Leistungscharakteristik des Domain Name Systems aus Clientsicht

Silvio Päpke

I. Einleitung

Auch wenn die Vernetzung des Internet insgesamt immer leistungsfähiger und schneller wird, gibt es grundlegende Dienste, welche teilweise zu vom Benutzer deutlich wahrnehmbaren Verzögerungen bei der Internetnutzung führen können. Gerade bei der Benutzung des Webs erwartet der Nutzer, dass sich innerhalb weniger 100 Millisekunden nach Anfordern der Webseite, diese auch im Browser aufbaut. Tatsächlich kann es gerade in dieser Nutzungssituation jedoch zu erheblichen Wartezeiten kommen, verursacht durch ein fundamentales Protokoll, welches für den Menschen unverzichtbar scheint, da es die für ihn merkbaren Domainnamen auf für Computer routbaren IP-Adressen abbildet. Das Domain Name System Protokoll (DNS), welches diese Umsetzung leistet, stellt den ersten Schritt der Kommunikation zwischen Browser und Webserver dar. Deshalb wirken sich Verzögerungen oder Ausfälle hier für den Benutzer als auch den Kommunikationsvorgang des Computers unmittelbar aus, für den Benutzer ist aber nicht immer transparent, weshalb eine Seite verzögert oder gar nicht dargestellt wird.

DNS wird von allen mit Domainnamen operierenden Vorgängen am Computer benutzt, das Nutzungsbeispiel des Webbrowsens eignet sich aus mehreren Gründen aber exzellent für die Darstellung und Untersuchung der mit DNS-Verzögerungen verbundenen Phänomene. Zum Einen werden beim Surfen vom Nutzer viele verschiedene Domains direkt eingegeben oder beim Folgen von Links innerhalb von Webdokumenten angefordert. Dabei erwartet der Nutzer einen möglichst verzögerungsarmen Aufbau der gewünschten Seite, welcher in der Anfangsphase der Verbindung direkt vom DNS abhängt. Die meisten der angeforderten Webseiten enthalten Material, welches von Servern mit anderen Domainnamen während des Seitenaufbaus nachgeladen wird, beispielsweise Werbescripte und -banner, Bilder von Hostingdiensten, Analysescripte von Statistikdiensten oder Videos, die über Content Distribution Networks (CDN) geladen werden. CDNs erschweren es zusätzlich ihre Domains zu cachen, da sie oft mit einer großen Anzahl von Subdomains und kurzen Time To Live Werte (TTL) operieren, um eine lokalisierte Lastverteilung auf ihre Server zu erreichen, dadurch aber das DNS belasten. Jedes dieser nachzuladenden Objekte, welches auf einem Server mit einem zuvor nicht benutzten DNS Namen liegt, benötigt eine Namensauflösung und wird den Seitenaufbau allein dadurch etwas verlangsamen. Des Weiteren sind Hostnamen, welche meist Domainnamen sind, aber auch IP-Adressen sein können, integraler Bestandteil des Hypertext Transfer Protocols und werden bei jeder Anfrage an den Webserver gesendet. Webserver können so für mehr als einen Domainnamen auf demselben Standardport Anfragen bearbeiten und vergrößern dadurch die Breite und Nutzbarkeit des Webs, welches sonst aufgrund der Knappheit von IPv4-Adressen kleiner oder ganz anders gestaltet sein müsste, beispielsweise könnte man sonst Portnummern zu verschiedenen Servern zuordnen, wie es bei vielen anderen Protokollen üblich ist.

Andere übliche Dienste im Internet nutzen DNS selbstverständlich auch, aber oft sind vom Endbenutzercomputer weitaus weniger Domains aufzulösen und die Kommunikation findet dann nur mit wenigen, einmal ermittelten Serveradressen statt, wie beispielweise bei IRC oder den typischen E-Mail-Protokollen.

<silvio.paepke@fu-berlin.de>, Matr.Nr. 4233749, FU Berlin, Betreuer: Matthias Wählisch

Diese Arbeit wird sich nicht mit der Performance von erweitertem Nutzen von DNS befassen, wie beispielsweise DNS basierten Blacklists. Außerdem steht auch nicht die Leistung von DNS aus Serversicht, oder der Vergleich von Serverimplementierungen im Blickpunkt, sondern es interessiert die Leistung des DNS, speziell die Geschwindigkeit der Namensauflösung, deren Einflussfaktoren und der Anteil von DNS an Verzögerungen im Web, aus Clientsicht.

Dazu werden zuerst die Grundlagen des DNS erklärt und dann mehrere Studien, die sich grundlegend mit den Leistungswerten des DNS nah am Client beschäftigen, nach ihrer Methodik und ihren Ergebnissen analysisert.

II. Das Domain Name System

Das Domain Name System wird in den entsprechenden RFCs [1], [2] grundlegend beschrieben, hier soll nur ein knapper Überblick über die Funktion und grundlegende Terminologie gegeben werden.

