beide Perioden liegen innerhalb unserer Referenzwoche. Für eine solche Referenzwoche müssen berücksichtigt werden:



- die Intervalle von „normalen“ Werten
- die Abhängig von der Tageszeit und Wochentag
- die Häufigkeiten der Beobachtungen.

In Abschnitt 4.1 erläutert die Konstruktion eine Referenzwoche, die den genannten Anforderungen genügt. Anschließend zeigt Abschnitt 4.2 auf, wie die Messergebnisse mit Hilfe dieser Referenzwoche analysiert werden.

4.1 Konstruktion einer Referenzwoche

Die Konstruktion einer Referenzwoche für die RTT unterscheidet sich von der Konstruktion einer Referenzwoche für den Paketverlust. Der erste Konstruktionsschritt bildet die, über viele Wochen gemessenen, RTT auf eine Woche ab. Dazu werden die gemessenen RTT so übereinander gelegt, dass Wochentag und Uhrzeit übereinstimmen. Für jede Minute, die einem Messintervall entspricht, in der Referenzwoche liegen nun verschiedene gemessene RTT vor. Das Messintervall, d.h. das Zeitintervall zwischen zwei RTT-Messungen, legt die zeitliche Auflösung der Referenzwoche fest.

Im zweiten Konstruktionsschritt werden für jede Minute zwei Werte ausgewählt, die den „normalen“ Zustand definieren sollen: Minimum und Maximum. Schwankungen aufgrund der Tageszeit oder des Wochentages bleiben damit erhalten. Die Genauigkeit der Referenzwoche steigt mit der Menge an einbezogenen Daten, wodurch auch neue Pfade und andere Veränderungen in der RTT berücksichtigt werden. Die Wahl des maximalen Wertes sollte deshalb Störungen ausschließen (für Einzelheiten siehe [Le04]).

Werte innerhalb des Referenzkorridors aus Minimum und Maximum definieren den „normalen“ Zustand. Tageszeitliche und Wochentages bedingte Schwankungen bleiben ebenfalls erhalten. Die Genauigkeit der Referenzwoche steigt mit der Menge an einbezogenen Daten, wodurch auch neue Pfade und andere Veränderungen in der RTT berücksichtigt werden.

Die Konstruktion einer Referenzwoche für den Paketverlust verläuft ähnlich. Im Unterschied zur RTT ist Paketverlust zu jedem Zeitpunkt ein binäres Ereignis, d.h. er findet statt oder nicht. Folglich ist die Bestimmung von Minima und Maxima sinnlos. Allerdings kann eine Verlustrate aus den Messergebnissen, die einem Zeitpunkt der Referenzwoche zugeordnet sind, berechnet werden. Ein Beispiel: Wenn an jedem zweiten Montag innerhalb eines Monats um 8.32 Uhr ein Paketverlust aufgezeichnet worden ist, dann liegt eine Verlustrate für diese vier Messungen von 50% vor. Störung treten zu unterschiedlichen Zeiten auf. Bezogen zu einem Zeitpunkt bleibt ihre Häufigkeit deshalb gering und ohne nennenswerten Einfluss auf die Referenzwoche.

4.2 Abweichungen erkennen

Ein Vergleich von beobachtetem Paketverlust und beobachteter RTT mit den Referenzdaten ist der erste Schritt, um die Messungen zu interpretieren. Messungen, die innerhalb des Referenzbereichs liegen, deuten auf einen normalen Betriebszustand hin und bleiben unbeachtet. Nur von den Referenzdaten abweichende Beobachtungen bedürfen einer weiteren Analyse.



Weicht nur eine Messung von der Referenzwoche ab, dann ist eine Lastspitze als Ursache wahrscheinlich und diese Messung wird nicht weiter betrachtet. Erst wenn hintereinander zwei oder mehr Messungen abweichen, kann eine Störung vorliegen.

