IPv6: Mehr als ein größerer Adressraum

Benedikt Stockebrand

11. März 2004

Zusammenfassung

IPv6 ist anders als das gewohnte IP, oder genauer gesagt IPv4. Es hat mehr als genug Adressen, konfiguriert sich weitgehend automatisch und bietet eine Reihe neuer Funktionen, die teilweise bisher nur aus Telefonie-Netzen bekannt sind.

Daraus folgt, daß einige Interessengruppen über IPv6 nicht glücklich sind und möglicherweise versuchen werden, die Einführung von IPv6 zu verhindern oder mindestens zu verlangsamen.

Trotzdem ist es an der Zeit, daß wir uns auf IPv6 einrichten, wenn wir nicht von der nächsten großen Entwicklungswelle überrollt werden wollen.

1 Die Adressraum-Diskussion

In den letzten Monaten hat sich IPv6, das seit einigen Jahren designierte Nachfolgeprotokoll für IPv4, zum Thema heißer Debatten entwickelt.

Vordergründig dreht sich die Frage darum, ob der Adressraum von IPv4 noch „ausreicht“. Mit Network Address Translation (NAT) ist es natürlich möglich, IPv4-Adressen mehrfach zu benutzen, wenn auch „mit gewissen Einschränkungen“, über deren Relevanz sich dann weiter am eigentlichen Thema vorbei streiten läßt.

Wie wir alle in den letzten dreiundzwanzig Jahren gelernt haben, reichen bekanntlich 640 Kilobytes *nicht* aus, egal was der eine oder andere „große IT-Visionär“ damals behauptet hat.[1] Als IT-historisch bewanderte Techniker können wir also an dieser Stelle die offensichtliche Parallele sehen, die Diskussion abbrechen, die Ärmel hochkrempeln und uns in IPv6 einarbeiten.

Dabei werden wir sehen, daß IPv6 neben einer großzügigen Zahl[2] global gerouteter Adressen für jeden einzelnen Interessenten eine Reihe anderer interessanter Vorteile bietet; Vorteile, die für einige Parteien allerdings erhebliche Nachteile sein können. Mit diesem Wissen können wir die tatsächlichen Gründe hinter der Diskussion wenigstens im Ansatz durchschauen und entscheiden, wo wir mit unserer Meinung stehen.

2 IPv6 ist anders

Während wir den IPv4-Adressraum vergleichsweise unstrukturiert immer weiter zerstückeln und uns von Anfang an mit A-, B-, und C-Netzen, dann mit frei gewählten Subnetzmasken, Variable Length Subnet Masks (VLSM) und Network Address Translation (NAT) das Leben schrittweise immer schwerer gemacht haben, um aus den 2^{32} möglichen Adressen möglichst viel herauszuholen, verfolgt IPv6 den Ansatz, durch einen ausreichend großen Adressraum diese Herausforderung auf lange Zeit aus der Welt zu schaffen.

IPv6-Adressen sind groß. Statt, wie im Hardware-Sektor üblich, die Anzahl der Adressbits auf 64 Bits zu verdoppeln, was immerhin ausreichen würde, um jeder einzelnen IPv4-Adresse einen Adressraum zuzuordnen, der so groß ist wie der gesamte bisherige IPv4-Adressraum, hat man die Adressbits auf 128 Bits vervierfacht. Was sich bezogen auf die Anzahl der Bits noch vorstellen läßt, wird unvorstellbar, wenn man die Anzahl der Adressen betrachtet. Auf jede IPv4-Adresse kommen

$$2^{128-32} = 2^{96} = 79\,228\,162\,514\,264\,337\,593\,543\,950\,336$$

[1] “640 K ought to be enough for anybody.” Bill Gates, 1981.

[2] Die IETF sieht vor, für Endbenutzer Blöcke mit $2^{80} = 1\,208\,925\,819\,614\,629\,174\,706\,176$ Adressen zu vergeben

IPv6-Adressen, also fast achtzig Quadrilliarden. (An dieser Stelle ist es normal, sich zu fragen, wozu das gut sein soll.)