A. Hintergrund

Das DNS ist eine global verteilte, hierarchische Datenbank, welche die Hostnamenverteilung im Internet verwaltet. Es bildet dabei in der Hauptfunktion für Menschen gut les-, schreib- und merkbare Domainnamen auf für Computer berechen-, verwalt- und routbare IP-Adressen in A-Einträgen ab, hat aber auch noch weitere wichtige Funktionen wie die Rückübersetzung von IP-Adressen in Hostnamen (inverse Auflösung über PTR-Records) und die Verweise auf Mailserver (MX-Records). Die hierarchische Struktur geht von 13 Root-Servern baumförmig ab, wobei jeder Unterknoten von eigenen Servern verwaltet werden kann. Die Unterknoten sind durch auf ihrer Baumebene einmalige Textlabels identifiziert, welche im Fully Qualified Domain Name per Punkt getrennt werden. Die Unterserver sind für ihre Zone verantwortlich und können autoritative Antworten auf Anfragen geben. Besondere Bedeutung kommt den Unterservern auf erster Ebene, den Top-Level-Domain-Servern zu, welche in gTLD-Server, welche die generischen Top-Level-Domains verwalten, und die ccTLD-Server, welche die länderspezifischen (*country code*) TLDs verwalten, da diese die einzigen von den Root-Servern offiziell unterstützten (d.h. von ihnen aufgelösten) TLDs betreuen. Diese Delegation an Unterserver wird per Nameserver-Eintrag (NS-Record) durchgeführt, welcher den für einen Domainnamen verantwortlichen Nameserver enthält. Eine Anfrage kann grundlegend auf drei Arten beantwortet werden: Entweder wird die Antwort nichtautoritativ aus einem lokalen oder nahen Cache gegeben, dabei dürfen die Werte für eine vom autoritativen Server für jeden Domainnamen spezifizierte Zeit, die Time To Live (TTL), zwischengespeichert werden, oder es wird eine rekursive Anfrage gestellt, welche, wenn sie nicht beantwortet werden kann, vom Namenserver an den ihm zugeordneten Namenserver geschickt wird, bis sich eine Antwort findet. Die Anfrage kann auch iterativ erfolgen, was bei Anfragen an Root-Server immer geschieht. Hier fragt der Client selbstständig die ihm als Antwort gegebenen Nameserver ab, bis er den gewünschten Namen auflösen kann oder eine negative Antwort erhält. Die iterative Auflösung beginnt dabei soweit oben im Baum wie nötig und läuft nach unten, rekursive Anfragen funktionieren meist anders herum. Wichtige negative Antworten sind `NXDOMAIN` für nicht existierende Domainnamen und `SERVFAIL` wenn ein Serverproblem vorliegt oder ein Server beispielsweise für eine Zone nicht verantwortlich ist, während positive Antworten den vom Client angefragten Eintrag oder einen Verweis auf einen anderen Server zurückgeben.

B. Leistungsbewertung

Durch dessen Globalität muss das DNS skalierbar und hoch verfügbar sein und gleichzeitig eine geringe Latenz bei Benutzeranfragen bieten, da es Grundlage für die meisten neuen ausgehenden Verbindungen eines Rechners, besonders bei Nutzerinteraktion, ist. Genau diese Latenz ist das letztendlich entscheidende und auch umfassende Maß für die Leistungsbewertung des Domain Name Systems aus Clientsicht. Die Latenz ist charakterisiert als von Beginn

der Anfrage des lokalen DNS-Servers bis zu einer positiven oder negativen Antwort eines Caches, autoritativen oder nichtautoritativen Servers laufend. Da die Antwortzeiten von lokalen oder netzwerkinternen Caches meist nur wenige Millisekunden beträgt, ist hier zur Leistungsbewertung nicht die eigentliche Auslieferungszeit entscheidend, sondern wie viele Einträge tatsächlich aus dem Cache beantwortet werden können, die Cache-Trefferrate also, welche hauptsächlich von der Benutzung des Caches sowie von den vorgeschriebenen Vorhaltezeiten, den TTLs der einzelnen Einträge bestimmt wird. Eine weitere, zwar über die Latenz indirekt bestimmbare, aber doch eigene wichtige Metrik ist die Ausfallrate oder Fehlerrate. Da die meisten DNS-Resolver Anfragen, auf die sie keine Antwort erhalten haben nach 2, 3 oder 4 Sekunden erneut übermitteln, kann man an sprunghaft vorhandenen Latenzen in diesen Größenordnungen versuchen. die Ausfallrate zumindest der ersten übermittelten Pakete zu bestimmen oder man definiert die Ausfallrate als alle nach einem bestimmten Zeitraum, wie z.B. 30 Sekunden, nicht beantworteten Anfragen. Manche Studien beziehen auch negative Antworten in die Fehlerrate mit ein.

III. Messmethodik

Alle für diese Arbeit relevanten Studien verwendeten Messungen der Namensauflösung von einem Client aus (bzw. in der Nähe eines Clients); Studien, die mit Messungen direkt an DNS-Servern arbeiteten, blieben unberücksichtigt. Bei den clientseitigen Studien gab es jedoch große Unterschiede im individuellen Vorgehen: Man kann die Datensammlung nach Einbeziehung oder Nichteinbeziehung von gecachten DNS-Antworten, der Quantität und Diversifikation der Testsites, der Herkunft des analysierten DNS-Traffics, real oder generiert, der Auswahl der untersuchten Domainnamen, Zeitpunkt und Zeitspanne sowie geographischen und datenflusstopologischen Ort der Messungen gruppieren. Außerdem wurden verschiedene Parameter gemessen und in Bezug zu ebenfalls anderen Parametern gesetzt, die Antwortzeit auf eine DNS-Anfrage (Latenz) und die Anzahl der erfolgreichen Anfragen waren jedoch in allen respektive fast allen Studien grundlegende Maße.

Die nachfolgenden Abschnitte erläutern den Testaufbau der analysierten Studien und versuchen dabei das Vorgehen in die vorgenannten Gruppierungen einzuordnen.

