

# Protecting BGP Routes to Top Level DNS Servers

Gunnar Bornemann  
(borneman@in.tum.de)

Seminar „Internetrouting“,  
Technische Universität München

WS 2004/2005 (Version vom 28. Februar 2005)

## **Zusammenfassung**

In diesem Papier wird ein Mechanismus zum Schutz der Pfade zu wichtigen DNS-Servern im Internet vorgestellt.

Hierbei wird erklärt, warum ein solcher Schutz überhaupt notwendig ist, wie er funktioniert, wie er getestet wurde und welche Auswirkungen er hat.

Des Weiteren wird eine kurze Einführung in das Domain Name System (DNS) sowie in das Border Gateway Protocol (BGP) gegeben und der vorgestellte Mechanismus am Ende des Papiers bewertet.

# 1 Einleitung

In der heutigen Zeit spielt das Internet eine immer größer werdende Rolle. Mehr und mehr Menschen bzw. ihre Rechner erhalten Internetkonnektivität, viele moderne Kommunikationsformen wie Chat oder Voice-over-IP (VoIP) lösen daher die klassische Telefonie ab.

Kommunikation findet im Internet von einer IP-Adresse zur Anderen statt. Da man sich aber nicht tausende von kryptischen IP-Adressen merken kann (und will), wurde das Domain Name System (DNS) zur Erleichterung eingeführt. DNS erlaubt unter anderem das Auflösen eines Namens in eine IP-Adresse und umgekehrt.

Da das Internet kein statisches System ist, d.h. sich die Struktur des Internets ständig ändert, z.B. kommen neue Kommunikationsleitungen hinzu oder andere fallen weg, sind feste Einstellungen nicht möglich. Eine dynamische Anpassung und Bereitstellung der zur Verfügung stehenden Pfade ist nötig. Zu diesem Zweck wurden Routingprotokolle entwickelt. Das im Internet am häufigsten eingesetzte Protokoll ist das Border Gateway Protocol (BGP).

Die Erreichbarkeit der DNS-Server ist für die meisten Dienste im Internet Voraussetzung. Sollte dies nicht der Fall sein, kann es zu fatale Folgen kommen. Daher ist es also notwendig, nicht nur das DNS selbst, sondern auch die Pfade zu den DNS-Servern zu schützen. Ein solcher Schutz für Pfade wurde in [1] vorgestellt, welches die Grundlage dieses Papiers bildet und im Folgenden behandelt wird.

Des Weiteren gibt dieses Papier zunächst eine Einführung in DNS sowie in BGP in Kapitel 2. Daraufhin werden in Kapitel 3 die Ideen hinter dem Algorithmus erläutert und der Mechanismus selbst vorgestellt. Kapitel 4 beschäftigt sich mit den durchgeführten Tests sowie deren Resultaten. Den Abschluss des Papiers bildet eine Zusammenfassung in Kapitel 5.

## 2 Grundlagen

Im folgenden Kapitel werden zunächst Grundlagen behandelt, die für dieses Papier benötigt werden. Diese umfassen das Domain Name System sowie das Border Gateway Protocol.

### 2.1 Domain Name System (DNS)

Wichtiger Bestandteil des Internets ist das Domain Name System (DNS) [2] [3]. Es wurde entwickelt, um den Umgang mit den kryptischen IP-Adressen des Internets zu erleichtern. Es erlaubt das Zuordnen eines Namens zu einer IP-Adresse und bietet Möglichkeiten, einen solchen Namen in seine zugehörige IP-Adresse aufzulösen und umgekehrt. Im Falle des Lehrstuhl-Webservers zum Beispiel ist dies die Zuordnung des Namens `www.net.in.tum.de` zu der IP-Adresse `131.159.15.242`.

Des Weiteren ist das DNS hierarchisch aufgebaut, d.h. es werden nicht alle Zuordnungen in einer großen Datenbank aufgehoben, sondern der Namensraum in Domänen und Subdomänen aufgeteilt. Ein für eine Domäne zuständiger DNS-Server kennt alle Namen und IP-Adressen der Rechner seiner Domäne. Außerdem kennt er die Adressen der DNS-Server seiner Subdomänen, wodurch eine weitere Bearbeitung der Anfrage ermöglicht wird.

Zu der obersten Domäne, der sogenannten Root-Domain, gehören 13 DNS-Server. Da alle Server gleichen Datenbestand enthalten, wird eine hohe Redundanz und Lastverteilung erzielt. Ein Ausfall von 5 der 13 Root-Server stellt keine Gefahr für die Funktionsfähigkeit des Systems dar.

