

HTWK Leipzig
Fachbereich IMN
Wintersemester 2013/2014

Die Internet Protokolle in Version 4 und 6 im Vergleich - ein Überblick

Beleg im Fach Hochgeschwindigkeitsnetze bei Prof. Dr. Klaus Hänsgen

Marcel Kirbst, B.Sc.
Sieglitz 39
06618 Molauer Land
marcel.kirbst@htwk-leipzig.de
15. Mai 2014

Inhaltsverzeichnis

1 Einleitung	4
2 Probleme bei der Verwendung von IPv4	5
2.1 Probleme mit IPv4	5
2.1.1 Adressenknappheit bei Verwendung von IPv4	5
2.1.2 Konfiguration von Netzwerkgeräten unter Verwendung von IPv4	6
2.2 NAT	7
2.3 Ineffizienz in IPv4	8
3 Überblick zu IPv6	9
3.1 Größe des Adressraums	9
3.2 Mehrere IPv6-Adressen pro Netzwerkschnittstelle	10
3.3 Spezielle IPv6-Adressen	11
3.4 Automatische Netzwerkkonfiguration	11
4 Lösungsansätze in IPv6 zu den Problemen mit IPv4	13
4.1 Beseitigung der Adressknappheit auf absehbare Zeit	13
4.2 Vereinfachte Netzwerkwartung	14
4.3 Verkleinerung der Routingtabellen	15
4.4 Flexible Paketheader in IPv6	17
4.5 NAT in IPv6	18
5 Praxisbeispiel - Konfiguration eines Rechners für IPv6-Konnektivität	20
5.1 IPv6-Konnektivität nativ vom Internet Service Provider	20
5.2 IPv6-Konnektivität per Tunnel	20
5.3 Beispielkonfiguration eines IPv6-Tunnels	21
5.3.1 eingesetzte Hardware	21
5.3.2 eingesetzte Software	22
5.3.3 Vorgehensweise bei der Implementierung	22
6 Zusammenfassung und Ausblick	23
7 Quellenverzeichnis	24

Abbildungsverzeichnis

1	Beispielhafte Standardkonfiguration eines Internetanschluss mit NAT, Quelle: Autor, verwendete Symbole unterliegen der GPL	8
2	IP-Konfiguration beispielhaft beim Autor, Quelle: Autor,	12
3	Illustration: Mengenvergleich IPv4-Adressen für die gesamte Erdbe- völkerung zu IPv6-Adressen pro Quadratmillimeter Erdoberfläche. Quelle Illustration: Autor, Quelle Erdfoto: http://upload.wikimedia.org/wikipedia/commons/6/6f/Earth_Eastern_Hemisphere.jpg	14
4	Visuelle Darstellung des Umfangs der Routingtabellen in IPv4 und IPv6, Quelle: http://greenbyte.ch/wp-content/uploads/2012/08/ipv4-ipv6.gif?cf3116	16
5	Beispielhafte Standardkonfiguration eines Internetanschluss mit al- leiniger IPv4-Konnektivität. Da nur eine öffentliche IPv4-Adresse zur Verfügung steht, ist der Einsatz von NAT zwingend erforderlich. Quel- le: Autor, verwendete Symbole unterliegen der GPL	19
6	Beispielhafte Standardkonfiguration eines Internetanschluss mit nati- ver IPv6-Konnektivität, Quelle: Autor, verwendete Symbole unterlie- gen der GPL	19
7	Webseite der Anbieters https://sixxs.net für einen kostenfreien IPv6-Tunnelendpunkt	21
8	Webseite zum Testen der IPv6-Konnektivität: http://test-ipv6.com/	22

Tabellenverzeichnis

1	Laut RFC 5161 vordefinierte Adressprefixe in IPv6	11
---	---	----

1 Einleitung

Diese Arbeit befasst sich mit der Vorstellung der Protokollfamilie IPv6. Neben einem kompakten Überblick über IPv6 soll auf die Notwendigkeit sowie die Vorteile von IPv6 im Vergleich zu IPv4, der derzeit weltweit am meisten im Internet genutzten Protokollfamilie, eingegangen werden.

Im ersten Kapitel [Probleme bei der Verwendung von IPv4](#) werden einige Probleme erläutert, die bei der Verwendung der Protokollfamilie IPv4 auftreten. In Kapitel [Überblick zu IPv6](#) wird die Protokollfamilie IPv6 vorgestellt. Welche Probleme gelöst werden, wenn anstelle von IPv4, IPv6 verwendet wird, wird im Kapitel [Lösungsansätze in IPv6 zu den Problemen mit IPv4](#) erläutert. Im Kapitel [Praxisbeispiel - Konfiguration eines Rechners für IPv6-Konnektivität](#) wird anhand eines Praxisbeispiels erläutert wie sich IPv6-Konnektivität an einem Rechnersystem konfigurieren lässt. Abschließend erfolgt im Kapitel [Zusammenfassung und Ausblick](#) eine Zusammenfassung der Arbeit.

2 Probleme bei der Verwendung von IPv4

Das Internet ist heute überall im täglichen Leben präsent und wird von der UN inzwischen zu den Menschenrechten gezählt.[3] Die im Internet heute noch am häufigsten verwendete Protokollfamilie ist IPv4. Wie der Abschnitt [Probleme mit IPv4](#) darlegt, ist die weitere Verwendung von IPv4 aber mit immer mehr Problemen behaftet.

2.1 Probleme mit IPv4

Zu Beginn der Entwicklung des Internets war nicht abzusehen wie stark sich das Internet bis heute verbreitet. Da das Ziel anfangs war, einige wenige Rechnersysteme mit einander zu verbinden, waren im Jahr 1972 nur 40 Rechner vernetzt.[4] Aus damaliger Sicht ist der Adressraum mehr als ausreichend dimensioniert worden. IPv4 spezifiziert für IPv4-Adressen 32 Bit, das entspricht $2^{32} = 4.294.967.296$ eindeutigen Netzwerkadressen. In den 1970er Jahren entsprach das immerhin annähernd einer IPv4-Adresse pro Erdbewohner.

2.1.1 Adressknappheit bei Verwendung von IPv4

In den 1970er Jahren begannen auch Bildungseinrichtungen und nichtmilitärische Konzerne das Internet zu nutzen. Zu dieser Zeit wurde IPv4 Adressraum relativ großzügig verteilt. Die meisten amerikanischen Unternehmen und Bildungseinrichtungen dieser Zeit erhielten 24 Bit große Adressblöcke. Das bedeutet, dass dem jeweiligen Unternehmen ein Adressblock zugeteilt wurde, welcher 2^{24} also 16.777.216 IPv4 Adressen umfasst. Beispiele für solche Unternehmen sind IBM (Adressraum 9.*.*.*), Hewlett-Packard (15.*.*.*.) und Apple (17.*.*.*.). Eine vollständige Liste lässt sich unter [5] einsehen.