A. Jung et al.

Die Studie von Jung et al. [3] aus 2002 bezieht sich auf Daten, die zwischen Januar 2000 und Mai 2001 für drei Zeiträume von 6-7 Tagen von Routern, die einige Subnetze des Massachusetts Institute of Technology (MIT) sowie des Korea Advanced Institute of Science and Technology (KAIST) mit dem Rest des Internet verbinden, gesammelt wurden und repräsentieren 500 (MIT) bzw. 1000 Nutzer (KAIST). DNS-Abfragen an Caches innerhalb der Subnetze konnten somit nicht mitgeschnitten werden und außerdem wird die Laufzeit der Daten innerhalb der Universitätsnetze nicht berücksichtigt. Daten von Caches außerhalb des eigenen Netzes sind in den Messungen einbezogen, jedoch wurden aus den beiden MIT Mitschnitten rekursive Anfragen entfernt um die Anzahl der Serververweise für alle Antworten zu haben, während sie beim KAIST enthalten sind, da es dort aufgrund der Wahl des Messpunktes fast nur weitergeleitete rekursive Anfragen gab.

Jung et al. waren neben der Latenz und dem Anteil erfolgreicher Antworten besonders am Einfluss der Anzahl der Verweise auf andere Namenserver während des Antwortprozesses interessiert. Außerdem wird die Effizienz von Nameserver-Caching untersucht sowie damit zusammenhängend die Interaktionen mit Root-Servern, sowie Anderes, für die clientseitige Performance weniger Wichtiges, wie das Verhältnis von TCP-Verbindungen zu DNS-Anfragen, erneute Übertragung von DNS-Paketen, die Arten der negativen Antworten und negatives Caching.

Um die Effektivität von Caching und den Einfluss der TTL beurteilen zu können, führten Jung et al. eine zweite Untersuchungsreihe durch, bei der Simulationen aufgrund der zuvor mitgeschnittenen Daten durchgeführt wurden.

B. Liston et al.

Liston et al. [4] arbeiteten in ihrer Studie aus 2002 nur mit zum Großteil ungecachten Antwortdaten, welche sie direkt bei 75 freiwilligen Clients aus 21 verschiedenen Ländern im Januar und März/April 2002 über einen modifizierten Named-Server protokollierten. Sie erzwangen kein Leeren des internen Caches, so dass beispielsweise Informationen über Nameserver zwischengespeichert sein konnten, achteten aber darauf dass alle Second-Level-Domains im Datensatz einmalig waren. Die von jedem Client abgefragen, insgesamt knapp 15.000 gültigen Domains wurden zuvor aus mehreren zufälligen Crawls fest zusammengestellt. 80% der Domains stammten aus den Bereichen .com, .net, .org (CNO), .edu und .gov.

Besonders interessiert waren Liston et al. daran, welche Metriken sich für Clients an unterschiedlichen Standorten und Zugriffspunkten wie verhalten um die Unterschiede aufzuzeigen. Sie bestimmten dazu die Latenzzeiten, die Anzahl komplettierter sowie erfolgreicher Anfragen, die bevorzugten Root- und gTLD-Nameserver und als statisch erwartete und für die Anwenderperformance weniger interessante Daten wie die Verteilung der TTLs und den Anteil von Aliasnamen.

C. Huitema und Weerahandi

Im Januar 2000 haben Huitema und Weerahandi [5] ihre Studie veröffentlicht, in der sie ihre seit September 1998 laufenden Datensammlung auswerten, welche von einem Standort bei Telcordia in den USA aus täglich 100 zufällige Seiten aus einer wachsenden Crawler-Datenbank von anfänglich 100.000, später 500.000, Seiten abruft und dabei die Zeit für die Domainnamenauflösung, den Verbindungsaufbau, die Zeit zwischen dem HTTP GET Kommando und dem ersten Byte der Antwort sowie die Downloadzeit und Größe der Webseite misst. Zusätzlich messen sie das Selbe seit September 1999 für 100 ausgesuchte, große Webseiten, da die vorherige Methode kleine Seiten systematisch bevorzugt.

Konnte auf eine der zufällig gewählten Seiten nicht zugegriffen werden wurde eine andere zufällige Seite gewählt, der Grund und die Ausfallrate wurden jedoch nicht ausgewertet, stattdessen maßen Huitema und Weerahandi im Januar 2000 die Ausfallraten für die in ihrem Experiment fünf häufigsten Domainendungen CNO, .edu und .co.uk indem sie zufällig gewählte Domainnamen direkt über die Root-Server abfragten. Um die Repräsentativität ihres Hauptexperiments zu überprüfen, ließen sie es für Januar 2000 ebenfalls an 5 anderen Orten durchführen und gaben die Anteile von Verbindungsversuchen und von DNS-Antworten an, welche über zwei Sekunden benötigten.

D. Wills und Shang

Wills und Shangs Institut, das Worcester Polytechnic Institute (WPI) war eine der Orte für den Repräsentativitätstest von Huitema und Weerahandi und sie haben im Juli 2000 ihre eigene Studie, auch unter Nutzung von Huitemas Testtool, veröffentlicht [6], die auf ähnlichen Metriken aufbaut, jedoch besonders den Einfluss der TTL auf die Effizienz von Caching, die DNS-Performance von populären gegenüber zufälligen Seiten und den Anteil von DNS an der Gesamtladezeit von Webseiten untersucht.

Ihre Studie gliedert sich in drei Teile: Zuerst simulierten sie verschiedene Cachingtaktiken wie das Benutzen einer minimalen TTL durch das Wiederabspielen von drei Proxylogs aus 1999 und 2000 mit 500.000 bis 800.000 Einträgen, ohne dabei jedoch Antwortzeitmessungen vorzunehmen. Der zweite Studienteil untersuchte die Antwortzeiten auf DNS-Abfragen für 100 populäre Webseiten im Gegensatz zu 100 zufällig aus einem ihrer Proxylogs ausgewählten Webseiten im Stundentakt, wobei Caching zum Einsatz kommen durfte. Im dritten Teil luden sie Webobjekte von 859 populären Servern und maßen dabei den Anteil der Zeit für DNS-Abfragen im Vergleich zur Gesamtdownloadzeit. Alle Messungen wurden von ihrem Institut aus getätigt.