Alle deutschen Websites, d.h. die Domänen mit der Endung `.de`, z.B. `tum.de`, sind in der Länderdomäne `.de` zusammengefasst. Diese ist eine Subdomäne der Root-Domain. Anfragen betreffend einer Subdomäne werden von den Root-Servern mit der Rückgabe der Adressen von den zuständigen Servern dieser Domäne beantwortet. Dadurch wird dem Anfrager ermöglicht, sich durch die Hierarchie zu fragen.

Ein Ausfall aller Root-Server würde zu einem Totalausfall des DNS führen, wobei keine Adresse mehr unter ihrem Namen erreichbar wäre. Ein Ausfall aller Server einer Subdomäne führt zur Nichterreichbarkeit der in der Domäne verwalteten Rechner sowie der Subdomänen dieser Domäne – eine deutlich kleinere Beeinträchtigung des Systems. Somit lässt sich folgern, je höher ein DNS-Server in der Hierarchie positioniert ist, umso besser sollte er geschützt sein. Dieses gilt vor allem für die Root-Server.

Der Ausfall eines oder mehrerer DNS-Server bleibt meistens nicht unbemerkt. So kann schnell darauf reagiert werden. Ein größeres Problem stellt hingegen das sogenannte Domain Hijacking (zu Deutsch: Domänen-Entführung) dar. Hierbei wird die DNS-Anfrage von einem nicht-autorisierten Server beantwortet und der Anfrager zu einer falschen IP-Adresse geleitet. Ob und wie so etwas möglich ist, hängt vom Routingprotokoll ab, welches im Internet typischerweise BGP ist, und im Folgenden erläutert wird.

### 2.2 Border Gateway Protocol (BGP)

Das Internet besteht aus vielen autonomen Systemen (AS), d.h. Netze und Router unter der Kontrolle jeweils einer Organisation. Routing zwischen ASen findet mit Hilfe des Border Gateway Protocols (BGP) [4] [5] statt. Innerhalb eines AS kann ein beliebiges Routingprotokoll verwendet werden. Neben BGP kommen hier unter anderem noch OSPF und RIP zum Einsatz.

Wird an einem Router ein neuer Kommunikationspfad geschaltet, informiert der Router seine Nachbar-Router über das neue Ziel. Mit Hilfe eines solchen Router-Announcements (zu Deutsch: Routerankündigung) können die Nachbar-Router ihre Rou-

tingtabellen aktualisieren und ihre Nachbar-Router informieren. Dabei wird auch der Routingpfad aufgebaut, da jeder beteiligte Router seine eigene Adresse einfügt, bevor er die Ankündigung weiterleitet. Somit wissen alle Router, die eine Ankündigung erhalten haben, welches neue Ziel es gibt und wie es zu erreichen ist.

Kommt es zu Fehlern in den Router-Announcements, können so Teile des Internets falsch geroutet werden und in größerem Maße Paketverluste auftreten. Solche Fehler treten vereinzelt von Zeit zu Zeit auf. Meistens ist eine falsche Implementierung von BGP in einem Router der Auslöser.

Aber auch ein Angreifer könnte mit Hilfe einer Router Ankündigung einigen Schaden anrichten. Hierzu leitet er eine eigene Ankündigung ins Internet, mit der Absicht den Adressraum seines Opfers, z.B. die Adresse eines DNS-Servers, an eine beliebige, vom Angreifer bestimmbare Adresse umzuleiten. Alle Anfragen an den ursprünglichen DNS-Server könnten so von einem DNS-Server des Angreifers beantwortet werden. Somit hat der Angreifer Kontrolle über die auf dem DNS-Server des Opfers verwalteten Domänen – die Domänen sind entführt worden (Domain Hijacking).

Die Meisten solcher Angriffe sind durch BGP-interne Methoden oder vernünftige Router-Konfigurationen abwehrbar. Beispielsweise braucht ein Router nicht Ankündigungen von jedem Router zu akzeptieren, sondern nur von solchen, die vom Administrator als sicher eingestuft wurden. Dieses bedeutet jedoch einen erhöhten Konfigurationsaufwand. Des Weiteren wird der weiterentwickelte Standard DNSSEC unter anderem eine Authentifizierung von DNS-Servern gegenüber Clients ermöglichen. Clients können somit über die Echtheit der erhaltenen Antworten entscheiden. Bis wann dieser Standard eingeführt wird ist unklar und ob jemals alle DNS-Server umgestellt werden ist fraglich. DNSSEC wird in Zukunft eine Reihe von Angriffen ausschließen oder erschweren. Derzeit bietet DNS jedoch keinen eigenen Schutz.