Während abweichende RTT, die nicht innerhalb des Referenzbereichs liegen, einfach zu bestimmen sind, gilt das nicht für den Paketverlust als binäres Ereignis. Die Referenzwoche für Paketverlust gibt zu jedem Zeitpunkt an, wie hoch die beobachtete Häufigkeit für den Paketverlust ist. Diese Häufigkeit kann als Wahrscheinlichkeit dafür aufgefasst werden, dass der beobachtete Paketverlust „normal“ ist. Betrachtet man nun den Paketverlust an mehreren aufeinander folgenden Zeitpunkten, dann lässt sich einfach multiplikativ die Wahrscheinlichkeit berechnen, dass der Paketverlust durch eine Lastspitze verursacht worden ist. Sinkt die Wahrscheinlichkeit, dass der Verlust mehrerer Pakete hintereinander normal ist, unter eine festgelegte Schwelle, dann zeigt der Internet Monitor einen ungewöhnlichen Paketverlust an. Als Schwelle wird das in der Statistik gebräuchliche Signifikanzniveau von 5% verwendet.

5 Anwendung auf das Domain Name System

Der Internet Monitor am Forschungszentrum Jülich bittet jeden DNS-Server alle 60 Sekunden um eine Adressauflösung und bestimmte gleichzeitig die RTT mit Hilfe eines Pings. Grundlage für hier vorgestellten Auswertung sind die erhobenen Messwerte zwischen dem 25.03.2004 07:20 Uhr (UTC) dem 23.04.2004 05:36 Uhr (UTC). Insgesamt wurden 36.251 Messwerte pro Server erhoben. Die Referenzwochen basieren auf Messwerten aus dem Zeitraum vom 29.08.2003 bis zum 22.03.2004.

Zuerst wird die Zuverlässigkeit der DNS Rootserver untersucht (Abschnitt 5.1). Anschließend vergleicht Abschnitt 5.2 diese mit der Zuverlässigkeit der DeNIC DNS-Server. Zusätzlich wird gezeigt, wie ein typischer Lastverlauf für Deutschland aus den Referenzdaten der DeNIC-Server gewonnen werden kann.

5.1 DNS-Rootserver

Im Beobachtungszeitraum erwiesen sich die Verbindungen zu den DNS-Rootserver als unterschiedlich zuverlässig. Der J-Server ist mit einem Paketverlust von 0,28% der zuverlässigste und der G-Server der unzuverlässigste, weil er 7,43% der Anfragen nicht beantwortete. Der Internet Monitor erlaubt die Gründe für nicht beantwortete Anfragen einzugrenzen. Geht nur eine Anfrage verloren, sprechen wir von einem zufälligen Paketverlust. Gehen zwei Anfragen hintereinander verloren gilt eine Lastspitze als Ursache. Erst wenn drei und mehr Anfragen hintereinander verloren gehen, dann bezeichnen wir dieses als Ausfall. Ob die Störungsursache auf Seiten des Servers oder in der Verbindung zum Server zu suchen ist, kann der Internet Monitor konstruktionsbedingt nicht feststellen.

Abbildung 1 zeigt die Ausfallwahrscheinlichkeit der DNS-Rootserver, klassifiziert nach Ursachen. Der A Server sticht durch seinen hohen Anteil an ausfallbedingter Nichterreichbarkeit hervor. Dies ist auf zwei mehrstündige Ausfälle zurückzuführen: am 31.03.2004 ab 13:01 Uhr für 3 Stunden und 11 Minuten und am 13.04.2004 ab 08:59 Uhr für 2 Stunden und 41 Minuten. Die übrigen Rootserver zeigen keinen ähnlich langen Ausfall.

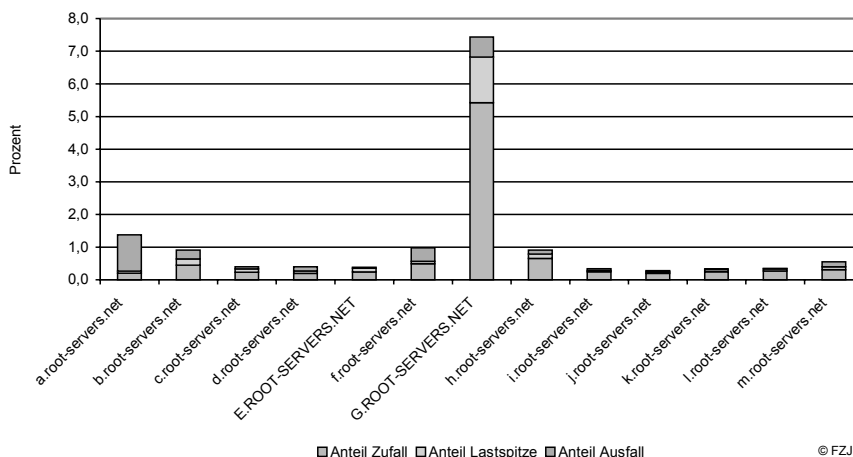


Abbildung 1: Ausfallwahrscheinlichkeit von DNS-Rootservern klassifiziert nach Ursachen.