E. Habib und Abrams

In der Studie von Habib und Abrams [7] aus dem Jahr 2000 wird neben anderen möglichen Engpässen auch die DNS-Verbindungszeit untersucht. Sie benutzen dabei dieselben vier Metriken wie Huitema und Weerahandi und untersuchen diese von drei Clients in den USA und drei in Paris, London und Tokyo an drei Tagen zu drei verschiedenen Uhrzeiten mit unterschiedlichen Trafficsituationen und rufen jede URL drei Mal hintereinander auf, wobei sie zwei Cachetreffer provozieren. Ihre URLs sind 100 populäre Seiten aus dem *PC magazine*, 80 Universitäten in den USA sowie 60 und 50 nicht näher spezifizierte Seiten in Brasilien respektive Südafrika.

IV. Messergebnisse

A. DNS-Antwortzeit

1) Jung et al.: Die Studie von Jung et al. zeigt Latenzen mit einem Medianwert von 85, 97 respektive 42ms für ihre Messungen am MIT im Januar 2000, Dezember 2000 und am KAIST im Mai 2001, wobei die KAIST-Daten einen hohen Anteil an Cachetreffern eines weiterleitenden Nameservers kurz hinter dem Messpunkt von etwa 35% haben. Weitaus schlechter ist in Korea aber die Performance nach dem Median, was sich durch längere Laufzeiten für einige internationale Anfragen erklären lässt. Auch für die MIT Daten sind die Mindestlatenzen des 90er Perzentils innerhalb eines Jahres von 447ms auf 1176ms gestiegen, für das KAIST kann man ein 90er Perzentil von etwa 7000ms ablesen. Als Vergleich zu Huitema und Weerahandis Maß von Anfragen, die über zwei Sekunden benötigen, zeigen Jung et al. dass 10% bis 24% ihrer Anfragen diesen Wert erreichen, geben aber erneut zu bedenken, dass ihr Messpunkt interne Netzwerklaufzeiten nicht aufzeichnet.

Jung et al. untersuchen auch den Einfluss der Anzahl iterativer Verweise auf die Latenz, welche sich natürlich mit steigender Zahl von Verweisen verschlechtert. Sie zeigen ein Diagramm der Latenzverteilung im MIT Dezember Datensatz abhängig von der Zahl der Verweise (0, 1, 2 und Durchschnitt über alle Daten), aus welchem man (anders als im Text geschrieben) ablesen kann, dass 60% der Anfragen ohne Verweise in unter 100ms beantwortet wurden, während dies für einen Verweis nur noch bei 20% und für zwei Verweise bei unter 5% der Fall ist. Da 81% der Anfragen ohne Verweise auskommen, folgt die Verteilung der Gesamtdaten stark der Verteilung für null Verweise und etwa 53% der Anfragen dauern unter 100ms. Die Anzahl der Anfragen die über eine Sekunde benötigen liegt für null Verweise bei 7,3%, im Durchschnitt bei 10%, für einen Verweis aber schon bei 20% und für zwei bei fast 50%, was aber insgesamt nur geringe Auswirkungen hat, da nur weniger als ein Prozent aller Anfragen in diesem Datensatz zwei oder mehr Verweise hatten, 18% dagegen einen.

Zuletzt zeigen Jung et al. noch die Vorteile von Nameserver-Caching auf, indem sie die Latenz der Anfragen in Verbindung dazu setzen, ob für eine Anfrage zuerst ein Root- oder gTLD-Server kontaktiert werden muss, was sie mit dem Fehlen eines Cacheeintrages gleichsetzen, oder nicht. Hierbei lassen sie einige kleinere Einträge, die gecached sein können, wie die von ccTLD-Servern außer Acht, kommen aber vermutlich aufgrund des großen Anteils der generischen Domains zu einem signifikanten Unterschied in den Antwortzeiten. Etwa 70% ihrer Anfragen sind nach dieser Definition gecached und bekommen eine Antwort nach spätestens 100ms in 60% der Fälle, während bei ungecachten dies nur für etwa 37% stimmt. Betrachtet man Antwortzeiten von über einer Sekunde sind unter 8% der Anfragen mit gecachten aber fast 20% der mit ungecachten Nameservern betroffen.

2) Liston et al.: Durch das Nutzen vieler auch in ihrer Netzanbindung und Lokalisierung verschiedenartiger Clients haben Liston et al. sich um einen Faktor von über zwei unterscheidende Mittelwerte für weitgehend ungecachte Antworten je nach Client zwischen 0,95s und 2,31s und versuchen die Gründe für diese Schwankungen durch Untersuchen der Korrelation zwischen diesen Mittelwerten und anderen Werten aus ihren Daten zu erklären. Dabei ergibt die minimale Antwortzeit, welche als Maß für die Geschwindigkeit der Netzanbindung gesehen wird,