Auch IPv4 hat mit 32 Adressbits theoretisch erheblich mehr Adressen zur Verfügung als heute gebraucht werden—aber die Strukturierung des Adressraums führt zu erheblichen Verlusten. Und IPv6 ist in dieser Beziehung noch „ineffizienter“ als IPv4. Im Gegenzug ist IPv6 fester strukturiert aufgebaut als IPv4, was den operationellen Aufwand reduziert und die Zuverlässigkeit erhöht.

Wie Abbildung 1 zeigt, sind global geroutete Adressen aus drei Teilen aufgebaut:

Global Routing Prefix: Die ersten 48 Bits[3] sind das „Global Routing Prefix“. Core-Router interessieren sich nur für diese 48 Bits, weil nach ihnen im „Backbone“ geroutet wird. Dabei kommt, genau wie bei IPv4, Classless Inter-Domain Routing (CIDR) zum Einsatz, um die Routing-Tabellen überschaubar zu halten.

Subnet ID: Die nächsten 16 Bits heißen „Subnet ID“ und adressieren innerhalb einer Site ein Subnetz. Es werden also immer gleich Blöcke von $2^{16} = 65\,536$ Subnetzen vergeben.

Interface ID: Schließlich folgen 64 Bits für die „Interface ID“, mit denen innerhalb eines Subnetzes ein Interface adressiert wird.

Global Routing Prefix und Subnet ID bilden zusammen das *Subnet Prefix*.

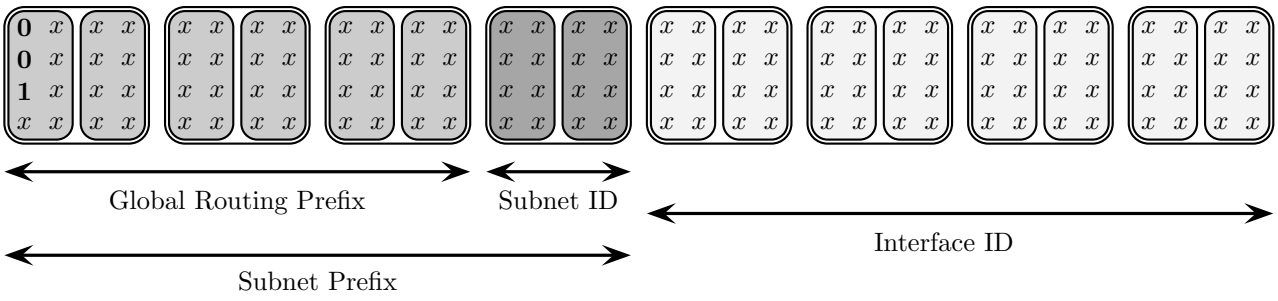

Abbildung 1: Der Aufbau von global gerouteten IPv6-Adressen

Die Verantwortung über die Adressteile liegt in drei verschiedenen Händen: Das Global Routing Prefix betreut der jeweilige ISP[4]. Die Subnet ID liegt in der Obhut des lokalen Netzwerkmanagements. Die Interface ID schließlich verwaltet jedes Gerät selbst. Weil die Länge des Subnetz-Prefixes fest definiert ist, kann es nicht mehr zu fehlkonfigurierten Netzmasken und daraus folgenden „Kompetenzstreitigkeiten“ kommen.

Warum das Global Routing Prefix und die Subnet ID diese Größe haben, ist hoffentlich nachvollziehbar. Mit IPv6 gibt es, eine ansatzweise sinnvolle Zuteilung von Adressbereichen an geographische Regionen vorausgesetzt, keine Probleme mehr mit regional beschränkter Adressknappheit.

Aber was sollen $2^{64} = 18\,446\,744\,073\,709\,551\,616$ Adressen in einem einzelnen Subnetz? Hätte man nicht das Subnet Prefix insgesamt etwas straffen und zusammen mit einer acht bis zehn Bit großen Interface ID in insgesamt 64 Bit großen Adressen unterbringen können?

Der Grund für die langen Interface IDs heißt „Stateless (Address) Autoconfiguration“. Wenn ein IPv6-Interface in Betrieb genommen wird, generiert es zuerst eine Interface ID. Dabei kann es zum Beispiel die Ethernet-Adresse als Basis benutzen, es kann aber auch eine Interface ID zufällig generieren oder eine fest konfigurierte Interface ID verwenden. Anschließend stellt es sicher, daß diese Interface ID unbenutzt ist; anders als bei IPv4 über Ethernet kann es deshalb nicht mehr zu einer doppelt vergebenen Link-Layer-Adresse mit den daraus resultierenden Unannehmlichkeiten kommen.