Mit Hilfe des Verhältnisses von Paketverlust durch Lastspitzen zu Paketverlust durch Ausfälle lassen sich die DNS-Rootserver klassifizieren. Überwiegen Lastspitzen als Ursache, liegen Performanceengpässe vor. Davon sind die Rootserver C, E, G, H, J, K und L betroffen. Andernfalls scheint der Server gegen Ausfälle ungenügend gesichert zu sein, oder es wurden längere Wartungsarbeiten durchgeführt. Dies ist für die Rootserver A, B, D, F, I und M der Fall.

Der Paketverlust verteilt sich nicht gleichmäßig über den Tag. Vielmehr bestimmen der übliche Tagesrhythmus aus Aufstehen, Berufstätigkeit, Freizeit und Schlaf und der Wochenrhythmus aus Werktagen und Wochenende zusammen den Verlauf des Paketverlustes, der Aufschluss über die Auslastung der Verbindungen zu den DNS-Rootservern gibt. Abbildung 2 zeigt exemplarisch die Paketverlustwahrscheinlichkeit pro Stunde für die Rootserver G und M über die Referenzwoche. Der G-Server steht in Vienna, VA, (USA) und der M-Rootserver in Tokio (Japan). Deutlich sind die Tageszyklen beim G-Server zu erkennen, der durchgängig eine höhere Paketverlustwahrscheinlichkeit als der M-Rootserver aufweist. Beide Verläufe zeigen sowohl unterschiedliche Höhen als auch verschiedene Lagen der Maxima. Insgesamt besteht eine qualitative Ähnlichkeit der Kurvenform für alle Rootserver. Unterschiede liegen aber in der Anzahl und Lage der Maxima und Minima. Eine wichtige Ursache ist, dass sich unterschiedliche Lebenszyklen in den USA, Europa und Asien jeweils unterschiedlich überlagern.

5.2 DNS-Server von DeNIC

Betrachten wir nun die Zuverlässigkeit der DNS-Server von DeNIC, die für die Top Level Domain „de“ zuständig sind. Der DeNIC B-Server ist mit einem Paketverlust von 0,72% der zuverlässigste und der DeNIC D-Server der unzuverlässigste (5,09%). Abbildung 3 zeigt die Ausfallwahrscheinlichkeit der DNS-Server klassifiziert nach Ursachen. Der D Server sticht durch seinen hohen Anteil an ausfallbedingter Nichterreichbarkeit hervor.

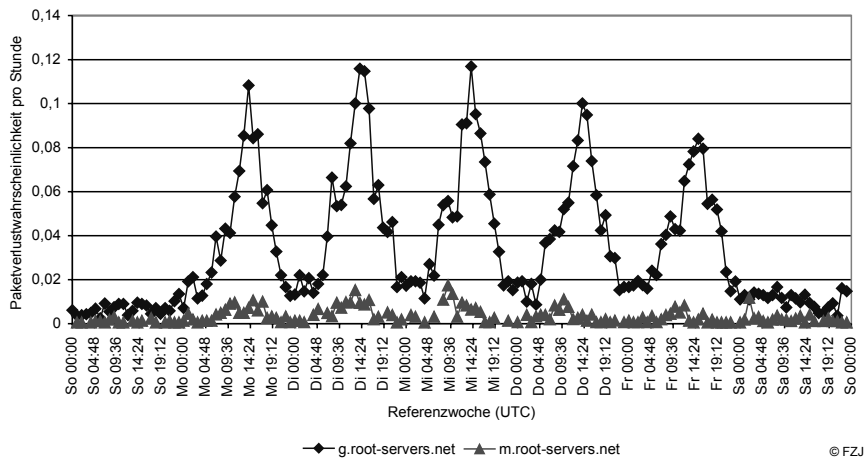


Abbildung 2: Verlauf der Paketverlustwahrscheinlichkeit pro Stunde über die Referenzwoche.

Dieses verursacht ein langer Ausfall am 27.03.2004 ab 07:16 Uhr für 25 Stunden. Die übrigen DeNIC-Server zeigen keinen ähnlich langen Ausfall.