## 3 Ein Filter zum Schutz von Pfaden zu DNS-Servern

Zur Erläuterung der Idee ist ein Blick auf die Positionierung der Root-Server im Internet notwendig. Sie befinden sich an strategisch wichtigen Knoten mit sicheren und stabilen Anbindungen und sind weltweit verteilt. Da sich an der Konnektivität der DNS-Server selten etwas ändert, weisen die Pfade zu den DNS-Servern ebenfalls eine gewisse Stabilität und damit Statik auf. Die Idee hinter dem Filter ist nun, die Dynamik des BGP-Systems zu bremsen, d.h. BGP-Ankündigungen, die zu kurzfristigen Pfadänderungen zu einem Root-Server führen, abzulehnen. Sollte dadurch die Verfügbarkeit eines Root-Servers für einen gewissen Zeitraum verloren gehen, ist dieses akzeptabel, da das Domain Name System durch die hohe Redundanz in seiner Funktionalität nicht beeinträchtigt wird.

### 3.1 Umsetzung 1: Ein einfacher Filter

Eine einfache Umsetzung dieser Idee zeigt sich in folgendem Algorithmus. Ein Provider wählt für jeden der Root-Server genau einen gültigen Pfad aus. Alle BGP-Ankündigungen, die zu Änderungen in einem dieser Pfade führen würden, werden vom Filter abgelehnt. Dadurch wird sichergestellt, dass keine Änderung, ob gewollt oder nicht, in der Wegewahl zu den Root-Servern geschieht.

Sollte nun der Pfad zum Root-Server ausfallen und eine Ankündigung über den zeitweiligen Ersatzpfad eintreffen, wird dieser abgelehnt. Der betreffende Root-Server ist damit vom Provider aus nicht mehr erreichbar. Da die 13 Root-Server identischen Datenbestand enthalten, ist für einen Provider wichtig, dass zu jedem Zeitpunkt mindestens ein Root-Server erreichbar ist. Der Ausfall von bis zu 12 Root-Server-Pfaden ist somit über einen gewissen Zeitraum akzeptabel.

Ist der Ausfall der Leitung über einen längeren Zeitraum nicht behebbar oder sollte eine permanente Änderung im Pfad zu dem Root-Server auftreten, muss der neue Pfad vom Administrator manuell eingepflegt werden, da der Filter über keinerlei Anpassungsautomatik verfügt.

### 3.2 Umsetzung 2: Ein adaptiver Filter

Das Einpflegen von Pfadänderungen durch den Administrator ist aber zeit- und dadurch kostenintensiv. Eine gewisse automatische Anpassungsfähigkeit, z.B. Einsatz eines Backup-Pfades, wäre daher wünschenswert. Hierzu wird der Algorithmus erweitert. Bei der Einrichtung des Filters wird vom Administrator eine Liste gültiger Pfade hinterlegt, die ausschließlich verwendet werden dürfen.

Des Weiteren wird die Arbeit des Filtersystems in drei Phasen unterteilt. Zunächst beobachtet der Filter für eine festgelegte Zeiteinheit eintreffende Ankündigungen ohne diese einzupflegen. Anschließend werden die durch die Ankündigungen gefundenen potentiellen Pfade getestet. Nur alle für gültig befundene Pfade kommen für die nächste Zeiteinheit in den Filter – ungültige Pfade werden verworfen. Damit beginnt der Filter seine Arbeit erneut mit Beobachten.

#### 3.2.1 Phase 1: Beobachten der Router-Announcements

Zunächst muss vom Administrator festgelegt werden, wie lange der Filter Router-Announcements beobachtet und sammelt. Dieser Zeitraum beträgt typischerweise eine Woche. Während dieser Zeit wird über Ankündigungen Statistik geführt. Nur Pfade, die während dieser Zeit und in einer gewissen Häufigkeit angekündigt wurden, kommen überhaupt als gültige Pfade während der nächsten Zeiteinheit in Frage. D.h. alle bereits im Filter befindlichen Pfade müssen erneut angekündigt werden, da sie sonst aus dem

Filter gelöscht werden. Da gültige Pfade regelmäßig angekündigt werden, stellt dies kein Problem dar. Außerdem wird dadurch ein regelmäßiges Überprüfen der bereits bekannten Pfade sichergestellt.