Das weitere Verhalten des Interfaces hängt davon ab, ob es einem Router gehört oder nicht. In der IPv6-Terminologie ist alles, was IPv6 spricht, aber kein Router ist, ein „Host“.

Bei einem Host fragt das Interface innerhalb des Subnetzes nach Routern. Von denen bekommt es Subnet-Prefixe. Das Interface vervollständigt jedes Subnet-Prefix mit seiner Interface ID zu einer IPv6-Adresse. Anders

[3] Genau genommen handelt es sich hierbei nur um eine Empfehlung der IETF, während die Länge der Interface ID laut RFC 3587 zwingend festgelegt ist.

[4] ISP=Internet Service Provider.

als bei IPv4 werden bei IPv6 neue Adressen einem Interface hinzugefügt, ohne existierende Adressen zu löschen. In IPv4-Terminologie würde man sagen, es werden zusätzliche Interface Aliases angelegt. Schließlich merkt sich das Interface, welche Router es gefunden hat und routet anschließend allen Traffic weiter an diese Router. Dabei belastet es sich nicht mit konfigurierten Defaultrouten, Routing-Tabellen, dynamischem Routing oder ähnlichem; Routing in IPv6 ist alleinige Aufgabe der Router.

Die Konfiguration von IP-Adressen, Prefixen und Routen ist damit nur noch auf den Routern notwendig, an den Hosts gibt es nichts mehr zu (ver-)konfigurieren. Auch die Verwaltung einzelner vergebener Adressen, wie sie in der IPv4-Welt mit DHCP üblich ist, wird unnötig.

3 Permanente Adressen für alle

Mit der allgemeinen Verfügbarkeit fester, global gerouteter Adressen, ist es nicht mehr nötig, auf temporär zugeteilte Adressen oder gar ungeroutete Adressen nach RFC 1918[5] und NAT zurückzugreifen, um den Internet Access für Privat- und kleine Geschäftskunden zu realisieren.

Damit wird es möglich, ohne zusätzliche Kosten selbst unter einer festen Adresse Services im Internet anzubieten—weit über die Webseite mit eigenen JavaScript-Kreationen, den neuesten MP3s der eigenen Band und den Baby-Fotos des Nachwuchses hinaus. „Always On“ ist in Zeiten von DSL-Flatrates weder neu noch aufregend, aber mit festen, gerouteten Adressen kann man auch über die statische, bei einem Provider gehostete Home Page hinaus aktiv das Internet mit eigenen Diensten gestalten.

Peer-to-Peer-Netze werden mit permanenten Adressen einfacher zu implementieren, weil sie keine Broker-Instanz mehr brauchen—allerdings werden sie auch einfacher zu überwachen, wenn man keine Anonymizer benutzt.

Mit Stateless Autoconfiguration ist es vergleichsweise trivial, die globalen IP-Adressen in einem Netz systematisch umzustellen—und das normalerweise auch im laufenden Betrieb.

Daß die Webspace-Provider damit unter Druck geraten, ist wohl offensichtlich. Auch die so laut klagende Musikindustrie wird sich nicht glücklich über die Möglichkeiten allgemein verfügbarer statischer IP-Adressen zeigen—egal ob berechtigt oder nicht. Schließlich fällt für ISPs die Kundenbindung durch die einmal vergebenen gerouteten Adressen weitestgehend weg, so daß sie in Zukunft wohl auch mit ihren Altkunden pfleglich umgehen müssen.

4 Appliances

Alleine die Tatsache, daß Hosts sich ohne explizite Konfiguration in ein existierendes IPv6-Netzwerk einstöpseln lassen, eröffnet interessante Möglichkeiten im Zusammenhang mit Appliances, also Geräten, die für eine spezielle Aufgabe konzipiert sind.

