Proseminar: Technische Informatik

Seminararbeit

„Home Gateways – Ready for the current and future Internet?“

von Johannes Klick

Gliederung:

1. Einleitung
2. Definition: Home Gateway
3. Existierende Problemstellungen des Internets
   1. Staukontrolle
   2. Knapper Adressraum
   3. Sichere Namensauflösung
4. Mögliche Weiterentwicklungen von Home Gateways
   1. Peer-to-Peer - Unterstützung
5. Fazit
   1. Bereit für das aktuelle Internet?
   2. Bereit für das zukünftige Internet?

1. Einleitung: Home / Residential Gateway

Das Internet hat in den letzten Jahren enorm an Bedeutung für das alltägliche Leben zugenommen. So dient das Internet heutzutage oft zu Zwecken der Kommunikation, den Erwerb von Informationen bzw. Wissen, der Beschaffung von Gütern, Unterhaltung oder Inanspruchnahme von Dienstleistungen wie z.B. Online-Banking. [1]

Entwicklung der Onlinenutzung in Deutschland 1997 bis 2009
gelegentliche Onlinenutzung

	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
in %	6,5	10,4	17,7	28,6	38,8	44,1	53,5	55,3	57,9	59,5	62,7	65,8	67,1
in Mio.	4,1	6,6	11,2	18,3	24,8	28,3	34,4	35,7	37,5	38,6	40,8	42,7	43,5
Zuwachs in %	-	61	68	64	36	14	22	4	5	3	6	5	1,9

Basis: Erwachsene ab 14 Jahren in Deutschland (2009: n=1806, 2008: n=1802, 2007: n=1822, 2006: n=1820, 2005: n=1857, 2004: n=1810, 2003: n=1955, 2002: n=2293, 2001: n=2520, 2000: n=3514, 1999: n=5661, 1998: n=9673, 1997: n=15431).

Abbildung 1:

Quelle: ARD-Onlinestudie 1997, ARD/ZDF-Onlinestudie 1998 – 2009, http://www.ard-zdf-onlinestudie.de/index.php?id=onlinenutzung-entwic

Wie man der obigen Abbildung 1 entnehmen kann benutzten im vergangenen Jahr 2009 ca. 67,1%

aller Deutschen ab 14 Jahren gelegentlich einen Internetanschluss. Dies entspricht der Statistik nach 43,5 Mio. Menschen, wenn man nun zugrunde legt dass allein in den letzten 3 Jahren mehr als 35,5 Mio. PCs verkauft wurden, kann man davon ausgehen dass sich des Öfteren mehrere Computer pro Haushalt befinden. So besitzen folglich viele Haushalte ein kleines Heimnetzwerk und benötigen ein sogenanntes Home bzw. Residential Gateway (auch Heimrouter genannt), welches für alle Rechner den Zugang zum Internet ermöglicht.
Da es keinen Standard gibt, welcher Protokolle vorschreibt die von einem Home Gateway implementiert werden sollten, implementieren viele Hersteller nur die nötigsten Standards, welche direkt für das Surfen durch das Web des Internets von Nöten sind. So werden z.B. noch teilweise Standards von 1987 für das Domain Name System implementiert ohne die aktuellen Erweiterungen für diesen Standard mit zu implementieren. [2]
Des Weiteren werden kurz- bis mittelfristig die IPv4-Adressen knapp werden, da die Anzahl der Nutzer des Internets die Anzahl der verfügbaren Adressen bald übersteigen wird. Dies könnte für potenzielle Nutzer des Internets bedeuten, dass sie keine IPv4-Adresse erhalten und sich somit nicht mit dem Internet verbinden können. Da das Internet aufgrund seiner Informationsfülle und Kommunikationsmöglichkeiten einen wichtigen sozialen Aspekt darstellt, wäre der Ausschluss von einigen Personen aus dem Internet eine gesellschaftliche Katastrophe. Zwar gibt es Möglichkeiten der IPv4-Adressknappheit zu begegnen, indem man auf IPv6 umsteigt und somit 2^{32} mal so viele Adressen zur Verfügung hätte wie jetzt, jedoch verläuft der Umstieg eher schleppend. Denn zur Zeit sind Homegateways mit IPv6-Unterstützung die absolute Seltenheit auf dem Markt, wodurch für die Internetserviceprovider kein Anreiz besteht auf IPv6 umzusteigen, weil die Hardware ihrer Endkunden dies nur selten unterstützt.
Diese Arbeit wird Protokolle analysieren, welche in Home Gateways implementiert werden könnten, um die Integrität des Internets zu verbessern. Als Beispiel hierfür werden das angesprochene Protokoll IPv6, aber auch Protokolle für eine bessere Verkehrskontrolle von Daten wie ECN besprochen und analysiert. Zusätzlich werden auch Protokolle analysiert, welche die Sicherheit der Nutzer erhöhen, dabei wird neben IPv6, welches eine Verschlüsselung von Verbindungen ermöglicht, auch DNSSEC näher erläutert.
Des Weiteren werden mögliche sinnvolle Erweiterungen von Home Gateways wie z.B. Peer-to-Peer diskutiert, wobei auch Bezug auf mögliche Anwendungsszenarien genommen wird.
Abschließend wird diese Arbeit bewerten, ob nach heutigen bzw. nach möglichen zukünftigen Maßstäben die zur Zeit erhältlichen Home Gateways in Bezug auf ihre Funktionalität tatsächlich bereit sind für das Internet oder nur vorgeben dies zu sein.

[1] Studie: Internet facto 2008-I, AGOF - Arbeitsgemeinschaft Online Forschung e.V.,
http://www.agof.de/studienarchiv.587.html
[2]
Test Report: DNSSEC Imposant in Broadcast Routers ans Firewalls, Rat Rebellisch, Lisa Philister, Sept. 2008

2. Definition

Ein Resident bzw. Home Gateway ist eine technische Schnittstelle zwischen dem Netz des Internet Service Providers bzw. dem Internet (der Außenwelt) und dem Heimnetzwerk eines Haushaltes. Umgangssprachlich wird dieses Gerät auch „Router“ genannt, wobei es heutzutage wesentlich mehr Funktionen als das einfache Routen von IP-Paketen beherrscht. So sind in den meisten Gateways auch Firewalls implementiert, welche bestimmte IP-Pakete mit Absicht verwerfen um Angriffe auf das Heimnetzwerk zu verhindern. Oft beherrschen Home Gateways auch DHCP, welche eine dynamische IP-Adressenverwaltung innerhalb des Netzwerkes ermöglicht.
Betrachtet man die vergangene Entwicklung von einem damaligen einfachen Router mit einem externen Modem bis hin zu den heutigen viel leistungsfähigeren multimedialen Home Gateways, welche u.a. IPTV, VoIP, ISDN, DECT unterstützen, kann man erahnen, dass das Home Gateway

bald zum Zentrum unseres Haushaltes werden wird. [1]
Ein gutes Beispiel für die rasante Entwicklung der Home Gateways ist z.B. die neue Fritz Box von AVM, die „FRITZ!Box Fon WLAN 7390“. [2]
Dieses Resident Gateway kann neben den normalen Routinefähigkeiten auf IP-Ebene sogar IPsec unterstützen, wodurch es möglich ist, dass dieses Gateway über eine sichere VPN-Verbindung direkten Kontakt zu einem anderen Netzwerk herstellt. Dies ermöglicht, dass nicht jeder einzelne Rechner des Heimnetzwerkes eine eigene VPN-Verbindung mit den Netz, z.B. einer Universität, herstellen muss. Des Weiteren kann dieses neue Gateway, mittels eines fest integrierten Speichers (512 Megabyte) oder via USB angeschlossene Speichermedien, Mediendateien streamen.
Zusätzlich können an diesem Gerat ISDN sowie auch analoge Telefongeräte angeschlossen werden. Man könnte dieses Gerät nicht nur als Home Gateway sondern als ein Kommunikations-Media-Center bezeichnen.
Besonders bemerkenswert ist, dass nach einem Firmwareupdate (Betaversion) die Möglichkeit besteht eine IPv6 Unterstützung zu erhalten. In Anbetracht des später folgenden Kapitels 3.3 ist dies ein interessanter Fakt.