Begünstigt wurde diese Problematik durch die anfängliche strikte Adresseinteilung in Klassen (Class A - E Netze), wobei es sich bei Class-A Netzen um besagte Netze mit 8 Bit langem Netzprefix handelt. Class-B Netze besitzen ein Netzprefix von 16 Bit und Class-C Netze einen Netzprefix von 24 Bit. Es konnten somit nur Netzblöcke für $2^{32} - 2^{24} = 256$ oder weniger Teilnehmer (Class-C Netze), $2^{32} - 2^{16} = 65.536$ oder weniger Teilnehmer (Class-B Netze) oder besagte $2^{32} - 2^8 = 16.777.216$ zugeteilt werden. Beispielsweise bedeutete das für jede Einrichtung, die wenig mehr als 256 IPv4-Adressen benötigte, ein Class-B Adressblock zu beantragen, auch wenn dann ein Großteil der Adressen ungenutzt blieb.

Die nachträgliche Einführung einer Technik namens „Classless Interdomain Routing“ (Abkürzung: CIDR) verbesserte temporär die Problemstellung in der Weise, dass eine so genannte Netzwerkmaske zu jeder IPv4-Adresse angegeben wird, die angibt wieviele Bits der IPv4-Adresse den Netzwerkpräfix zugeordnet werden. Die Netzwerkmaske 255.255.0.0 für die IPv4-Adresse 192.168.12.34 definiert das Netzwerkpräfix 192.168 sowie die Teilnehmeradresse 12.34. Als Kurzschreibweise hat sich alternativ folgende Form verbreitet: 192.168.12.34/16. Hier gibt die Zahl nach dem Schrägstrich die Bitanzahl der Netzmaske an.

Außerdem ist zu erwähnen, dass sich die IPv4-Adressen in einem Netzwerksegment nicht vollständig Teilnehmern zuordnen lassen, da bestimmte Adressen wie beispielsweise 192.168.12.0/24 (Bezeichner für dieses Netzsegment) oder 192.168.12.255/24 (Broadcastadresse in diesem Netzsegment) eine besondere Bedeutung haben.

Ein weiterer Umstand, der die Problematik verschärft, ist das die Zuteilung von IPv4-Addressblöcken durch die IANA endgültig ist. Eine Möglichkeit, IPv4-Adressen zurück zugewinnen ist nicht vorgesehen.

2.1.2 Konfiguration von Netzwerkgeräten unter Verwendung von IPv4

Vor der Entwicklung von DHCP (Dynamic Host Configuration Protocol)[7] musste jedes neue Netzwerkgerät von Hand durch den Benutzer konfiguriert werden um im Netzwerk kommunizieren zu können. Das umfasst mindestens die Vergabe einer IPv4-Adresse mit der zugehörigen Netzmaske um mit Netzwerkgeräten im gleichen Subnetz kommunizieren zu können. Soll das Gerät außerdem noch mit dem Internet kommunizieren können, ist die Angabe der IPv4-Adresse des zuständigen Routers in diesem Subnetz sowie mindestens eines Domain Name Service-Servers (Abkürzung: DNS-Server) erforderlich.

Um unerfahrenen, beziehungsweise unachtsamen Benutzern diese potentielle Fehlerquelle zu ersparen, wurde eine Technik namens Dynamic Host Configuration Protocol (Abkürzung: DHCP) spezifiziert, die es ermöglicht die Konfiguration eines Netzwerkgerätes ohne Eingriff des Benutzers, nur durch einen DHCP-Server, welcher zustandsbasiert arbeitet, in diesem Netzwerksegment vorzunehmen. Dieser Mechanismus arbeitet jedoch nicht zuverlässig und fehlerfrei, beispielsweise wenn der DHCP-Server neu gestartet wird, die Netzwerkgeräte jedoch ihre DHCP-Leases des DHCP-Servers behalten, die dieser vor dem Neustart verteilte. Weiterhin ist es beispielsweise für ein Netzwerkgerät durchaus möglich manuell eine IPv4-Adresse zu

konfigurieren und zu verwenden, die innerhalb des IPv4-Adresskontingentes liegt, der einem DHCP-Server zur Zuteilung an anfragende DHCP-Klienten zugeteilt wurde. Solche Adresskonflikte führen in der Regel zu Netzwerkproblemen.

2.2 NAT

Network Address Translation (Abkürzung: NAT)[6] ist eine weitere Technik, die entwickelt wurde um die Adressknappheit in IPv4 zu umgehen. In den meisten Fällen ist ein Netzwerkgerät nicht direkt mit dem Internet verbunden, sondern nur Teilnehmer in einem Netzwerk. Anwendungsbeispiele hierfür sind Privathaushalte, Unternehmen sowie Bildungseinrichtungen, hier sind die Benutzer in der Regel nicht direkt (mit eigener, öffentlicher IPv4-Adresse) sonder durch einen vorgesetzten Router mit dem Internet verbunden. In den meisten Netzwerken werden so genannte „private IPv4-Adressen“ genutzt um die Netzwerkgeräte zu adressieren. Das sind IPv4-Adressen die von der IANA speziell für diesen Zweck spezifiziert wurden und aus diesem Grund auch nicht im Internet genutzt werden können. Router im Internet verwerfen Pakete, die als Sender- oder Empfängeradresse eine solche private IPv4-Adresse enthalten. Private IPv4-Adressen sind alle IPv4-Adressen aus den Blöcken 10.0.0.0/8 bis 10.255.255.255/8, 172.16.0.0/12 bis 172.31.255.255/12 sowie 192.168.0.0/16 bis 192.168.255.255/16.

Ein Router hat die Aufgabe, Daten zwischen mindestens zwei Netzwerken zu vermitteln. Ein Anwendungsbeispiel ist ein Router in einem Privathaushalt, siehe Abbildung 5. In diesem Szenario vermittelt der Router Daten zwischen dem Internet (in der Abbildung rot) und dem lokalen Netzwerk (in der Abbildung grün). Router, die solche Szenarien bedienen, nutzen fast ausnahmslos NAT. Die Funktion eines Routers, der NAT implementiert ist prinzipiell, dass alle Pakete von Netzwerkteilnehmern mit privater IPv4-Adresse im lokalen Netzwerk, die ins Internet geroutet werden sollen, vom Router so umgeschrieben werden, dass die private Absender-IP jedes Paketes durch die öffentliche IP-Adresse des Routers ersetzt wird. Erhält der Router Antwortpakete aus dem Internet die an diesen adressiert sind, schreibt er die Empfänger-IP wieder auf die private IP-Adresse des Netzwerkgerätes um und leitet es dann weiter.

In einigen Szenarien, in denen weniger komplexe, verbindungsorientierte Protokolle wie beispielsweise HTTP eingesetzt werden funktioniert NAT einigermaßen problemlos. In komplexeren Protokollen wie dem File Transfer Protokoll (Abkürzung: FTP) oder dem Session Initiation Protokoll (Abkürzung: SIP), in denen zum Beispiel im Laufe der Etablierung der Kommunikation weitere Ports für die Kommunikation