Ob der RFID-lesende Kühlschrank, den wir von unterwegs per Web Interface nach dem Verfallsdatum der Milch fragen können, unbedingt erstrebenswert ist, kann man vermutlich lange und ergebnislos diskutieren. Aber die Möglichkeit, in einem Haus nach Belieben IP-Telefone anzuschließen, die Thermostatventile der Heizkörper gegen netzwerkgesteuerte Modelle auszutauschen, das Babyphone auch über Entfernungen von mehr als dreißig Metern zuverlässig abhören zu können oder zentral das Licht im Haus an- oder auszuschalten, ist auch für IT-Laien sehr interessant.

Auch in geschäftlich genutzten Netzen eröffnen sich ähnliche Möglichkeiten. Alleine die Themen „Voice over IP“ (VoIP) und IP-Telefonie, mit denen sich die Telefonkosten von Unternehmen deutlich senken lassen, sollten zeigen, welches Potential hier wartet. Selbst mit IPv4 entwickelt sich hier ein schnell wachsender Markt für Unternehmenslösungen; mit IPv6 wird diese Technologie auch für Kleinunternehmer und Privathaushalte ohne IT-Kenntnisse praktikabel.

Andererseits wird aber auch klar, daß Verlierer bei der Einführung von IPv6 vermutlich die etablierten Telcos und die Hersteller von proprietärer Haustechnik sein werden.

[5] In RFC 1918 sind die bekannten Adressbereiche 10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16 für den internen Gebrauch reserviert.

5 Mobile IP

Mit „Mobile IP“ bringt IPv6 eine Funktionalität mit, die es ermöglicht, trotz wechselnder Netzverbindungen eine feste IP-Adresse beizubehalten. Auch beim Übergang von einem Netz in ein anderes bleiben offene TCP-Verbindungen erhalten.

Wer viel unterwegs ist, wird solche Funktionen schnell zu schätzen lernen. Egal ob er sich nur samt Notebook von seinem Schreibtisch in einen Besprechungsraum bewegt oder mit seinem PDA quer durch Deutschland fährt, alleine die schwankende Bandbreite fällt noch auf.

Auch hier darf jeder für sich entscheiden, ob das wirklich immer erstrebenswert ist. Aber es gibt sicherlich genug Fälle, wo Mobile IP sehr interessant ist.

Wer könnte Interesse daran haben, daß diese Technologie nicht verfügbar wird?

Wieder einmal sind die Telcos, in diesem Fall vor allem die Mobilfunkanbieter, die Leidtragenden. Nachdem mit viel Mühe UMTS dazu bewegt wurde, einen automatischen Übergang in die GSM-Netze und zurück zu ermöglichen, wird diese Leistung durch IPv6 in vieler Hinsicht ad absurdum geführt—und damit nicht mehr teuer verkaufbar. Durch das inhärente „Least Cost Routing“, das Mobile IP bietet, werden auch eher bequeme (Geschäfts-)Kunden nicht unnötig die vergleichsweise teure UMTS-Anbindung nutzen, wenn WLAN vorhanden ist. Das macht wiederum WLAN auch dann interessant, wenn eine lückenlose Abdeckung nicht gewährleistet ist.

Aber auch der eine oder andere Software-Hersteller, der zwar vielleicht gerne über Sicherheit redet, aber dessen Produkte immer noch auf Konzepten basieren, die von einem vertrauenswürdigen Netz ausgehen, das höchstens über eine Firewall mit dem großen, bösen Internet verbunden ist, steht an dieser Stelle vor einem grundlegenden Problem.

Schließlich bin ich persönlich nicht glücklich darüber, daß ohne mein Wissen oder Einverständnis der mobile Kundenberater meiner Bank oder Krankenversicherung mit seinem unzureichend geschützten mobilen Endgerät meine finanzielle oder medizinische Situation der Welt bekanntgibt…

6 Resource Reservation und Quality of Service

Ein weiteres Feature, das mit IPv6 verfügbar wird, ist *Resource Reservation* als Basis für garantierte *Quality of Service (QoS)*. Damit können wir für einzelne Datenströme („Flows“) durchgehend Ressourcen fest reservieren und so sicherzustellen, daß eine festgelegte Leistung garantiert zur Verfügung steht.

Beim Verbindungsaufbau verlangen wir beispielsweise eine garantierte Bandbreite von 64 kbit/s bei einer maximalen Latenz von 100 ms. Alle Router entlang der Verbindung stellen sicher, daß sie diese Anforderungen eingehalten.