nur eine wenig starke Korrelation von 0,62 mit der mittleren Latenz, ebenso wie die Verlustrate der Verbindung, welche über ihr Datum Wiederholungen von Anfragen im kritischen DNS-Pfad approximiert wird und mit 0,5 korreliert. Eine stärkere Wechselbeziehung besteht zwischen der mittleren Antwortzeit von Root- und gTLD-Servern und der Gesamtantwortzeit der ungecachten Anfragen, was nicht verwundert, waren doch in 60% respektive 7% aller Anfragen gTLD- und Rootserver involviert — die Korrelationsstärke ist hier 0,94 respektive 0,86. Trotzdem wird der Großteil der Zeit für Anfragen nicht mit dem Warten auf Root- oder gTLD-Server verbracht, diese Zeit beträgt über alle Clients und Anfragen gemittelt etwas unter 25%, was sich auch damit erklärt, dass nicht alle Anfragen diese Servertypen abfragen und dass sie dann meist auch nur einmal angefragt werden. Als letzte, stark mit der mittleren DNS-Latenz in Verbindung stehende Größe benutzten Liston et al. die gemittelte Antwortzeit von knapp 500 Servern, die als letzte auf dem kritischen Pfad von DNS-Antworten lagen, was sie als „Entfernung zum Rest des Internets“ bezeichnen. Dass dieses Maß eher die Entfernung zu vielen Nameservern misst ist offensichtlich, wird von ihnen aber nicht erwähnt, und so erstaunt die Korrelation der Antwortzeit von DNS-Servern auf spezifische Anfragen mit der Antwortzeit aller letzten Server auf dem kritischen Pfad aller DNS-Anfragen von 0,90 nicht.

3) Huitema und Weerahandi: Huitema und Weerahandi setzen durch die zufällige Auswahl auf weitgehend ungecachte Namen und müssen feststellen, dass fast 30% aller Namensauflösungen länger als zwei Sekunden benötigen, also wahrscheinlich wiederholt werden mussten. Nach etwas über zwei und drei Sekunden konnten sie sprunghafte Anstiege der Auflösungsantworten um etwa jeweils 10 Prozentpunkte erkennen — diese Zeiten entsprechen den üblichen Zeitüberschreitungsschwellen, nach welchen ein unbeantwortetes DNS-Abfragepaket erneut gesendet wird. So sind nach vier Sekunden fast 95% aller Anfragen beantwortet. Der untere Schwellwert liegt bei 70% Antworten nach etwas unter einer Sekunde.

4) Wills und Shang: Wills und Shang fragten von ihrem Institut aus stündlich populäre und zufällige Servernamen ab und teilten sich dabei den Cache mit anderen Nutzern ihres Netzes, so dass populäre Seiten mit TTLs von über eine Stunde durch die Studie selbst im Cache sein werden, was später auch versucht wurde herauszurechnen indem nur die ersten Anfrage pro Tag betrachtet wurde. Generell brauchten etwa 20-25% der ungecachten Antworten bei ihnen über eine Sekunde.

Interessant ist ihre Unterscheidung zwischen populären und zufälligen Servernamen, welche unter fast allen Bedingungen eine schnellere Namensauflösung für populäre Namen aufzeigt. So sind an Wochentagen bei stündlicher Abfrage 61% der populären Namen lokal gecached und an Wochenenden 42%. Für zufällige Seiten liegen diese Werte bei nur 32% respektive 13%. Betrachtet man nur den ersten Aufruf am Tag fallen diese Zahlen für populäre Server um 18 beziehungsweise 10 Prozentpunkte, während die Zufallsseiten sich nicht signifikant ändern.

Betrachtet man die Durchschnittswerte der ungecachten Antworten der Studie von Wills und Shang ohne die Beschränkung auf nur die erste Abfrage, erhielten sie zu höchstens 10% (aller Antworten inkl. Cachetreffern) nichtautoritative Antworten und diese brauchten bei populären Servern 0,85 Sekunden in der Woche und 1,72 Sekunden am Wochenende, bei zufälligen dagegen 1,57 respektive 2,28 Sekunden. Stellt man dem die viel häufigeren (31-81%) autoritativen Antworten entgegen, welche bei populären Seiten nur 0,55 und 0,44 Sekunden und bei beliebigen Seiten 0,79 und 1,01 Sekunden brauchten, erkennt man einen deutlichen Geschwindigkeitsvorteil der autoritativen Antworten von 35-75%.

5) Habib und Abrams: Habib und Abrams geben leider nur gering detaillierte Auskunft über die Antwortzeiten, sie geben aber einen Anteil der DNS-Antwortzeit am Gesamtvorgang des Downloads der Indexseite verschiedener Webseiten von „10-25%“ an und sagen, dass die DNS-Antwortzeit besonders bei internationalen Seiten „signifikant“ sei. Beispielhaft kann man aus einer Grafik in ihrem Paper die Antwortzeiten für die 100 populären Seiten von Paris aus ablesen. Für nichtgecachte Namen liegt die Gesamtzeit für den Download von 1kB bei 0,66s und der Anteil von DNS daran bei einem Drittel also 0,22s, während bei Cachetreffern darauf nur noch 9% der Gesamtzeit von

0,485s verwendet werden, was etwa 0,044s entspricht, also einem Fünftel der ungecachten Zeit, während Habib und Abrams davon sprechen, dass Cachetreffer 90-98% der Zeit für DNS-Abfragen einsparen. Die üblichen Latenzen zwischen Nordamerika und Europa lassen diese Zeitwerte jedoch sehr gering erscheinen, geht man davon aus, dass von einer Amerikanischen PC Zeitschrift wohl hauptsächlich in den USA gehostete Seiten in die Top 100 erhoben werden. Möglicherweise sind die empfohlenen Websites aber auch soweit international, dass diese zum größten Teil auch Server in Europa haben, was die Resultate von Habib und Abrams möglich macht.