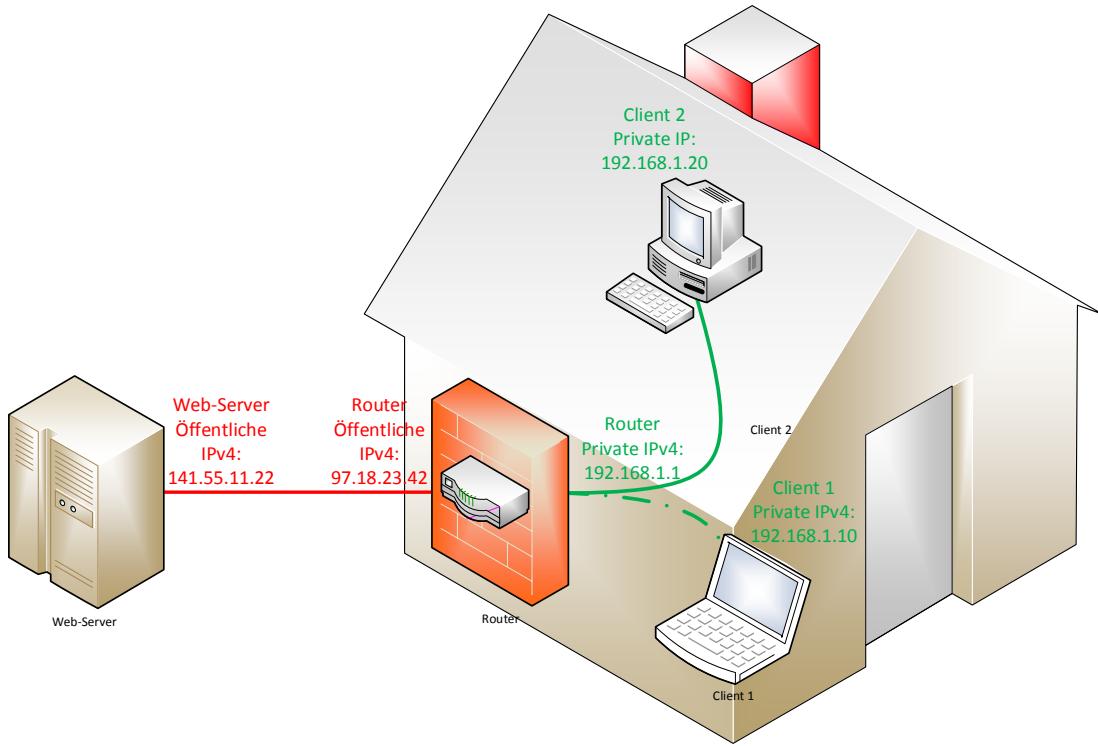


Abbildung 1: Beispielhafte Standardkonfiguration eines Internetanschlusses.

zwischen den Endgeräten ausgehandelt werden müssen, versagt NAT, mit der Folge das diese Protokolle sich dann nicht, oder zumindest nicht oder nur unzuverlässig einsetzen lassen.

Zwar kann dem zum Beispiel teilweise durch den Einsatz von spezifischen Proxy-Diensten auf dem Router für jedes einzelne Protokoll entgegen gewirkt werden, jedoch erhöht dieses Vorgehen die Komplexität, den Verwaltungs- und Wartungsaufwand für die betreffenden Router.

2.3 Ineffizienz in IPv4

Einige Designentscheidungen bei der Entwicklung von IPv4 haben sich als ineffizient erwiesen. Beispielhaft sei hier die Verwendung einer Prüfsumme für den Paketheader genannt. Jedes mal wenn ein IPv4-Paket verändert wird muss die Prüfsumme des Paketheaders neu berechnet werden. Vor allem bei Netzwerkgeräten, die hohe Durchsätze an Datenmengen bewältigen sollen, beispielsweise die Core-Router von Internet Service Providern, sorgt das für Ressourcenengpässe beziehungsweise aufwändiger und damit teurere Hardware.

Fixe Header der IPv4 Pakete sind unter mehreren Gesichtspunkten von Nachteil, da sie nicht nur die Flexibilität in der Verwendung des IPv4 Protokolls einschränken, sondern durch ihre fixe Größe auch eine Entlastung durch Weglassen nicht benötigter Teile des Paketheaders eine Steigerung der Effizienz verhindern.

Ein weiteres Effizienzproblem bei der Verwendung von IPv4 ist der im Laufe der Zeit stark angewachsene Umfang der Routingtabellen. Wünschenswert ist, dass der Umfang der Routingtabellen möglichst gering bleibt, um die Router im Internet so gut wie möglich zu entlasten. Durch die immer problematischere Adressknappheit im IPv4-Adressraum ist auch eine immer stärkere Segmentierung der IPv4-Adressen und IPv4-Adressbereiche zu beobachten mit der Konsequenz immer stärker anwachsender Routingtabellen in den Routern.

3 Überblick zu IPv6

Nachdem im vorangegangenen Kapitel viele der Nachteile von IPv4 erwähnt wurden, sollen nun die wichtigsten Neuerungen von IPv6 vorgestellt werden.

3.1 Größe des Adressraums

Offenkundigste Neuerung von IPv6 ist die Erweiterung des Adressraums auf 128 Bit. Mit einem 128 Bit breiten Adressraum lassen sich $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$ individuelle Adressen bilden. Vergleichweise gering fällt der 32 Bit breite IPv4-Adressraum aus, denn hier lassen sich „nur“ $2^{32} = 4.294.967.296$ individuelle Adressen bilden.

Bestand eine IPv4-Adresse aus vier durch einen Dezimalpunkt getrennten Ziffern mit Werten von jeweils zwischen 0 und 255, also zum Beispiel 85.114.130.113, musste für IPv6 mit seinen 128 Bit großen Adressen ein neues Konzept entwickelt werden. Der Ziffernbereich umfasst jetzt den Bereich aller Hexadezimalziffern, also 0 bis 9 und A bis F.¹ Bis zu vier Hexadezimalziffern werden zu einem Block zusammen gefasst, wobei führende Nullen nicht ausgeschrieben werden müssen. Acht dieser Blöcke, welche durch Doppelpunkte von einander abgegrenzt werden, bilden eine gültige

¹ In heute verbreiteten Betriebssystemen (Linux, Mac OS X, Windows) werden IPv4-Adressen durch Dezimalziffern und IPv6-Adressen durch Hexadezimalziffern dargestellt.

IPv6-Adresse, die vollständig ausgeschrieben beispielsweise so aussehen kann:

2001 : 41d0 : 0001 : f7bb : 0000 : 0000 : 0000 : 0001

Um den Umgang mit IPv6-Adressen komfortabler zu gestalten, gibt es mehrere Möglichkeiten, IPv6 Adressen verkürzt darzustellen. So müssen, wie bereits erwähnt, führende Nullen innerhalb eines Block nicht zwingend angegeben werden. Weiterhin ist es pro IPv6-Adresse möglich einen Bereich aus Nullen, der sich über mehrere Blöcke erstrecken kann, wegzulassen und stattdessen nur die Doppelpunkte am Beginn und dem Ende dieses Null-Bereiches darzustellen. Es ist jedoch zu beachten das pro IPv6 Adresse jeweils immer nur ein Nullbereich weggelassen werden darf, da die IPv6 Adresse sonst nicht mehr eineindeutig ist. Durch Anwendung dieser Konventionen lässt sich die oben genannte, voll ausgeschriebene IPv6 Adresse

2001 : 41d0 : 0001 : f7bb : 0000 : 0000 : 0000 : 0001

nun viel kürzer, jedoch trotzdem eineindeutig darstellen:

2001 : 41d0 : 1 : f7bb :: 1

3.2 Mehrere IPv6-Adressen pro Netzwerkschnittstelle

Ein Umstand, der in IPv4 oft zu Problemen führte ist, dass pro aktiver Netzwerkschnittstelle nur eine IPv4-Adresse zugewiesen werden kann. Soll einem Netzwerkclient zum Beispiel dynamisch eine IPv4-Adresse zugewiesen werden, kann der Client mit dem Server (und umgekehrt) nur über Broadcast-Adressen kommunizieren, bis der Client eine IPv4-Adresse zugewiesen bekommen hat.