[1] White Paper, Home Gateway, Satish Gupta (Wipro Technologies), 2002, S. 4
[2] Datenblatt der Fritz!Box Fon Wlan 7390,
http://www.avm.de/de/Produkte/FRITZBox/FRITZ_Box_Fon_WLAN_7390/index.html

3.1 Staukontrolle

Durch Datenstaus kann die Funktionalität des Netzwerkes eingeschränkt werden, weshalb die Staukontrolle von Bedeutung ist.
Normalerweise wird ein Paket von Host A nach Host B verschickt, indem es von einem oder mehreren Routern im Netzwerk in Zielrichtung weitergeleitet wird. Leider kommt es des Öfteren vor, dass ein Router Z mehr Pakete weiterleiten soll als er verarbeiten kann, dann bearbeitet der Router Z erst alle Pakete die am Anfang seiner Warteschlange (Puffer) stehen und verwirft alle anderen ankommenden Pakete bis er wieder Kapazitäten hat, um neue IP-Pakete zu verarbeiten. Diesen naiven Ansatz nennt Tail-Drop-Algorithmus. Natürlich kommt es hier nicht nur zur Paketverlusten sondern auch zu Paketverzögerungen denn die Pakete in der Warteschlange müssen schließlich warten und kommen daher verspätet beim Sender an. Dies kann für Echtzeitanwendungen wie z.B. Voice over IP (VoIP) unangenehm werden, da veraltete Sprachpakete nicht mehr nützlich sind. [1]
Das Internet und viele andere Netzwerke basieren zu großen Teilen auf TCP, einem Protokoll der Transportsicherungsschicht (OSI-Schicht 4), welches von der IETF 1981 im RFC 293 standardisiert wurde. Bei TCP wird für jedes empfangende Paket eines Hosts A an einen Host B, welches z.B. über Router Z geleitet wird, als Empfangsbestätigung für Host A ein sogenanntes ACK-Paket geschickt. Wenn Host A mehr Pakete hintereinander sendet als Router Z verarbeiten kann, droht der Puffer von Router Z über zulaufen. Wenn dies geschieht, wird Router Z alle weiteren ankommenden Pakete verwerfen und somit kann Host B keine Bestätigung in Form eines ACK-Paketes verschicken. Nach einem gewissen Timeout oder durch fehlende bzw. doppelte ACK-Pakete weiß Host A, dass bestimmte gesendete Pakete nicht angekommen sind und halbiert daraufhin die Anzahl der Pakete (*Congestion Window Size)* die er schicken kann, ohne dafür eine Bestätigung erhalten zu haben. [2]
Dadurch werden weniger Pakete von Host A hintereinander versendet, was zu einer Entlastung des Routers führt, wodurch weniger Pakete verworfen werden und somit nicht nochmal gesendet werden müssen. Nach der Verringerung der *Congestion Window Size (CWS)* versucht der Sender diese dann wieder bis zu einem gewissen Grad zu erhöhen. [3]
Jedoch kann dieser Slow Start bzw. Congestion Avoidance Algorithmus zu einer sogenannten globalen Synchronisation führen. Diese entsteht, wenn mehrere Sender gleichzeitig eine

Überlastung des Netzwerkes registrieren, die z.B. den Router Z betrifft. Daraufhin verringern alle Sender, deren Pakete über Router Z geschickt werden, **gleichzeitig** ihre Sendekapazität und erhöhen sie später gleichzeitig wieder. Dies führt dann jedoch zu einer, sich zyklisch wiederholenden, Überlastung des Routers Z. [4]

Um diese Problematik zu lösen gibt es 2 Ansätze:

Bei dem ersten Ansatz wird die Warteschlangenverwaltung des Routers so verändert, dass sie nicht einfach alle weiteren Pakete verwirft sobald die Warteschlange voll ist. Stattdessen erkennt sie bereits früh, dass sich eine Überlastung des Routers anbahnt und entfernt daraufhin zufällig einige Pakete aus der Warteschlange. Dieser Algorithmus namens RED (Random-Early-Detection) erhöht tatsächlich die Effizienz des Netzwerkes und beugt dem Phänomen der globalen Synchronisation vor. Jedoch kann dadurch keine Dienstpriorisierung im Sinne von QoS (Quality of Service) garantiert werden, da auch Pakete eines priorisierten Dienstes verworfen werden könnten. [5]
Der zweite Ansatz verfolgt das Ziel, die Flusssteuerung nicht nur dem Sender und Empfänger anhand der Ermittlung von verloren gegangenen Paketen zu überlassen. Vielmehr soll dem Netzwerk selber die Möglichkeit gegeben werden, den Endpunkten der Verbindung eine Überlastung des Netzwerkes anzuzeigen, indem es die Erweiterung des TCP/IP-Protokolls namens ECN (Explicit Congestion Notification) nutzt.

Bei ECN (2001 von der IETF im RFC 2581 standardisiert) werden die letzten 2 Bits des Type-of-Service-Feldes eines IP-Header je nach Zustand verändert. Da bei 0 angefangen wird zu zählen, handelt es sich hier um das Bit 6 und 7 des TOS-Feldes. ECN funktioniert genau dann, wenn alle beteiligten Router und Hosts einer Verbindung auch ECN unterstützen. Bei ECN verschickt der Sender IP-Pakete bei denen die Bits 6 und 7 entweder 0,1 oder 1,0 gesetzt sind, wodurch jedem Empfänger des IP-Paketes signalisiert wird, dass ECN genutzt wird. Stellt ein Router eine Überlastung fest, so wird anstatt das Paket zu verwerfen einfach der „Congestion Experienced Codepoint“ (CE) gesetzt, wobei nur Bit 6 und 7 auf 1 gesetzt werden.
Der Empfänger des Paketes wird feststellen, dass der CE Codepoint gesetzt wurde und wird dann ein TCP-ACK Paket mit gesetzten ECN-Echo-Flag im TCP-Header für das empfangende IP-Paket senden. [6]
Der sendende Host A wird nach Erhalt des ACK-Paketes mit gesetzten ECN-Echo-Flag seine Congestion Window Size (CWS) um den Faktor 2 verringern, wodurch das Netzwerk bzw. der Router entlastet wird.