6) Zusammenfassung: Über alle Tests sieht man dass ein Großteil (etwa 60%) der Anfragen vom DNS-System ausreichend schnell (meist weit unter einer Sekunde) beantwortet werden können und besonders der Einsatz von Caches kann diesen Anteil noch steigern und die Antwortzeiten für diesen Anteil stark senken. Die meisten Tests wurden von sehr gut angebundenen Netzen durchgeführt, betrachtet man ein weiteres Spektrum ohne Caches können durchschnittliche Antwortzeiten von zwei Sekunden und mehr auftreten. Besonders das Nameserver-Caching ist wichtig um sich eine zeitaufwändige Iterationsstufe von den Root-Servern zu sparen und diese gleichzeitig zu entlasten. Sehr schlecht ist jedoch der hohe Anteil von Antwortzeiten von mehr als zwei Sekunden, der zwischen 10% und fast 30% ausmachen kann, ein Wert der in Nutzerinteraktion mit Sicherheit wahrgenommen wird. Sehr hohe einzelne Antwortzeiten von stellenweise über 4 Sekunden erhöhen den Durchschnittswert der Antwortzeiten oft so stark, dass der Medianwert sich um eine Größenordnung davon unterscheiden kann.

B. Fehlerraten

1) Jung et al.: Da Jung et al. mit Mitschnitten realer Netzwerkkommunikation arbeiteten, kann man hier einen guten Überblick über DNS-Fehlerraten in natürlichen Szenarios gewinnen. Etwa 64% aller Anfragen in ihren MIT-Mitschnitten hatten erfolgreiche Antworten, in Korea galt dies für 36,4% und während dort über 42% der Anfragen negative Antworten erhielten, war dies am MIT für etwa 12% der Fall. Leider geben die Autoren keine Gründe für die hohe Anzahl negativer Antworten am KAIST an, sagen aber dass negative Antworten generell `NXDOMAIN`- oder `SERVFAIL`-Antworten waren. Am MIT wurden diese zu einem Großteil durch inverse Suchen, also für die Abbildung von IP-Adressen auf DNS-Namen verursacht, was für gewöhnlich nebenläufig zu Nutzerinteraktion geschieht, also nur geringe Auswirkungen auf eine wahrgenommene Reaktivitätsverschlechterung haben sollte.

Zwischen 20% und 23,5% aller DNS-Anfragen erhielt überhaupt keine Antwort, trotz erneuten Übertragens und eines redundant ausgelegten DNS-Systems mit vielen Root-Servern und meist mindestens zwei Nameservern pro Domain.

2) Liston et al.: Liston et al. arbeiteten mit einem vorselektierten Satz von Domains, wodurch ihre Fehlerrate durchschnittlich bei nur drei Prozent lag, während der Rest der Anfragen eine positive oder negative Antwort bekam. Erfolgreiche Antworten lagen zwischen 92,7% und 94,7%. Da sie einen Teil ihrer Daten etwa zwei Monate nach dem ersten Teil sammelten, sind etwa 0,6% der Domains in der Zwischenzeit ungültig geworden, wodurch diese nicht mehr erfolgreich abgerufen werden konnten. Diese Differenz wurde nicht herausgerechnet.

3) Huitema und Weerahandi: Huitema und Weerahandi maßen die Paketverluste von ihrem Netz aus, welche 6% pro Verbindung betrugen, gingen von lediglich zwei Verbindungen für eine DNS-Auflösung aus und versuchten eine Ursache für die fehlenden 18% der wiederholten Namensauflösungsversuche, welche zu 30% durchgeführt wurden, zu finden. Dabei gruppierten sie Antwortzeiten von über zwei und drei Sekunden nach Top-Level-Domain-Endungen und stellten die höchsten Wiederholungsraten für Namen aus den Bereichen .net (25%), .com (32%) und .org (46%) fest, während am anderen Ende des Spektrums beispielsweise .jp und .edu bei etwa 10% lagen. Verwundert über die Unterschiede bei CNO-Domains, welche von den gleichen Servern verwaltet werden, fragten sie die fünf populärsten Top-Level-Domains noch einmal direkt von den Root-Servern ab und maßen die Ausfallrate, definiert als keine Antwort nach 30 Sekunden, welche sich jetzt zwischen 11% und 23% bewegte und mit der Wiederholungsrate

nach zwei Sekunden nur „locker in Beziehung“ stünde. Eigentlich ist dort aber kein signifikanter Zusammenhang mehr zu sehen, beispielsweise sind die vorher am schlechtesten dastehenden .org-Domains mit knapp 14% in der Mitte des Feldes und mit .org einer der vorherigen Bestwerte jetzt bei fast 19% Ausfällen und damit Vorletzter. Diese eher zufällige Verteilung können die Autoren erklären, indem sie die Ausfallrate der verschiedenen Root-Server von ihrem Netz aus aufzeigen. Scheinbar wählt deren lokaler DNS-Server daraus nicht nach Leistung, sondern eher nach Belieben aus und gerät dabei an Root-Server mit Ausfallraten von 12%, 20%, 30% und über 60%. Weitere angebotene Erklärungen für die gute Leistung von .edu im normalen Test sind die gewöhnlich gute Netzwerkanbindung von Universitäten gegenüber z.B. Non-Profit-Organisationen und deren normalerweise viel hierarchischerer Aufbau von Domainnamen, in dem sich fast immer Subdomains für verschiedene Dezernate der Universität befinden, wodurch eine hohe Chance besteht, dass Teile der DNS-Informationen für die Domain gecached sind.

Zusätzlich zu den Tests von ihrer Seite aus führten Huitema und Weerahandi den Test an fünf weiteren Standorten durch, welche Verbindungswiederholungen von durchschnittlich 4,7% zeigten und unabhängig von diesen DNS-Antwortzeiten von über zwei Sekunden zwischen 24% und 29%.