Ein fester und grundlegender Umstand vom IPv6 ist die Tatsache, dass jede Netzwerkschnittstelle mit mehreren IPv6-Adressen umgehen können muss. Sobald eine Netzwerkschnittstelle in einem IPv6-fähigem System den betriebsbereiten Zustand erreicht, ist ihr schon mindestens eine IPv6-Adresse zugewiesen. Dabei handelt es sich um die so genannte Link-Local-Adresse. Diese ist nur im lokalen Netzwerkkontext gültig und wird unter anderem aus der MAC-Adresse der jeweiligen Netzwerkschnittstelle unter Zuhilfenahme von Zufallsalgorithmen gebildet. Mit der Link-Local-Adresse kann ein Netzwerkclient mit anderen lokalen Netzwerkteilnehmern kommunizieren sowie weitere Netzwerkparameter austauschen und aushandeln.

3.3 Spezielle IPv6-Adressen

Von den 2^{128} IPv6-Adressen sind laut [9, RFC5156] bestimmte Adressbereiche für besondere Aufgaben reserviert, von denen nachfolgend beispielhaft einige genannt seien.

Adressprefix	Bezeichnung laut IETF	Beschreibung
::1/128	Node-Scoped Unicast - loopback address	Lokale Loopback-Adresse (ähnlich 127.0.0.1 in IPv4), sollten nicht im Internet auftauchen
::1/128	Node-Scoped Unicast - unspecified address	bisher unpezifiziert (Stand RFC5156 von April 2008)
::FFFF:0:0/96	IPv4 mapped address	IPv4 gemappte Adressen. Adressen dieses Typs sollten im öffentlichen Internet nicht auftauchen.
::<ipv4-address>/96	IPv4-Compatible Addresses	Adressbereich um IPv4-Adressen für andere IPv6-Geräte kompatibel einzubetten

Tabelle 1: Laut RFC 5161 vordefinierte Adressprefixe in IPv6

3.4 Automatische Netzwerkkonfiguration

Bei Verwendung von IPv6 ist es den Netzwerkgeräten möglich, über so genannte “Neighbor Discovery Protocol“ [10, RFC3122], [11, RFC4861] zu erfragen, ob sich Router im gleichen Netzwerksegment befinden, wie die Netzwerkclients selbst. Dazu generiert ein Netzwerkgerät das in einem IPv6-Netzwerk kommunizieren möchte, zuerst eine so genannte “Link Local Adresse“. Diese Link-Local-Adresse generiert sich das Gerät selbst, unter anderem aus der MAC-Adresse der betreffenden Netzwerkschnittstelle. Charakteristisch für diese Link-Local-Adressen ist, dass diese immer mit dem Prefix *fe80 ::* beginnen. Eine weitere Besonderheit ist der Gültigkeitsbereich von Link-Local-Adressen, diese sind nur im aktuellen Netzwerksegment gültig und werden nicht geroutet. In der Konsequenz bedeutet das, dass ein Netzwerkgerät über die Link-Local-Adresse nur mit anderen Netzwerkgeräten kommunizieren kann, die sich im gleichen Netzwerksegment befinden. In der Abbildung 2 ist eine beispielhafte IP-Konfiguration des Autors abgebildet, die für diesen Beleg erstellt wurde.

Während der Erstellung dieser Arbeit wurde eine Konfiguration implementiert, die einem Rechner IPv6-Konnektivität zur Verfügung stellt (Ausführlich wird im Kapi-

```
m@m-HP-EliteBook-8470w-kub1310:~$ ifconfig sixxs
sixxs      Link encap:UNSPEC  Hardware Adresse 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet6-Adresse: fe80::8004:d600:180:2/64 Gültigkeitsbereich:Verbindung
inet6-Adresse: 2a02:8204:d600:180::2/64 Gültigkeitsbereich:Global
          UP PUNKTZUPUNKT RUNNING NOARP MULTICAST MTU:1280 Metrik:1
          RX-Pakete:4074810 Fehler:0 Verloren:0 Überläufe:0 Fenster:0
          TX-Pakete:1918428 Fehler:0 Verloren:0 Überläufe:0 Träger:0
          Kollisionen:0 Sendewarteschlangenlänge:500
          RX-Bytes:5158529267 (5.1 GB)  TX-Bytes:143449914 (143.4 MB)
m@m-HP-EliteBook-8470w-kub1310:~$
```

Abbildung 2: IP-Konfiguration beispielhaft beim Autor

tel 5 - Praxisbeispiel - Konfiguration eines Rechners für IPv6-Konnektivität auf die Durchführung dieser Implementierung eingegangen). Der Aufruf des Befehls *ifconfig* meldet auf diesem Rechner für die Netzwerkschnittstelle “sixxs“ (Anmerkung: sixxs.net ist ein Netzwerk tunnel um Internetzugängen ohne natives IPv6 IPv6-Konnektivität zu verschaffen, siehe dazu folgendes Kapitel) zeigt rot umrahmt die Link-Local-Adresse *fe80 :: 8004 : d600 : 180 : 2/64*, die nur lokal gültig ist, sowie die global gültige IPv6-Adresse *2a02 : 8204 : d600 : 180 :: 2*, in der Grafik gelb umrahmt.

Nachdem sich ein Netzwerkgerät eine Link-Lokal-Adresse zugewiesen hat, kann dieses, wie bereits oben erwähnt, mit allen anderen Netzwerkgeräten im gleichen Netzwerksegment kommunizieren, beispielsweise um so genannte Router-Advertisements abzusetzen. Das sind Netzwerkanfragen, auf die jeder IPv6-fähige Router im Netzwerksegment antworten muss. Der Router kann dann in der Antwort dem anfragenden Netzwerkgerät seine eigene IPv6-Adresse sowie das global gültige IPv6-Prefix für dieses Netzwerksegment mitteilen. Wenn dies erfolgt ist, kann sich das anfragende Netzwerkgerät aus dem globalen Prefix eine IPv6-Adresse mit globaler Gültigkeit generieren, mit deren Hilfe eine vollständige Netzwerkkonnectivität gegeben ist.

4 Lösungsansätze in IPv6 zu den Problemen mit IPv4

In diesem Kapitel werden zu einigen Problemen, die bei der Verwendung von IPv4 auftreten können, Lösungsansätze in IPv6 vorgestellt.