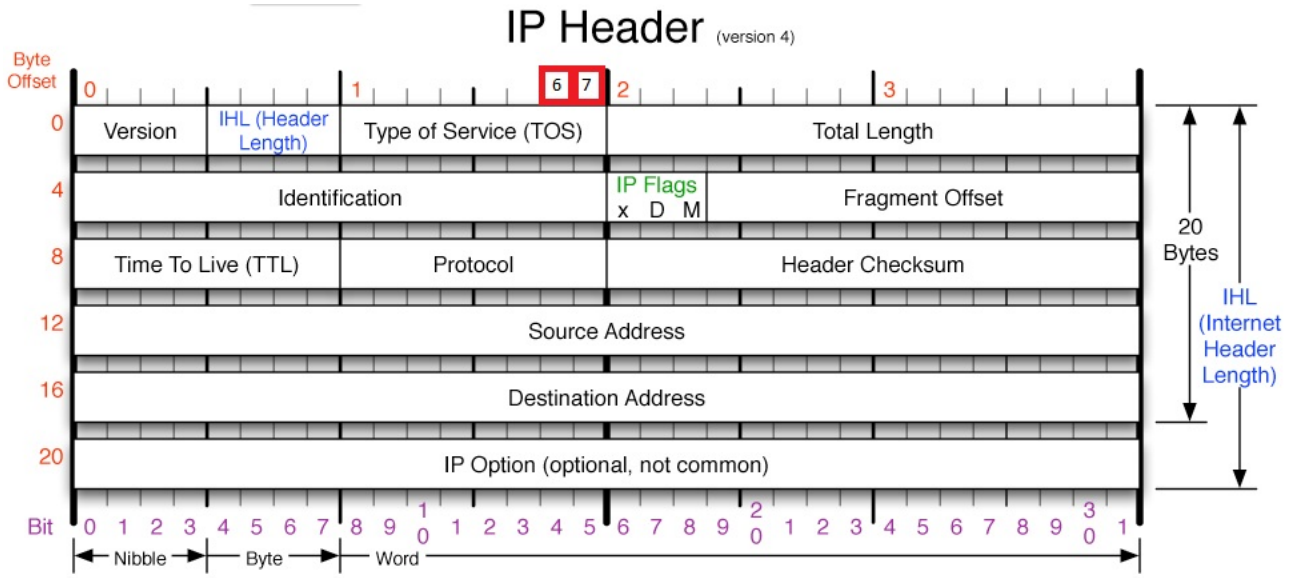


Abbildung 1: IPv4 Paketkopf nach IETF [RFC 291] *Bildquelle: www.visi.com*

Es ist durchaus wahrscheinlich, dass Host B mehrere IP-Pakete mit gesetzten CE Codepoint hintereinander empfängt, woraufhin er auch mehrere TCP Pakete mit gesetztem ECN-Echo-Flag an Host A sendet. Würde der Sender nun bei jedem dieser ACK-Pakete immer wieder die CWS halbieren, wäre die Performance stark beeinträchtigt. Um dies zu vermeiden, wartet er zunächst eine gewisse Periode ab.
Wie man schnell erkennt, ist ECN eine effektive Art und Weise der Staukontrolle, da keine Pakete verworfen werden müssen und der Sender nicht erst auf ein Timeout seiner Pakete warten muss, um eine Überlastung der Verbindung festzustellen.
Da folglich keine Pakete zwei mal versendet werden müssen, bietet ECN mehr Durchsatz und gewährleistet eine verzögerungsärmere und schnellere Kommunikation zwischen den Endpunkten.
Leider kann ECN auch zu Problemen führen, weil viele Router im Internet, die meisten Residential Gateways und auch Firewalls kein ECN unterstützen und so, mangels richtiger Interpretation, eventuell Pakete mit gesetzten ECN-Bits im IP-Header einfach verworfen werden.[7]
Zwar wird bei dem Aufbau einer TCP-Verbindung zwischen den Endpunkten (Host A und Host B) ausgehandelt, ob ECN unterstützt wird oder nicht, jedoch kann es passieren, dass sich nach erfolgreichen Verbindungsaufbau die Route der IP-Pakete durch das Netz ändert und auf einmal über Router geleitet wird, die ECN nicht korrekt unterstützen.
Da immer mehr Home Gateways in den Haushalten Einzug halten, wäre es empfehlenswert, dass die Hersteller ECN implementieren. Ohne die Unterstützung eines Home Gateways würde ECN einfach bei den letzten Metern der Verbindung zum empfangenden Host scheitern. Dies ist insbesondere unerfreulich, da ECN die Zuverlässigkeit und Schnelligkeit des Internets verbessern könnte. Des Weiteren würde auch der Druck auf die Routerbetreiber im Internet steigen ECN zu unterstützen.

[1] Networking Bible,Barrier Sosinsky,John Wiley and Sons, 2009, S. 198
[2] Technik der IP-Netze - TCP/IP incl. IPv6 : Funktionsweise, Protokolle und Dienste , Erwin Hoffman, Hanser Verlag, 2007, S. 126-139
[3] TCP Congestion Control, RFC 2581, http://www.ietf.org/rfc/rfc2581.txt
[4] Geoff Huston, Faster, In: ISP Column, Juni 2008
[5] Computer networks: a systems approach 4. Auflage, Larry L. Peterson & Bruce S. Davie, Morgan Kaufmann Verlag, 2007, S. 487
[6] The Addition of Explicit Congestion Notification (ECN) to IP, RFC 2581
http://www.ietf.org/rfc/rfc2581.txt
[7] Linux Firewalls mit Iptables & Co, Ralf Spenneberg, Pearson Education, 2006, S. 422

3.2 Adressknappheit

Vor ca. 30 Jahren wurde das Internet Protokoll der Version 4 (IPv4) eingeführt, um die damaligen Rechner des Pentagons und diverser amerikanischer Hochschulen über das Arpanet (dem Ursprung des Internets) miteinander zu verbinden. Die damaligen Entwickler des IPv4 Protokolls gingen davon aus, dass eine Adresslänge von 32 Bit, das entspricht 2^{32} = 4.294.967.296 verschiedenen Adressen, ausreichen würde. Jedoch entwickelte sich das Internet unerwartet schnell, so dass die Entwickler der Internet Engineering Task Force (IETF) bereits Anfang der 90er Jahre erkannten, dass der bisherige IPv4-Adresspool langfristig nicht ausreichen würde und begannen aus diesem Grund mit der Entwicklung einer neuen Version des IP-Protokolls. Als Ergebnis wurde dann im Dezember 1998 das RFC 2460 fertiggestellt, welches durch eine Adresslänge von 128 Bit 2^{128} Adressen zur Verfügung stellt und damit 2^{96} mal so viel Adressen beherbergt wie IPv4. [1]
Bei Betrachtung des IPv6 Paketkopfes (siehe Abb. 2) fällt auf, dass dieser wesentlich schlanker und übersichtlicher wirkt als der Paketkopf des IPv4 Protokolls.
Dies liegt daran, dass die Felder IHL, Type of Service (TOS), Identification und Header Checksum komplett gestrichen wurden und eine einheitliche Paketkopfgröße von 40 Byte festgelegt wurde. Denn bei IPv6 wurde nicht nur der Adressbereich vergrößert, sondern auch viele zusätzliche

nützliche Eigenschaften hinzugefügt.
So werden IP Pakete nicht mehr anhand von Checksummen auf Konsistenz überprüft und zu große IP Pakete werden auch nicht mehr fragmentiert. Dies entlastet die Router des Internets stark, da die Checksummenberechnung und Fragmentierung von IP Paketen als Hauptaufgabe von IPv4 Routern gilt. [2] Ist ein IPv6-Paket zu groß für einen IPv6 Router, so wird das Paket verworfen und eine Meldung an den Absender geschickt, welcher anschließend die gesendeten Pakete an die entsprechende Maximum Transmission Unit (MTU) anpassen muss.