Des Weiteren wird eine Statistik über die Benutzung der im Filter befindlichen Pfade geführt.

### **3.2.2 Phase 2: Testen aller gefundenen Pfade**

Als nächsten Schritt müssen die während der Beobachtungsphase gefundenen Pfade auf Gültigkeit getestet werden. Dieses kann manuell geschehen. Beispielsweise kann hier auf BGP-Anomalien geprüft werden oder ob das AS, von dem die Router-Announcements ausgingen, überhaupt für das angekündigte Ziel zuständig ist. Diese Möglichkeiten sind jedoch zeitaufwendig und nicht immer aussagekräftig.

Alternativ kann der Pfad mit Hilfe der Redundanz im DNS überprüft werden. Hierzu werden verschiedene, zufällig ausgewählte DNS-Anfragen sowohl über den neuen als auch über einen der alten und damit gültigen Pfade verschickt. Die jeweiligen Antworten werden miteinander verglichen. Liefert der neue Pfad dieselben Antworten wie der alte, so wird der neue Pfad als gültig eingestuft.

Einzigster Schwachpunkt dieser Methode ist, dass ein im neuen Pfad befindlicher Angreifer zunächst korrekte Antworten schicken kann, um in die Liste der gültigen Pfade aufgenommen zu werden. Da alle Pfade jedoch kontinuierlich überprüft werden, wird im Laufe der Zeit eine falsche Antwort des Angreifers bemerkt und der Pfad gelöscht werden.

### **3.2.3 Phase 3: Einpflegen gültiger Pfade in den Filter**

In dieser Phase werden ungültige Pfade sofort verworfen und überhaupt nur als gültig eingestufte Pfade betrachtet. Ist ein solcher Pfad neu, wird er in den Filter eingepflegt. Hierdurch wird der Filter erweitert. War der Pfad bereits während der letzten Zeiteinheit im Filter, so wird mittels der Häufigkeit, wie oft der Pfad während der letzten Zeiteinheit benutzt wurde, über den Verbleib des Pfades im Filter entschieden. Nur wenn der Pfad oft genug verwendet wurde, bleibt er im Filter – ansonsten wird er verworfen und der Filter verkleinert.

## **3.3 Anmerkungen**

Gewisse Parameter haben direkte Auswirkungen auf den durch den Mechanismus gebotenen Schutz bzw. die Erreichbarkeit der geschützten DNS-Server.

Die Länge der Beobachtungsphase bestimmt die Häufigkeit der Tests. Während eine lange Beobachtung genauere Statistiken zu den Ankündigungen liefert, finden jedoch auch weniger Tests statt. Dadurch tritt zwar weniger Last auf, aber es verbleiben irrtümlich gültige oder ungültig gewordene Pfade länger im Filter. Eine zu kurze Beobachtungsphase liefert eventuell keine stabile Zuordnung ob ein Pfade gültig ist oder nicht. Es kann zu alternierendem Einpflegen und Löschen des Pfades in den bzw. aus dem Filter kommen. Hierdurch wird wiederum nur unnötig Last erzeugt.

Der zweite Aspekt ist die Häufigkeit, mit der Ankündigungen erfolgen müssen. Setzt man diesen Wert zu hoch an, haben neue Pfade keine oder geringe Chancen in den Filter zu gelangen. So schützt der Filter auch vor von Angreifern angebotenen Pfaden sehr effektiv. Sollte dieser aber ein Ersatz für einen ausgefallenen Pfad zu einem DNS-Server sein, so kann die Erreichbarkeit des DNS-Servers auf längere Sicht verhindert werden. Zieht man zu viele sporadisch angekündigte Pfade in Betracht, erzeugt man unnötig Testlast und erhöht das Risiko einen manipulierten Pfad zu erwischen.

Als Letztes sollte erwähnt werden, dass ein neuer gültiger Pfad, der kurz nach Beginn der Beobachtungsphase eintrifft, um die Länge der Beobachtungsphase verzögert wird, bevor er in den Filter aufgenommen werden kann. Dieses ist bei Ausfall eines wichtigen Pfades, für den ein Ersatzpfad angekündigt wird, besonders verheerend. Der vorgestellte Mechanismus sollte verändert werden, um auf diese Situation schnell reagieren zu können. Dazu wird zusätzlich zur Länge der Beobachtungsphase ein viel kleineres Intervall betrachtet. Übersteigt die Häufigkeit der Ankündigungen eines bestimmten Pfades innerhalb dieses neuen Intervalls einen definierten Schwellwert, wird der Pfad sofort als gültig angesehen und in den Filter eingepflegt, womit er für die Wegewahl zur Verfügung steht. Am Ende der Beobachtungsphase durchläuft auch dieser Pfad die Tests und wird gegebenenfalls wieder aus dem Filter entfernt.