4.1 Beseitigung der Adressknappheit auf absehbare Zeit

Durch den 128 Bit großen Adressraum und der damit verbundenen enormen Menge an zur Verfügung stehenden IPv6-Adressen sollten hinreichend viele IPv6-Adressen zur Verfügung stehen. Um die enorme Menge von Adressen des Adressraums von IPv6 zu verdeutlichen, soll ein kurzes Rechenbeispiel dienen:

Die Oberfläche der Erde umfasst grob geschätzt 510 Millionen Quadratkilometer, also $510.000.000.000.000.000\text{mm}^2$. Stellt man diese Fläche der Anzahl der möglichen IPv6-Adressen von $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$ gegenüber kommt man zu dem Ergebnis, das jedem Quadratmillimeter der Erdoberfläche immernoch theoretisch 667.220.327.295.957.771 IPv6-Adressen zugewiesen werden können. Praktisch betrachtet ist diese Zahl nicht ganz korrekt, da wie im voran gegangenen Kapitel beschrieben, bestimmte Adressen im IPv6-Adressraum reserviert sind. Dieser Vergleich soll dem Leser aber dennoch verdeutlichen, dass jedem Quadratmillimeter der Erdoberfläche circa. 155 Millionen mal mehr IPv6-Adressen zugewiesen werden können, als im gesamten IPv4-Adressraum (der ja nur 32 Bit groß ist) zur Verfügung stehen. Die Abbildung 3 soll den enormen Umfang an IPv6-Adressen im Vergleich zum Umfang der IPv4-Adressen für den Leser noch einmal illustrieren:

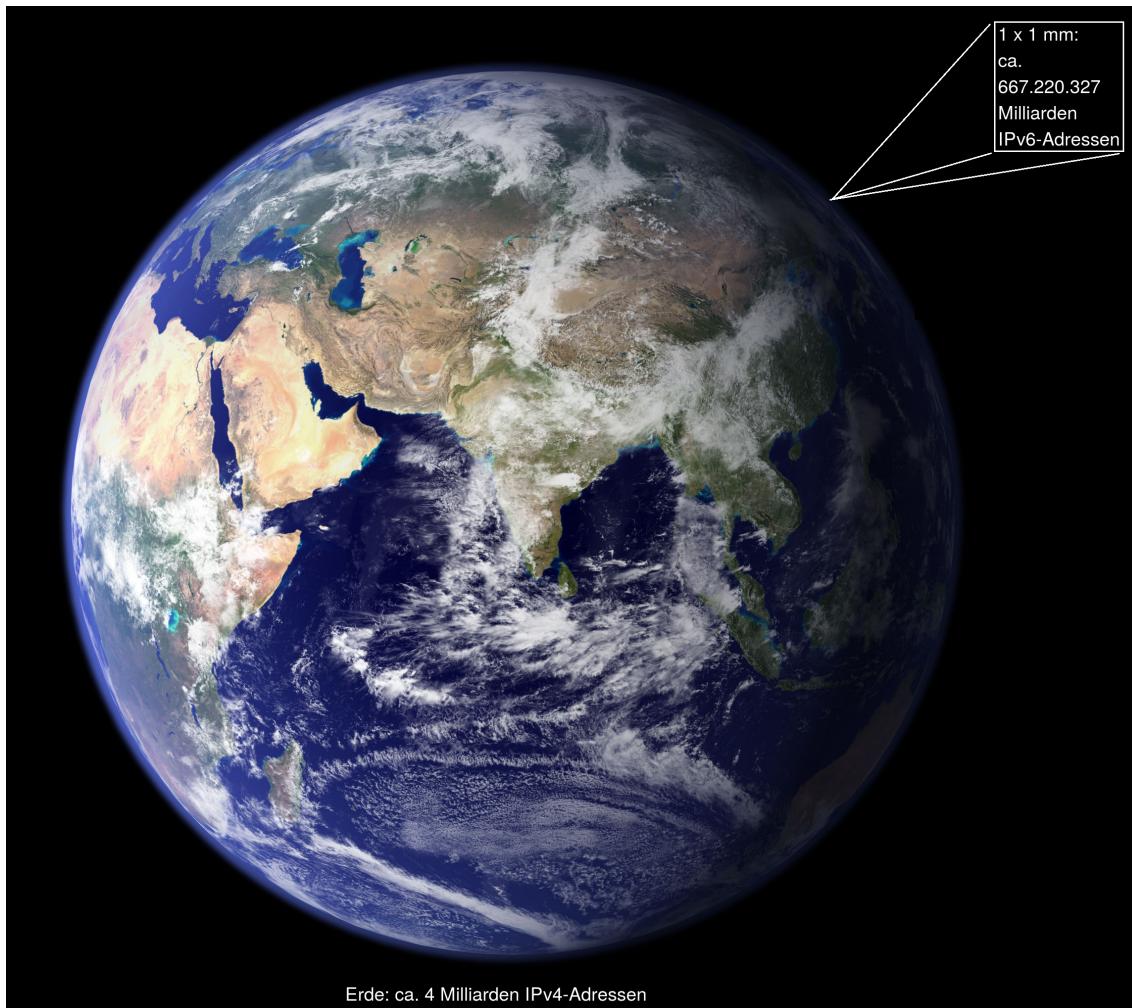


Abbildung 3: Illustration: Mengenvergleich IPv4-Adressen für die gesamte Erdbevölkerung zu IPv6-Adressen pro Quadratmillimeter Erdoberfläche.

4.2 Vereinfachte Netzwerkwartung

Eines der grundlegenden Konzepte von IPv6 ist es, möglichst viele Konfigurationsvorgänge zu automatisieren. Damit werden einerseits unerfahrene Benutzer entlastet, andererseits werden potentielle Fehlerquellen durch Fehlkonfigurationen des Benutzers verringert. Im Normalfall muss der Benutzer nichts weiter tun, als sein Gerät mit dem Netzwerk verbinden und einschalten. Somit sinkt auch die Fehlerquote durch Fehlkonfigurationen. Beispielsweise müssen Router nicht mehr von Hand konfiguriert werden. In IPv6 existieren so genannte *Router-Advertisements*. Wenn ein Netzwerkclient in einem IPv6-Netzwerk benachbarte Router anfragt, müssen sich laut IPv6-Standard alle Router in diesem Netzwerk mit einem Router-Advertisement dem Netzwerkclient gegenüber bekannt machen. Dem Netzwerkgerät stehen im An-

schluss alle Informationen zur Verfügung, die für eine vollständige Internetkonnektivität erforderlich sind.

4.3 Verkleinerung der Routingtabellen

In den Standards zu IPv6 ist vorgesehen, dass jedem Kunden mindestens ein /64-Netz zugewiesen wird. Indem man Kunden komplettete Netze zuteilt und die Adressverteilung dem Kunden, beziehungsweise dessen Router selbst überlässt, schrumpft der Umfang der Routingtabellen, die öffentliche Router im Internet vorhalten müssen, erheblich. Die Abbildung 4, die der Website unter [8] entliehen ist, soll diesen Umstand visualisieren.