4) Wills und Shang: Wills und Shang erklären, dass es für fast 20% aller 859 von ihnen beim Downloadtest überprüften Servernamen im ersten Versuch keine DNS-Antwort gab, so dass die Anfrage von ihrem lokalen DNS-Server nach vier oder fünf Sekunden wiederholt wurde, was natürlich für den Downloadtest bei diesen Servern den DNS-Abfrageanteil signifikant werden ließ.

5) Habib und Abrams: Habib und Abrams zeigen zwar ein Diagramm, welches einen DNS-Zeitanteil von 89% darstellt, geben aber weder die Häufigkeit dieser „Ausreißer“ noch deren zeitlichen Aufwand an und machen keine Angaben, ob sie diese Werte bei der Mittelwertbildung entfernt haben, sondern sagen nur, dass sie solche Werte als Ausreißer identifizierten.

6) Zusammenfassung: Bei Studien ohne Vorauswahl der Domains zeigt sich eine hohe Ausfall- oder zumindest Wiederholungswahrscheinlichkeit der DNS-Anfrage von 10% bis 30%.

Selbst bei einem sorgfältig vorselektierten Satz von Domains gab es wie bei Liston et al. noch mehr als 5% negative Antworten oder Ausfälle des Domainsystems, und diese Zahl beinhaltet nur ultimative Antworten selbst mit mehreren neuversuchten Anfragen, was man als instabil bezeichnen kann. Zu diesem Bild passen auch die erschreckend hohen Ausfallzahlen eines großen Teils der Root-Server, die Huitema und Weerahandi maßen.

C. Time To Live und Caching

1) Jung et al.: Jung et al. zeigen, dass populäre Seiten generell eine kürzere TTL haben und dass sich innerhalb des Jahres 2000 die Anzahl der Seiten mit kurzen TTLs von unter 15 Minuten in ihren Beobachtungen von 12% auf 25% verdoppelt hat. Sie untersuchten die Auswirkungen der TTLs auf erfolgreiches Caching sowie die Größe von sinnvollen Clientgruppen für Caches, welche laut ihnen bereits ab zehn bis zwanzig Clients kaum merkbare Verbesserungen der Cachetrefferrate bringt. Sie merken selbst an, dass die meisten unpopulären, also oft nur einmal abgefragten Domains am besten mit Client- oder Anwendungscaches zu bewältigen sind — erwähnen aber nicht, dass ihre Methode genau solche in der Realität wirkenden Caches nicht berücksichtigt, sondern zählen jede einzelne neue simulierte TCP-Verbindung zu einem Host entweder als Cachetreffer oder, wenn die TTL abgelaufen war, als Nichttreffer, teilen ihre Cache-Messung also nicht in lokale und externe Caches. Dies erklärt die sehr hohe Mindesttrefferrate von 71% selbst für einen Client, welche sich für die Maximalpopulation von allen über 1.200 Clients in einem einzelnen Cache auf 89% steigert — was nicht mit der Cachetrefferrate von etwa 35% in ihren realen Daten vom KAIST korreliert. Der Einfluss der TTL selbst auf die Cachetrefferrate wird von ihnen ebenfalls simuliert, ist aber wieder, wie sie selbst schreiben, mit derselben, besonders durch das viele ähnlich Verbindungen aufbauende

Webbrowsing hervorgehobenen, Auslassung behaftet, so dass sie für TTLs größer als etwa 1000 Sekunden keine bedeutsamen Verbesserungen durch Caching feststellen können. Sie schlussfolgern, dass niedrige TTLs für DNS-A-Einträge wenig nachteilig sind und dass clientseitiges Caching allein hier „fast vollständig“ ausreichend ist um Latenzsenkungen auf Clientseite zu erreichen, weisen aber darauf hin, dass dies natürlich nicht für das Cachen von NS-Einträge gilt.

2) Liston et al.: Liston et al. zeichnen zwar alle TTL-Werte auf, untersuchen aber lediglich die Schwankungen der Werte zwischen Clients, welche erwartungsgemäß mit durchschnittlich unter einem Prozent sehr gering ausfällt, da diese vom Domainadministrator festgelegt werden. Erkennbar ist aber dass die populärsten TTLs ein Tag und eine Stunde sind und dass sehr kurze Werte von unter zwei Minuten häufiger auftreten als sehr lange Werte von länger als zwei Tagen. Leider setzen sie diese Werte nicht mit Antwortzeiten oder anderen für die Clients interessanten Maßen in Bezug.

3) Wills und Shang: Wills und Shang zeigen die Latenz einer autoritativen Antwort als Funktion der TTL, woraus zwar erkennbar ist, dass die von ihnen gemessenen Seiten mit einer TTL von null die weitaus langsamste Antwortzeit und die Werte zwischen null und einer Minute die beste haben, ansonsten sind der Darstellung aber wenig Informationen zu entnehmen, außer dass die Latenz ungecachter Antworten von der TTL unabhängig zu sein scheint und auf die restlichen TTL-Werte gleichmäßig verteilt ist. Ein Resultat das wenig überrascht, spielt die TTL doch erst beim Caching von Antworten eine entscheidende Rolle, welche sie auch im ersten Teil ihrer Studie untersuchen: Sie stellen Cachetrefferraten von autoritativer TTL und einer künstlichen minimalen TTL von 15 Minuten gegenüber, einmal unter Ausschluss jeglichen clientseitigen Cachings und einmal unter der Annahme von fünfzehnsekündigem Caching der Clients (bzw. der Simulation von persistenten Verbindungen von maximal 15s Länge). Es ergeben sich im zweiten Fall Verbesserungen der Cachetrefferrate um 5-7 Prozentpunkte bei Benutzung der Minmal-TTL, auf 77-82%. Gleichzeitig verringert sich die Rate von vorhandenen aber abgelaufenen Einträgen um 4-7 Prozentpunkte auf 7-12%, während die Nichttrefferrate exakt gleich bei 11% für alle drei abgespielten Logs bleibt.