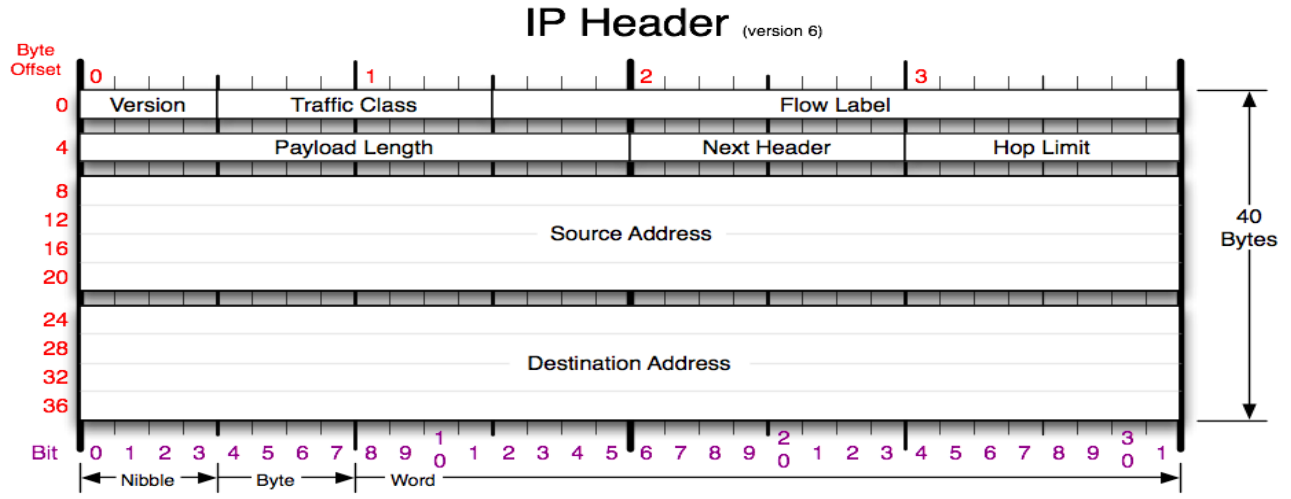


Abbildung 2: IPv6 Paketkopf nach IETF [RFC 2460] *Bildquelle: www.visi.com*

Zusätzlich bietet IPv6 theoretisch durch die Felder Traffic Class und Flow Label die Möglichkeit IP-Paketen eine bestimmte Priorität zuzuweisen. Der Router ist nun in der Lage zu differenzieren, welche Pakete aufgrund ihrer Dringlichkeit als erstes geroutet werden sollten. So ist es möglich IP-Pakete von bestimmten Echtzeitanwendungen wie z.B. VoIP, IPTV oder auch Online -Spielen zu priorisieren, da diese besonders anfällig gegenüber höher Latenzzeit oder Paketverlusten sind.
Durch die stärkere Integration des Internets in den täglichen Lebensablauf steigt auch der Bedarf an Sicherheit, wie z.B. beim Online-Banking. Für solche sicherheitsrelevanten Bereiche wurden Mechanismen wie z.B. SSL entwickelt. Diese beschränken sich jedoch meist auf bestimmte Anwendungen.
Ein anderer Ansatz besteht darin, die Daten bereits auf OSI-Schicht 3 (Networklayer) zu verschlüsseln. Diesen Ansatz verfolgt das Protokoll IPSec, welches von der IETF in den RFCs 2401 bis 2409 standardisiert wurde. Des Weiteren ist IPsec in IPv6 standardmäßig integriert, was bei IPv4 nicht der Fall war. Ipsec umfasst Verschlüsselung, Schlüsselverwaltung und Authentifizierung. Die Authentifizierung verhindert, dass Pakete auf dem Weg zum Empfänger manipuliert bzw. ersetzt werden können. Die Verschlüsselung gewährleistet eine vertrauliche Verbindung zwischen den Kommunikationspartner, während die Schlüsselverwaltung sich um den Austausch der Schlüssel kümmert. Für die Bildung von sog. Virtual Privat Networks (VPN) wird oft IPsec verwendet, welches durch verschlüsselte Tunnel ein logisches Netzwerk auf der bestehenden Netzwerkinfrastruktur bildet.
Jedoch wird das Protokoll IPv6 trotz der vielen Vorteile heute, nach mehr als 10 Jahren der Standardisierung der IETF, kaum genutzt, obwohl sich die real existierende Problemstellung der IPv4-Adressknappheit immer stärker abzeichnet. So werden laut Aussage des Chief Scientist des Asia-Pacific Network Information Center´s (APNIC), ein großer Regionaler Zuteiler von IP-Adressen, die noch zur Verfügung stehenden und unbenutzten IPv4 Adressen global im Jahr 2011 verbraucht sein [3] . Dies würde bedeuten, dass man nicht mehr jedem Nutzer der ins Internet will, garantieren kann, dass er eine IPv4 Adresse erhält. Da das Internet eine wichtige Basis zur Informationsbeschaffung geworden ist, hätte dies für die heutige Informationsgesellschaft gravierende Folgen.

Die Nation China mit ihren Milliarden an Einwohnern wird sieht sich mit dieser Problematik mit als erstes konfrontiert sehen, weshalb China bereits jetzt schon ein Vorreiter bzgl. der Nutzung von IPv6 ist. [4][5]
Der Wechsel von IPv4 zu IPv6 wird jedoch aufgrund der verteilten autonomen Systeme des Internets nicht von Heute auf Morgen möglich sein. Vielmehr wird es dazu kommen, dass viele Geräte „Dual Stack“ fähig sein müssen. Sie müssen also in der Lage sein, beide IP-Versionen zu beherrschen. So können z.B. IPv6 Pakete auch über IPv4 Router via Tunneling (IPv6 Pakete werden in IPv4 Pakete verpackt) geroutet werden. Die genaue Funktionsweise wie IPv6-fähige Geräte mit IPv4-fähigen Geräten zusammenarbeiten können, wurde von der IETF im RFC 4213 mit dem Titel „Basic Transition Mechanisms for IPv6 Hosts and Routers“ bereits im Jahr 2005 definiert. Trotz der rechtzeitigen und weitreichenden Definitionen seitens der IETF läuft die Umstellung auf IPv6 nur schleppend an.
Wie Abb. 3 verdeutlicht, steigt der relative Anteil von IPv6 Adressen an IPv4-Adressen nicht, sondern stagniert eher bei einem Wert von ca. 0,0045 IPv6 Adressen pro IPv4-Adressen.