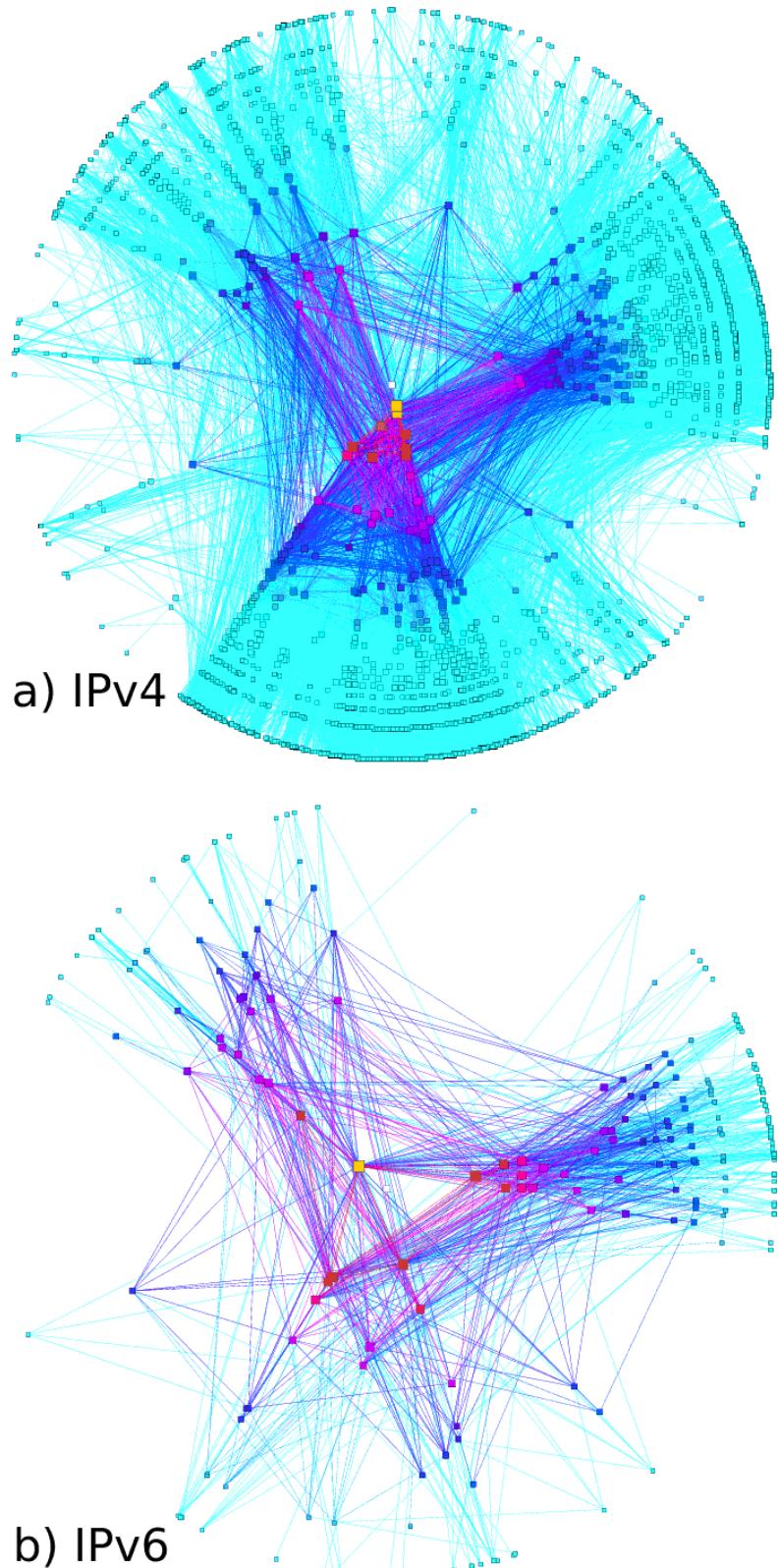


Abbildung 4: Visuelle Darstellung des Umfangs der Routingtabellen in IPv4 (a) und IPv6 (b)

4.4 Flexible Paketheader in IPv6

Bei der Verwendung von IPv6 existieren keine statischen Paketheader mehr, wie es bei der Verwendung von IPv4 der Fall ist. IPv6-Paketheader haben zwar eine fixe Größe von 40 Byte, lassen sich je nach Bedarf flexibel durch so genannte “Extensions Header“ erweitern. Ein Paketheader in IPv6 besteht aus den Feldern

- IP-Version (4 Bit)
- Traffic Class (8 Bit)
- Flow Label (20 Bit)
- Payload Length (16 Bit)
- **Next Header** (8 Bit)
- Hop Limit (8 Bit)
- Source Address (128 Bit)
- Destination Address (128 Bit).

Die Gesamtgröße eines IPv6-Pakets beträgt also 320 Bit, was 40 Byte entspricht. Im Feld Next Header können dann gegebenenfalls Erweiterungsheader angegeben werden.

Ein solcher Erweiterungsheader besteht dann aus den Feldern:

- Hop by Hop Options (variable Größe)
- Routing (variable Größe)
- Fragment (64 Bit)
- Authentication Header (variable Größe)
- Encapsulating Security Payload (variable Größe)
- Destination Options (variable Größe)
- Mobility (variable Größe) und
- No Next Header, welches das Ende des Erweiterungsheaders anzeigt.

Somit ist sichergestellt, dass die IPv6-Header so klein wie möglich und so groß wie unbedingt nötig sind.

4.5 NAT in IPv6

Wenn IPv6 den Vorgaben entsprechend betrieben wird, umfasst das unter anderem, dass jedem Teilnehmer im Internet von seinem Internet Service Provider ein 64 Bit großer IPv6-Adressblock zugeteilt wird. Im Detail wird dem Kunden nur noch ein Adressprefix von 64 Bit zugeteilt. Wie der Kunde beziehungsweise dessen Netzwerkgeräte die restlichen 64 Bit im lokalen Netzwerk verteilen, ist dem Kunden beziehungsweise dessen Netzwerkgeräten überlassen. Ein großer Vorteil ist hierbei, dass jede einzelne IPv6-Adresse aus diesem 64 Bit großem Adressblock global routbar ist und somit nicht mehr die Notwendigkeit besteht, Technologien wie NAT einzusetzen zu müssen, um nur lokal gültige IPv4-Adressen auf eine einzelne, global gültige IPv4-Adresse des Routers abzubilden.

Ein Router, der im heimischen Netzwerk die Schnittstelle zum Internet darstellt, ist nun nicht mehr, wie bei ausschließlicher Verwendung von IPv4 gezwungen, die Netzwerkpakete für jedes Netzwerkgerät im lokalen Netzwerk per NAT zu modifizieren. Da jedes Netzwerkgerät bei Verwendung von IPv6 seine eigene öffentliche und somit global gültige Adresse hat, ist eine eindeutige Zuordnung der eingehenden und ausgehenden Netzwerkpakete zu den Netzwerkgeräten für den Router ohne Probleme möglich. Die Abbildung 6 soll beispielhaft den Sachverhalt verdeutlichen: Im Vergleich zu Abbildung 5 haben hier nicht nur die rot dargestellten Netzwerkschnittstellen, die sich im Internet befinden öffentliche IP-Adressen. Auch die grün dargestellten Netzwerkschnittstellen im lokalen Netzwerk sind mit öffentlichen IPv6-Adressen ausgestattet. In dieser Konfiguration besteht keine Notwendigkeit, Technologien wie NAT einzusetzen. Somit sind in dieser Konfiguration auch die Probleme, die sich beim Einsatz von NAT ergeben, eliminiert.