## 4 Durchgeführte Tests und gewonnene Erkenntnisse

Für die Tests wurden BGP-Announcements verwendet, die im Laufe eines Jahres von einem RIPE-Beobachtungsknoten gesammelt wurden. An diesem Knoten waren insgesamt neun Provider aus USA, Japan und Europa angeschlossen. Jeder dieser Provider hatte zumindest zeitweise Konnektivität zu allen 13 Root-Server des DNS. Mit Hilfe dieser Daten lässt sich die Arbeitsweise des Filters überprüfen und die gewollte Beeinträchtigung auf das BGP-System abschätzen.

### 4.1 Pfadstabilität der Root-Server

Da der Filter auf Basis von stabilen Pfaden zu den Root-Servern arbeitet, muss dies zunächst verifiziert werden. Hierzu wurde für jeden Provider und Root-Server ermittelt, wann welcher Pfad im Laufe des Jahres verwendet wurde. Es stellte sich heraus, dass die meisten Provider zu allen Servern hauptsächlich nur wenige Pfade benutzten. Alternative Pfade wurden nur sehr selten und nur für sehr kurze Zeit hergenommen. Im Schnitt wechselte ein Provider dreimal im Jahr seinen Pfad zu einem Root-Server – er benutzte also vier Hauptpfade.

### 4.2 Test des einfachen Filters

Für einen Router, der mit dem einfachen Filter ausgestattet wäre, bedeutet dies, dass der Administrator pro Root-Server dreimal im Jahr die Konfiguration anpassen und den neuen Pfad eintragen muss, da der Root-Server sonst auf Dauer nicht mehr erreichbar ist. In den kurzen Intervallen, in denen ein alternativer Pfad verwendet wurde, wäre der Root-Server infolge des Filterns nicht erreichbar gewesen.

Auf die Erreichbarkeit der Root-Server bezogen, zeigt sich erst für 12 Server eine Differenz – 100 Prozent Erreichbarkeit ohne Filter gegenüber 96 Prozent Erreichbarkeit mit Filter. Für die Erreichbarkeit aller 13 Servern beträgt die Differenz 11 Prozent. Aber sowohl mit als auch ohne Filter war immer mindestens ein, meistens jedoch 11 von 13 Root-Server erreichbar. D.h. das Domain Name System hätte zu jedem Zeitpunkt einwandfrei funktioniert.

Bei einem der Provider fiel die Erreichbarkeit aller 13 Root-Server auf 35 Prozent mit Filter. Das lässt sich darauf zurückführen, dass der Provider regelmäßig verschiedene Pfade benutzt hat. Da der einfache Filter nur einen Pfad je Root-Server erlaubt, käme es zu massiven Ausfällen. Meistens wäre mindestens ein Root-Server zu erreichen, jedoch zeigt dieses Beispiel die Unflexibilität des einfachen Filters sehr gut auf.

### 4.3 Test des adaptiven Filters

Würde man den Router mit dem adaptiven Filter ausstatten, zeigt sich ein deutlich besseres Bild. Zunächst bleibt festzuhalten, dass, abgesehen von der erstmaligen Einrichtung, kein weiterer Aufwand auf den Administrator zugekommen wäre.

Die wichtigsten Erkenntnisse waren:

- Sechs der neun Provider konnten mindestens einen Root-Server 100 Prozent der Zeit erreichen, die anderen drei über 99,97 Prozent der Zeit.

- Sechs Root-Server konnten von zwei Providern immer erreicht werden, die anderen mindestens 99,85 Prozent der Zeit.

- Konnektivität zu allen 13 Root-Servern bestand bei allen Providern zu mehr als 90 Prozent der Zeit – außer bei einem Provider. Dieser hatte auch ohne Filter zu einem der 13 Root-Server während 71,5 Prozent der Zeit keinen Pfad.

Daraus ergibt sich, dass dieser Filtermechanismus nicht von Providern eingesetzt werden darf, die ohne Filter bereits Probleme mit der Erreichbarkeit der DNS-Server

haben. Auf Provider mit stabiler und alternativenreicher Konnektivität hat der Filter jedoch so gut wie keine negativen Auswirkungen.