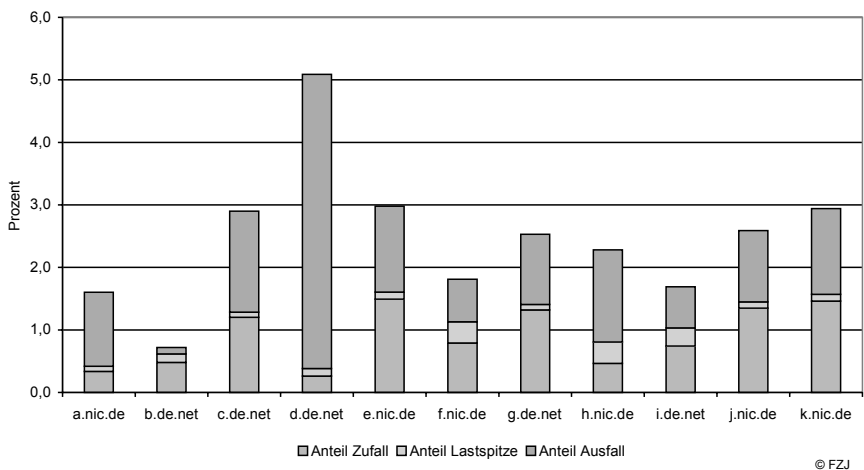


Abbildung 3: Ausfallwahrscheinlichkeit von DeNIC DNS-Servern klassifiziert nach Ursachen.

Weisen die DNS-Rootserver in ihrer Klassifikation nach Ursachen für den Paketverlust ein fast ausgeglichenes Verhältnis zwischen Lastspitze und Ausfall auf, so eindeutig ist die Klassifikation der DeNIC-Server: Bei 10 der 11 Server sind Ausfälle für mehr als die Hälfte aller nicht beantworteten Anfragen verantwortlich. Lediglich der DeNIC-Server B zeigt Performanceengpässe. Insgesamt ist die Verfügbarkeit der DeNIC DNS-Server ge-

ringer als die der Rootserver, denn zwei Rootserver aber 10 DeNIC-Server weisen eine Verfügbarkeit von weniger 99% auf, d.h. eine von hundert Anfragen wird nicht beantwortet.

Vier DeNIC Server stehen in Deutschland: A und D in Frankfurt, B in Berlin und C in Stuttgart.³ Weder von der Höhe des Paketverlustes noch von den Ursachen unterscheiden sich diese DNS-Server von DeNIC DNS-Server, die außerhalb von Deutschland stehen. Die vier in Deutschland stehenden DeNIC-Server eignen sich deshalb, um einen „typischen“ Lastgang für Deutschland zu extrahieren, weil primär Abfragen aus Deutschland und den Nachbarländern an diese Server gerichtet werden. Amerikanische Anfragen landen bei den beiden in den USA stehenden DeNIC-Servern (I und J) und asiatische beim Servern in Tokio (K). Abbildung 4 zeigt den Verlauf der Paketverlustwahrscheinlichkeit pro Stunde über die Referenzwoche für die vier in Deutschland stehenden DeNIC-Server A bis D. Die Paketverlustwahrscheinlichkeit der Server A und B streut deutlich über den Tagesverlauf.

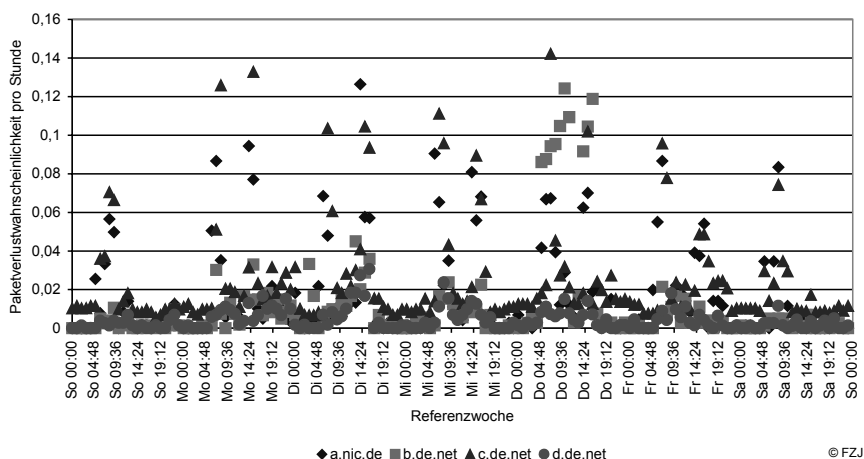


Abbildung 4: Verlauf der Paketverlustwahrscheinlichkeit pro Stunde über die Referenzwoche für die vier in Deutschland stehenden DeNIC-Server.