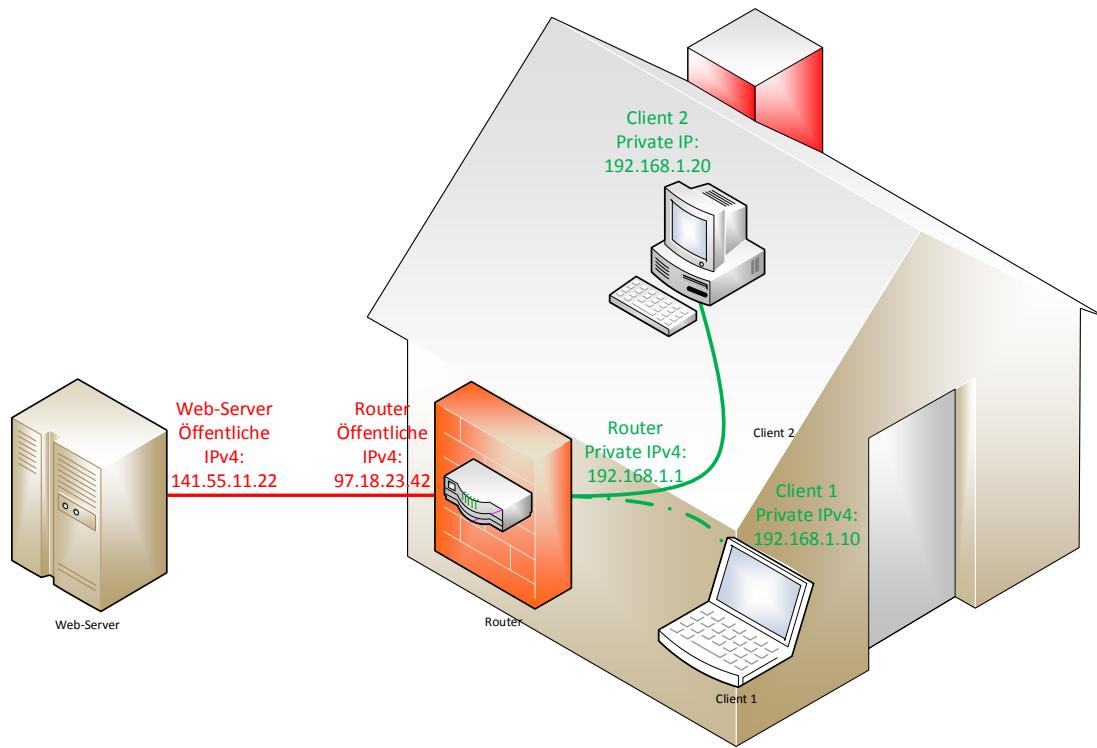


Abbildung 5: Beispielhafte Standardkonfiguration eines Internetanschlusses mit alleiniger IPv4-Konnektivität. Da nur eine öffentliche IPv4-Adresse zur Verfügung steht, ist der Einsatz von NAT zwingend erforderlich.

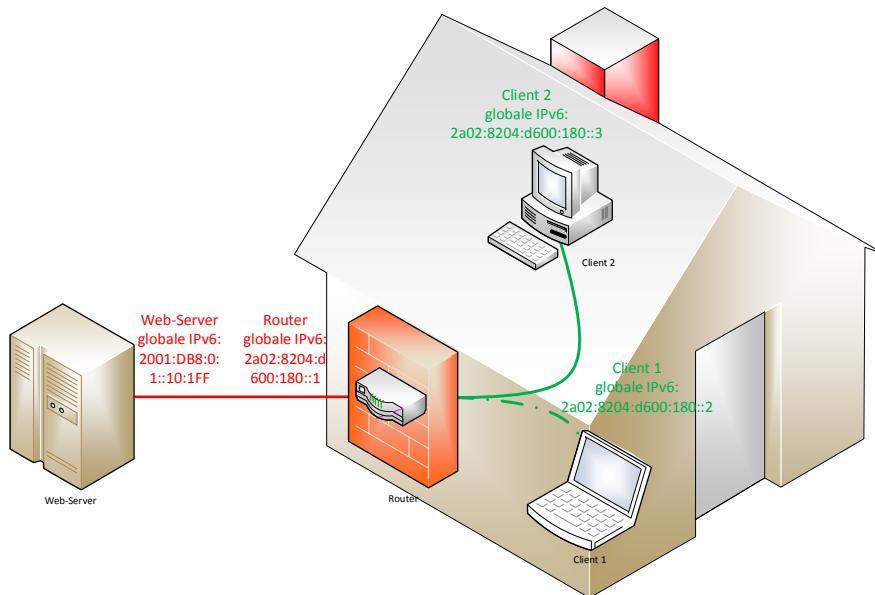


Abbildung 6: Beispielhafte Standardkonfiguration eines Internetanschlusses mit nativer IPv6-Konnektivität. Vergleiche dazu Abbildung 5

5 Praxisbeispiel - Konfiguration eines Rechners für IPv6-Konnektivität

Wenn man Webinhalte über IPv6 abrufen möchte, benötigt man einen Internetanschluss mit IPv6-Konnektivität. Dazu gibt es zwei Möglichkeiten, entweder der verwendete Internet Service Provider stellt IPv6 am Internetnetzschluss direkt zur Verfügung, oder man muss selbst nachbessern. Die beiden Möglichkeiten werden in diesem Kapitel erläutert, sowie eine Beispielkonfiguration vorgestellt.

5.1 IPv6-Konnektivität nativ vom Internet Service Provider

Falls der verwendete Internet Service Provider IPv6 nativ am verwendeten Internet Anschluß zur Verfügung stellt und auch die eingesetzten Router IPv6-fähig sind, hat der Benutzer nichts weiter zu tun, als sein IPv6-fähiges Netzwerkgerät mit dem Netzwerk zu verbinden. Durch die in den voran gegangenen Kapiteln vorgestellten, fortschrittlichen Adressfindungsmechanismen in IPv6 wird vollständige Netzwerkkonnektivität ohne manuelles Eingreifen des Benutzers hergestellt.

Vom Autor muss an dieser Stelle negativ angemerkt werden, dass zum derzeitigen Zeitpunkt, dass heißt im Jahr 2014, also 15 Jahre nach der finalen Verabschiedung des IPv6-Standards, keiner der in Deutschland im Privatkundenmarkt tätigen Internet Service Provider in der Lage, beziehungsweise Willens ist, dem Kunden IPv6 in nennenswerten Umfang zur Verfügung zu stellen. Entweder wurde noch garnicht mit der Umstellung begonnen, oder der Prozentsatz der Kunden mit nativer IPv6-Konnektivität liegt noch im unterem einstelligen Prozentbereich.

Geschäftskunden genießen in der Regel den Vorzug einer vielfältigen Auswahl im Bezug auf die Internet Service Provider. Es kann daher vom Autor nur angeraten werden, bei der Auswahl der zukünftigen Internet Service Provider die native IPv6-Konnektivität zu einem Schlüsselkriterium zu machen.

5.2 IPv6-Konnektivität per Tunnel

Ist der Anwender an einen Internet Service Provider gebunden, der noch kein natives IPv6 an seinem Internetanschluss zur Verfügung stellt, gibt es noch die Möglichkeit mit Hilfe eines IPv6-Tunnels IPv6-Konnektivität zu ermöglichen. Es ist bei Anbietern wie <https://www.sixxs.net/> möglich, sich kostenfrei einen IPv6-Tunnelendpunkt inklusive eines global routbaren 64 Bit großen IPv6-Adressblock

zuteilen zu lassen.