#### **4.4 Sonstige Erkenntnisse**

In den BGP-Daten waren nicht nur gültige Ankündigungen. Durch Fehlkonfiguration wurden auch ungültige Pfade angekündigt. So gingen von einem AS Ankündigungen über einen DNS-Server als neues Ziel aus, obwohl dieses AS für diesen DNS-Server gar nicht zuständig war. Von den neun ungefilterten ASen nahmen vier diese Ankündigungen an und stellten ihre Wegewahl zu dem DNS-Server um. Der Filter hätte alle bis auf eine der Ankündigungen ignoriert. Der Pfad der verbliebenen Ankündigung wäre in die Testphase zur weiteren Untersuchung gereicht worden.

Des Weiteren werden im Filter keine kryptografischen Routinen verwendet. Dadurch werden extrem rechenintensive Operationen vermieden und der Mechanismus gegenüber wohl bekannten und effektiven Knackalgorithmen unempfindlicher.

Abschließend bleibt festzuhalten, dass die durchgeführten Tests zwar positiv verliefen, d.h. der vorgestellte Mechanismus im Prinzip funktioniert, aber weitere Verbesserungen nötig sind.

## 5 Zusammenfassung

Dieses Papier gibt eine Einführung in den unter [1] vorgestellten Mechanismus zum Schutz der Pfade zu Root-Servern und geht näher auf die Thematik ein. Der Filter verwendet zwei wichtige Eigenschaften des Internets. Mögliche kurzzeitige Ausfälle eines Root-Servers werden durch die hohe Redundanz im DNS kompensiert. Kurzlebige und ungültige Pfade zu Root-Servern können wegen einer gewissen Stabilität in den Pfaden zu Root-Servern aussortiert werden. Im Wesentlichen akzeptiert der Filter nur langfristig angekündigte Pfade. Ungültige oder instabile Pfade, welche eine deutlich kürzere Verweilzeit im BGP-System aufweisen, werden dadurch herausgefiltert. Tests mit über einen längeren Zeitraum gesammelten BGP-Daten zeigten, dass der Filter so funktionieren kann und weder das DNS noch das BGP-System stark beeinträchtigt. Dennoch sollte dieser Mechanismus nicht der einzige Schutz bleiben. Die Weiterentwicklung sowohl des Filters als auch von BGP und DNS ist zwingend erforderlich. Im Falle von DNS ist ein neuer Standard, DNSSEC, in Arbeit. Aber auch DNSSEC wird alleine keinen ausreichenden Schutz bieten. Daher ist eine Kombination verschiedener Methoden erforderlich. Beispielsweise könnte die mit DNSSEC mögliche Authentisierung der DNS-Server als weiteres Prüfkriterium während der Testphase des Filters verwendet werden. Nachteil des vorgestellten Mechanismus bleibt, dass die Arbeit des Filters rechenintensiv ist, d.h. unter Umständen müssten vorhandene Netzkomponenten aufgerüstet werden. Daher sind Sicherheitskonzepte, die nur auf DNS und/oder BGP basieren und auf aktuellen Netzkomponenten problemlos laufen, zu bevorzugen.

## Literatur

- [1] Lan Wang, Xiaoliang Zhao, Dan Pei, Randy Bush, Daniel Massey, Allison Mankin, S. Felix Wu, Lixia Zhang: *Protecting BGP Routes to Top Level DNS Servers*; Proceedings of the 23rd International Conference on Distributed Computing Systems, Mai 2003; [http://www.cs.colostate.edu/~massey/pubs/conf/massey\\_icdcs03.pdf](http://www.cs.colostate.edu/~massey/pubs/conf/massey_icdcs03.pdf).
- [2] LRZ: *Was ist das Internet? - Eine Einführung*; <http://www.lrz-muenchen.de/services/netzdienste/internet/>.
- [3] *Programmed Instruction Course - Section 2: Domain Naming*; Connected: An Internet Encyclopedia; <http://www.freesoft.org/CIE/Course/Section2/index.html>.
- [4] Timothy G. Griffin: *An Introduction to Interdomain Routing and BGP*; 28. August 2001; [http://www.cambridge.intel-research.net/~tgriffin/talks\\_tutorials/tutorials/sigcomm2001/](http://www.cambridge.intel-research.net/~tgriffin/talks_tutorials/tutorials/sigcomm2001/).
- [5] Paul Ferguson: *Introduction to the Border Gateway Protocol (BGP)*; 9. Februar 1997; <http://www.academ.com/nanog/feb1997/BGPTutorial>.