Wie sehr und ob sich die Zuordnung von IP-Adressen zu Hostnamen während des Abspielens der Logs überhaupt ändert wurde ebenfalls getestet. Dabei gab es 6-10% an Hostnamen mit mehreren IP-Adressen. Von den Hosts mit kurzen TTLs (unter 15 Minuten) haben sich tatsächlich nach Ablauf der TTL nur etwa 20-22% der Zuordnungen geändert und bei Anwendung der Minimal-TTL von 15 Minuten sind dies noch 10-13%, was bedeutet, dass sich tatsächlich etwa 80% der kurzen Zuordnungen nicht und 50% der kurzen langsamer als 15 Minuten ändern — was dann solch kurze TTLs nicht rechtfertigt.

4) Zusammenfassung: Insgesamt ist festzuhalten, dass Caching natürlich äußerst positive Auswirkungen auf die vom Client wahrgenommene Leistung des DNS hat, auch wenn deren Minimalbenutzeranzahl und Effizienz von Jung et al. durch Nichtberücksichtigung von vorhandenen clientseitigen Caches etwas überschätzt wird. Wills und Shang können dagegen aufzeigen, dass viele kurze TTLs länger sein dürften, da sich die Zuordnungen nicht so schnell ändern, was den Cachingerfolg verbessern sollte.

V. Zusammenfassung und Ausblick

Für den überwiegenden Teil der DNS-Abfragen arbeitete das Domain Name System in den Studien, die in der Zeit von 1998 bis 2002, durchgeführt wurden schnell und zufriedenstellend, besonders wenn Caching zum Einsatz kommt. Trotzdem gab es Verbesserungsbedarf, besonders bei den schlechtesten 10%-30% der Antworten, die für interaktive Nutzung durch Menschen zu lange brauchten oder gar nicht beantwortet wurden. Die teilweise sehr schlechten Antwortraten von Root-Servern und der beschränkten Anzahl dieser wurde mittlerweile bei einigen Servern mit Anycast begegnet [8], wo mehrere geographisch weit verteilte Server je nach Routing unter einer

Adresse ansprechbar sind. Es gibt auch andere innovative Ansätze wie CoDNS [9], in dem sich Gruppen von Clients zusammenschließen um ihre Anfragen gegenseitig zu beantworten, also eine aktive Cache- und Weiterleitungsgruppe bilden.

Es ist verwunderlich, dass die aktuellsten für den Autor auffindbaren Studien zur tatsächlichen Leistungsmessung des DNS aus Clientsicht aus den Jahren 2000 bis 2002 stammen und in den letzten 8 Jahren dazu scheinbar keine veröffentlichte wissenschaftliche Arbeit getan wurde, außer es ging um Leistungen von konkreten Implementierungen von Verbesserungsideen. Es stellt sich die Frage, ob sich die Daten nicht geändert haben, welche aber unwahrscheinlich mit *ja* zu beantworten ist, oder ob es einfach kein Interesse daran gab, ob und wie sich die in den letzten Jahren eingeführten Veränderungen und die Netzevolution grundlegend auswirken.

LITERATUR

[1] P. V. Mockapetris, "RFC 1034: Domain names — concepts and facilities," Nov. 1987, status: STANDARD. [Online]. Available: ftp://ftp.internic.net/rfc/rfc1034.txt

[2] ——, "RFC 1035: Domain names — implementation and specification," Nov. 1987, status: STANDARD. [Online]. Available: ftp://ftp.internic.net/rfc/rfc1035.txt

[3] J. Jung, E. Sit, H. Balakrishnan, and R. Morris, "DNS performance and the effectiveness of caching," *IEEE/ACM Trans. Netw.*, vol. 10, no. 5, pp. 589–603, 2002.

[4] R. Liston, S. Srinivasan, and E. Zegura, "Diversity in dns performance measures," in *IMW '02: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*. New York, NY, USA: ACM, 2002, pp. 19–31.

[5] C. Huitema and S. Weerahandi, "Internet measurements: The rising tide and the DNS snag," in *Proc. of ITC Specialist Seminar, IP Traffic Measurement, Modeling and Management*, 2000.

[6] C. E. Wills and H. Shang, "The contribution of DNS lookup costs to web object retrieval," *Worcester Polytechnic Institute Technical Report TR-00-12*, 2000.

[7] M. A. Habib and M. Abrams, "Analysis of sources of latency in downloading web pages," in *Proceedings of WebNet 2000 - World Conference on the WWW and Internet, San Antonio, Texas, USA, October 30 - November 4, 2000*, G. Davies and C. B. Owen, Eds. AACE, 2000, pp. 227–232.

[8] S. Sarat, V. Pappas, and A. Terzis, "On the use of anycast in DNS," in *SIGMETRICS '05: Proceedings of the 2005 ACM SIGMETRICS international conference on Measurement and modeling of computer systems*. New York, NY, USA: ACM, 2005, pp. 394–395.

[9] K. Park, V. S. Pai, L. Peterson, and Z. Wang, "Codns: improving dns performance and reliability via cooperative lookups," in *OSDI'04: Proceedings of the 6th conference on Symposium on Opearting Systems Design & Implementation*. Berkeley, CA, USA: USENIX Association, 2004, pp. 199–214.