The screenshot shows a web browser window with the URL <https://www.sixxs.net/home/>. The page is titled "SixXS". The left sidebar contains links for "User Home", "User info", "View log", "Request tunnel", "Request subnet", "GRH Peering", "Cool IPv6 Stuff", "Forum", "My Tickets", "Tickets", "Change password", "Remove account", and "Logout". The main content area has a green header bar with the text: "When you have a problem with the services provided by SixXS contact us and report the problem. Of course, c...". Below this is a section titled "User Home" with a welcome message and information about the user's ISK balance. It also includes a note about tunnels being up and running. A "Tunnels" section lists one tunnel entry:

Details	Tunnel to PoP	Your IPv4	Your IPv6	Name	State
T143193	deolo01 - EWE TEL GmbH	ayiya	2a02:8204:d600:180::2	My First Tunnel	Enabled

The "Subnets" section lists one subnet entry:

Details	Subnet Prefix	Tunnel Endpoint	Tunnel ID	Subnet Name	State
R242057	2a02:8204:d600:8180::/64	2a02:8204:d600:180::2	T143193	Routed /64 Subnet	Enabled

A note at the bottom states: "Tunnels or subnets which are deleted remain visible for the purpose of history and traceability".

Abbildung 7: Webseite der Anbieters <https://sixxs.net> für einen kostenfreien IPv6-Tunnelendpunkt

5.3 Beispielkonfiguration eines IPv6-Tunnels

5.3.1 eingesetzte Hardware

In der Beispielkonfiguration wird als Hardwaregrundlage ein Laptop vom Hersteller Hewlett Packard eingesetzt. Es handelt sich dabei um das Modell Elitebook 8470w mit folgender Ausstattung:

Prozessor: Intel(R) Core(TM) i7-3740QM CPU: 4 physische Kerne, 8 logische Kerne, Standardtakt 2,7 GHz, Cache 6MB

Hauptspeicher: 16GB DDR3-RAM

Festplatte: Micron SSD, Kapazität 256 GB

Es kann jedoch auch jedes andere i386 oder amd64-basierte Rechnersystem verwendet werden.

5.3.2 eingesetzte Software

Als Betriebssystem dient die Linux-Distribution Kubuntu 12.04.1 LTS, welches mit den von der Installationsroutine vorgeschlagenen Standardeinstellungen installiert wurde. Weiterhin wurde das Softwarepaket AICCU installiert.

5.3.3 Vorgehensweise bei der Implementierung

Ein solcher Tunnel lässt sich an einem Router oder auch direkt in einem Netzwerkendgerät konfigurieren. Setzt man beispielsweise Linux ein, kann man mit dem Softwarepaket *aiccu* sehr einfach die Konfiguration des IPv6-Tunnels vom Typ AYI-YA (Anything in Anything, siehe[12, sixxsayiya])abschließen. Für das Testsystem mit dem Betriebssystem Kubuntu 12.04 LTS war es nur erforderlich das Paket *aiccu* mittels

```
$ sudo apt-get install aiccu
```

zu installieren und während der Installation die Anmelde Daten zu sixxs.net, dass heißt Benutzer und Passwort mitzuteilen. Es werden im Verlauf der Installation dann sämtliche Tunnelparameter selbstständig ermittelt und alle Einstellungen so übernommen, dass nach der Installation IPv6-Konnektivität über den Tunnel gewährleistet ist. Testen lässt sich das beispielsweise über die Webseite <http://test-ipv6.com/>, die dann folgendes Resultat liefern sollte:

The screenshot shows a web browser window with the URL 'test-ipv6.com' in the address bar. Below the address bar, there are three buttons: 'IPv6 testen', 'FAQ', and 'Mirrors'. The main content area has a heading 'Testen Sie Ihre IPv6 Konnektivität.' Below this, there are several status items with icons: a blue info icon for IPv4 and IPv6 addresses, a green checkmark for reaching other IPv6 sites, a yellow warning icon for tunnel usage, and a green checkmark for DNS server support. At the bottom, a large green '10/10' score is displayed, followed by the text 'Ihre Bereitschafts Ergebniss für Ihre IPv6 Stabilität und Bereitschaft, wenn Inhalte nur via IPv6 verfügbar sind'. Below this, a link 'Hier Klicken Testergebnisse' and a note '(Serverseitige IPv6 Bereitschafts-Statisik aktualisiert)' are shown. At the very bottom, social sharing links for Facebook ('Like') and Twitter ('Twitter') are present.

Abbildung 8: Webseite zum Testen der IPv6-Konnektivität: <http://test-ipv6.com/>

6 Zusammenfassung und Ausblick

Allein durch die immens fortgeschrittene Knappheit an IPv4-Adressen ist ersichtlich, dass der Umstieg zu IPv6 unumgänglich ist. Umso schmerzlicher ist im Jahr 2014 festzustellen, wie wenig verbreitet IPv6 noch immer ist. Das gilt für Internet Service Provider genauso, wie für Weltkonzerne wie Apple oder IBM, deren Webpräsenzen bis heute nicht über IPv6-Konnektivität verfügen. Es gibt aber auch positive Beispiele, wie beispielsweise der deutsche Hardwarehersteller <http://www.avm.de> oder <http://www.heise.de>. Es bleibt zu hoffen, dass viele Menschen verstehen, dass IPv6 nicht nur den verfügbaren Adressraum signifikant erhöht, sondern auch viele andere technische Unzulänglichkeiten ausmerzt, die im Laufe der Jahre bei der Verwendung von IPv4 zu Tage getreten sind. Der Autor ist der Meinung, dass durch hinreichend viele aktive IPv6-Nutzer auch größere Konzerne, wie auch öffentliche Einrichtungen² endlich dazu übergehen, IPv6 nicht mehr so “stiefmütterlich,” zu behandeln, wie es vielerorts bis heute leider der Fall zu sein scheint.

² Die HTWK Leipzig ist im Bezug auf IPv6-Konnektivität leider auch kein positives Beispiel

7 Quellenverzeichnis

Quellenverzeichnis

- [1] Goncalves, Marcus: *IPv6 Networks* McGraw-Hill Professional, 1998,
ISBN: 978-0-07024-807-6
- [2] Dittler, Hans Peter: *IPv6 - Das neue Internet-Protokoll, 2. Auflage.* dpunkt-Verlag Heidelberg, 2002,
ISBN: 978-3-89864-149-4
- [3] <https://www.un.org/Depts/german/menschenrechte/a-hrc-20-L.13.pdf>
abrufbar am 03.03.2014
- [4] <http://www.hki.uni-koeln.de/node/14956>
abrufbar am 14.05.2014
- [5] <https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.txt>
abrufbar am 05.03.2014
- [6] RFC1631 - The IP Network Address Translator
<https://www.ietf.org/RFC/RFC1631.txt>
abrufbar am 06.03.2014
- [7] RFC2131 - Dynamic Host Configuration Protocol
<http://tools.ietf.org/html/RFC2131>
abrufbar am 05.03.2014
- [8] Übersichtsgrafik zum Umfang der Routingtabell für IPv4 und IPv6
<http://greenbyte.ch/wp-content/uploads/2012/08/ipv4-ipv6.gif?cf3116>
abrufbar am 19.03.2014
- [9] RFC5156 - Special-Use IPv6 Addresses
<http://tools.ietf.org/html/RFC5156>
abrufbar am 19.03.2014
- [10] RFC3122 - Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification

<http://tools.ietf.org/html/RFC5156>

abrufbar am 25.03.2014

- [11] RFC4861 - Neighbor Discovery for IP version 6 (IPv6)

<http://tools.ietf.org/html/RFC4861>

abrufbar am 25.03.2014

- [12] AYIYA: Anything In Anything draft-massar-v6ops-ayiya-02

<http://tools.ietf.org/html/draft-massar-v6ops-ayiya-02>

abrufbar am 28.03.2014