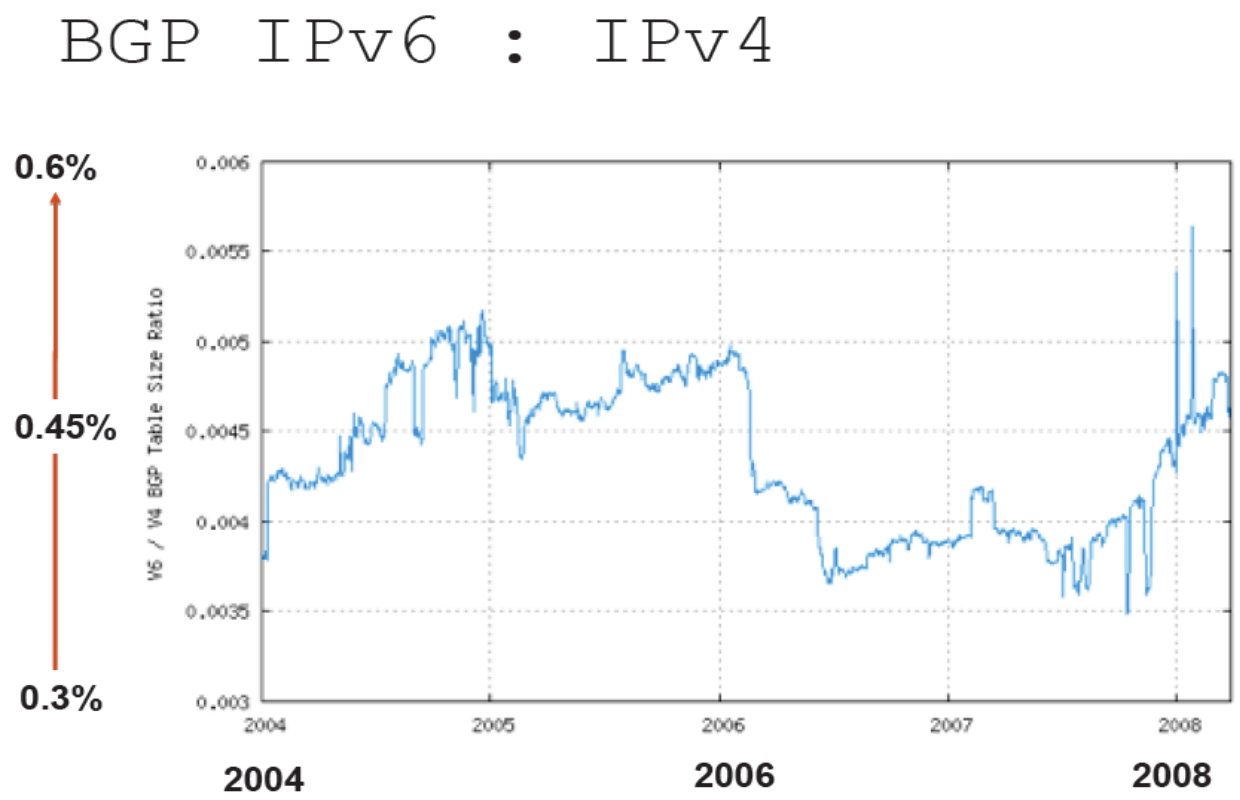


Abbildung 3: Verhältnis von IPv6-Adressen zu IPv4-Adressen in den Router-Tabellen des Border Gateway Protokolls (BGP)

Bildquelle: Maesuring IPv6 Deployment, Geoff Hustman und George Michealson, 56. Ripe Meeting in Berlin, 07.05.2008, Seite 15

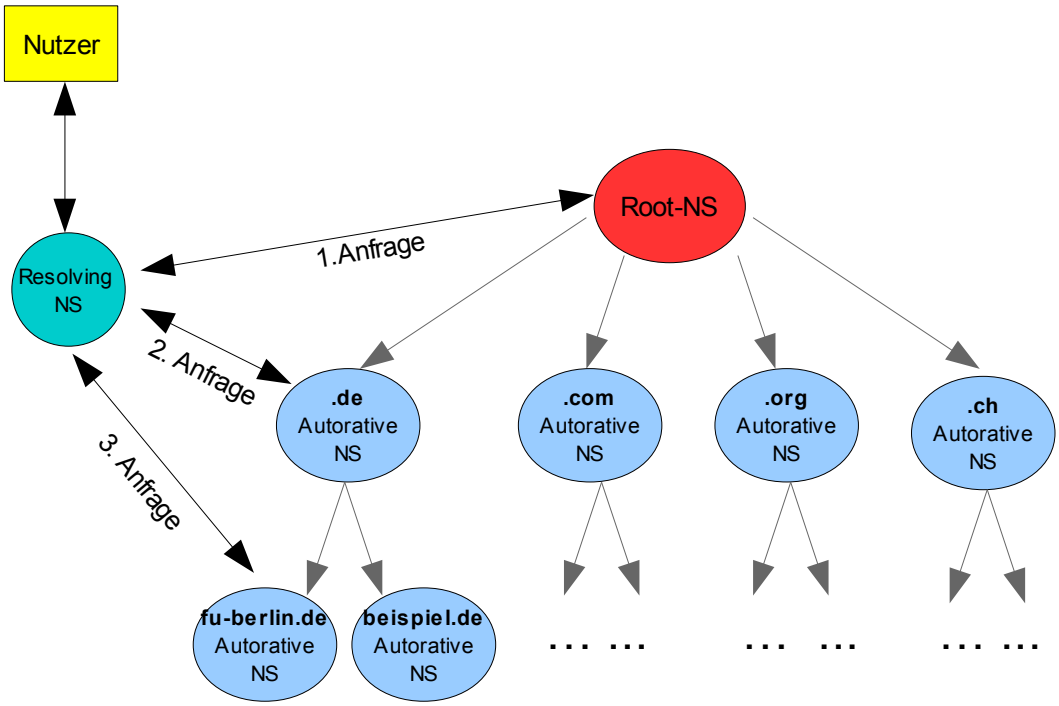
Sicherlich kann man den Internet Service Providern eine gewisse Mitschuld an diesem Zustand einräumen, jedoch verfügt kaum ein Kunde eines ISPs über ein IPv6 fähiges Home Gateway, da diese so gut wie nicht auf dem Markt erhältlich sind. Somit bilden die Gateways der Endnutzer eine wichtige, zu beseitigende Hürde für die weltweite IPv6 Umstellung dar.
Sobald die Bedrohung der Adressknappheit oder die Nichterreichbarkeit von Diensten bzw. Dienstleistungen, die nur über IPv6 angeboten werden, für den Kunden real wird, wird IPv6-Unterstützung ein wichtiges Kaufkriterium sein. Zusätzlich sei angemerkt, dass die gängigen Betriebssysteme wie Windows XP (ab Service Pack 2), Windows 7 und fast alle aktuellen Versionen der verschiedenen Linux-Distributionen IPv6 unterstützen.
Alles in Allem bringt IPv6 mehrere Vorteile und Verbesserungen in Hinsicht auf Performance,

Sicherheit und Adressierbarkeit von Endgeräten im Vergleich mit IPv4. Auch Mechanismen wie NAT und Portforwarding sowie die damit verbundenen Probleme wären nicht mehr notwendig. Abschließend sei bemerkt, dass eine zu spät erfolgte Umstellung auf IPv6 dazu führen könnte, dass auf Grund der dann herrschenden IPv4 Adressknappheit nicht einmal mehr das Dual-Stack-Verfahren möglich wäre, da dafür schließlich jeweils eine IPv4 und eine IPv6 Adresse benötigt werden würde.