Aus den Paketverlustwahrscheinlichkeiten dieser vier Server berechnen wir einen „typischen“ Verlauf der Paketverlustwahrscheinlichkeit über der Referenzwoche. Dazu bilden wir für jeden Zeitpunkt den Median aus den Referenzwerten der Server A bis D. Diese so ermittelten Werte beschreiben den typischen Verlauf der Paketverlustwahrscheinlichkeit. Der Median hat den Vorteil robust gegenüber Extremwerten zu sein. Abbildung 5 zeigt das Ergebnis. Werktags tritt die erste Spitze um 8 Uhr deutscher Winterzeit auf. Um 16 Uhr oder 17 Uhr folgt die zweite meist größere Spitze, die Freitags allerdings kleiner ausfällt und am Wochenende nicht erkennbar ist. Am Wochenende ist nur eine Spitze gegen 9 Uhr zu erkennen. Weil Paketverluste auch eine Reaktion auf Lastspitzen sind, kann der Verlauf

³ http://www.denic.de/de/faqs/detail_82.html

um 8 Uhr noch gegen 12 Uhr in der Lage ihrer Spitzen überein. Verschiedene Ursachen scheinen für die Spitzen verantwortlich zu sein. Hier besteht weiterer Forschungsbedarf.

Weil die DNS-Anfragen das Netz des Forschungszentrums durchqueren müssen, wird die RTT – nicht aber die Paketverlustwahrscheinlichkeit, weil deren Verläufe sich nicht so stark ähneln – durch die Arbeit des Forschungszentrums beeinflusst. Dies könnte ein Grund für die Spitzen um 12 Uhr und um 16 Uhr sein und wäre damit eine mögliche Ursache für die unterschiedlichen Verläufe der RTT und der Paketverlustwahrscheinlichkeit.

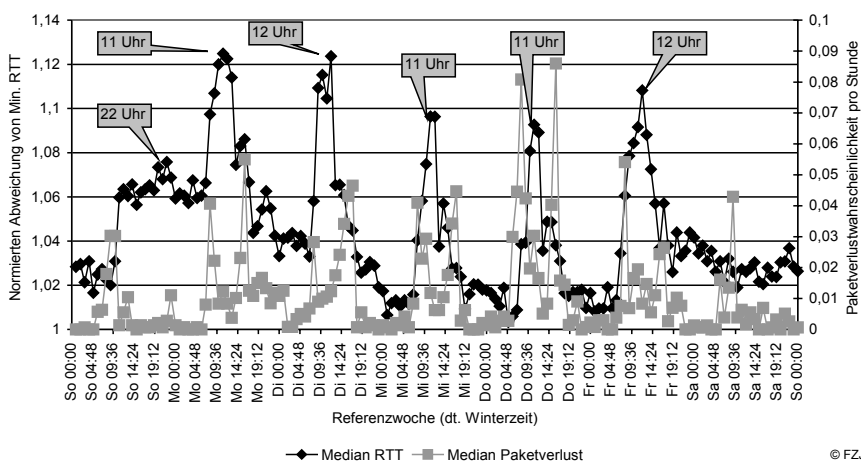


Abbildung 6: Verlauf typischer Round Trip Times (RTT) und Paketverlustwahrscheinlichkeiten gebildet aus den jeweiligen Medianen für die Server A bis D.