Die Möglichkeiten, die sich mit diesem Feature über Sprach- und Videotelefoniedienste hinaus eröffnen, sind noch nicht abzusehen.

Aber wieder einmal gibt es Verlierer. Die Telcos, die bisher für Sprachverbindungen ein Vielfaches dessen berechnen, was die gleiche Datenmenge als normaler IP-Traffic kostet, werden mit zunehmend besser funktionierendem Voice over IP konfrontiert. In dem Maße, wie sie sich entweder grundsätzlich oder mit überzogenen Gebührenmodellen dagegen sperren, auf den eigenen Routern Resource Reservation zur Verfügung zu stellen, wächst das Risiko, daß alternative Anbieter rohe Leitungskapazitäten anmieten oder selbst legen, darauf Resource Reservation zur Verfügung stellen und damit den Telcos erhebliche Konkurrenz machen.

7 Verschlüsselung und Authentisierung

Schließlich bringt IPv6 mit der zwingend vorgesehenen Integration von IPSec auch kryptographische Mechanismen mit, die es erlauben, weitestgehend sicher zu kommunizieren.

Auch hier gibt es einige Parteien, die damit nicht unbedingt glücklich sind. Offensichtlich wird die in Deutschland bekanntermaßen an der Telefonüberwachung sehr interessierte Polizei daran so wenig Interesse haben wie international operierende Geheimdienste und Industriespione. Aber auch in Unternehmen wird das Filtern von problematischen Inhalten, angefangen mit viren- und wurmverseuchten Mails, auf vorgeschalteten Firewalls unmöglich oder potentiell umgehbar. Die Sicherheit jedes einzelnen Arbeitsplatzrechners wird damit sehr

wichtig. Genau wie Mobile IP führt das zu erheblichen Problemen mit Software, die keine entsprechenden Sicherheitskonzepte mitbringt und konsequent umsetzt.

8 Software-Migration

Um existierende Software IPv6-fähig zu machen, ist in vielen Fällen zwar etwas Arbeit nötig, es ist aber weder eine Geheimwissenschaft noch macht es die Neuentwicklung größerer Programmteile nötig. Mit Ausnahme der DNS-Auflösung sollten IPv4 und IPv6 weitestgehend kompatibel sein.

Wer allerdings mit schlecht programmierter Software am Markt sein Glück versucht, nach dem Zusammenbruch der „New Economy“ die Entwickler verloren hat, die die Software noch hätten warten können, oder sich von externen Entwicklern unter Zeitdruck eine schlechte und nicht mehr wartbare Software bauen lassen hat, steht vor einer existentiellen Herausforderung, sobald IPv6 Stand der Technik wird.

9 Schrittweises Deployment

Die herausragendste Leistung um IPv6 ist meiner persönlichen Meinung nach, daß IPv4 und IPv6 nicht nur problemlos nebeneinander funktionieren, sondern ein Deployment in vielen kleinen, kontrollierten Schritten möglich ist.

Damit gibt es keinen Grund, eine Umstellung in Hauruck-Alles-oder-Nichts-Manier durchzuprügeln. Nicht daß das nicht möglich (und von dem einen oder anderen „Dienstleister“ gerne vermarktet) wäre, aber nötig ist es nicht. Aber das ist nur ein Problem der Marketing- und Vertriebsleute, die trotzdem ein großes „Projekt“ verkaufen wollen—und derjenigen, die so lange die Entwicklung verschlafen, daß es dann irgendwann ganz schnell gehen muß.

10 Offene Herausforderungen

Bei allem Optimismus um IPv6, der Aussicht auf positive Entwicklungen in vielen Bereichen und einer gewissen Technikbegeisterung, die sich der eine oder andere über die Jahre hinweg erhalten hat, gibt es noch genug Schwierigkeiten, die bei der Einführung von IPv6 zu meistern sind.

Wie schon angedeutet ist das Thema DNS im IPv6-Umfeld recht spannend. Hier gibt es noch immer Diskussionen, wie die Auswirkungen der Stateless Autoconfiguration sauber zu integrieren sind.