[1] IPv6: Grundlagen, Funktionalität, Integration 2. Auflage, Silvia Hagen, Sunny Edition, 2009, S. 1-3
[2] Telekommunikation: Grundlagen, Verfahren, Netze 5. Auflage, Dieter Conrads, Vieweg Verlag, 2004, S. 229
[3] Presentation von Geoff Hustman und George Michealson, 56. Ripe Meeting in Berlin, 07.05.2008, S. 4
[4] Global IPv6 Strategies: From Business Analysis to Operational Planning, Network Buisness Series, Patrick Grossetete, Ciprian Popoviciu, Fred Wettling, Cisco Press, 2008, S. 112
[5] IPv6 Essentials: integrating IPv6 into your IPv4 network, 2. Auflage, Silvia Hagen, O'Reilly Media, Inc, 2006, S. 12-13

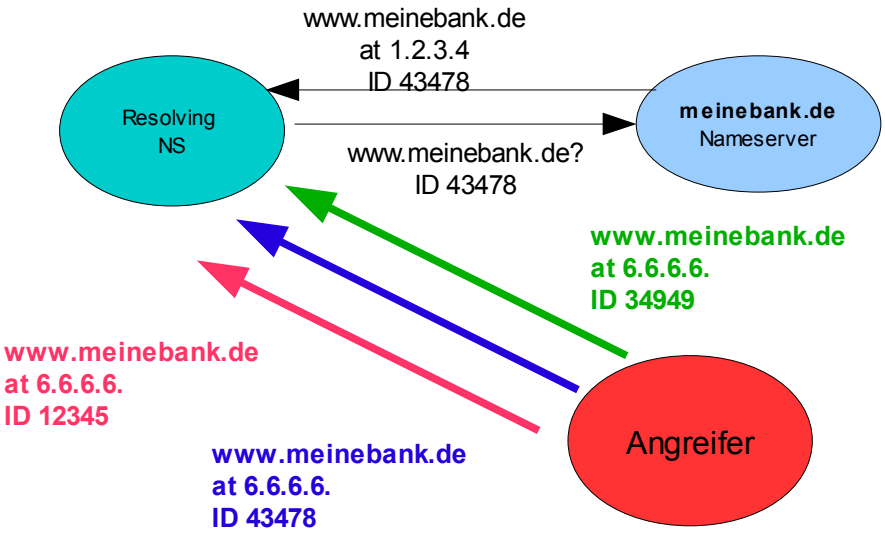
3.3 DNSSEC

Das Domain Name System (1987 von der IETF im RFC 1034 und 1035 standardisiert), oder auch einfach DNS genannt, ist eines der wichtigsten Protokolle des Internets. DNS ermöglicht die Zuordnung von einfach zu merkenden Namen wie z.B. www.fu-berlin.de zu den jeweiligen IP-Adressen. Dies ermöglicht das Auffinden des zu einer Domain gehörenden Web-Dienstes, sowie das Zustellen von E-Mails. Ein Nichtfunktionieren von DNS kommt aus Nutzersicht oft einem Nicht-funktionieren des Internets bzw. des World Wide Webs gleich.
Da das Domain Name System eine wichtige Rolle im täglichen Gebrauch des Internets spielt, ist es auch ein Ziel von Angriffen. Denn durch falsch eingeschleuste Daten in das DNS können Angreifer die Internetbenutzer ohne deren Wissen auf falsche Webseiten umleiten oder auch deren e-Mails abfangen. Zwar bietet das 20 Jahre alte DNS Sicherheitsmaßnahmen, welche jedoch aus heutiger Sicht in Betrachtung der zur Verfügung stehenden Rechen- und Leitungskapazitäten nicht mehr zeitgemäß sind.
Aus diesem Grund hat die IETF im Jahre 1999 die Domain Name Security Extensions standardisiert (ursprünglich definiert im RFC 2535, durch die RFCs 4033,4034 und 4035 im Jahre 2005 aktualisiert). Durch DNSSEC müssen sich die informationsanbietenden Server gegenüber den anfragenden Hosts authentifizieren, wodurch das böswillige Einschleusen von falschen Informationen erschwert wird. Dieses Kapitel wird sich mit den Funktionsweisen von DNS und DNSSEC sowie mit den damit einhergehenden Problemen in Bezug auf Home Gateways beschäftigen.
Die Struktur des DNS Namensraums ist baumförmig. Ein Domainname wird durch Punkte und Labels getrennt, die den Knoten des Baums entsprechen. Zonen sind mehrere Labels, die zusammengefasst wurden. Jede Zone wird von mindestens einem autoritativen Namensserver verwaltet. (siehe Zeichnung 1)
Die Auflösung des Domainnamens erfolgt von rechts nach links, um z.B. den Domainname www.fu-berlin.de aufzulösen, sendet der Nutzer bzw. der stub-Resolver des Betriebssystems eine DNS-Anfrage an einen sog. resolving Nameserver des Internet Service Providers, welcher diese dann an den Root-Nameserver sendet. Anschließend antwortet der Root-Nameserver und verweist auf den für die .de Domaine zuständigen autoritativen Nameserver. Nun wird dieser vom resovling Nameserver nach der Adresse des Webservers mit den Domainnamen www.fu.berlin.de gefragt und erhält als Antwort die IP-Adresse des Webservers. Damit jedoch nicht bei jeder DNS Anfrage der Root-Nameserver kontaktiert werden muss, besitzen die resolving Nameserver Caches, welche die Antworten bereits getätigter Anfragen solange zwischen puffern bis sie ihre Gültigkeit verlieren.



Zeichnung 1: Funktionsweise des Dynamic Name Systems

Der zuletzt antwortende autoritative Nameserver, welcher dem resolving Server die IP-Adresse des gewünschten Webservers liefert, teilt gleichzeitig auch die Time to Live (TTL) mit. Diese legt fest wie lange ein Eintrag in dem Cache des resolving Nameservers gültig bleiben darf.
Exakt an dieser Stelle liegt ein Schwachpunkt im DNS. Falls es ein Angreifer schaffen sollte, den Cache eimes resolving Nameservers mit einem falschen Eintrag bestimmer Domains zu versorgen, können Nutzer zu falschen Webservern weitergeleitet werden.
So könnten Angreifer den Eintrag für www.meinebank.de so verändern, dass alle Nutzer des manipulierten Nameservers, welche www.meinebank.de aufrufen wollen, zu einem anderen Webserver weitergeleitet. Dieser Webserver kann z.B. die Website www.meinebank.de imitieren, so dass ein Nutzer sich dort völlig ahnungslos einloggt und Überweisungen tätigt. Dabei werden in Wahrheit seine Logindaten sowie iTans dem Angreifer übermitteln. So können Angreifer an alle Daten gelangen, die notwendig sind, um selber Überweisungen zu tätigen. Solche Angriffe werden Cache Poisening genannt, weil der Cache quasi mit falschen Einträgen „vergiftet“ wird.
Wenn der resolving Nameserver eine Anfrage an einen autoritative Nameserver stellt, auf eine IP-Adresse wartet und ein Angreifer dies mitbekommt, kann dieser versuchen vor dem autoritativen Nameserver eine Antwort mit einem gefälschten Eintrag und einer hohen TTL zu senden, damit der resolving Nameserver möglichst lange auf einen falschen Server verweist. (siehe Zeichnung 2)
Um solche Angriffe abzuwehren sendet der resolving Nameserver eine 16 Bit lange Query-ID mit und akzeptiert nur Antworten, welche ebenfalls diese Query-ID enthalten. Da sich gegenüber 1987 die heutigen Kapazitäten von Computern und Datenleitungen vervielfacht haben, können Angreifer durch vermehrtes Senden von Antworten, die eine zufällige Query-ID enthalten, versuchen die richtige ID zu erraten, was bei $2^{16} = 65\,536$ möglichen IDs durchaus möglich ist.
Nachdem Dan Kaminsky, ein anerkannter Sicherheitsspezialist, bei seiner Presentation mit dem Titel „*Its The End Of The Cache As We Know It*“, auf der US Black-Hat 2008 aufzeigte, wie schnell man diese Angriffe durchführen konnte, führte dies zu einer raschen Veränderung des Domain Name Systems, indem jetzt nicht nur eine Query-ID sondern zusätzlich auch noch ein bestimmter Port vom resolving Nameserver mitgeschickt wird.
Somit müsste der Angreifer neben der Query-ID noch zusätzlich den richtigen Port erraten, wodurch die Gesamtwahrscheinlichkeit eines erfolgreichen Angriffes zwar stark sinkt, jedoch systematisch nichts an dem bestehenden Problem verändert.
Genau an diesem Punkt setzt DNSSEC an um diese Art von Angriffen systematisch abzuwehren.