6 Schlussfolgerung

Weil das Internet für Wirtschaft und Gesellschaft eine immer unverzichtbarere Rolle einnimmt, steigt das Bedürfnis die Zuverlässigkeit des Internets zu bestimmen und zu bewerten. Einer Messung der Round Trip Time (RTT) und des Paketverlusts ist nur ein erster Schritt. Die Interpretation der Messungen ist der oft vernachlässigte zweite Schritt, der wegen des dynamischen Routings im Internet unverzichtbar bleibt. Weil das Internet dynamisches Routing einsetzt, wechseln die Pfade der Pakete. Dadurch ändert sich auch die RTT. Nutzungsweisen des Internets hängen von Tageszeiten und Wochentagen ab und prägen der RTT und dem Paketverlust ihre Perioden auf. Deshalb ist die Interpretation der Messungen eine eigenständige Herausforderung, die in der Literatur kaum behandelt worden ist. Erste Abhilfe schafft der vom Forschungszentrum Jülich entwickelte „Internet Monitor“, der die Zuverlässigkeit ausgewählter Router, DNS-Server und WWW-Server beobachtet. Besonderes Augenmerk bei der Entwicklung gilt der automatischen Datenanalyse.

Am Beispiel von Erreichbarkeitsmessungen für 13 DNS-Rootserver und DeNIC-DNS-Server wird der Nutzen des Internet Monitors vorgestellt. Er demonstriert, wie häufige

Vorkommnisse von den ungewöhnlichen getrennt werden können. Dabei zeigt sich, dass die Zuverlässigkeit der Rootserver bei über 99% liegt. Lediglich die Rootserver A und G weisen eine geringere Zuverlässigkeit auf. Als Ursachen kommen Lastspitzen und Ausfälle in etwa zu gleichen Teilen in betracht. Bei den DeNIC-Servern ist die Zuverlässigkeit geringer. Bereits 10 der 11 Server weisen eine Zuverlässigkeit von weniger als 99% auf. Im Unterschied zu den DNS-Rootserver sind Ausfälle die eindeutige Hauptursache für die geringere Zuverlässigkeit der DeNIC-Server.

Der Internet Monitor kann selbstverständlich auch auf andere Ziele wie WWW-Server und Router angewendet werden. Einem Einsatz innerhalb von Unternehmensnetzen für eine Verfügbarkeitsanalyse steht auch nichts im Wege.

Literatur

- [Ca00] Càceres, R., Duffield, N.G., Feldmann, A., Friedmann, J., Greenberg, A., Greer, R., Johnson, T., Kalmanek, C., Krishnamerthy, B.; Lavelle, D., Mishra, P.P., Ramakrishnan, K.K., Rexford, J., True, F., van der Merwe, J. E.: Measurement and Analysis of IP Network Usage and Behavior. *IEEE Communications Magazine* 38/5, 2000; S. 144-151.
- [Pa98] Paxson, V., Mahdavi, J., Adams, A., Mathis, M.: An Architecture for Large-Scale Internet Measurement. *IEEE Communications* 36/8, 1998; S. 48-54.
- [Bo93] Bolot, J.-C.: End-To-End Packet Delay and Loss Behavior in the Internet. *Proceedings of SIGCOMM '93*, 1993; S. 289-298.
- [Pa97] Paxson, V.: Measurements and Analysis of End-to-End Internet Dynamics. PhD dissertation, University of California, Berkeley. URL: <http://www.icir.org/vern/papers.html>, 1997
- [La00] Labovitz, C., Ahuja, A., Bose, A., Jahanian, F.: Delayed Internet Routing Convergence. *Proceedings of SIGCOMM 2000*, 2000; S. 175-187.
- [LAJ99] Labovitz, C., Ahuja, A., Jahanian, F.: Experimental Study of Internet Stability and Backbone Failures. *Digest of Papers. Twenty-Ninth Annual International Symposium on Fault-Tolerant Computing. IEEE* 1999; S. 278-285.
- [La01] Labovitz, C., Ahuja, A., Wattenhofer, R., Venkatachary, S.: The Impact of Internet Policy and Topology on Delayed Routing Convergence. *Proceedings of the INFOCOM 2001, vol 1, IEEE* 2001; S. 537-546.
- [LMJ98] Labovitz, Craig; Malan, G. Robert; Jahanian, Farmam: Internet Routing Instability. *IEEE/ACM Transaction on Networking*, vol. 6, no. 5, 1998; S. 515-528.
- [DG01] Duffield, N. G., Grossglauser, M.: Trajectory Sampling for Direct Traffic Observation. *IEEE/ACM Transactions on Networking* June 2001; S. 271-282.
- [RFC 792] RFC 792: Internet Control Message Protocol, 1981
- [Le04] Lepperhoff, N.: Internet Monitoring: Einfaches Erkennen von Störungen. *Informatik Spektrum*, Nr. 3, 2004.





Ad-hoc-Netzwerke