IPv6 sprengt viele Sicherheitskonzepte, wie sie mit IPv4 lange etabliert sind. Das fängt damit an, daß sich IP-Adressen und ganze Netzwerk-Prefixe dynamisch ändern können, was jeden Firewall-Administrator dank der daraus folgenden Unkündbarkeit nur freuen kann. Die Auswirkungen von Mobile IP und IPSec haben wir ja schon erwähnt, andere Effekte sind möglicherweise zu diesem Zeitpunkt noch nicht absehbar.

Schließlich sollte der Anfang des Vortrags gezeigt haben, daß jeder System- und Netzwerkadministrator lernen muß, in einigen Punkten umzudenken. Das ist sicherlich nicht unmöglich, bringt aber Einarbeitungsaufwand und vielleicht in der Einführungsphase die eine oder andere Panne mit sich.

11 Jetzt und Hier: Was gibt es zu tun?

Was bedeutet das für uns an dieser Stelle?

- Es wird Zeit, daß wir uns in das Thema IPv6 allmählich einarbeiten; ansonsten werden wir wieder einmal auf teuer bezahlte, externe „Experten“ angewiesen sein, deren Fachkompetenz wir nur anhand ihrer horrenden Stundensatzforderungen beurteilen können.
- Bei existierender Hard- und Software, die nicht IPv6-tauglich ist, sollten wir uns mit den Herstellern in Verbindung setzen und nach deren IPv6-Strategie fragen, um in unserer Planung eventuell nötige Änderungen oder sogar Neuanschaffungen berücksichtigen zu können.
- Anschaffungen und Änderungen an der IT-Infrastruktur, die eine erwartete Laufzeit von mehr als drei bis fünf Jahren haben, sollten IPv6 als zwingende Anforderung berücksichtigen.

Andererseits gibt es—noch—keinen Grund, in Torschlußpanik ohne Rücksicht auf Kosten IPv6 gewaltsam einzuführen. Viel wichtiger ist, bei der mittel- und langfristigen Planung IPv6 von Anfang an mit einzubeziehen. Das kostet nur etwas Aufmerksamkeit, aber kein wesentliches Geld, und ist eine langfristige „Zukunftsinvestition“, die in einigen Jahren ihre ganze Tragweite zeigen wird.

12 Fazit

Abseits aller Diskussion um den Adressmangel hat IPv6 viel zu bieten.

Die Möglichkeiten, die es eröffnet, werden früher oder später dazu führen, daß sich IPv6 als neuer Standard etablieren wird—auch wenn ich persönlich zu diesem Zeitpunkt alle Spekulationen, wann es soweit ist, für eher unseriös halte.

IPv6 stellt existierende Pfründe in Frage und ist damit für einige einflußreiche Interessengruppen eine ernstzunehmende Bedrohung.

Wer heute bei langfristigen Entscheidungen IPv6 ignoriert, wird in einigen Jahren teuer für diese Entscheidung bezahlen müssen.

Über dieses Manuskript

Dies ist das Manuskript zum gleichnamigen Vortrag, den ich am 11. März 2004 im Rahmen des Frühjahrsfachgesprächs der German Unix User Group (GUUG) an der Ruhruniversität Bochum gehalten habe.

Einige Aspekte gehen auf Diskussionen mit und Anregungen von Wolfgang Beck zurück, dem ich für seine Unterstützung herzlich danke.

Über den Autor

Der Autor ist Dipl.-Inform. und freischaffender Systemarchitekt im Unix- und TCP/IP-Umfeld.

Mit Schulungen vermittelt er herstellerunabhängig Kenntnisse zu Unix, TCP/IP, zum Design von sicheren, zuverlässigen, effizienten und skalierbaren Systemen und vor allem zu seinem liebsten Thema, IPv6.

Im Projektgeschäft unterstützt er IT-Projekte dabei, Software auf real existierender Hardware in real existierenden Rechenzentren in einen effizienten und zuverlässigen Betrieb zu nehmen, bringt die Infrastruktur von Rechenzentren auf den Stand der Technik und führt vor allem die IT-Bausünden der New Economy in die betriebwirtschaftliche Realität.

Wenn er nicht gerade tauchen geht oder mit dem Fahrrad Kontinente sammelt, ist er unter `stockebrand@guug.de`, `me@benedikt-stockebrand.de` und `http://www.benedikt-stockebrand.de/` zu erreichen.