Zeichnung 2: Schematische Darstellung von DNS-Cache-Poisening

Anders als bei DNS müssen sich die Server authentifizieren. Denn bei DNSSEC erstellen die autoritativen Nameserver der Zone für jeden Eintrag (Record) eine digitale Signatur (RRSIG Record). [1] Wenn nun der resolving Nameserver einen Eintrag abfragt, wird der autoritative Namensserver mit dem zugehörigen Eintrag und der digitalen Signatur antworten, des Weiteren wird auch noch der öffentliche Schlüssel des autoritativen Nameservers mitgeschickt. Durch den öffentlichen Schlüssel und das Public-Private-Key Verfahren , ist der resolving Nameserver nun in der Lage die digitale Signatur zu überprüfen. [2] Da jedoch der Schlüssel und Inhalt der Nachricht vom selben Absender stammen, ist dies allein noch nicht vertrauenswürdig. Schließlich könnte ein Angreifer eine Nachricht inkl. seines öffentlichen Schlüssel mit seinem eigenen privaten Schlüssel verschlüsseln und absenden. Aus diesem Grund gibt es bei DNSSEC die Vertrauenskette (Chain of trust). Jedem resolving Nameserver wird der öffentliche Schlüssel des Rootservers fest einprogrammiert, so dass jeder resolving Nameserver die Antwort des Rootserver validieren kann. Wenn nun z.B. ein resolving Nameserver aufgrund einer Hostanfrage www.fu-berlin.de auflösen möchte und der Eintrag nicht im Cache vorhanden ist, muss er wie oben beschrieben zuerst den Rootserver fragen. Dieser wird dann die IP-Adresse des autoritativen Nameservers der .de Zone, die digitale Signatur und einen Fingerprint (Hashwert) des .de Zonen-Namenserverschlüssels senden. Anschließend fragt der resolving Nameserver nun den autoritativen .de Namensserver. Als Antwort bekommt dieser nun die IP-Adresse des autoritativen Nameservers für die Zone fu-berlin.de, den Schlüssel und die Signatur sowie einen Fingerprint des *fu-berlin.de* Zonen Namenserverschlüssels. Nach dem Erhalt dieser Informatonen überprüft der resolving Nameserver ob der übermittelte Schlüssel mit dem gesendeten Fingerprint des Rootservers übereinstimmt. Nur wenn dies der Fall ist, werden die Informationen als valide erachtet und es wird fortgefahren.
Nun fragt der resolving Nameserver den autoritativen Nameserver der Zone *fu-berlin.de* nach der IP des Webservers und erhält als Antwort nicht nur diese sondern auch die digitale Signatur und den öffentlichen Schlüssel. Auch hier überprüft wieder der resolving Nameserver ob der übertragende öffentliche Schlüssel des Namesevers mit dem gesendeten Fingerprint des .de Zonen-Nameservers übereinstimmt. Wenn eine Übereinstimmung vorliegt, wird für www.fu-berlin.de ein Eintrag mit der IP des Webservers im Cache des Nameservers vorgenommen und anschließend an den anfragenden Host inkl. einer Information, dass es sich um authentifizierte Daten handelt, geschickt.
Da das oben beschriebene Verfahren die Sicherheit der Namensauflösung stark erhöht, ist es von hoher Bedeutung, dass residential Gateways DNSSEC unterstützen, um zu einem den Endnutzern mehr Sicherheit zu verschaffen und zum anderen DNSSEC bei der Verbreitung zu unterstützen. Jedoch ist die DNSSEC-Unterstützung zur Zeit eher als mangelhaft zu bezeichnen, wie eine Studie von Ray Bellis und Lisa Phifer von 2008 [3] zeigt. Bei dieser Studie wurden 8 Home Gateways, 12 dual Ethernet-Gateway und 4 Hardwarefirewalls getestet. Es ergab sich dass nur 6 Geräte ohne

zusätzliche Konfigurationen sofort DNSSEC fähig waren.
Des Weiteren waren 18 von 22 Geräten mit integrierter DNS-Proxy-Funktion nicht in der Lage Pakete größer als 512 Byte zu bearbeiten. Betrachtet man den Fakt das DNSSEC Pakete oft größer sind als 512 Byte kann dies zu Fehlern führen.
Anscheinend haben die Hersteller dieser Geräte nur den DNS Standard von 1987 (RFC1035) implementiert (welcher eine Limitierung von 512Byte festlegt) und keine seit dem erschienenen Erweiterungen wie z.B. die im Jahre 1999 von der IETF im RFC 2671 spezifizierten Extensions Mechanisms for DNS (EDNS0) welche neben der Aufhebung der 512 Byte-Limitierung auch noch andere wichtige funktionien für DNSSEC beinhaltet.
Offensichtlich ist die Nichtimplementierung von DNSSEC in Home Gateways und Firewalls eine der größten Hemmschwellen für die Verbreitung von DNSSEC. Denn Firewalls und Home Gateways die dieses Protokoll nicht kennen verwerfen oder evtl. verändern die Pakete, so dass die Authentifizieren der Informationen fehlschlägt. In Anbetracht der hohen Bedeutung der sicheren Zuordnungen von Domänennamen und den jeweiligen IP-Adressen der Webserver für die Nutzer des Internets sollten die Hersteller von Home Gateways zwingend die erfordlichen RFCs für DNSSEC der IETF implementieren.

[1] Technik der IP-Netze - TCP/IP incl. IPv6 : Funktionsweise, Protokolle und Dienste , Erwin Hoffman, Hanser Verlag, 2007, S. 185-186
[2] Public/Private Key Pairs , Microsoft Library,
http://msdn.microsoft.com/en-us/library/aa387460%28VS.85%29.aspx
[3] Test Report: DNSSEC Impact on Broadband Routers and Firewalls, Ray Bellis, Lisa Phifer, Sept. 2008, S.1

4.1 Peer-To-Peer

Die zur Zeit für den Konsumbereich zur Verfügung stehenden residential Gateways besitzen nicht die Möglichkeit selbst an einem Peer-to-Peer-Netzwerk wie z.B. Gnutella oder BitTorrent teilzunehmen. Dabei können Peer-to-Peer-Netze wesentlich besser skalieren als typisch Client-Server-Applikationen. Denn ein Peer-to-Peer-Netz (Abk. P2P-Netz) stellt ein dezentrales System zum wechselseitigen Austausch von Ressoucren dar. Alle Computer sind gleichberechtigte Peers, welche miteinander kommunizieren. Jeder Teilnehmer des Netzwerkes ist Server und Client zugleich. Um sich mit einem Peer-to-Peer-Netz zu verbinden muss meistens eine Client-Software installiert werden, welche die Kommunikation unter den einzelnen Peers ermöglicht. Des Weiteren muss mindestens ein Knoten des bestehenden Peer-to-Peer Netzes bekannt sein mit dem eine Verbindung aufgenommen werden kann. In der Regel teilt dieser Knoten dann der Client-Software des Nutzer noch weitere Peer-to-Peer-Teilnehmer mit. Diese wiederum teilen dem Nutzer nach Kontaktaufnahme wieder weitere ihnen bekannte Netzteilnehmer bzw. Knoten mit. So kann aus Nutzersicht eine gewisse Netzwerktopologie des P2P-Netzes wahrgenommen werden. [1][2][3]
Durch die Implementierung von Protokollen der bekannten P2P-Netze könnte das residential Gateway z.B. genau dann Datei bzw. Informationsaustausch betreiben wenn es gerade keine signifikante Auslastung des Netzes durch einen Nutzer des Heimnetzwerkes gibt. So können Beinträchtigung durch den aufkommenden P2P-Datenverkehr verhindert werden. Als Voraussetzung bräuchte das Gateway ein Speichermedium, welches z.B. allen Nutzern des Heimnetzwerkes zur Vefügung gestellt werden könnte. Denke wäre eine interne Festplatte auch auch externe Speichermedien, die per USB angeschlossen werden könnten.
Auch in anderen Bereichen wie dem IPTV kann P2P eine sinnvolle alternative gegenüber den bisherigen kostenpflichtigen Angeboten diverser Anbieter sein. So gibt es die Möglichkeit eine Liveübertragung der sonst kostenpflichtigen Bundesligaspiele sich über ein P2P-Netzwerk anzuschauen. Hintergrund ist in diesem Beispiel ein Chinesischer Fernsehsender, welcher die Rechte an den Spielen der Deutschen Fußball Liga für den Chinesischen Raum erworben hat. Der Chinesische Sender stellt seine TV-Inhalte auch über Online-Streams zu Verfügung, da dies nach Chinesischen Recht erlaubt ist. Es gibt verschiedene P2P-Programme, welche den Stream in ihrem

Netz verteilen und somit nicht nur Chinesischen sondern auch Deutschen Fußballfans einen Fernsehgenuss bereiten. [4] Nachteile dieser Art des Fußballkonsums ist der der Fakt dass es zu einem rechtlich bedenklich ist und zum anderen dass die Fernsehübertragung teilweise einige Minuten verzögert übertragen wird und des Öfteren die Qualität nicht optimal ist.

[1] Internet-Politik in Deutschland: vom Mythos der Unregulierbarkeit,Stefan Scholz,LIT Verlag Berlin-Hamburg-Münster, 2004 S. 319
[2] Peer-to-Peer- Überblick über Konzepte, Architekturen, Plattformen und aktuelle Entwicklungen, Mathhias Bauer, GRIN Verlag, 2007, S. 5
[3] Filesharing: Verantwortlichkeit in Peer-to-Peer-Tauschplattformen,Guido Brinkel, Mohr Siebeck Verlag, 2005, S. 15
[4] Internet-Artikel über P2P-TV, 18.08.2007, http://www.netzwelt.de/news/73316_2-bundesliga-kostenlos-uebers-internet.html

5.1 Bereit für das aktuelle Internet?

Real existierende Probleme die das Internet in den Punkten Performance, Sicherheit und Verfügbarkeit bedrohen, werden anscheinend von den Herstellern der Home Gateways nicht wahrgenommen. Schließlich gibt es bei Home Gateways kaum Unterstützung für Protokolle wie ECN, DNSSEC und IPv6.
Wobei die mangelnde Unterstützung von DNSSEC und IPv6 wirklich fatal ist, weil beide Protokolle einen starken Sicherheitszugewinn für das Internet bedeuten. Da immer mehr sicherheitsrelevante Bereiche wie Banküberweisungen oder Einkäufe über das Internet geschehen, wächst natürlich auch das Sicherheitsbedürfnis der Nutzer des Internets und wenn auf dieses Bedürfnis nicht eingegangen wird, werden viele Nutzer das Internet für sicherheitsrelevante Bereiche nicht mehr Nutzen. Aus diesem Grund kann durchaus die Aussage treffen, dass die Home Gateways oft nur in der Lage sind die absoluten Grundvoraussetzungen für einen Internetzugang zu gewährleistet, da sie teilweise noch Standards von 1987 implementieren und damit als „internetfähig“ bezeichnet werden können. Jedoch scheinen sie nicht bereit zu sein für die aktuellen Herausforderungen des Internets wie z.B. die Adressknappheit und die schwache Sicherheit im bestehende Domain Name System.

5.2 Bereit für das zukünftige Internet?

Da wir in vorherigen Kapitel 5.1 festgestellt haben, dass die zur Zeit verfügbaren Home Gateways nicht in der Lage sind die aktuellen Herausforderungen des Internets zu beherrschen können diese wohl kaum die zukünftigen Herausforderungen des Internets bewerkstelligen. Durch die hohe Anzahl von Menschen ohne Internet in Asien und die kommende Interneterschließung in diesen Gebieten wird folglich der Datenverkehr des Internets rapide ansteigen. Um diesen Datenansturm zu entgegnen wird es allein aus logistischen sowie kosten technischen Gründen eine stärkere Verlagerung von Inhalten des Internets in P2P-Netze geben.
Trotzdem werden Möglichkeiten wie Implementierungen von bekannten P2P-Protokollen zur Zeit von den Gatewayherstellern noch nicht ausgeschöpft, obwohl der von P2P-Anwendunegn verursachter Datenverkehr laut einer Studie von Ipoque (einem ISP Ausrüster) des Jahres 2007 bei 69,25% des gesamten Deutschen Datenverkehrs lag, wohingegen das normale Surfen bzw. der verursachte HTTP-Verkehr bei nur 10% lag. [1] Anhand dieser Zahlen kann man erkennen dass unter den Nutzern sicherlich ein Bedarf an residential Gateways mit P2P-Implementierung besteht. Zwar lassen Lichtblicke wie die FRITZ!Box Fon WLAN 7390 von AVM durch IPv6 und VPN Unterstützung Hoffnung für zukünftige Home Gateways entstehen, jedoch sind die meisten von den zur Zeit auf dem Markt vorhanden Geräte eindeutig nicht bereit für das zukünftige Internet.

[1] Internetstudie 2007, Ipoque, http://www.ipoque.com/resources/internet-studies/internet-study-2007